Exhibit 33

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. RIPPLE LABS INC., BRADLEY GARLINGHOUSE, and CHRISTIAN A. LARSEN, Defendants.	No. 20-cv-10832 (AT)

REBUTTAL EXPERT REPORT OF DR. PETER ADRIAENS

TABLE OF CONTENTS

I. Introduction

1. I am a Professor of Engineering, Finance and Entrepreneurship, Director of the Center for Smart/Digital Infrastructure Finance, and co-founder of the University of Michigan FinTech Collaboratory. My complete CV and the nature of my retention and compensation in connection with this case were set forth in my expert report of October 4, 2021.

2. I have been provided the expert report of Dr. [redacted] (the "Report") and asked to evaluate the methodology and conclusions set forth in that report.

3. The facts and data I have relied on and considered in forming my opinions are disclosed in the report. Should additional relevant documents or information be made available to me, I may adjust or supplement my opinions as appropriate.

4. As further set forth below, I conclude:

(1) Dr. [redacted] principal opinion – that "the XRP Ledger does not satisfy a basic definition of a decentralized system" (Report at 27) – is not the product of a generally accepted methodology for evaluating the decentralization of a distributed ledger. That is because of three facts that the relevant academic literature establishes, but the Report ignores: (i) neither the scientific community nor the blockchain community[1] has reached consensus about the appropriate definition of "decentralization;" (ii) neither community has reached consensus about the appropriate criteria that should be used to determine

[1] *See* Angela Walch, *Deconstructing 'Decentralization:' Exploring the Core Claim of Crypto Systems*, *in* CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES 41–42, 47–48, 68 (Chris Brummer ed., 2019) (discussing how "decentralization" is used "in academic works of relevant disciplines, in discussions within the crypto space, in conference names galore, and in countless reports by businesses, governments and international organizations" and yet "in mainstream discourse, it has been rare to see clear explanations of 'decentralized' or 'decentralization' when they are used").

whether a given blockchain satisfies any such definition; and (iii) neither community has reached consensus about the appropriate metrics to use to quantify whether a given ledger satisfies such criteria. Given the reasonable disagreement within the literature about the appropriate criteria to define decentralization, and the appropriate metrics to quantify those criteria, Dr. [redacted] identification of what he calls "four main aspects of decentralization" (Report at 5) can only be described as novel; it rests on assumptions and choices he has made that are, in the respects discussed below, unsupported by or inconsistent with the prevailing literature and/or lacking in reliability.

(2) Dr. [redacted] related opinion that "[t]he XRP Ledger is centralized compared to Bitcoin and even Ethereum" (Report at 24) also is not the product of a generally accepted methodology. That is so, first, because it rests on an unstated assumption – that it is even possible to compare those three blockchains based on uniform criteria – that fails to account for the fundamental differences in their respective consensus mechanisms. That assumption is demonstrably in conflict with the prevailing literature. Moreover, Dr. [redacted] application of his stated methodology is unreliable because the metrics by which he purports to quantify whether the Bitcoin, Ethereum, and XRP blockchains are decentralized do not have an agreed-upon system of measurement. Accordingly, even if Dr. [redacted] methodology were reliable (and it is not), his application of that methodology to this case is fundamentally flawed in ways independently sufficient to undermine his conclusions.

II. Dr. [redacted] Opinions Regarding Whether the XRP Ledger is Decentralized Rest on a Selective Methodology of His Own Creation That Finds Insufficient Support in the Prevailing Literature.

A. There is no accepted definition of "decentralization" for purposes of evaluating a particular distributed system, like a blockchain.

5. Dr. [redacted] report depends on his adoption (Report at 5) of a particular definition of a decentralized system. [redacted] draws this definition from a 2017 paper by Troncoso et al., which defines decentralized systems as "a subset of distributed systems where multiple authorities (parties) control different system components and no authority is fully trusted by all."[2] Dr. [redacted] then, in his own words, "refine[s]" this definition by selecting the "four main aspects of decentralization" that comprise his methodology for applying the definition, which then leads him to conclude that "the XRP Ledger does not satisfy the basic definition of a decentralized system." (Report at 5.) Accordingly, his opinion rests, in the first instance, on the assumption that the Troncoso definition is authoritative.

6. One immediately apparent flaw in Dr. [redacted] approach is that he selectively chooses the Troncoso definition of decentralization and treats it as authoritative, when in fact the Troncoso definition is not generally accepted within the literature – indeed, given the nascency of the field, *no* particular definition of a decentralized system has achieved general acceptance within the literature. Even within the peer-reviewed literature, there is disagreement regarding what features of a system must be examined, and how, when evaluating decentralization. The Troncoso paper cited by Dr. [redacted] for a purported "basic definition of a decentralized system"

---

[2] Carmela Troncoso et al., *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments*, PROC. PRIV. ENHANCING TECH. (4) 307, 307 (2017).

(Report at 5) itself recognizes that, within the relevant literature, "there does not exist a foundational treatment *or even an established common definition* of decentralization."[3]

7. While the Troncoso paper was one attempt to craft such a definition, Dr. [redacted] report offers no basis to conclude that the Troncoso definition has become an accepted definition within the field. To the contrary, the Sai paper that Dr. [redacted] cites (Report at 9–11), which was published in March 2021 (five years after the Troncoso paper), undertakes a "systematic literature review" to "study decentralization in blockchain" and present "the first in-depth analysis of centralization in blockchains."[4] The Sai paper identifies 89 articles as "relevant blockchain literature"[5] – yet does not cite the Troncoso paper at all. Rather, the Sai paper relies on a definition of decentralization from a paper by Davidson et al., published in 2016, that Dr. [redacted] report does not consider. Davidson offers a substantively distinct definition of decentralization from Troncoso, namely that a system is decentralized "where participants can read, write data, and contribute to consensus without authorization."[6] To give another example, Wu et al., in a 2020 paper, defined decentralization as a system where "no single individual can destroy transactions in the network, and any transaction request requires the consensus of most participants."[7] This definition again is substantively different from the Troncoso paper and emphasizes participation as opposed to authorization.

---

3 *Id.*

4 A.R. Sai et al., *Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review*, 58 INFO. PROCESS & MGMT. 1, 3 (2021).

5 *Id.* at 3, 32–35.

6 *Id*. at 4 (citing Davidson et al., *Economics of Blockchain* (Mar. 8, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751).

7 Keke Wu et al., *A Coefficient of Variation Method to Measure the Extents of Decentralization for Bitcoin and Ethereum Networks*, 22 INT'L NETWORK. SEC. 191, 192 (2020).

8. Moreover, in connection with drafting this report, I have reviewed the sources cited by Dr. [redacted] as well as others I identified through my own research. They do not offer an accepted definition of "decentralization" or the factors relevant to determining whether a particular distributed system or blockchain is or is not "decentralized." In my reading of the peer-reviewed literature, there is currently no generally settled opinion on the definition of decentralization, nor any generally accepted, reliable tools or metrics to compare or quantify different systems.

9. Dr. [redacted] report neither acknowledges the ongoing lack of consensus (in both the scientific and professional blockchain communities)[8] on a definition of "decentralization," nor defends his choice to adopt the Troncoso definition. That is, he never explains why he chose that definition, let alone whether or why it is superior to other proposed definitions in any respect. This approach renders his opinions fundamentally flawed. It is important and necessary, as a baseline starting point for analyzing the issue of decentralization, to acknowledge the lack of consensus among scientific and professional blockchain communities, which continue to wrestle with, debate, and study what "decentralization" means and how to measure it – as even the papers on which Dr. [redacted] relies make clear.[9]

---

[8] Walch, *supra* note 1, at 41–42 (providing a descriptive account of the varied and inconsistent uses of the term "decentralized" among the academic, professional, governmental, and international communities, and noting "it has been rare to see clear explanations of 'decentralized' or 'decentralization' where they are used"); *see id.* at 47 ("No One Knows What Decentralization Means"); *id.* at 39 (noting that, on June 15, 2018, one day after an official of the Securities and Exchange Commission gave a speech discussing decentralization, the Director of the MIT Digital Currency Initiative said on Twitter, "I'm a little worried people from government agencies are throwing around the word 'decentralization' like we know what it means and how to evaluate it").

[9] Those papers set forth a range of metrics for analyzing centralization or decentralization that Dr. [redacted] ignores without explanation even as he relies on the literature for other, narrower purposes. I offer no opinion as to the utility of these metrics, since Dr. [redacted] does not apply them in his Report, but rather identify them as evidence of the lack of

B. There are no accepted criteria to use to determine whether a given system satisfies a given definition of decentralization.

10. Dr. [redacted] report, as part of his "refine[ment]" of the Troncoso definition of decentralization, asserts that there are four main criteria by which to evaluate decentralization: (1) Resilience (which Dr. [redacted] states should be measured by a metric called the Nakamoto Coefficient), (2) Inclusiveness, (3) In-Protocol Incentives, and (4) Governance (which Dr. [redacted] further refines to (a) Public Face and (b) Tokens Allocated at Genesis). (Report at 5.) These criteria form the structure of Dr. [redacted] application of the Troncoso definition of decentralization to Bitcoin (Report at 15–17), Ethereum (Report at 18–19), and the XRP Ledger. (Report at 22–24).

11. Dr. [redacted] putative refinement of the Troncoso definition compounds his selection of that definition's flaws, because it, too, rests on an unproven assertion rather than any authoritative source or methodology. To start, Dr. [redacted] offers no citation or support for the proposition that these four factors are either necessary or sufficient to determine whether a particular system is decentralized. To the contrary, Dr. [redacted] himself recognizes that there are "additional aspects of decentralization" that relate to various aspects of a blockchain system (sometimes grouped into "layers," to which I return below), but states without explanation or

---

consensus around appropriate metrics to evaluate the basic concept Dr. [redacted] Report purports to address. *See, e.g.*, Sarah Azouvi et al., *Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance, in* FIN. CRYPTOGRAPHY AND DATA SEC. 127, 132 (Aviv Zohar ed., 2018) (analyzing "centrality metrics" including Interquartile range, Interquartile mean, Kolmogorov-Smirnov test, Nakamoto index, Satoshi index, and the Sorensen-Dice index); Adem Gencer et al., *Decentralization in Bitcoin and Ethereum Networks*, *in* FIN. CRYPTOGRAPHY AND DATA SEC. 439, 440 (Aviv Zohar ed., 2018) (presenting "a comprehensive measurement study on decentralization metrics" including "(1) direct measurements of [Bitcoin and Ethereum] from multiple vantage points, (2) a Bitcoin relay network called *Falcon* that we deployed and operated for a year, (3) blockchain histories of Bitcoin and Ethereum"); Sai et al., *supra* note 4, at 12 (summarizing in Table 2 a taxonomy of centralization-related aspects of public blockchains that includes 6 layers and 13 factors within those layers).

citation that his report "opt[s] to focus on decentralization aspects of systems proper." (Report at 11.) Dr. [redacted] offers no explanation or justification for his decision to abandon those "additional aspects," nor why his methodology and conclusions remain sound despite that decision.

12. A basic methodological step in creating any novel definition in social and informational sciences[10]—which I argue includes key applications of blockchain technology[11]—is to establish that the components of the definition are both *necessary* and *sufficient* to the conclusion.[12] This is because the purpose of definitions is to establish sufficient shared meaning such that a class of entity can be investigated by a scientific community. This does not preclude that a definition may be adjusted in the light of new understandings as they emerge. However, without meeting the necessary-sufficient criteria, a definition will become either overinclusive (if it contains components that are not necessary) or underinclusive (if its components are not sufficient) to reach a relevant conclusion. Yet Dr. [redacted] does not attempt to establish that his four selected criteria are necessary or sufficient to define a blockchain as decentralized. To be clear, I do not deny that the four aspects he focuses on are (or, at least, can be) relevant. But others are discussed in the literature, and it appears that Dr. [redacted] subjectively chose those four metrics, omitted others, and ignored key insights from the literature in that regard.

---

10 Blockchain is an emerging technology in the field of computer science, with many of its applications relating to the field of information science, an academic field primarily concerned with analysis, collection, classification, manipulation, storage, retrieval, movement, dissemination, and protection of information.

11 *See* Jaideep Ghosh, *The Blockchain: Opportunities for Research in Information Systems and Information Technology*, 22 J. GLOBAL INFO. TECH. MGMT. 4, 235–242 (2019).

12 Geoffrey M. Hodgson, *Taxonomic Definitions in Social Science, with Firms, Markets and Institutions as Case Studies*, 15 J. INST. ECON . 207, 212–13 (2019).

13. To understand this point, recall from my opening report (at ¶¶ 30–40) that not all blockchains share an identical basic architecture. Bitcoin is an example of a proof-of-work blockchain. (Expert Report of Peter Adriaens (Oct. 4, 2021) ("Adriaens Report") at 17.) The current state of Ethereum is another example of a proof-of-work blockchain (though, as Dr. [redacted] recognizes, Ethereum is transitioning to a different model known as proof of stake). The XRP Ledger uses neither proof-of-work nor proof of stake, but rather a federated consensus model.[13] Dr. [redacted] use of the four factors he selects depends on an assumption that they provide a reliable way to assess, objectively test, quantify, or compare substantively distinct blockchain architectures. That assumption is flawed. First, as the Troncoso paper itself underscores, the criteria used to measure decentralization in a particular blockchain system must account for differences in **network infrastructure** ("the distribution of tasks needed for maintaining service within the system"), **network topology** ("the connections between nodes used to route traffic"), and **authority topology** ("the power relations between the nodes"), lest they ignore important differences in how different blockchains realize or achieve decentralization in practice.[14] Dr. [redacted] report does not address this.

14. An example helps to illustrate the importance of having reliable mechanisms to compare substantively different architectures before reaching useful conclusions. For decades, "miles per gallon" (MPG) was a reliable mechanism for comparing the efficiency of two different cars, and an observer who was only aware of gasoline-powered cars might therefore assume that all cars can be assigned an MPG measurement. If, however, that observer were then introduced to a Tesla, which does not run on gasoline and cannot be assigned an MPG, the measurement

---

13 *See Consensus Protections Against Attacks and Failure Modes*, XRPL.ORG, https://xrpl.org/consensus-protections.html.

14 *See* Troncoso et al., *supra* note 2, at 309–13, 320.

criterion would fail to recognize the Model 3 as a car, because it failed to account for differences in the underlying architecture.

15. Dr. [redacted] assumption that his four selected criteria can be reliably applied to assess and compare Bitcoin, Ethereum, and the XRP Ledger is further flawed because it does not consider decentralization at various *layers* of those three blockchain systems. A recent review on the taxonomy of metrics to characterize and measure (de)centralization indicates that the techniques that are useful depend on the layer in the blockchain one wants to compare, and on the particular blockchain architecture at issue.[15] Whereas the subsystems (or "layers") are defined differently between Srinivasan and Lee[16] or Sai, the results in Chart 1, taken from Sai, indicate that multiple techniques are favored.[17] Sai identifies a total of 13 aspects spread over six architectural layers that are relevant to the issue of decentralization in public blockchains – and for several of those aspects, Sai observes that no measurement techniques can even be found yet within the literature (see the "Not found" notations in Chart 1).[18]

Layer	Centralization factor	Measurement techniques
Application layer	Wallet concentration Exchange concentration Reference client concentration	Not found Centrality & Percentage value Satoshi index
Operational layer	Storage constraint Specialized equipment concentration	Ratio of growth Not found
Incentive layer	Wealth concentration	Gini coefficient & Percentage value
Consensus layer	Consensus power distribution	Percentage value & Gini coefficient & Theil index & Centralization factor
Network layer	Node discovery protocol control Geographic distribution Bandwidth concentration Routing centralization	Not found Gini coefficient & Latency Clustering of provisioned bandwidth AS-Level coverage
Governance layer	Owner control Improvement protocol	Fractional measurement Centrality metrics

Chart 1. Decentralization metrics considered across blockchain layers (from Sai et al., 2021)

15 Sai et al., *supra* note 4, at 5, 12–28.

16 Balaji S. Srinivasan & Leland Lee, *Quantifying Decentralization*, EARN.COM (July 27, 2017), https://news.earn.com/quantifying-decentralization-e39db233c28e.

17 Sai et al., *supra* note 4, at 12.

18 *Id.*

16. The active study of decentralization factors – and the development of appropriate metrics and techniques to measure them – in the scientific literature indicates an on-going need for research to compare blockchains, and demonstrates that this area is unsettled, and that there is currently no standard or benchmark for use in the profession.[19] This observation is exemplified in Chart 1 by measurement techniques labeled "Not found," indicating that even as to factors relating to decentralization that have been proposed, there is no reliable way to measure or objectively assess different blockchains as to those factors.

17. By way of further example, a 2020 study called "Measuring Decentrality in Blockchain Based Systems" emphasizes the need to measure decentralization at different layers of the system, using "various metrics" to capture decentrality in "respective layers."[20] For measuring decentrality at the governance layer (the layer in which the nodes reach a consensus), the authors propose using seven different metrics including: "fairness index, entropy, Gini coefficient, Euclidean distance, Minkowski distance, cosine similarity and Kullback-Leibler divergence metrics."[21] I express no view on whether those seven metrics are the right ones or not – as this is an emerging area of study lacking consensus on approach – but it is striking that the prevailing literature is both layer-sensitive and architecture-sensitive in proposing metrics, whereas Dr. [redacted] approach is not.

18. Hence, the differences in incentive, governance, operational, and validation mechanisms (proof-of-work for Bitcoin and Ethereum; federated consensus for the XRP Ledger) do not allow

---

19 *See id.* at 5 (explaining that the "study of centralization in public blockchain is still fragmented" and current models "do not provide adequate insights," therefore setting out to design a "novel centralization taxonomy" to "overcome th[at] limitation").

20 Sarada Prasad Gochhayat et al., *Measuring Decentrality in Blockchain Based Systems*, 8 IEEE ACCESS 178372, 178376 (2020).

21 *Id.* at 178373.

for a direct metrics comparison on the same basis. Given there is no consensus in the literature and the practice to measure these metrics objectively **at the subsystem or layer** evaluated, there is a lack of methodology and process to compare **entire blockchains** at a systems level. Dr. [redacted] does not acknowledge this lack of consensus, nor does he offer a basis to conclude that his novel four-factor framework is (or is based on) a generally accepted methodology.

C. There are no accepted metrics to use to quantify whether a given ledger satisfies criteria for decentralization, especially for purposes of comparing Bitcoin, Ethereum and the XRP Ledger.

19. In addition, to the extent that Dr. [redacted] identifies a series of criteria that he asserts are relevant to whether a particular blockchain is decentralized, he does not substantiate – and the relevant literature does not provide – metrics by which one may reliably and consistently quantify the four criteria in question. I will address each of the four in turn.

20. **Resilience (Nakamoto Coefficient).** The concept of resilience is often described as a major benefit of blockchains, and it refers generally to a blockchain's persistence in moving forward in a trusted way and ability to withstand challenges such as hacking, malware, fraud, server or network failure, and human error. Dr. [redacted] report decides to assess and measure Resilience across the Bitcoin, Ethereum, and XRP Ledger systems using a metric he calls the "Nakamoto Coefficient" – "the number of parties that need to be corrupted to subvert key properties of a distributed system." (Report at 5 n.1.) I am not aware of any peer-reviewed literature that considers the Nakamoto Coefficient, as a term or as defined by Dr. [redacted] as a suitable or accepted metric for measuring the decentralization of a blockchain. Dr. [redacted] cites

a (non-peer-reviewed) YouTube video and blog post in relying on the concept of a Nakamoto Coefficient for this purpose.[22]

21. The blog post Dr. [redacted] cites explains that calculating the Nakamoto Coefficient requires that one:

> (a) enumerate the essential subsystems of a decentralized system, (b) determine how many entities one would need to be compromised to control each subsystem, and (c) then use the minimum of these as a measure of the effective decentralization of the system. The higher the value of this minimum Nakamoto Coefficient, the more decentralized the system is.[23]

22. That post concludes by stating that the authors "recognize that there is plenty of room for debate over which subsystems of a decentralized system are essential."[24] Dr. [redacted] does not offer, and I am not aware of, any basis to conclude that the debate around identifying essential subsystems that these authors acknowledge has been resolved in favor of considering solely "safety" and "liveness," which Dr. [redacted] asserts are the two principal properties of Resilience. (Report at 9.) Indeed, neither word appears anywhere in the blog post that defined the Nakamoto Coefficient (nor do the

---

22 Stacks, *Balaji Srinivasan of 21: "Quantifying Decentralization" Blockstack Summit 2017,* YOUTUBE (Aug. 11, 2017), https://www.youtube.com/watch?v=4UXT5YVJwB4. The YouTube video in question, *Quantifying Decentralization*, is related to a blog post on Earn.com by the same author. Srinivasan & Lee, *supra* note 16 Later in his report, Dr. [redacted] defines Resilience as the ability of a system "to withstand Byzantine behavior of components of the system." (Report at 9.) He then states that Resilience "may apply to different properties of the system, namely safety and liveness," which he defines as the properties of a system that bad things do not happen (safety) and good things do eventually happen (liveness). (*Id.*) Dr. [redacted] again offers no citation for this notion. For the reasons explained later in this report, none of this supplies a reliable metric for measuring blockchain systems' decentralization.

23 Srinivasan & Lee, *supra* note 16.

24 *Id.*

words "double-spend resistance" or "censorship," which Dr. [redacted] uses as examples of safety and liveness properties).

23. Rather, the authors of that post calculate the Nakamoto Coefficient by drawing on two concepts from economic theory – the Lorenz curve and the Gini coefficient – which itself was a leap by the (non-peer-reviewed) post's authors.[25] The Lorenz curve and the Gini coefficient were originally designed to measure non-uniformity within a population.[26] Originally defined as a measure of the distribution of income across a population, the Gini coefficient is often used as a gauge of economic inequality, measuring income distribution or, less commonly, wealth distribution among a population.[27] The application of the Gini coefficient to analyze inequality in internet communities such as blockchains is flawed because it conflates two different problems: lack of resources and concentration of power.[28] These aspects should be considered separately since resource allocation is a network-dependent feature and power concentration is a feature of allocation of tokens. Absent a basis to conclude that allocation of tokens corresponds to authority, power, or control over a blockchain's functioning, there is no basis to conclude that

---

25 *Id.*

26 UNITED STATES CENSUS BUREAU, *Gini Index*, https://www.census.gov/topics/income-poverty/income-inequality/about/metrics/gini-index.html (last revised Oct. 8, 2021) (explaining that the Gini coefficient "summarizes the dispersion of income across the entire income distribution," "based on the difference between the Lorenz curve (the observed cumulative income distribution) and the notion of a perfectly equal income distribution").

27 *Id.*; *see generally* Oded Stark, *Status Aspirations, Wealth Inequality, and Economic Growth*, 10 REV. DEV. ECON. 171 (2006) (utilizing a Gini coefficient of wealth inequality in suggesting how such inequality corresponds to economic growth).

28 *Compare* Srinivsan & Lee, *supra* note 16 (describing the Nakamoto coefficient as a measure of the number of entities needed to control a subsystem, inspired by the Gini coefficient and Lorenz curve), *with* Frank A. Farris, *The Gini Index and Measures of Inequality*, 117 AM. MATHEMATICAL MONTHLY 851 (2010) (describing the Gini index as a "single number that measures how equitably a resource is distributed in a population").

token allocation is relevant to decentralization. (I further address this point below, when considering Dr. [redacted] definition of Governance.)

24. In addition, the Nakamoto Coefficient (like the Lorenz curve and Gini coefficient on which it is based; *see* Chart 2) is designed to measure the distribution of scarce resources (originally, money) within a defined population.[29] Accordingly, it is only a valid analytical tool to the extent it is analyzing a scarce resource (in economic theory, money) whose distribution has some relationship to the distribution of power within the system (for example, buying power).

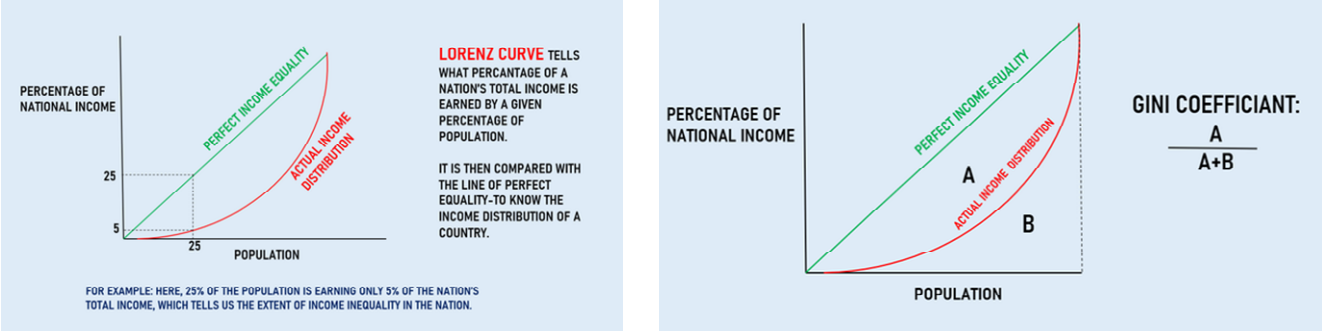


Chart 2. Illustration of Lorenz Curve and Gini Coefficient.[30]

25. Even if the concept of the Nakamoto Coefficient that was proposed by this non-peer reviewed blog post were reliable, Dr. [redacted] application of the Nakamoto Coefficient to the XRP Ledger rests on an undefended logical leap. In particular, he overlooks the fact that the XRP Ledger uses a completely different consensus mechanism – one that *does not* use scarce resources to allocate authority. Rather, it permits each participant to independently choose which other participants to trust, as each validator has complete control over the contents of its Unique Node List, which a validator may change at any time without needing the permission of any other party. As a consequence, I do not believe that the Nakamoto Coefficient can be

29 Srinivsan & Lee, *supra* note 16.

30 Arsh, *What are the Main Merits of the Lorenz Curve?*, QUORA (2021), https://www.quora.com/What-are-the-main-merits-of-the-Lorenz-curve.

sensibly applied to evaluate the XRP Ledger's Resilience. At a minimum, Dr. [redacted] has failed to defend his application of that metric.

26. In the context of Bitcoin and Ethereum, the scarce resource Dr. [redacted] measures is mining power, which is relevant because of the authority given to successful miners in proof-of-work blockchain systems who may propose new blocks and the ability of a miner or miners that control the majority of the hash rate to undermine the validity of the system (in what is referred to as a "51% attack").[31] I therefore agree that Dr. [redacted] decision to apply the Nakamoto Coefficient to Bitcoin and Ethereum to determine the distribution of mining power across the network is reasonable. But I do not agree that Dr. [redacted] offers a complete analysis of the Nakamoto Coefficient's application. The nature of the Nakamoto Coefficient is that it can only offer a point-in-time result: in other words, just as the Gini coefficient of the United States changed from 1920 to 1950 to 1990 to 2020, the Nakamoto Coefficient of Bitcoin and Ethereum is not static.[32] It is public knowledge that mining-power concentrations have changed over time for Bitcoin and Ethereum.[33] And Dr. [redacted] report recognizes that he is calculating the Nakamoto Coefficient of Bitcoin and Ethereum by measuring the concentrations of mining power "at the time of writing this report." (Report at 15.) That is insufficient to reach any conclusions about the blockchains themselves, and could only (and at most) permit an analysis of

---

31 *See* Digital Currency Initiative, *51% Attacks*, MIT MEDIA LAB, https://dci.mit.edu/51-attacks (last visited Nov. 11, 2021).

32 *See, e.g.*, Juliana Horowitz et al., *Trends in Income and Wealth Inequality*, PEW RSCH. (Jan. 9, 2020), https://www.pewresearch.org/social-trends/2020/01/09/trends-in-income-and-wealth-inequality.

33 *See e.g.*, Cambridge Centre for Alternative Finance, *Bitcoin Mining Map*, U. CAMBRIDGE, https://ccaf.io/cbeci/mining_map (last visited Nov. 11, 2021); ETHERSCAN, *Ethereum Network Hash Rate Chart*, https://etherscan.io/chart/hashrate (last visited Nov. 11, 2021).

the relative ownership of scarce resources by the participants in each blockchain's network at a given point in time.

27. An objective analysis of the Nakamoto Coefficients of Bitcoin and Ethereum based on Dr. [redacted] own definition – the minimum number of parties that need to be corrupted to subvert key properties of the systems (Report at 5 n.1) – would necessarily conclude that the Nakamoto Coefficients of both systems are no greater than 1 as to the two features of Resilience that Dr. [redacted] identifies: **safety** (that "'bad things' do not happen (Report at 9)) and **liveness** (that "'good things' do eventually happen" (*id.*)).

28. As to safety, an example of which Dr. [redacted] gives as double-spend resistance, both Bitcoin and Ethereum are vulnerable, as Dr. [redacted] recognizes, to a "51% attack." (Report at 15, 18.) If one entity controls 51% of the hash power of the network, they are able to compromise the safety of the entire network.[34]

29. As to liveness, an example of which Dr. [redacted] gives as censorship resistance (Report at 9), both Bitcoin and Ethereum grant successful miners complete discretion to censor or reject transactions.[35] Accordingly, a single miner (even without 51% of the hash rate) has the ability to void a proposed transaction for any reason without any oversight.[36] For the user who proposed

---

34 This degree of control over the Bitcoin hash rate has occurred, albeit briefly, in the past. *See* Alex Hern, *Bitcoin Currency Could have been Destroyed by '51%' Attack*, THE GUARDIAN (June 16, 2014), https://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io.

35 Andreas M. Antonopoulos, MASTERING BITCOIN 275 (2d ed. 2017); Johnnatan Messias et al., *On Blockchain Commit Times: An Analysis of How Miners Choose Bitcoin Transactions*, *in* PROC OF. THE SECOND INT'L KDD WORKSHOP ON SMART DATA FOR BLOCKCHAIN AND DISTRIBUTED LEDGER, 3–4 (Aug. 2020), https://people.mpi-sws.org/~johnme/pdf/messias-sdbd-20.pdf.

36 *See* Hern, *supra* note 3426.

the voided transaction, there is no in-network recourse other than resubmitting the transaction, which does not satisfy Dr. [redacted] definition of liveness.[37]

30. **Inclusiveness.** Dr. [redacted] defines inclusiveness (solely by citation to his own, unpublished manuscript, which refers to the concept as "openness") as "the ability of the system to welcome new participants in a way which provides them with equal opportunities compared to existing participants." (Report at 9.) Dr. [redacted] then defines the concept of "equal opportunities" (again solely by citation to his own, unpublished manuscript) as a system that "(a) allows any participant Alice to have an equal role in the system as any other (new or existing) participant Bob, provided Alice makes the same investment in system resources as Bob, and (b) the system does not prevent Alice from making such an investment." (Report at 9.)

31. Again, I find Dr. [redacted] methodology to be flawed. Dr. [redacted] report does not substantiate the relationship between "Inclusiveness" and decentralization. The report does not offer any citation to authoritative literature that describes Inclusiveness (or the sub-defined concept of equal opportunities) as necessary to determining whether a system is decentralized.

32. Even assuming that "Inclusiveness" is an appropriate criterion for evaluating decentralization, Dr. [redacted] report again offers no metrics that would permit one to reach conclusions about the significance of greater or lesser degrees of Inclusiveness in particular layers of distinct blockchain models.[38] Accordingly, even if Dr. [redacted] could substantiate his

---

[37] This censorship authority has been deployed in practice. *See* Collin Harper, *Marathon Miners Have Begun Censoring Bitcoin Transactions*, COINDESK (May 7, 2021), https://www.coindesk.com/tech/2021/05/07/marathon-miners-have-started-censoring-bitcoin-transactions-heres-what-that-means/.

[38] Dr. [redacted] report asserts that Inclusiveness may relate to whether a particular blockchain is *permissioned* or *permissionless*, but offers no analysis or citation to conclude – as he asserts – that "permissionless systems are to be considered more decentralized than permissioned systems." (Report at 9.) Indeed, the simple example of the U.S. dollar refutes the premise: the dollar is a permissionless currency to access and

assertions, the failure to supply meaningful comparison metrics or benchmarks is an independent reason that his conclusions are impossible to trust or validate objectively.

33. Dr. [redacted] criterion of "equal opportunities" appears to be based only on [redacted].[39] For Dr. [redacted] to assert that Bitcoin and Ethereum provide "equal opportunities" to participants, but the XRP Ledger does not, is particularly problematic. The literature has, for at least the past few years, been critical of Bitcoin and proof-of-work blockchains because the significant costs of mining and the manner in which the in-protocol incentives favor those with massive computing power, such that in practice "only a few nodes are contributing blocks for the Blockchain."[40] Dr. [redacted] does not address this literature, which explains that it is insufficient to consider abstract equality of opportunity when structural barriers

---

spend, but is issued and controlled by a centralized authority (the U.S. government). INVESTOPEDIA, *See Who Prints Money in the United States?*, https://www.investopedia.com/ask/answers/082515/who-decides-when-print-money-us.asp (last updated May 29, 2021).

Similarly, as noted above, blockchains contain multiple functional layers. It is possible for a blockchain to be permissioned as to certain layers and permissionless as to others (for example, one blockchain might have a permissioned code base but permissionless transaction proposal and validation; another might have permissionless governance through a decentralized autonomous organization (DAO) model but have permissioned transactions).

39 [redacted]

40 Gochhayat et al., *supra* note 20, at 178381; *see also id.* at 178374 ("Despite envisioned decentralization in Bitcoin, the high cost of mining has led to considerable centralization of consensus in practice"); Sai et al., *supra* note 4, at 29 ("A high concentration of consensus power can induce an arm's race to attain the most efficient hardware. Our survey reports that this race often results in specialized proprietary hardware. The practical implication of this type of hardware concentration is an indirect limitation to participation as only efficient, and often proprietary hardware, can result in a profitable operation."); Gencer et al., *supra* note 9, at 9–11 (noting "[w]ith the current mining difficulty of Bitcoin and Ethereum, using commodity hardware to generate blocks is not feasible which centralizes the mining process somewhat," and finding that in the ten week study period four Bitcoin miners had more than 53% of the average mining power and three Ethereum miners had 61% of average mining power).

prevent new entrants from meaningfully contributing to the system.[41] By contrast, operating a fully functioning validation server on the XRP Ledger requires minimal computing power.[42] As Dr. [redacted] report fails to recognize, any person or entity may operate an XRP Ledger validation server and participate in the consensus process without the permission or approval of any other entity – exactly the type of equal opportunity his report defines as key to Inclusiveness. (Report at 9.)

34. **In-Protocol Incentives.** Dr. [redacted] defines Incentives as "whether the system has rewards for protocol participants, paid out to protocol participants within the protocol itself." (Report at 10.) To support his definition, and the relevance of Incentives to decentralization, Dr. [redacted] relies on the Sai and Troncoso papers.[43] However, neither paper supports Dr. [redacted] conclusions.

35. Sai et al. discuss the "incentive layer" of blockchains by observing that whether Bitcoin (and, by extension, Ethereum) actually offers economic incentives to its participants is contingent on factors external to the system. Specifically, if "the exchange rate" of Bitcoin to fiat currency "falls below a given threshold of profitability" it no longer provides an economic incentive and participants may withdraw from mining.[44] Put another way, if the cost of mining (measured by the cost of obtaining and operating the computing equipment) over any given

---

41 Sai et al., *supra* note 4, at 22 ("[T]he specialized equipment requirement severely contains . . . participation."); Igor Makarov & Antoinette Schoar, *Blockchain Analysis of the Bitcoin Market*, 23 (Oct. 13, 2021), https://ssrn.com/abstract=3942181 ("[T]he set of large miners is relatively stable, and it is small miners which enter and leave the mining business in response to price shocks.").

42 *System Requirements: Minimum Specifications*, XRPL.ORG, https://xrpl.org/system-requirements.html ("A rippled server should run comfortably on commodity hardware").

43 *See* Report at 10 (citing Sai et al., *supra* note 4; Troncoso et al., *supra* note 2).

44 Sai et al., *supra* note 4, at 19.

period is greater than the mining rewards received, the network does not effectively offer economic incentives.[45]

36. Dr. [redacted] asserts that the Troncoso paper "argue[s] that the development of adequate incentives is necessary to build a successful decentralized system." (Report at 10.) However, the conclusions of Troncoso et al. do not support Dr. [redacted] assertion. To the contrary, the Troncoso paper concludes that Incentives (1) need not be economic, and (2) may in fact undermine decentralized systems if not constructed carefully: "Designers of decentralized systems must carefully engineer such incentives, to ensure that natural (non adversarial) selfishness does not lead to dysfunction. *Monetary incentives, reputation, and reciprocity can be the basis of such incentives – but off the shelf such mechanisms are often central points of failure.*"[46] Dr. [redacted] ignores this essential aspect of the Troncoso paper's analysis when he asserts that Incentives must be "in-protocol" to be significant. (Report at 10.[47]) Instead, Dr. [redacted] report narrowly focuses on rewards earned through the energy and cost-intensive mining process (Report at 10, 16), and he ignores the XRP Ledger's inherent structural and design benefits, including the ability to quickly, efficiently, and cheaply transfer value, which I detailed in my opening report. (Adriaens Report at 22, 25.) Each of these features of the XRP

---

45 According to public reports, the exchange rate of Bitcoin has fallen to levels that rendered mining unprofitable in the past. *See* Evelyn Cheng, *Bad News for Bitcoin Miners: It's No Longer Profitable to Create the Cryptocurrency, by Some Estimates*, CNBC (Mar. 15, 2018), https://www.cnbc.com/2018/03/15/bad-news-for-bitcoin-miners-as-its-no-longer-profitable-to-create-the-cryptocurrency.html.

46 Troncoso et al., *supra* note 2, at 313 (emphasis added).

47 A related problem with Dr. [redacted] argument is that he does not explain why it is sufficient that Bitcoin and Ethereum provide "in-protocol incentives" solely to miners, when he defines this aspect of his analysis as relating to "whether the system has rewards for protocol participants." (Report at 10.) Miners are far from the only participants in the Bitcoin and Ethereum ecosystems; for other participants – like those who submit transactions and must pay a fee to miners – there are either no incentives or economic disincentives.

Ledger offer incentives – for example, to payment processors who want to ensure their transactions clear more quickly and cheaply than on the Bitcoin or Ethereum blockchains and therefore have an incentive to ensure the XRP Ledger continues to exist.

37. Moreover, the Troncoso paper observes that "[s]ome decentralized system[s] consist solely of nodes that are users and there is no additional infrastructure. They rely solely on users to collectively contribute resources (bandwidth, storage) in order to provide a service."[48] Troncoso labels such a system decentralized, even though there are no Incentives provided.[49]

38. Dr. [redacted] also offers no methodology or metrics to quantify the significance or adequacy of incentives in order to reliably compare the incentives offered by distinct blockchain architectures. This renders it impossible to validate his results. Nor does Dr. [redacted] account for issues considered by the literature, like the fact that the "in-protocol incentives" offered by Bitcoin and Ethereum are only economic incentives if external factors align correctly.[50]

39. Although Dr. [redacted] concludes that the XRP Ledger does not provide incentives because it has no equivalent to mining rewards, Dr. [redacted] never considers other forms of incentives identified by Troncoso – like reputation and reciprocity.[51] Indeed, reputation and reciprocity can form significant incentives in the context of distributed systems, as communities that see value in an innovative technological solution may be inclined to support them regardless of whether the solution offers "in-protocol" incentives.[52] As I set out in my original Report and

---

48 Troncoso et al., *supra* note 2, at 310.

49 *Id.* Troncoso refers to these systems as "decentralized" and lists Freenet and Cachet as examples, neither of which offer incentives. *See e.g.,* FREENET, https://freenetproject.org/index.html.

50 *See supra* at ¶ 35.

51 Troncoso et al., *supra* note 2, at 313.

52 *See, e.g.*, *Incentives to Develop Free Software*, THE LINUX INFORMATION PROJECT, http://www.linfo.org/open_source_development_incentives.html (listing ten reasons why

discuss further *infra* in Part III, the XRP Ledger offers many such innovative technological advances that would provide non-economic yet meaningful incentives.

40. **Governance.** Dr. [redacted] final criterion for evaluating decentralization is Governance, which he defines in two distinct ways in different places in his report. First, in his summary and Table 1, he identifies two aspects of Governance: public face, and tokens allocated at genesis. (Report at 5.) Second, in Section 3.1, he defines Governance as "the level of power, if any, of human stakeholders to influence and change key rules in the system, e.g. through software updates." (Report at 10–11.) He then notes three "parameters for evaluating decentralization of governance power" that have been "proposed or discussed in the literature" – namely: (1) improvement control (the number of developers contributing to the codebase), (2) existence of a public face (a personality or institution that is a representative of the system), and (3) owner control (measured by examining the total tokens accumulated by the stakeholders in the early adoption period). (Report at 11.) As with the other criteria Dr. [redacted] analyzes, the Governance criterion is not reliable both because it does not have an agreed-upon definition (as Dr. [redacted] admits in noting that the parameters he identifies have merely been "proposed or discussed" (Report at 11)), and because there is no agreed-upon metric for evaluating quantitatively any of the parameters he identifies in a manner that would permit comparisons across blockchains.

---

developers contribute to open-source projects, like the Linux operating system and the Internet itself, including the desire to use the system they are developing or maintaining, prestige, and profit from downstream businesses that contributors operate); Josh Lerner & Jean Tirole, *The Simple Economics of Open Source*, NAT'L BUREAU ECON. RSCH. (2000) https://www.nber.org/system/files/working_papers/w7600/w7600.pdf (concluding that future career advancement, peer recognition, and related incentives were powerful drivers behind the development of key software projects in the 1990s).

41. *Improvement Control.* Although not identified in Dr. [redacted] summary Table 1, he defines Improvement Control as relevant to Governance. (Report at 11.) According to Dr. [redacted] (Report at 16, 18), Bitcoin has "relatively few 'core' developers" and Ethereum is "largely similar" to Bitcoin in terms of improvement proposals – though the literature he cites indicates that, at least for Ethereum, one person – Vitalik Buterin – is the source of the "vast majority" of the code base.[53]

42. Also, Dr. [redacted] asserts that "the overwhelming majority of code commits and lines of code" in rippled "comes from the developers who are or have been affiliated with or funded by Ripple Labs, Inc." (Report at 23.) Unlike the Azouvi paper Dr. [redacted] cites,[54] however, the Report offers no quantitative analysis to support those assertions, so it is not possible to determine, for example, whom he considers to be the "core" developers of Bitcoin or Ethereum, or a developer "affiliated with or funded by Ripple Labs, Inc." (Report at 23.) Dr. [redacted] analysis in this regard is therefore not replicable.[55]

43. However, taking Dr. [redacted] assertions as true for the sake of argument, Dr. [redacted] offers no metrics to quantitatively measure Improvement Control such that it could be compared

---

53 *See, e.g.*, Sai et al., *supra* note 44, at 3 ("According to the empirical analysis of Azouvi et al. (2018), the authors report that the vast majority of the improvement proposal in Ethereum are authored by a single user, Vitalik Buterin, the founder of Ethereum.").

54 *See* Report at 11 (citing Azouvi et al., *supra* note 9).

55 To support the proposition that Improvement Control is relevant to his decentralization aspects, Dr. [redacted] cites to a paper by de Filippi and Loveluck (Report at 11) that reports that five individuals who held "administration rights for the development of the Bitcoin project became known as the *core developers*." Primavera de Filippi & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure*, 5 INTERNET POL'Y REV. 1, 9 (2016), https://policyreview.info/pdf/policyreview-2016-3-427.pdf. This fact further undermines Dr. [redacted] use of the term to refer to the top contributors to a particular blockchain project since the Bitcoin "core developers" were selected by Gavin Andresen and defined by the fact that they controlled the Bitcoin code, as discussed *infra* note 56.

across different blockchain systems (which is perhaps why Dr. [redacted] does not include this facet of Governance in his summary Table 1). Dr. [redacted] report lacks any reliable methodology to measure Improvement Control, making it impossible to use this parameter to evaluate Governance or any other aspect of decentralization.

44. *Public Face.* Dr. [redacted] asserts that Bitcoin has no "public face," while Ethereum and the XRP Ledger do. (Report at 16, 18, and 23.) Dr. [redacted] conclusion in this regard as to Bitcoin is highly temporally contingent. As has been widely reported, early in Bitcoin's development, a single individual – Gavin Andresen – was the principal developer of the Bitcoin software code, and worked with a small team of core developers to make the necessary improvements to Bitcoin that allowed it to flourish.[56] Similarly, as Dr. [redacted] acknowledges, Vitalik Buterin is responsible for the original design and development of Ethereum and remains its public face. (Report at 18.)

45. As with the other parameters he identifies, Dr. [redacted] offers no reliable metric to evaluate the Public Face of a particular blockchain, and no explanation of its relevance to the concept of decentralization as he (which is to say, Troncoso) defined it. The mere existence of a recognizable Public Face associated with a blockchain project has no apparent connection to whether "multiple authorities (parties) control different system components and no authority is

---

[56] Tom Simonite, *The Man Who Really Built Bitcoin*, MIT TECH. REV. (Aug. 15, 2014), https://www.technologyreview.com/2014/08/15/12784/the-man-who-really-built-bitcoin/ ("When Andresen took over from Satoshi Nakamoto in 2010 he laid out the way the project would operate, drawing on his experience managing teams building software products and what he knew of major open source projects such as Linux. A group of five core developers emerged, with Andresen as the most senior. Only they had the power to change the code behind Bitcoin and merge in proposals from other volunteers. That gave them unique power over the currency's basic operation and economic parameters. While the price of Bitcoin soared over the years, Andresen and the other core developers toiled to improve the software that made it all possible. They fixed security bugs that had permitted digital heists, made the software less prone to crashes, and spruced up the interface to make it easier to use.").

fully trusted by all," (Report at 5) (citing Troncoso et al., at 308), because it is entirely possible for those defined features to be met even where a single individual is responsible for the creation of the project. For example, Satoshi Nakamoto – the pseudonymous creator of Bitcoin – was clearly a significant contributor to the Bitcoin project, having developed its initial source code, but the actual governance and functioning of the blockchain is not impaired by his anonymity and lack of ongoing (known) support for the project.[57]

46. *Token Allocation at Genesis.* Finally, Dr. [redacted] asserts that the "total tokens accumulated by the stakeholders in the early adoption period" of a blockchain is a relevant parameter of Governance. (Report at 11.) As an initial matter, Dr. [redacted] offers no explanation for why control of a blockchain's tokens (which are inherently solely units of account recorded on the blockchain) is relevant to whether the blockchain itself is decentralized. Except in a proof of stake blockchain (which none of Bitcoin, Ethereum, or the XRP Ledger are at present), ownership of tokens provides no mechanism to control the operations of the ledger, nor any obligation on others in the system to trust the token holder, and accordingly does not have relevance to the features of a decentralized system as Dr. [redacted] defines it. Nor does Dr. [redacted] offer any quantifiable metrics that would allow for a meaningful comparison of one blockchain project to another, even were one to accept the utility of this parameter.

47. Dr. [redacted] description of the Token Allocation at Genesis for Bitcoin, Ethereum, and XRP are also flawed as a factual matter.

48. As to Bitcoin, Dr. [redacted] asserts that 0% of the tokens were allocated at genesis and that "Bitcoin did not have a hidden owner accumulation phase." (Report at 17.) Dr. [redacted] leaves

[57] Jamie Redman, *Ten Years Ago Satoshi Nakamoto Logged Off*, BITCOIN.COM (Dec. 13, 2020), https://news.bitcoin.com/ten-years-ago-satoshi-nakamoto-logged-off-the-final-message-from-bitcoins-inventor.

to a footnote, however, an acknowledgement of the widespread reports that wallets controlled by Bitcoin's inventor, Satoshi Nakamoto, contain approximately 1.1 million BTC that were mined in the early days of the protocol.[58] Dr. [redacted] also acknowledges that those BTC "were never transacted on the network," (Report at 17 n. 12), meaning that Nakamoto presumably still controls a sizeable percentage of BTC – 1.1 million out of the 21 million that can ever be created, which would be worth over $70 billion today.[59]

49. As to Ethereum, Dr. [redacted] initially asserts in Table 1 that 61.5% of the current supply of ETH tokens were allocated at genesis, with about 10% "owner controlled." (Report at 5.) Dr. [redacted] later acknowledges that 72 million ETH were pre-allocated in the genesis block (Report at 18–19), which would be about 61% of the approximately 118 million ETH in circulation today.[60] However, Dr. [redacted] calculation of the amount of originally mined ETH that was "owner controlled" fails to account for the fact that all ETH in the genesis block was effectively controlled by the ETH development team,[61] which sold a significant quantity of the pre-mined ETH to fund the development of the system (which Dr. [redacted] refers to as "the ICO" or Initial

---

58 *See* Sergio Demian Lerner, *The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin Creator, Visionary and Genius*, BITSLOG, https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/.

59 Based on an observed exchange rate of approximately 1 BTC = USD $65,000. *See* CRYPTOCOMPARE, *Bitcoin (BTC) – USD*, https://www.cryptocompare.com/coins/btc/overview/ (as observed Nov. 11, 2021).

60 ETHERSCAN, *Ether Total Supply and Market Capitalization Chart*, https://etherscan.io/stat/supply (as observed Nov. 11, 2021) (reporting the total ether token supply as 117,783,769.76 ETH).

61 CONSENSYS, *A Short History of Ethereum* (May 13, 2019), https://consensys.net/blog/blockchain-explained/a-short-history-of-ethereum; Luit Hollander, *History of Ethereum Hard Forks*, MYCRYPTO (May 4, 2020), https://medium.com/mycrypto/the-history-of-ethereum-hard-forks-6a6dae76d56f (describing how the Ethereum development team included the 8,893 pre-sale transactions in the Ethereum genesis block and manually set the gas limit for the first few days of the Ethereum blockchain's existence).

Coin Offering of ETH).[62] Accordingly, a more accurate description of the Token Allocation of ETH is that the allocation of all 72 million was controlled by the owners at the beginning of the ICO, and the owners sold all but 10% to fund the development of the blockchain.[63]

III. Additional Responses to Dr. [redacted] Report.

50. Dr. [redacted] at various places in his report, seizes upon the default Unique Node List ("dUNL") present in the rippled software that underlies the XRP Ledger as grounds to conclude that the XRP Ledger as of October 2021 "is centralized" and that the dUNL is "a root cause of inequality in the system." (Report at 22.) Dr. [redacted] states that the dUNL contains a list of "[p]articipants required for the proper operation of" the XRP Ledger. (Report at 6.) However, no participant in the XRP Ledger's validation process is required to use the dUNL to participate in validation.[64] Indeed, as Dr. [redacted] observes, the code of the XRP Ledger itself identifies two alternative UNLs—neither published by Ripple—that are available for validators to use. (Report at 20.) That one UNL is the "default" within the rippled code does not establish that use of the dUNL is *required*.[65] Moreover, Dr. [redacted] willingness to conclude that the "issue of a centralized dUNL publisher, alone, is in my opinion sufficient to render the XRP Ledger centralized" (Report at 6), demonstrates the insufficiency of his analysis in light of the literature

---

62 Vitalik Buterin, *Launching the Ether Sale*, ETHEREUM FOUNDATION BLOG (July 22, 2014), https://blog.ethereum.org/2014/07/22/launching-the-ether-sale.

63 Camila Russo, *Sale of the Century: The Inside Story of Ethereum's 2014 Premine*, COINDESK (July 11, 2020), https://www.coindesk.com/markets/2020/07/11/sale-of-the-century-the-inside-story-of-ethereums-2014-premine.

64 *See FAQ: What are Unique Node Lists (UNLs)?*, XRPL.ORG, https://xrpl.org/faq.html ("Each server operator can choose their own UNL.").

65 *See FAQ: Which UNL Should I Select?*, XRPL.ORG, https://xrpl.org/faq.html ("Currently, three publishers (Ripple, the XRP Ledger Foundation, and Coil) are known to publish recommended default lists of high quality validators, based on past performance, proven identities, and responsible IT policies. However, ***every network participant can choose which validators it chooses as reliable and need not follow one of the three publishers noted above***." (emphasis added)).

in the field. I am not aware of any peer-reviewed paper, and Dr. [redacted] cites none, that suggests that it is sufficient to examine one aspect of one layer of a blockchain and reach a conclusion as to whether the blockchain itself is centralized. To the contrary, the literature (including, but not limited to, Sai et al.) makes clear that a more thorough analysis is necessary before it is appropriate to draw any global conclusions regarding centralization, and further recognizes that not all layers of a blockchain must be fully decentralized for the blockchain to be considered decentralized on the whole.[66]

51. Dr. [redacted] also draws extensively from a 2018 paper by Chase and MacBrough (which was not peer-reviewed) to argue – without any independent analysis by Dr. [redacted] himself to substantiate the paper's conclusions – that a high amount of overlap is required between different validators' UNLs for the XRP Ledger to "provide" safety and liveness and for the "correct operation" of the XRP Ledger.[67] (Report at 21–22 and Appendix B.) Dr. [redacted] report, in turn, seizes on this overlap to opine that the XRP Ledger is centralized. (Report at 22.) I offer a few responses.

52. As an initial matter, Dr. [redacted] reliance on the Chase and MacBrough paper is misplaced because his report and the Chase and MacBrough paper analyze different versions of the rippled code. The research by Chase and MacBrough was performed as of February 21,

---

66 Sai et al., *supra* note 4, at 29–30; *see also*; Steven Ehrlich, *Do Crypto and Blockchain Need To Be Decentralized To Succeed In 2019?*, FORBES (Dec. 17, 2018), https://www.forbes.com/sites/stevenehrlich/2018/12/17/do-crypto-and-blockchain-need-to-be-decentralized-to-succeed-in-2019/?sh=55d667034442.

67 Notably, Chase and MacBrough make clear that their analysis only addresses the question of what might be necessary to "guarantee correctness" – not what is necessary for the XRP Ledger to function or operate. Brad Chase & Ethan MacBrough, *Analysis of the XRP Ledger Consensus Protocol* 2 (Feb. 21, 2018), https://arxiv.org/abs/1802.07242. As Dr. [redacted] report admits, neither Bitcoin nor Ethereum guarantee correctness under any conditions, as they are always vulnerable to a 51% attack. (Report at 15, 18.)

2018, apparently based upon a 2018 version of the rippled code.[68] In contrast, Dr. [redacted] says he looked at the "current" version of the rippled code in effect as of the date of his report – October 4, 2021. (Report at 7.) It would therefore be unsound for Dr. [redacted] to base his analysis or conclusions of the "current" rippled code upon a study that looked at a version of the software that is more than three years out of date. In that regard, the history of changes to the rippled code (which is open source and public) indicates that significant changes to the code have occurred between 2018 and the present.[69] Dr. [redacted] offers no basis to establish that the Chase and MacBrough analysis, nor his own conclusions based on Chase and MacBrough, are still valid more than three years after that paper was released and after multiple updates to the rippled software that modified the consensus mechanism on which Dr. [redacted] grounds his opinions.

53. Dr. [redacted] also does not consider that federated consensus models inherently require human agreement – the selection of a list of trusted validators – as a basic element, yet no peer-reviewed or other literature suggests or states that federated consensus blockchains are always centralized or cannot be decentralized. This is a limitation of Dr. [redacted] "Governance"

---

[68] According to Github, which contains the history of the open-source rippled code, version 0.90.0 of rippled was released on February 20, 2018. Assuming that Chase and MacBrough did not complete their article in a single day, it is likely that they were referring to an even earlier version of the rippled code, such as version 0.81.0 (released February 2, 2018) or version 0.80.2 (released December 15, 2017). *See* Releases - rippled, *https://github.com/ripple/rippled/releases*.

[69] Rippled version 0.90.0 contains "several features and enhancements that improve the reliability, scalability and security of the XRP Ledger." *Rippled Version 0.90.0*, GITHUB, https://github.com/ripple/rippled/releases/tag/0.90.0. Rippled version 1.6.0 "introduces several new features including changes to the XRP Ledger's consensus mechanism to make it even more robust in adverse conditions," including changes that "can improve the liveness of the network during periods of network instability." *Rippled (XRP Ledger server) Version 1.6.0*, GITHUB, https://github.com/ripple/rippled/releases/tag/1.6.0. Both of these versions of rippled were released between the version considered by Chase and MacBrough and the version considered by Dr. [redacted]

analysis that means he is unable to conduct a comparison between the XRP Ledger and proof-of-work systems (*e.g.* Bitcoin and Ethereum).

54. Dr. [redacted] report concludes by purporting to analyze "[w]hat risks to the XRP Ledger would or might materialize if Ripple 'walked away' or 'disappeared.'" (Report at 25.) As an initial matter, Dr. [redacted] cites no authority – and I am aware of none – to establish a methodology for such an analysis in the blockchain context. Dr. [redacted] analysis is purely speculative, grounded in unsupported assumptions about the behavior of multiple parties within the XRP Ledger ecosystem, and cannot form the basis for a reliable or repeatable conclusion. For example, Dr. [redacted] asserts that universities who have received funding from Ripple in the past may cease to operate validators if Ripple's funding disappeared. (Report at 26.) Dr. [redacted] offers no support for this assumption, and given the exceedingly low cost of operating a validator,[70] there is ample basis to believe Dr. [redacted] assumptions could prove incorrect.

55. Dr. [redacted] assumptions about what might happen if Ripple disappears are subjective and based on the assumption that the current state of the XRP Ledger predominantly or entirely contains validator nodes that use Ripple's dUNL. This assumption is visible in assertions like "[i]n the case where more than 20% of validators in the dUNL disappear, the network would not be operational. The current dUNL (as of October 4, 2021) contains 41 validators . . . . Hence, the network would cease to be operational if nine validators disappeared." (Report at 26.) Dr. [redacted] never establishes as a matter of fact, however, that the current operational XRP Ledger validators actually use the current dUNL, such that 20% of current dUNL validators disappearing could impact the operation of the network. As Dr. [redacted] acknowledges, two other UNLs that are not published by Ripple exist and, indeed, are referenced in the rippled code base. (Report at

[70] *See supra* note 42.

23.) Moreover, rippled does not require any validator to use any dUNL, or include any validator in particular in its own UNL.[71] Dr. [redacted] never explains why XRP Ledger nodes could or would not just switch to another already-published UNL.

56. Dr. [redacted] assumptions about the consequences of Ripple's disappearance also ignore that the XRP Ledger offers significant additional advantages to its users, such as increased speed and decreased transaction cost, with less negative environmental impact. (Adriaens Report at 22, 24–25.) These advantages – validating transactions in seconds, compared to approximately 10 minutes for Bitcoin – provide a significant value proposition for the XRP Ledger and an incentive for those who are interested in facilitating or enabling rapid decentralized settlement of transactions. (Adriaens Report at 22.)

57. While Dr. [redacted] report focuses narrowly on "in-protocol incentives" offered by Bitcoin and Ethereum (Report at 10 and 16), he ignores the significant competitive advantages that the XRP Ledger offers and the corresponding incentives for those interested in the success of such an ecosystem. (Adriaens Report at 25.) It is therefore unsurprising that participants in the XRP Ledger ecosystem – from exchanges like Bitrue to developers like XRPL Labs – operate validators without the need for in-protocol incentives.[72] Dr. [redacted] report offers no basis to conclude that these validator operators (whom I offer as mere examples of the over 120 validators currently active on the XRP Ledger system)[73] would cease operating their validators if Ripple were to disappear, and accordingly no basis to believe the XRP Ledger itself would disappear without Ripple.

---

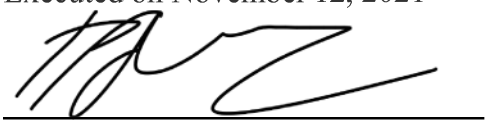
71 *See supra* note 64.

72 *See Validator Registry*, XRPSCAN, https://xrpscan.com/validators (as observed Nov. 11, 2021).

73 *Id.*

I declare under penalty of perjury that the foregoing is true and correct.

Executed on November 12, 2021



Peter Adriaens

Exhibit 34

Expert Report of Dr. [redacted]

Securities and Exchange Commission v.
Ripple Labs, Inc., Bradley Garlinghouse and Christian A. Larsen

Confidential

October 4, 2021
Updated January 25, 2022

Contents

1 Introduction

1.1 Assignment

I have been engaged by the Securities and Exchange Commission ("SEC"), through [redacted] ("[redacted]") to provide expert testimony in the matter of Securities and Exchange Commission v. Ripple Labs, Inc., Bradley Garlinghouse and Christian A. Larsen, pending in the United States District Court for the Southern District of New York. The SEC has retained me to independently analyze and opine on: (1) whether the distributed ledger system on which XRP token is transacted ("XRP Ledger") is a centralized or a decentralized system as of the date of this report, and (2) what would likely happen to the XRP Ledger if Ripple Labs Inc. ("Ripple") ceased functioning.

Before reaching those questions, SEC asked me to provide answers to certain background questions:

Prefatory Questions:

- (P1) Describe the basic operating principles of blockchain technology and explain how its consensus mechanisms work.
- (P2) Explain the XRP Ledger consensus mechanism, including the concept of Unique Node Lists ("UNLs").

The SEC then asked me to analyze and opine on the following questions:

Questions for Expert Opinion:

- (E1) To what extent is the XRP Ledger centralized or decentralized when compared to generally recognized blockchain protocols such as those used by Bitcoin and Ethereum?
- (E2) To what extent have Ripple's efforts been needed to support the proper functioning of the XRP Ledger?
- (E3) What risks to the XRP Ledger would or might materialize if Ripple "walked away" or "disappeared"?

1.2 Qualifications

I am a computer scientist with 18 years of specialization in fault-tolerant distributed systems, an area of computer science that is at the core of blockchain and decentralized systems. In particular, my core area of expertise are so-called "Byzantine" fault-tolerant ("BFT") distributed consensus protocols. *Byzantine* here refers to the ability of participants in a distributed system, to deviate from the algorithm prescribed to them (e.g., by being malicious, that is by acting to purposefully attempt to disrupt the functioning of the system). The consensus protocol that underlies the XRP Ledger aspires to be in the category of BFT consensus protocols.

I hold a [redacted] from the [redacted] (1996-2001) and a [redacted] degree from [redacted] in distributed systems (2003-2008). My PhD thesis entitled [redacted]

[redacted], dealt with BFT distributed consensus protocols. Before Bitcoin, BFT consensus was only a rather niche area of research. [redacted]

After my PhD, I was a Postdoctoral researcher at [redacted]. After that, in the period from 2010 to 2014, I worked in academia. [redacted]

I am an author of many research papers and patents which are often cited by other researchers. [redacted]

I respectfully ask you to refer to my enclosed CV for additional details.

I have been retained through [redacted], a forensic data analytics and litigation consulting firm. I am compensated by the SEC via [redacted] at the rate of $700 per hour. My compensation is not dependent on me reaching any specific opinion. Members of [redacted] team also performed work in connection with this report and are compensated at a rate ranging from $235 to $520 per hour.

1.3 Documents Relied Upon

For the analysis of the XRP Ledger protocol, I relied on two papers authored by current and former Ripple employees, the official documentation of the XRP Ledger, as well as on reviewing the code of the XRP Ledger server. These sources are listed in detail in Section 4.1.

Furthermore, the "References" section of this report contains a list of other documents and data sources I relied upon in completing the analysis in this report, including a body of scientific research related to the definition of decentralized systems.

Where appropriate, the data sources are given inline in the text, as a web link, footnote or a citation.[1]

2 Summary of Findings

I reviewed the scientific literature on decentralized systems, with which I was familiar, to establish a methodology for evaluating the extent of decentralization of distributed systems.

- I first adopt the basic definition of a decentralized system, as defined by Troncoso et al. [21], which defines decentralized systems as a subset of distributed systems where multiple authorities (parties) control different system components and no authority is fully trusted by all.
- I then refine this basic definition, with the support of the scientific literature, to identify four main aspects of decentralization: Resilience, Inclusiveness, In-Protocol Incentives, and Governance. I define each of these aspects of decentralization in Section 3.1.

I proceed to explain the inner workings and to evaluate the decentralization levels of the Bitcoin (Sec. 3.2) and Ethereum (Sec. 3.3) blockchains, respectively. I thereby answer Prefatory Question P1 and prepare the ground for answering Expert Question E1 (as defined in Sec. 1.1).

I then turn to analysis and explanation of the XRP Ledger protocol in Section 4, in particular to its concept of Unique Node Lists (UNLs), thereby answering Prefatory Question P2. In my analysis of the XRP Ledger I rely solely on the material which I consider endorsed by Ripple and/or its employees, as listed in Section 4.1.

Finally, in Section 5, I give my expert opinion, answering questions E1, E2 and E3, as stipulated in Section 1.1. Below, I give an overview of these findings.

I answer Question E1 in Section 5.1, where I evaluated the decentralization of the XRP Ledger (i.e., its Resilience, Inclusiveness, In-Protocol Incentives, and Governance aspects) and compared it to the decentralization of the Bitcoin (itself evaluated in Sec. 3.2.3) and Ethereum (Sec. 3.3.1) blockchains. An overview of this comparison is given in Table 1.

In summary, the XRP Ledger has low Resilience as it takes corrupting only a single party to be able to compromise key properties of the system.[2] In fact, as a result of its low Resilience, the XRP Ledger does not satisfy the basic definition of a decentralized system [21], and is, therefore, in my opinion, centralized.

The centralization here stems from the following facts pertaining to the XRP Ledger software, which I will detail later in this report:

1. Participants required for the proper operation of the system (nodes) are "curated" by Ripple for inclusion into a special list, called the dUNL, which is to be understood as a *default Unique Node List*.

[1] Beyond these sources, I further considered the following documents related to this case, none of which I relied on in forming my opinions set forth herein:

- "Submission to the Conference of State Bank Supervisors", submission by Ripple Labs Inc. Bates number RPLI_SEC 0086553.
- Case 1:20-cv-10832-AT Document 46 Filed 02/18/21, 79 pages.
- Case 1:20-cv-10832-AT Document 45 Filed 02/15/21, 9 pages.
- Case 1:20-cv-10832-AT Document 43 Filed 01/29/21, 93 pages.

[2] The number of parties that need to be corrupted to subvert key properties of a distributed system is also sometimes called the Nakamoto coefficient.

Decentralization aspect	**Ideal Decentralized System**	**Bitcoin Blockchain**	**Ethereum Blockchain (with Proof-of-Work)**	**XRP Ledger**
Nakamoto coefficient (Resilience)	always greater than 1, the higher the better	≥ 4	≥ 3	1
Inclusiveness	yes	yes	yes	no
In-Protocol Incentives	yes	yes	yes	no
Governance (public face)	no	no	yes	yes
Governance (tokens allocated at genesis)	0, the lower the better	0%	61.5% (about 10% owner controlled) of today's supply	100% (all owner controlled)

Table 1: Comparison of the XRP Ledger to the Bitcoin and Ethereum blockchains for key aspects of decentralization defined in the decentralization evaluation methodology of Section 3.1.

2. As of the latest release of the XRP Ledger software, referred to as "rippled v1.7.3", Ripple controls the web domain which hosts the service that provides the dUNL to the XRP Ledger participants. Namely, this dUNL provisioning service is deployed at the address `http://vl.ripple.com`.

3. Participants in the XRP Ledger, who use unmodified code of rippled v1.7.3, periodically refresh their locally referenced UNL, which serves as a local list of "trusted participants", by copying the contents provided by the dUNL provisioning service, i.e., the dUNL controlled by Ripple and disseminated at `http://vl.ripple.com`.

4. The design of the XRP Ledger requires, for correct operation of the protocol, a very large overlap (intersection) across UNLs that individual participants use.

5. Therefore, Ripple's dUNL provisioning service needs to be trusted for correct operation of the system.

   Otherwise, in the case of an untrusted dUNL provisioning service, it could provide participants with UNLs that do not have sufficient overlap, compromising key properties of the XRP Ledger. This makes it possible for a single authority, namely, Ripple as the dUNL publisher, to subvert key properties of the system. This makes the XRP Ledger, by definition of Troncoso et al. [21], and in my opinion, centralized.

This issue of a centralized dUNL publisher, alone, is in my opinion sufficient to render the XRP Ledger centralized. Nevertheless, I conducted an even more detailed evaluation of the XRP Ledger through the prism of other decentralization aspects. These are summarized below:

- I identified another Resilience vulnerability which makes it possible for a single party to subvert key properties of the system, independent of the centralized dUNL publisher issue. This is detailed later in the report (Appendix B).

- The XRP Ledger does not satisfy Inclusiveness, which, in short, refers to a system which provides equal opportunities to participants (see Section 3.1, for detailed definition). While the XRP Ledger allows any participant to join the system, it treats its participants unequally. This inequality stems,

again, from the existence of a Ripple-curated dUNL, which is, in turn, required for the XRP Ledger to function properly.

- Unlike other compared blockchains, the XRP Ledger does not have In-Protocol Incentives, which are defined, in short, as the existence of software-defined incentives for participants to join the system and which contribute to the decentralization of a blockchain (see Sec. 3.1). In contrast, the XRP Ledger solely relies on out-of-protocol actions of existing participants to incentivize new participants to join the XRP Ledger.
- Finally, the XRP Ledger scores poorly in the Governance aspect. For instance, while an ideal decentralized system should have no public face (representative) and should have not pre-allocated tokens at system's inception, the XRP Ledger sits at the opposite end of the spectrum, having pre-allocated all its tokens to people and organizations which serve or have served as its public face.

To answer the next question, Question E2 from Section 5.2, regarding the role of Ripple's efforts in supporting the proper functioning of the XRP Ledger, I first analyzed the situation as of the time of writing of this report, assuming no further changes to current rippled v1.7.3 code, as the answer depends on the software code. Given the nature of the question, I also analyzed some historical aspects of the system, namely the fraction of validators in the dUNL which Ripple and organizations that received funding from Ripple used to control.

My findings show that, today, Ripple's efforts are needed to maintain components of the XRP Ledger secure from internal and external attacks. These efforts relate primarily to publishing a dUNL, at `https://vl.ripple.com`, in a secure way so that a potential attacker (i.e., a malicious adversary, also called a Byzantine [13] attacker) cannot take control over the dUNL publishing service.

In addition, Ripple needs to ensure that the dUNL is curated and populated only with attested validators, since even a single Byzantine validator, combined with an unreliable network, may subvert key properties of the XRP Ledger— as detailed in Appendix B. For this same reason, Ripple needs to maintain security over the 6 validators it itself controls out of 41 validators contained in the dUNL as of October 4, 2021.

Ripple used to control a larger fraction of validators listed in the dUNL. I give a historical overview of this fraction at the end of Section 5.2. Throughout a large majority of the history of the XRP Ledger, Ripple controlled more than 20% of validators in the dUNL. Moreover, its level of control was actually at 100% of validators in the dUNL for much of its history. This is relevant because, as discussed below in more details, when an organization controls more than 20% validators in the dUNL, it becomes a single point of failure and needs to be trusted by other organizations that use the same dUNL.

Here, it is important to repeat and emphasize the result of my analysis related to Question E1. Even though Ripple today controls less than 20% of validators, it is still a single point of failure that needs to be trusted by all participants who use the only dUNL to which the rippled v1.7.3 software defaults, and which is controlled by Ripple and disseminated at `http://vl.ripple.com`.

Finally, in answering Question E3 (see Sec. 5.3), I consider the risks that might arise in the hypothetical case of Ripple's disappearance and the effects it might have on the XRP Ledger.

If Ripple disappears, it may be impossible to continue securely publishing the dUNL on the web address that Ripple currently controls (`http://vl.ripple.com`). For example, if the registration of the `ripple.com` domain expires, the attacker could register the domain on the attacker's name, take over control of the

domain and publish non-intersecting dUNLs hence subverting key properties of the system. If participants decide to ignore the dUNL to avoid such an attack, they would need to make changes to the XRP Ledger consensus software, or consent on UNLs through human agreement.

Finally, in the case where Ripple disappears but the dUNL somehow continues to be published correctly at `http://vl.ripple.com`, there are still potential risks. Namely, even assuming the complete absence of malicious attacks, the correct functioning of the XRP Ledger as a system requires 80% of validators within the dUNL to operate correctly and without faults or disappearance from the system. With 41 validators in the dUNL, this means that the XRP Ledger will halt if 9 or more validators (i.e., over 20% of 41 validators) stop functioning. With Ripple controlling 6 out of these 41, it may seem that the XRP Ledger might continue to operate even without Ripple.

However, if Ripple disappears, other validators may disappear as well. For example, 9 universities which have received funding from Ripple under the umbrella of the University Blockchain Research Initiative (`https://ubri.ripple.com/`) operate validators listed in the dUNL. If Ripple disappeared, the funding would eventually stop too, and the universities may realistically stop operating validators, in particular since the XRP Ledger offers no In-Protocol Incentives.[3] Disappearance of only 3 out of these 9 validators operated by universities, combined with the disappearance of 6 validators operated by Ripple would be sufficient for the XRP Ledger network to halt. In addition to the 9 universities, at least 4 companies that received funding from Ripple also operate validators listed in the dUNL. Operation of these validators could also be compromised if Ripple disappears.

3 Background

In this section, we[4] describe the methodology for evaluating the decentralization of a given blockchain system (Section 3.1) and the necessary technical background behind the Bitcoin (Section 3.2) and Ethereum (Section 3.3) blockchains. This background is needed in order to answer question E1 as stipulated in the "Assignment" section (Section 1.1).

3.1 Methodology for Evaluating Decentralization in Distributed Systems

Decentralized *blockchain* systems are a subset (i.e., a special case) of *decentralized* systems, which are in turn a subset of *distributed* systems.

In computer science literature, a *distributed system* is loosely defined as *a collection of independent computers that appear to its users as a single coherent system [20].*

In turn, *decentralized systems* can be defined as *a subset of distributed systems where multiple authorities control different components and no authority is fully trusted by all [21].*

For instance, popular cloud and social networks like Google, Facebook or Twitter, are examples of distributed systems. However, these systems are not decentralized, as each of them is controlled by a single authority (company). Note that it is not sufficient for a system to simply have its components controlled by

[3] As discussed in Section 5.3, this argument could be extended to commercial companies, business partners of Ripple, which operate validators listed in the dUNL.

[4] Conforming to the style of scientific writing I have been used to, I sometimes use "we" instead of "I".

multiple authorities, to be classified as decentralized — the absence of a single trusted authority is needed, meaning that any component in a decentralized system could be *Byzantine*.

Byzantine [13] here refers to the ability of a participant or a component in a distributed system to deviate from the algorithm prescribed to them. This includes any behavior, including acting to purposefully attempt to disrupt the functioning of the system (in this case we talk about *attacks*). Byzantine behavior in literature is also sometimes also called, e.g., *adversarial*, *malicious*, or *arbitrary*. In this report, we sometimes use these notions for better readability. Moreover, we use the notion of *adversary*, to denote an authority, or group of authorities, that can orchestrate behavior of individual Byzantine components to mount attacks on the system.

As we will argue later in detail, one example of a decentralized system is the Bitcoin blockchain, in which no single authority, even if Byzantine, can subvert the correct functioning of the system.

Beyond the above basic definition of a decentralized system, computer science literature considers multiple *aspects* of decentralization in an attempt to refine and characterize its nuances, as well as the differences among decentralized systems (see e.g., [17] for a recent survey). We summarize these into the following *decentralization aspects* which we will later use to evaluate the decentralization of the Bitcoin blockchain, the Ethereum blockchain and the XRP Ledger.

1. **Resilience** of a system refers to its ability to withstand Byzantine behavior of components of the system.

   Resilience itself may apply to different properties of the system, namely *safety* and *liveness* [12, 1].

   Informally, a safety property of a system stipulates that "bad things" do not happen. An example of such a safety property in the context of blockchains is *double-spend* resistance [16] which, in short, requires the system to prevent an adversary from spending the same amount of money twice.

   In turn, a liveness property stipulates that "good things" do eventually happen. An important liveness property of a blockchain system is *censorship* resistance [9] which, in short, requires the system to prevent the adversary from excluding (censoring) payment transactions. Another important liveness property of a system is not to stop making progress in its operation altogether. For instance, if a blockchain halts and stops processing transactions, it fails to satisfy liveness.

   We define the censorship and double-spend resistance properties more precisely later, in Section 3.2.

   In this context, the scientific literature and engineering practice is typically interested in the minimum number of authorities that the adversary needs to compromise to subvert a key property of the system, such as safety or liveness. In the context of blockchains this number is sometimes referred to as the *Nakamoto coefficient*[5] [19, 23]. Intuitively, the higher the Nakamoto coefficient, the higher the level of decentralization. As per the definition of a decentralized system we adopted [21], if this number is 1 — i.e., if a single participating authority can compromise a key property of the system — the system cannot be deemed decentralized.

2. **Inclusiveness** of the system refers to the ability of the system to welcome new participants in a way which provides them with equal opportunities compared to existing participants [22]. In short, a decentralized system provides *Equal Opportunities* if it [22]:

[5]Honoring Bitcoin's pseudonymous inventor, Satoshi Nakamoto. Citation [23] is an example of a scientific paper that explicitly mentions the Nakamoto coefficient.

(a) allows any participant Alice to have an equal role in the system as any other (new or existing) participant Bob, provided Alice makes the same investment in system resources as Bob, and

(b) the system does not prevent Alice from making such an investment.

Then, a decentralized system is defined as Inclusive if and only if it satisfies Equal Opportunities [22].

Inclusiveness is a refinement of a well-known classification of blockchain systems into *permissioned* and *permissionless* systems (see e.g., [15]). In short, in permissionless systems, participants self-elect into the system, whereas permissioned systems rely on an external selection process to be admitted into the system, where *authority to choose [participants] typically resides with an institutional or organizational process [15].* In other words, permissionless systems are *open membership* systems, whereas permissioned systems are *closed membership* systems. Therefore, as a general principle, permissionless systems are to be considered more decentralized than permissioned systems. Moreover, permissioned systems are never Inclusive, while permissionless systems may or may not be Inclusive.

For example, some permissionless systems, including the XRP Ledger, allow anyone to participate but in a way that prefers some participants over the others. This makes them permissionless but not inclusive. In the XRP Ledger, nodes that participate in the system but which are included into the dUNL have a different role than the nodes which may elect to participate in the system but are excluded from the dUNL, violating Equal Opportunities.

Related to Inclusiveness, there are other approaches to refining the notion of permissionless systems in the scientific literature, which aim to capture the equality of participants within the system, taking into account the size of their investment. For instance, Karakostas et al. [10] define *egalitarianism* in a rather technically involved way aiming at capturing the proportionality of rewards of participants in blockchains compared to their investment. In a related approach, Fanti et al. [7] define *equitability*, which quantifies how much a participant can amplify her token holdings compared to her initial investment. As both notions of equitability and egalitarianism are based on participants' rewards, i.e., In-Protocol Incentives, they cannot be applied to the XRP Ledger, as the XRP Ledger does not have any rewards for participants in the system, unlike the Bitcoin and Ethereum blockchains.

Finally, some authors recognize *operational decentralization* as an important aspect [17] that is related to Inclusiveness. Intuitively, operational decentralization aims at capturing special hardware requirements for participation in the system — the less specialized the hardware requirements, the higher the decentralization. For instance, a system which requires large amounts of storage (e.g., hard disk space) to participate in blockchain A would be deemed more centralized than blockchain B which requires less storage space [17].

3. **In-protocol Incentives** is the decentralization aspect which refers to whether the system has rewards for protocol participants, paid out to protocol participants within the protocol itself. Such payments are typically in the protocol's *native token*, e.g., "BTC" on the Bitcoin blokchain. In-protocol incentives are an important aspect of decentralized systems [17]. Troncoso et al. [21] argue that the development of adequate incentives is necessary to build a successful decentralized system.

   In general, In-protocol Incentives test if the system is genuinely open to new participants. On the one hand, a permissionless system that provides incentives for participants will attract new participants,

particularly if it is Inclusive.

On the other hand, a permissionless system that does not provide In-Protocol Incentives is only seemingly open, as new participants have less or no economic rationale to join the system. Such a system may resort to out-of-protocol incentives, in which case incentives are not governed by system software, but typically by people. Out-of-protocol incentives may involve existing participants establishing business and contractual relations with new participants to motivate them to join the system. This approach resembles and is more common in permissioned networks [2].

In the context of incentives, wealth distribution across token stakeholders is also considered an aspect of decentralization [17]. If the tokens of a system are held widely among many holders, the system is more likely to be considered more decentralized. If there is concentration of ownership, the system is more likely to be considered more centralized.

4. **Governance** of the system refers to the level of power, if any, of human stakeholders to influence and change key rules in the system, e.g., through software updates.

   Several parameters for evaluating decentralization of governance power have been proposed or discussed in the literature. These include:

   (a) *governance of the infrastructure* [8], or *improvement control* [17], often involving the number of developers contributing to a system codebase and the number of people contributing to the discussion around a system's design [3],

   (b) *existence of a public face* [8], which can be defined as a personality and/or institution that is widely recognized as a spokesperson or a representative of the system.

   (c) *owner control*, measured by examining the total tokens accumulated by the stakeholders in the early adoption period [17].

Finally, some authors [17] consider additional aspects of decentralization, including the decentralization at the *network layer*, i.e., pertaining to the decentralization of the network that underlies a distributed system, and the decentralization at the *application layer*, which includes, e.g., the diversity of wallets and applications that permit users to interface with the assets on the blockchain. Decentralization at the network layer requires that no single authority can control all the participants of a decentralized system at the network and infrastructure layers. For instance, a system which is controlled (administered) by multiple organizations that all host their participating nodes on a single cloud provider (e.g., Amazon Web Services) is not to be considered decentralized, as the cloud provider itself could be seen as a single trusted authority.

To maintain emphasis on the core distributed systems aspects, in this report we acknowledge these decentralization aspects that go beyond the core of a system, namely network and application layer decentralization, yet we opt to focus on decentralization aspects of systems proper.

3.2 Bitcoin Blockchain

Bitcoin is an open-source peer-to-peer computer network (also known as the "blockchain") for generating and transferring (transacting) electronic coins (denoted by BTC) among users of the blockchain. BTC is the *native coin* of the Bitcoin blockchain — this means that BTC does not represent any concept outside

the Bitcoin blockchain and that participants in the system are rewarded only in BTC. In the following, we denote by "Bitcoin" the Bitcoin blockchain, i.e., the peer-to-peer computer network and its software, and by "bitcoin", or "BTC", its native electronic coin.

Bitcoin was conceived [16] as an electronic cash network to allow online payments to be sent directly from one party to another without going through a financial institution or any other trusted middleman. This was not possible prior to Bitcoin as all electronic payments required trusted intermediaries, unlike physical, in-person, cash or barter transactions. Namely, prior to Bitcoin, electronic payments over the internet were sent only using trusted intermediaries such as PayPal, credit card processor companies (e.g., AMEX, VISA, MasterCard) or through traditional banking payment systems in which banks act as trusted payment intermediaries.

At a high-level, in Bitcoin, a user Alice wishing to send 1 BTC to another user Bob, uses her private cryptographic key to digitally sign a transaction to transfer 1 BTC from an *address A*, that Alice controls, to *address B* supplied to Alice by user Bob. Alice's private cryptographic key is like a very long password known only to Alice, which is cryptographically tied to *address A*.

Knowledge of the private key allows Alice to have control over address A and over the BTC digitally represented at that address. As a fundamental principle, whoever controls the private keys corresponding to a given address, controls bitcoin pertaining to that address.

The main challenge in such a system arises when users are not trusted by other users. This lack of trust is inherent to a system without trusted intermediaries. Namely, Alice could attempt to *double-spend* her BTC.

Consider the following example of a double-spend attempt. Alice signs transaction $tx_{Alice-to-Bob}$ in which she transfers 1 BTC from address A she controls, to Bob's address B. However, she also signs a conflicting transaction $tx_{Alice-to-Alice}$ in which she sends 1 BTC from address A to another address A' that Alice also controls.

Which of these conflicting transactions should be actually taken into account is the main technical problem Bitcoin solves. In the process called *consensus*, peers in the Bitcoin network, without trusting each other, agree on the global order of all transactions in the system thanks to a set of predetermined parameters (programmed into the software that created the Bitcoin network) that govern how to reach consensus.

In our example, all peers in the Bitcoin network would agree on the relative order between the two conflicting transactions $tx_{Alice-to-Bob}$ and $tx_{Alice-to-Alice}$. The first transaction in that order would be considered valid, whereas the other would be discarded. Or, the order could be the other way around — the point is that the consensus mechanism for recording transactions on the Bitcoin blockchain (explained in detail later) provides a mechanism for participants in the network, who may not even know each other and do not trust each other, to nevertheless agree to validate the exact same sequence of transactions.

Besides preventing double-spends, another important property Bitcoin provides is censorship-resistance. In short, censorship-resistance guarantees a correctly-behaving user Alice to have her transactions eventually included in the blockchain (while possibly having Alice pay a *transaction fee* for this service). In other words, censorship-resistance guarantees that transactions will not be excluded from the Bitcoin blockchain due to actions of a Byzantine adversary or due to peers disappearing from the system.

In the following, we explain the Bitcoin consensus mechanism, first describing consensus preliminaries (Section 3.2.1) followed by explaining its validation mechanism (Sec. 3.2.2).

3.2.1 Bitcoin Blockchain Consensus — Preliminaries

For efficiency reasons, Bitcoin processes transactions in blocks, which are groups of transactions together with protocol metadata. Blocks have a maximum block size. Effectively, the Bitcoin consensus mechanism establishes a global order on those blocks forming a *chain* of blocks (i.e., a "blockchain"). Consequently, Bitcoin establishes global order on the transactions contained in those blocks.

Bitcoin software defines a so-called *genesis* block, the first block in the chain, to which the latter blocks are appended. Bitcoin genesis block contains a link to the "real" (physical) world, with the headline of the cover page of *The Times* (British daily national newspaper) from January 3rd, 2009 reading *"Chancellor on Brink of Second Bailout for Banks"* being written into the Bitcoin genesis block. This link to the real world, beyond possibly conveying a motivation for the existence of Bitcoin, is important because it proves that the creator of the Bitcoin network, Satoshi Nakamoto, could not have run the code before that day to generate blocks which would be considered valid by the Bitcoin blockchain.

At the beginning of the Bitcoin blockchain's history there were really no bitcoin to transact, as none had been brought to existence (i.e, *minted* or *mined*) yet. To bring bitcoin into existence, Bitcoin software defines a *block reward*, which is at the same time an incentive for participants to participate in Bitcoin consensus. Bitcoin rewards every participant who successfully adds a block to the blockchain with a fixed reward, which halves every 210,000 blocks. The period of 210,000 blocks corresponds roughly to 4 years, as Bitcoin block production time is set to self-adjust to an expected 10 minutes between consecutive blocks. For the first 210,000 blocks, the block reward was 50 BTC per block. With maximum bitcoin supply, as stipulated by Bitcoin code, being 21 million BTC, 50% of all bitcoin have been mined in the first 210,000 blocks.[6] With block reward halving to 25 BTC, from block 210,001 to block 420,000, an additional 25% of bitcoin total supply have been minted in that period, and so on, with the current Bitcoin block reward conveniently conveying which percentage of the total supply has been minted within the current 4-year window. Currently, more than 12 years after the genesis block, the Bitcoin network has produced over 700,000 blocks with the current block reward being 6.25 BTC.[7]

Once a block reward brings bitcoin into existence, bitcoin can be transacted. For instance, assume Alice won the block reward at block number 100,000. Then, starting from the next block 100,001, Alice can transact those bitcoin and send them to other participants.

A participant in the Bitcoin network is an entity that runs a *full node*. Such a participant is sometimes also called a *peer* or a *validator*. Each Bitcoin full node keeps the entire history of the blockchain, validates new blocks and (optionally) participates in creating new blocks. Bitcoin's maximum block size and a relatively conservative time period interval of 10 minutes between the blocks imply that the blockchain does not grow too fast compared to advances in computer hardware.

Today, the size of the Bitcoin blockchain is about 400 GB of data,[8] which means that a full node can be easily run on low-cost hardware, with a mid-sized hard-disk and internet connection, basically by anyone.[9] Moreover, users can entirely opt-out from running full nodes, by maintaining only *client* wallets,

[6] See, for example, an illustration on `https://static.coindesk.com/wp-content/uploads/2020/03/bitcoin-supply-and-subsidy-775x500.png`.

[7] The reward may be fractional, as each bitcoin is divisible into 100 million smaller units, usually called satoshis. As an illustration of the value of Bitcoin block reward incentives, awarded on average every 10 minutes, the market price of the 6.25 BTC block reward today is, roughly, about $300,000 USD.

[8] `https://blockchair.com/bitcoin/charts/blockchain-size`.

[9] Bitcoin full node can be run on hardware which today costs about $200 USD, see `https://getumbrel.com`.

which protect their private keys and send Bitcoin transactions to others' (full) nodes. Finally, full nodes are incentivized to invest more into hardware and computing equipment, if they wish to have a higher probability of obtaining block rewards in the context of Bitcoin consensus, as explained next.

3.2.2 Bitcoin Consensus Validation

Bitcoin consensus proceeds as follows [16]:

1. New proposed transactions are broadcast to all nodes.

2. Each node collects new transactions into a block. A node cryptographically links the new block to its predecessor (parent) block. These parent links define the position of the new block in the blockchain and its path all the way to the genesis block. In short, a node chooses the predecessor block for the new block to be the one which has the *longest chain*[10] of blocks on its path to the genesis block, out of all blocks known to a node. In principle, a Bitcoin node only considers as valid only those transactions contained in the longest chain.[11]

3. In the process often called *mining*, or *Proof-of-Work* [16], each node repeatedly tries to find a final piece of information, called a *nonce*, which when embedded into the new block, will make other nodes accept and declare the new block as *valid*.

   This is the **key point** in the otherwise relatively straightforward Bitcoin consensus. This part of Bitcoin consensus relies on the widely-established cryptographic primitive called *cryptographic hash function*, or simply a *hash function*. A hash function $H()$ is a deterministic function which takes as input data of any length, e.g., a Bitcoin block, or a picture of a cat, or a YouTube video, and outputs a fixed length string of bytes, which uniquely represents the original input data. A cryptographic hash function has a few "magical" properties which Bitcoin makes use of, in particular that one cannot predict the output of a hash function by changing slightly the input, nor can it construct the otherwise unknown input which gives the desired output.

   So how does the hash function help establish block validity?

   The Bitcoin consensus validation mechanism requires a hash of a valid block to start with a specific number of zeros (0s) when represented as a bit string, that is a sequence of 0s and 1s. However, since the output of a hash function cannot effectively be predicted, a block hash with one specific nonce appears basically as a random string of 0s and 1s. Therefore, nodes need to try many nonces in order to be lucky and construct the required final data for the block such that the hash of the block will start with many 0s, as required by the validation code.

   The actual required number of leading zeros is self-adjusted by the Bitcoin blockchain during its lifetime, based on the Bitcoin code and the frequency of mined blocks, to maintain an expected block time of 10 minutes between the blocks.

   In summary, finding a nonce which makes the block valid is effectively a very simple but computationally intensive guessing game in which a node repeatedly tries different nonces, applies them to the rest of

[10] In fact, it is the chain which requires most work, which is most often the longest chain. For simplicity of narrative, we talk about "longest chain."

[11] Some blocks may potentially end up on branches off the longest chain. These blocks are called *orphaned* and transactions in such blocks are invalid and not taken into account.

the block, applies the hash function and sees if the output hash has the required number of leading zeros.

4. When a node finds a nonce and completes the Proof-of-Work, it broadcasts the block to all other nodes.

5. Other nodes run the *validation step* and accept the block only if: *(i)* all transactions in it are valid and do not contain already spent bitcoin, and *(ii)* the hash of the block starts with the required number of 0s.

   Unlike the mining step (Step 3) which is computationally very expensive to compute, and is typically completed only by nodes with high computing power, this validation step (Step 5) is very simple and inexpensive to compute even on low-cost hardware.

To summarize, Bitcoin Proof-of-Work (Step 3 above) consists of a miner node performing repeatedly the following substeps: a) changing the nonce, b) applying the hash function, c) seeing if the output starts with the required number of 0s, and going back to substep a) if it does not. In recent months, the Bitcoin network as a whole is estimated to have performed anywhere between 68 EH/s (exahashes per second) on June 28, 2021 and 190 EH/s (on May 9, 2021).[12] An exahash per second is one quintillion (a billion billion) hashes per second, a very large number of operations.

3.2.3 Evaluating Bitcoin Decentralization

In this section we evaluate Bitcoin consensus as described in the previous section, in the context of the decentralization methodology introduced earlier in Section 3.1. This will help us answer question E1 for expert opinion as stated in Section 1.1.

Resilience. As discussed in Section 3.1, Resilience of a decentralized system can be measured with respect to different properties.

We look at two major possible issues: the double-spending issue and the censorship of transactions issue.

To mount these attacks effectively on the Bitcoin network, the adversary needs to control more than 50% of the network computing power. This would allow the adversary to simply ignore blocks produced by the rest of the network and produce the dominant longest chain, which would then, by Step 2 of the Bitcoin consensus protocol (Sec. 3.2.2), be the effective history of transactions. In the case of censorship attacks - this new history could simply be empty of transactions, or could specifically exclude the transactions of certain participants the adversary wishes to censor. This is known as a 51% attack for Bitcoin and requires a majority of the hash power of the network.

Whereas it is difficult to precisely calculate the Nakamoto coefficient (number of different authorities required to mount the attack) for Bitcoin, this resilience can be conservatively estimated. Namely, Bitcoin nodes often group into so-called *mining pools* to spread out their earnings from block rewards more evenly over time. While individual nodes are often not directly under the control of a mining pool operator authority and could leave the mining pool if they detected that they were participating in an attack, for a *very conservative* estimate of Resilience one can assume that a mining pool fully controls all the nodes inside the pool. With

[12] `https://www.coinwarz.com/mining/bitcoin/hashrate-chart`.

this in mind, at the time of writing this report, more than 50% of Bitcoin mining power is controlled by 4 mining pools.[13] Therefore, the conservative estimate of the Nakamoto coefficient for Bitcoin is 4.

Finally, it is worth noting, in the context of later comparison to the XRP Ledger and the impact of Ripple's hypothetical disappearance (Sec. 5.3), that in the absence of Byzantine participants, the Bitcoin network is resilient to any number of participants disappearing from the system. This was effectively tested in the Bitcoin network recently, when the computing power in the Bitcoin network dropped by about 65% between May 9, 2021 (190 EH/s) and June 28, 2021 (68 EH/s), as we already discussed. This had little effect on the Bitcoin network, except that, for some time between periodic network self-adjustments, block production took more than 10 minutes on average.

Inclusiveness. Bitcoin is a permissionless system which provides Equal Opportunities, because:

- Bitcoin allows any two participants, new or old, that make the same investment into system resources (computing power) to play the same role in the system.[14]
- Furthermore, the nature of Proof-of-Work consensus does not prevent any participant from making such an investment into system resources. In particular, assuming a free market for computing power, existing participants cannot prevent new participants from entering the system.

  With innovation in computing and the seemingly unstoppable growth of computing power available to humans, often modeled by Moore's Law (see e.g., [14]), the computing power of the existing participants actually decays in time compared to the computing power available outside the system, which is free to join the Bitcoin network.

Consequently, as it provides Equal Opportunities, Bitcoin is Inclusive.

Bitcoin also allows a large degree of operational decentralization, as its full node requirements are relatively modest with the only notable full node hardware requirement being a hard disk capable of storing 400 GBs of blockchain data for the full blockchain history (see also Sec. 3.2.1).

In-protocol Incentives. Bitcoin provides incentives to nodes to participate in the system. Besides block rewards which we discussed in Sec. 3.2.1, Bitcoin also awards block miners with *per-transaction fees*.

Incentives provide a rational and transparent economic reason for new participants to join a decentralized system. Combined with Inclusiveness, which means that the system welcomes new participants, such incentives contribute to the rise of new participants promoting decentralization.

Finally, as indicated in the Bitcoin whitepaper [16], the economic incentives of Bitcoin make safety attacks towards compromising Resilience less likely than if the In-Protocol Incentives did not exist. If certain nodes control a large amount of computing power in Bitcoin they have an economic dilemma between using that power to attack the system or using that power to behave correctly and earn block rewards and transaction fees. This intuitively contributes to increasing the Nakamoto coefficient (Resilience measure) and consequently increasing the decentralization level of the network, in the presence of economically rational participants.

[13] As we observed at `https://taproot.watch/miners` and `https://btc.com/stats/pool`.

[14] Note that participants that do not make the same investment into system resources, do not necessarily have the same power in the system. For instance those that invest more into computing power can expect higher rewards from the system (e.g., more frequent block rewards).

Governance. Concerning code improvement proposals, anyone can propose a change to the Bitcoin open-source software via Bitcoin Improvement Proposals (BIPs).[15] In practice, relatively few "core" developers (developers of the Bitcoin Core reference node software) propose and implement changes. Major changes to software are relatively rare, with no BIP containing a backwards incompatible change to Bitcoin consensus (also known as a hard-fork) ever having been deployed in the software. For changes that implement more strict consensus validation rules, i.e., which reduce the space of valid blocks and are backwards compatible (soft-fork), consensus among core developers is required, together with approval of miners through on-chain voting.

That said, as Bitcoin is open-source software, anyone can make any change to the software. A number of such backwards incompatible changes to Bitcoin code have resulted in Bitcoin network forks and, effectively, separate blockchain networks.[16]

The Bitcoin network does not have a single individual or company acting as its public face [8]. This fact contributes to its decentralization. The absence of a public face is primarily due to the fact that its creator(s) acted under the pseudonym *Satoshi Nakamoto*, who disappeared from the public discourse more than 10 years ago.

Regarding owner control, Bitcoin did not have a hidden owner accumulation phase. The first transaction in the Bitcoin network happened in block #170, seemingly between Satoshi Nakamoto and a cryptographer Hal Finney, on January 12, 2009, 9 days after The Times newspaper timestamp contained in the genesis block.[17] The first block following the genesis block was mined, probably by Satoshi Nakamoto, 6 days after the genesis block,[18] on January 9, 2009.[19]

3.3 Ethereum Blockchain

Ethereum was announced in a post on the online Bitcoin forum, *bitcointalk*, in early 2014 by Vitalik Buterin [4], with the post designating Buterin as the inventor of Ethereum. The post mentions the other 6 members of the original Ethereum team.

Compared to Bitcoin, the main novelty of Ethereum was the introduction of the capability to code more complex and more general applications on top of a decentralized consensus. As Buterin stated in the Ethereum announcement post [4]: *"Up until this point, the most innovation in advanced applications such as domain and identity registration, user-issued currencies, smart property, smart contracts, and decentralized exchange has been highly fragmented, and implementing any of these technologies has required creating an entire meta-protocol layer or even a specialized blockchain."* Ethereum provides a platform for the development of such applications, one on which different applications can co-exist. In the Ethereum parlance, these applications are called "smart-contracts."

In the same forum post, a pre-sale of Ethereum's native token, called ether or ETH, was announced.

[15] `https://github.com/bitcoin/bips`

[16] Examples include Bitcoin Cash and Bitcoin Gold.

[17] Sources that discuss this include `https://thehunt.btcorigins.com/moments/the-first-transaction/` and `https://themoneymongers.com/first-bitcoin-transaction/`. I verified myself, by examining the Bitcoin transaction history, that the first transaction between two addresses indeed happened in block #170, see `https://www.blockchain.com/btc/block/170`.

[18] `https://www.blockchain.com/btc/block/1`.

[19] As it is widely believed, Satoshi Nakamoto may have mined a sizeable number of bitcoin in the early days of the network following the genesis, as an early participant. The exact number is practically impossible to support with hard evidence. However, we do have hard evidence, in the very Bitcoin transaction history, that an overwhelming majority of those early bitcoin that could be attributed to Satoshi Nakamoto were never transacted on the network.

The Ethereum genesis block defined roughly 72 million ETH (see `https://etherscan.io/stat/supply`), out of which about 60 million ETH tokens were sold in a crowdsale process called an initial coin offering (ICO) which ran in the summer of 2014. In the Ethereum ICO, people transferred their bitcoin (31,529 BTC in total, see e.g., `https://icoprice.com/ethereum/`) to the Bitcoin network address controlled by the Ethereum team and were allocated in return roughly 60 million ETH in the Ethereum genesis block, which appeared about a year later, in late July 2015. The difference of 12 million ETH was allocated in the genesis block for funding further development of the network.

Within the network, the native token ETH on the Ethereum network is used to pay for the computation performed by the applications (smart contracts) that run on top of the Ethereum network. This is called "gas." The Ethereum network does not have a hard cap on ETH supply.

3.3.1 Ethereum Consensus and its Decentralization

Since its inception, Ethereum has been using a variant of Bitcoin's Proof-of-Work for consensus. The two consensus protocols differ in subtle technical details, notably with respect to the approach of rewarding miners who mine blocks which do not end up on the "longest chain." Besides this difference, Ethereum uses a shorter time interval between blocks (about 15 seconds). At a high-level, the two consensus protocols can be considered very similar.

That said, practically since its inception, Ethereum has been planning to switch to an alternative consensus model called Proof-of-Stake, with the first software updates to the Ethereum network in this direction taking place recently. As the decentralization level of a distributed system fundamentally depends on its underlying consensus protocol, we evaluate the decentralization of the Ethereum network assuming its current consensus protocol, i.e., the one based on Proof-of-Work. After this, we briefly reflect on the potential impact of a Proof-of-Stake consensus to Ethereum decentralization.

Resilience. With Proof-of-Work as its underlying consensus mechanism, the reasoning about Ethereum Resilience shares similarities to that of Bitcoin. At the time of writing of this report, more than 50% of Ethereum mining power is controlled by 3 mining pools, making the conservative estimate of the Nakamoto coefficient for Ethereum equal to 3.[20]

Inclusiveness. With Proof-of-Work as the underlying consensus, Ethereum is a permissionless system which satisfies Equal Opportunities, which makes it Inclusive.

When it comes to operational decentralization, storing the full history of the entire state on Ethereum network has relatively high storage requirements of over 5 TB for an *archive* node which cannot be run on current commodity (i.e., widely available) hardware. However, the Ethereum network allows the pruning of old states with nodes maintaining the current state of the network (*full nodes*) requiring less than 1 TB of storage, which is still amenable to commodity hardware.[21]

In-protocol Incentives. Ethereum provides block rewards to Proof-of-Work miners similarly to Bitcoin. It also provides rewards to miners who mine blocks which do not end up on the longest chain.[22] It also

[20] `https://etherscan.io/stat/miner?range=1&blocktype=blocks` and `https://etherchain.org/miner`.
[21] `https://ethereum.org/sk/developers/docs/nodes-and-clients/#recommended-specifications`
[22] These are so-called "uncle" blocks, which include some of the blocks which Bitcoin would considered as "orphaned."

incentivizes miners by awarding them per-transaction fees. These incentives provide a rationale for new participants to join the network and contribute to decentralization.

Governance. Different research papers have analyzed the process of Ethereum improvement proposals (EIPs) and compared it to that of Bitcoin [3, 17]. The two communities are in this sense largely similar, with decentralization measures somewhat in favor of Bitcoin [3, 17].

Ethereum routinely deploys backwards incompatible updates (hard-forks). One of them was a reaction to a hacker exploit which affected several millions of ETH in June 2016, changing network rules to effectively refund the affected tokens.[23] This aspect of Ethereum governance remains controversial and has led to an alternative blockchain network (an Ethereum network fork) in which this refund did not take place.[24]

Other notable differences of Ethereum with respect to Bitcoin pertaining to the Governance aspect are the following: 1) several reputable sources (e.g., [11] and [6]) consider the inventor of Ethereum, Vitalik Buterin, to be its public face and 2) Ethereum development was funded using the proceeds of the ICO. Furthermore, the initial token distribution (owner control) of Ethereum is considerably different from that of Bitcoin, with 72 million ETH being pre-allocated in its genesis block (to crowdfunders and the development team), as we already discussed.

Impact of Proof-of-Stake on Decentralization. Proof-of-Stake and Proof-of-Work consensus protocols have fundamentally different implications on the decentralization of the network. In short, in Proof-of-Stake, "miners" do not expend electrical energy for mining but vote with their monetary power proportional to the size of their investments in the native token, i.e., ETH in this case. This implies considerably different economical dynamics compared to Proof-of-Work [7] and may outright lead to violation of Equal Opportunities and, consequently, Inclusiveness [22]. This may in turn lead to increased centralization of the network. Detailed analysis of the impact of Proof-of-Stake on decentralization seems, however, outside the scope of this report as that change has not yet occurred, and is available elsewhere [22]. In the context of this report, we evaluate the Ethereum network with its current consensus mechanism, i.e., Proof-of-Work.

4 XRP Ledger Description (Answer to Prefatory Question P2)

In this section, we describe the key technical aspects behind the XRP Ledger. In particular, we explain the concept of validation and consensus in the XRP Ledger and the concept of *Unique Node Lists* (UNL) in the XRP Ledger. We thereby answer Prefatory Question (P2), as stated in Section 1.1.

4.1 Validation, Consensus and Unique Node Lists (UNLs)

For clarity, in this section (Sec. 4.1), my personal comments and remarks are clearly marked as "(MV: ⟨text of a comment/remark⟩)." The rest of the description contained in this section is taken solely from the material which I consider endorsed by Ripple and/or its employees:

[23] See, e.g., [24], as well as `https://www.coindesk.com/understanding-dao-hack-journalists`, `https://eng.ambcrypto.com/ethereum-co-founder-vitalik-buterin-delves-into-infamous-dao-hack/`, or `https://www.gemini.com/cryptopedia/the-dao-hack-makerdao`.

[24] Ethereum Classic.

1. Brad Chase and Ethan MacBrough. "Analysis of the XRP Ledger Consensus Protocol", arXiv:1802.07242v1, 20 Feb 2018. [5].

   Chase and MacBrough are, respectively, current and former employees of Ripple.

2. Official XRP Ledger documentation, available at `https://xrpl.org/docs.html`.

3. Blockchain daemon implementing XRP Ledger in C++ (i.e., XRP Ledger, or rippled reference implementation), available at `https://github.com/ripple/rippled`, and in particular its latest release at the time of writing of this report, i.e., release 1.7.3 of 27 August 2021, as available at `https://github.com/ripple/rippled/tree/release`. We refer to this software as "rippled v1.7.3."

4. Original whitepaper by David Schwartz, Noah Youngs and Arthur Britto. "The Ripple Protocol Consensus Algorithm", available at `https://ripple.com/files/ripple_consensus_whitepaper.pdf` [18]. Since this document is marked as of "historical interest" only, this material is used only where explicitly designated and in the context which is still valid today.

4.1.1 Validators and UNLs

The XRP Ledger is a distributed blockchain system, with XRP as its native token. The XRP Ledger faces the same challenges as other digital assets in preventing double-spending and ensuring network-wide consensus [5].

XRP Ledger *nodes*, also called *rippled servers*, maintain (some amount of) a globally ordered history of *ledgers*, which in turn contain transactions. Each ledger is numbered with a *ledger index* and builds on a previous ledger whose index is one less, going all the way back to a starting point called the genesis ledger. (MV: A ledger can simply be viewed as a block. Basically, a "ledger" is to XRP Ledger what block is to Bitcoin.) Ledgers are cryptographically linked to their parent (predecessor) ledgers using a cryptographic hash function.[25] (MV: However, the number of leading zeros in a hash of a ledger is irrelevant, unlike in Bitcoin.)

XRP Ledger nodes can be configured in several modes and roles[26]. This includes the role of a *validator*, designating a rippled server which participates in the consensus protocol, called the XRP Ledger Consensus Protocol.

Each validator *Alice* in the XRP Ledger must have a *validator list*, or a *Unique Node List*, denoted by UNL_{Alice}. UNL_{Alice} represents the list of other validators *Alice* listens to as part of the XRP Ledger Consensus Protocol [5]. (MV: Messages sent to *Alice* by validators other than those in her UNL have no effect on the state of node *Alice* in the XRP Ledger Consensus Protocol and are effectively ignored by *Alice*.)

Each validator identifies itself with a unique cryptographic key pair that must be carefully managed. (MV: A validator is in fact identified by other validators by its public key part of the unique cryptographic key pair. A validator must keep the private part of its cryptographic key pair secret.)

The XRP Ledger reference implementation, rippled, provides a list of "curated default" [18] UNLs (dUNLs) to all validators (MV: containing public keys of a curated list of validators).

The only dUNL configured in rippled v1.7.3, in lines 55 and 56 of the file `https://github.com/ripple/rippled/blob/1.7.3/cfg/validators-example.txt`, is the one published at a *validator list site*

[25] See `https://xrpl.org/ledger-header.html`.
[26] See `https://xrpl.org/rippled-server-modes.html`.

located at `https://vl.ripple.com`. (MV: **This implies that the rippled software makes it such that a validator defaults to the dUNL that is controlled and published by Ripple Labs, Inc.** Other UNL publishers, including Coil, a company financially related to Ripple, are listed only as examples in the commented out section of the mentioned *validators-example.txt* configuration file, in lines 27-31. However, rippled v1.7.3 software defaults exclusively to the dUNL published by Ripple. In other words, when a new validator wishes to enter into the XRP Ledger, the rippled software it downloads defaults to installing a UNL list that was selected by Ripple.)

According to `https://github.com/ripple/rippled/blob/1.7.3/src/ripple/app/misc/ValidatorSite.h`, the software fetches the latest published recommended validator lists from the validator list site at *regular intervals*.

In addition to actually installing the default UNL list for new servers and making them periodically fetch the latest validator list, Ripple strongly recommends[27], for production servers, using the file `https://github.com/ripple/rippled/blob/1.7.3/cfg/validators-example.txt` for validator list sites (MV: i.e., the one which defaults solely to `https://vl.ripple.com`).

4.1.2 Consensus and Validation

The XRP Ledger Consensus Protocol is described as a Byzantine fault-tolerant (BFT) protocol, which "must operate in the presence of faulty or malicious participants [validators]." This can include "not responding to messages, sending incorrect messages, and even sending different messages to different parties" [5]. In general, the XRP Ledger Consensus Protocol aims to tolerate Byzantine validators, so long as they are no more than 20% of the total number of validators in any single UNL.

The goal of the XRP Ledger Consensus Protocol is to provide consensus properties across different validators. Roughly speaking, these properties are related to double-spending prevention and censorship resistance. Formally, safety properties relevant to the XRP Ledger Consensus Protocol are *Agreement* and *Linearizability* [5], which essentially mandate that correct validators fully validate transactions in the same global order (hence preventing double spending). Liveness, or *Censorship-Resistance* as stated in [5], mandates that if a correct client (i.e., user that might or might not run a validator) broadcasts a transaction to all validators, then all correct validators eventually fully validate that transaction.

The XRP Ledger Consensus Protocol starts with clients submitting proposed transactions to one or more validators in the network, who in turn broadcast the transaction to the rest of the network. The XRP Ledger Consensus Protocol consists of three primary steps [5]: *Deliberation*, *Validation* and *Preferred Branch*.[28]

In these steps, validators exchange messages with each other. As we already mentioned, in the XRP Ledger Consensus Protocol a validator takes into account only messages sent to it by validators in its UNL. If a validator is unable to receive messages from more than 80% of the validators in its UNL, the protocol eventually halts and is unable to guarantee liveness.

For two validators to agree on the same global order of transactions, their UNLs must intersect (or overlap). Chase and MacBrough provide, in Section 4 of [5], analysis of the required UNL intersection across different validators, in order to guarantee safety and liveness. The analysis in [5] shows that to ensure safety **the XRP Ledger Consensus Protocol requires the intersection between any 2 UNLs to be over**

[27] See `https://xrpl.org/run-rippled-as-a-validator.html`.
[28] These protocols steps are fairly involved and we describe them in detail in Appendix B.

60% (page 15, [5]). This is regardless of the underlying network behavior and assuming standard XRP Ledger Consensus Protocol assumptions that the potential adversary can control up to 20% of validators in the intersection of any two UNLs.

Further analysis done by Chase and MacBrough in [5], shows that, **under certain circumstances, a much higher intersection between any two UNLs is needed for the correct operation of the XRP Ledger Consensus Protocol**.

In particular, they show [5] that **if a communication network can be unreliable** (in short, network is *unreliable* if it can drop or delay messages sent between otherwise correctly functioning validators), **the XRP Ledger Consensus Protocol requires over 90% intersection between any two UNLs to provide safety** (see page 18, [5]) **and a 100% intersection across UNLs to provide liveness** (i.e., to guarantee censorship-resistance and that the network does not eventually halt) even if no validator is Byzantine (see Example 9, page 19, [5]).

We postpone the details of this argument, due to its technicalities, to Appendix B, where **we also extend the analysis of [5] to show that the XRP Ledger Consensus Protocol does not guarantee liveness even if the UNL overlap is 100%, in the case of an unreliable network with a single Byzantine validator**. The consideration of this argument is, however, optional and is not necessary for our expert opinion which is presented in the next section.

5 Expert Opinion

In this section I give my expert opinion, answering the "Questions for Expert Opinion" E1, E2 and E3, listed in Section 1.1.

5.1 Question E1: To what extent is XRP Ledger centralized or decentralized compared to Bitcoin and Ethereum?

To answer this question we first evaluate the decentralization of the XRP Ledger using the methodology of Section 3.1.

5.1.1 Evaluating Decentralization of the XRP Ledger

Resilience. The main attack vector through which a single party can violate key properties of the XRP Ledger is the following one:

If the publisher of a default UNL (dUNL) on `https://vl.ripple.com` is corrupted (Byzantine) it can serve a different UNL to different validators, without the necessary intersection among UNLs. Please refer to Section 4.1.2 for different intersection requirements which range between 60% and 100% intersection between any 2 UNLs, depending on the assumed underlying network conditions and the relevant XRP Ledger property (safety or liveness).

As a simple example, **a corrupted dUNL publisher may serve totally different UNLs (i.e., 0% intersection) to different validators, preventing the correct operation of XRP Ledger**.

For this reason, **the Nakamoto coefficient for the XRP Ledger is 1**. This implies that the XRP Ledger fails to satisfy the basic definition of a decentralized system as there is a single party which needs to

be fully trusted by all [21]. Therefore, in my opinion, the **XRP Ledger is centralized**.

In addition, even if the publisher of dUNL is correct and acts in a proper manner, as per our analysis of Appendix B, a single Byzantine member listed in the dUNL, combined with an unreliable network, can violate liveness of the XRP Ledger Consensus Protocol even when all other validators are correct and all use a dUNL with 100% overlap.

We again note that this last observation is not necessary for our opinion that the XRP Ledger is a centralized system. It simply strengthens the argument.

Inclusiveness. By allowing anyone to join the network as a validator, the XRP Ledger qualifies as a permissionless blockchain (in the sense that it allows anyone to participate).

However, the **XRP Ledger is not Inclusive** because it does not provide equal opportunities for validators to become listed in a dUNL.

Another way to look at this is that the very existence of a dUNL is a root cause of inequality in the system. If the system would not specify any dUNL, this inequality would disappear. This would however jeopardize Resilience further, as XRP Ledger safety and liveness with honest validators, critically depends on the large intersection across UNLs that validators use.

Being permissionless without satisfying Equal Opportunities does not make a system truly permissionless. The XRP Ledger is essentially an "open" system which anyone can join, but where a few participants hand-picked by Ripple have special status (which stems from their inclusion in a dUNL), and the other participants merely follow the commands of these special participants.

In-Protocol Incentives. The **XRP Ledger provides no In-Protocol Incentives** to participants, old or new.

Assuming economically rational participants, financial incentives for new participants to join the system may therefore come only externally to the system (out-of-protocol incentives), arguably through activities of entities that already have a financial interest in the system.

Business and financial relationships between Ripple and other participants that run XRP Ledger validators listed in the dUNL published by Ripple give reasonable evidence and examples of such out-of-protocol incentives.

For instance, 9 out of 41 validators in the dUNL that Ripple publishes belong to universities that are part of the University Blockchain Research Initiative (UBRI) (`https://ubri.ripple.com/`). The universities from UBRI that are on Ripple's dUNL are: IIT Bombay, Korea University, University of Nicosia, University College London, University of North Carolina, Australian National University, UC Berkeley, and University of Waterloo. Ripple has funded these universities through UBRI.

Additionally, 3 validators listed in the dUNL published by Ripple are operated by companies funded by Ripple or Ripple-affiliated entities as their main sources of funding according to Crunchbase, the leading data source for investments in the technology sector. These include Coil[29], XRPL Labs[30] and Towo labs[31], the latter two being funded by Xpring, a Ripple initiative that invests in projects related to the XRP Ledger.[32].

[29] `https://www.crunchbase.com/organization/coil-technologies/investor_financials`
[30] `https://www.crunchbase.com/organization/xrpl-labs/company_financials`
[31] `https://www.crunchbase.com/organization/towo-labs/company_financials`
[32] `https://www.crunchbase.com/organization/xpring`

In addition, one other company (Bitso) was funded by an investment round led by Ripple and had a Ripple senior executive as one of its board members.[33]

To summarize, unlike with the Bitcoin or Ethereum blockchains, which offer rewards in the form of digital tokens to those that engage in the blockchain validation process, the XRP Ledger provides no such incentives or rewards, which means that validators do not come organically to the XRP Ledger.

Governance. According to statistics available at `https://github.com/ripple/rippled/graphs/contributors`, the overwhelming majority of code commits and lines of code comes from the developers who are or have been affiliated with or funded by Ripple Labs, Inc. or predecessor companies.

XRP Ledger has a public face in Ripple Labs, Inc.

Regarding owner control (of initial tokens), the information is not available from the genesis ledger of the XRP Ledger as due to a bug ("mishap in the XRP Ledger history"[34]), ledgers 1 through 32569 were lost. According to the information about XRP Sales available at `https://xrpl.org/xrp.html`, "The XRP Ledger was built over 2011 – early 2012 by Jed McCaleb, Arthur Britto and David Schwartz. In September 2012, Jed and Arthur, along with Chris Larsen, formed Ripple (the company, called OpenCoin Inc. at the time) and decided to gift 80 billion XRP to Ripple in exchange for Ripple developing on the XRP Ledger." The maximum supply of XRP is 100 billion. The rest of 20 billion early XRP were, according to multiple public sources,[35] distributed among founders.

Therefore, we can conclude that 100% of the initial/total supply was under *owner control*, comprising Ripple Labs (i.e., its predecessor companies) and its founders. This clearly goes against decentralization, particularly when combined with absence of In-Protocol Incentives, as it limits the economic rationale for new participants to organically join the system.

5.1.2 Answer to Question E1: Comparison to Bitcoin and Ethereum

The XRP Ledger is centralized compared to Bitcoin and even Ethereum. Even if we evaluate the XRP Ledger outside the context of Bitcoin and Ethereum, it cannot be deemed decentralized and hence is centralized.

In short, unlike Bitcoin and Ethereum, the XRP Ledger is centralized as it takes corrupting only a single party to be able to compromise key properties of the system. Also, when considering the other decentralization aspects analyzed, the XRP Ledger evaluates worse and is more centralized than Bitcoin and Ethereum.

The summary of key decentralization aspects according to our analysis from Section 3.2.3 (Bitcoin), Section 3.3.1 (Ethereum) and Section 5.1.1 (XRP Ledger) is shown below, repeating for convenience Table 1 from Section 2.

[33] See `https://livenet.xrpl.org/validators/nHBidG3pZK11zQD6kpNDoAhDxH6WLGui6ZxSbUx7LSqLHsgzMPec` and `https://ripple.com/insights/our-investment-in-bitso/`.

[34] See https://xrpl.org/intro-to-consensus.html.

[35] See, for example, `https://blog.bitmex.com/the-ripple-story/`.

Decentralization aspect	**Ideal Decentralized System**	**Bitcoin Blockchain**	**Ethereum Blockchain (with Proof-of-Work)**	**XRP Ledger**
Nakamoto coefficient (Resilience)	always greater than 1, the higher the better	≥ 4	≥ 3	1
Inclusiveness	yes	yes	yes	no
In-Protocol Incentives	yes	yes	yes	no
Governance (public face)	no	no	yes	yes
Governance (tokens allocated at genesis)	0, the lower the better	0%	61.5% (about 10% owner controlled) of today's supply	100% (all owner controlled)

Table 1: Comparison of the XRP Ledger to the Bitcoin and Ethereum blockchains for key aspects of decentralization defined in the decentralization evaluation methodology of Section 3.1.

5.2 Question E2: To what extent have Ripple's efforts been needed to support the proper functioning of the XRP Ledger?

Ripple's effort needed *today* to support the proper functioning of the XRP Ledger, based on the current rippled software, includes:

1. Publishing a dUNL at `https://vl.ripple.com`. This includes maintaining security and ownership of ripple.com domain so an adversary cannot control a dUNL.

   This also includes making efforts to carefully change the published dUNL, even in the absence of actions of a malicious adversary. In a known incident that occurred in November 2018, which was also the topic of the May 26, 2021 deposition of David Schwartz in front of this court (pages 222-226 and Exhibit 44 therein), the XRP Ledger was stalled from making forward progress when one UNL expired and a new one was published.

   As indicated by an xrpchat online forum post which appeared later, in October 2020, from a user who appears to be Ripple's employee Nik Bougalis[36], following this November 2018 incident he *"personally restarted several validators,"* and *"the team at Ripple invested a significant amount of time troubleshooting the issue and proposed several improvements,"* illustrating the amount of human and in particular Ripple employees' effort needed to rectify the network halt in a case where changes in the published dUNL are not handled well.

2. Because of possible attacks on the network, that could result in safety or liveness violations, including the attack we describe in Appendix B, so long as it publishes a dUNL, Ripple needs to continue to curate and attest validators that it includes in a dUNL.

3. As of October 4, 2021, Ripple appears to directly control 6 out of 41 validators in the published dUNL. Due to possible Byzantine attacks, including the one we describe in Appendix B, Ripple needs to maintain security over these validators and ensure they behave honestly.

[36] See `https://www.xrpchat.com/topic/28872-the-network-is-down/?do=findComment&comment=850670`.

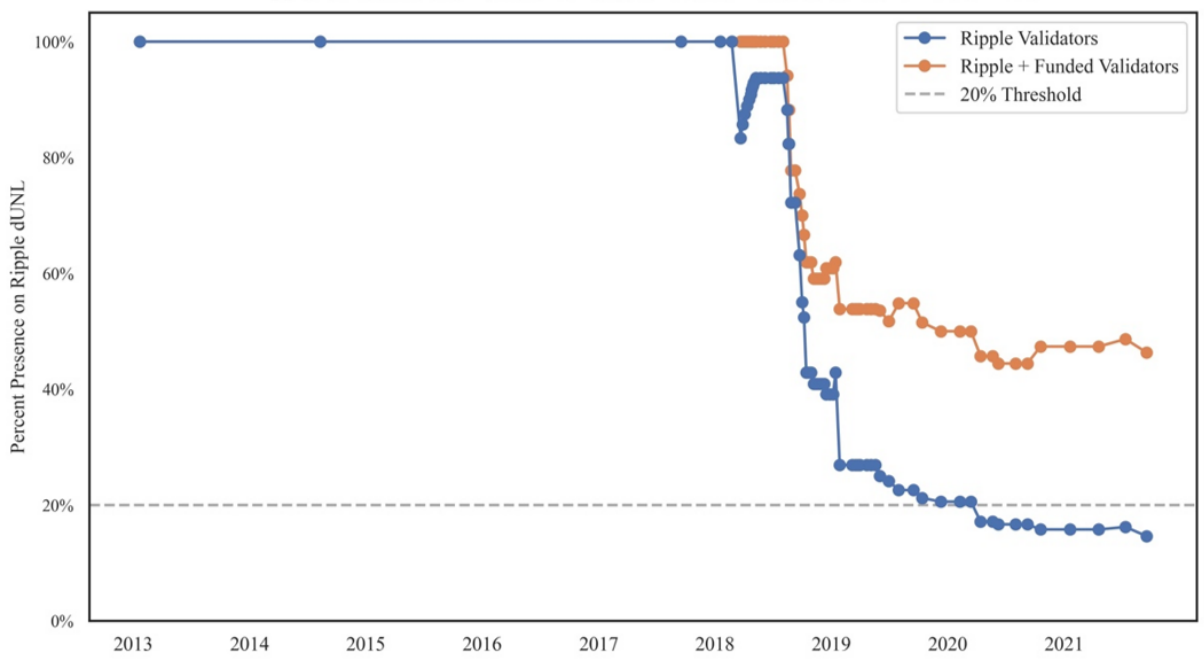


Figure 1: Ripple validators and validators operated by entities funded by Ripple, given as a fraction of the dUNL membership over time.

With modifications of software, points 1 and 2 above can, in principle, be done by an entity different from Ripple. Nevertheless, the XRP Ledger would still be centralized as this entity would still need to be fully trusted in the sense of the arguments pointed out in items 1 and 2.

In relation to point 3 above, it is worth noting that Ripple used to control a larger fraction of validators listed in the dUNL it publishes compared to the fraction it controls today. This fraction was even 100% for over half of the XRP Ledger history.

Figure 1 gives the change in time of the fraction of validators in the Ripple's dUNL belonging to Ripple as well as that of the fraction of validators belonging to Ripple or entities funded by Ripple.[37] These entities and their relation to Ripple are discussed in more detail in the next section, Section 5.3.

5.3 Question E3: What risks to the XRP Ledger would or might materialize if Ripple "walked away" or "disappeared"?

Like the previous question, we will answer this question assuming no software changes (i.e., assuming rippled v1.7.3). In short, if Ripple would disappear, serious risks related to the correct operation of the XRP Ledger network may arise.

We consider two cases: A) Ripple disappears and the network is still able to agree on the contents of the

[37] The main source for the data depicted in Figure 1 is obtained from `https://github.com/ripple/vl`, which contains validator public keys of every historical dUNL and the current dUNL. Validator ownership is classified using their respective domains found on `https://livenet.xrpl.org/validators/{publickeyofvalidator}`. Domains ownership was confirmed using the validator registry `https://xrpcharts.ripple.com/#/validators` and through `https://xrpscan.com/{public_key}`, or Google search of the public keys.

dUNL as currently published on `https://vl.ripple.com`, and B) Ripple disappears and leaves the network without a common UNL — that is, UNLs used by validators in the network change over time.

Consider the first case, case A:

- In the case where more than 20% of validators in the dUNL disappear, the network would not be operational. The current dUNL (as of October 4, 2021) contains 41 validators (data obtained from `https://xrpcharts.ripple.com/#/validators`).

  Hence, the network would cease to be operational if nine validators disappeared. Six validators are controlled by Ripple, i.e., they are shown to be resolving at a Ripple domain `validator.ripple.com`. In addition, many validators belong to entities which are funded by or have business relationships with Ripple, as we discussed in Section 5.1.1 (in the part regarding incentives).

  For instance, 9 out of 41 validators belong to universities part of the University Blockchain Research Initiative (`https://ubri.ripple.com/`). Ripple has funded these universities. If Ripple disappears, there is a risk that universities might cease to operate validators in absence of further funding. Three of such validators disappearing, in addition to Ripple's six, are sufficient for the network under the current dUNL to cease to be operational.

  Similar arguments can be made about the validators run by entities other than universities which have received significant funding from Ripple.

  For completeness, the list of validators controlled by Ripple and entities funded by Ripple, as well as the list of all 41 validators contained in the current dUNL are given in Appendix A.

- In addition, there is a separate risk that a validator in the common dUNL becomes compromised and Byzantine, enabling it to mount attacks against the network, such as the attack on liveness described in Appendix B.

  If Ripple is not there to evict such a validator from the dUNL, validators need to come up with different UNLs. This essentially reduces to the case B we consider next.

Consider now the second case, case B. In absence of the common UNL, network validators need to choose UNLs either by themselves, or based on some out-of-band communication with other validators.

If they choose UNLs themselves, they risk not getting a sufficient intersection among UNLs, jeopardizing the core properties of the XRP Ledger, safety and liveness. There is a high risk of state and ledger history forks in such a situation.

If they rely on out-of-band communication (i.e., outside the rippled software) with other validators and possibly entities external to the XRP Ledger to agree on a UNL, this could be done using software other than the XRP Ledger, or using human effort and communication. Using software other than XRP Ledger would basically imply another consensus (agreement) protocol, and could be viewed then as a change in XRP Ledger (rippled) software. The other option would be using human effort and communication to ensure agreement on sufficient intersection among UNLs (e.g., by relying on communication among human operators of individual validators). This defeats the very purpose for the existence of a software system that aims to implement distributed consensus.

6 Conclusions

In the context of the prefatory questions, I have been asked to explain the operation of consensus and validation in blockchain systems and, in particular, on the XRP Ledger. I have explained the concept of Proof-of-Work based consensus, used in Bitcoin, which is not based on validator identities, but rather relies on provable expenditure of a real-world resource (energy), and how it leads to a decentralized system.

In contrast, the consensus used in the XRP Ledger is based on a very different approach which puts validator identities at the core of the system.

In the case of the XRP Ledger this approach is technically executed in a manner contrary to decentralization principles, with a central authority controlled by Ripple given a task of publishing what can be seen as a special list of privileged validators.

With this in mind, it is easy to see that the answer to the expert opinion I was asked to provide—whether the XRP Ledger is a decentralized or centralized system—is that the XRP Ledger does not satisfy a basic definition of a decentralized system. To be decentralized, participants need not trust any single party. For the XRP Ledger, participants need to trust at least one other party, which is currently Ripple as the publisher of the dUNL to which the XRP Ledger software defaults.

To evaluate XRP Ledger characteristics related to decentralization in more depth, and to answer expert questions I have been asked to opine on, I surveyed scientific literature. The scientific treatment of the notion of decentralization has advanced in recent years to give a precise minimal definition of a decentralized system, as well as a more refined, general taxonomy of decentralized systems.

Summarizing this literature, I identified four decentralization aspects (Resilience, Inclusiveness, In-Protocol Incentives, and Governance) as, in my opinion, the most relevant ones. I based the methodology for evaluating the decentralization of distributed systems around those aspects, and I have evaluated Bitcoin, Ethereum and XRP Ledger through their lens.

XRP Ledger scores poorly in these aspects compared to Bitcoin and to Ethereum, which itself evaluates as more centralized than Bitcoin. The Resilience of the XRP Ledger is poor as it requires trusting a single party. It further is not Inclusive, as it makes distinctions among participants and does not provide them with equal opportunities. It has no In-Protocol Incentives, leaving the incentivization of new participants towards increasing the system size in the hands of entities that already have financial interest in the system, such as Ripple Labs Inc. Finally, its Governance related measures are poor.

In answering further questions for my expert opinion, I have identified the efforts required by Ripple towards the proper functioning of the XRP Ledger, as well as identified the risks that may arise in the case of Ripple's hypothetical disappearance. In short, in this case, serious risks related to the correct operation of the XRP Ledger network may arise.

The opinions expressed in this report are based on my review and analysis of the documents that I have reviewed. I reserve the right to supplement my report and analysis based on any new evidence brought to my attention.

References

[1] B. Alpern and F. B. Schneider. Recognizing safety and liveness. *Distributed Comput.*, 2(3):117–126, 1987.

[2] [redacted]

[3] S. Azouvi, M. Maller, and S. Meiklejohn. Egalitarian society or benevolent dictatorship: The state of cryptocurrency governance. In A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore, and M. Sala, editors, *Financial Cryptography and Data Security - FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers*, volume 10958 of *Lecture Notes in Computer Science*, pages 127–143. Springer, 2018.

[4] V. Buterin. [ANN] Ethereum: Welcome to the beginning. `https://bitcointalk.org/index.php?topic=428589.0`, 2014.

[5] B. Chase and E. MacBrough. Analysis of the XRP ledger consensus protocol. *CoRR*, abs/1802.07242, 2018.

[6] Encyclopaedia Britannica. 20 under 40: Young shapers of the future (business and entrepreneurship). `https://www.britannica.com/list/20-under-40-shapers-of-the-future-in-business-and-entrepreneurship`, 2021.

[7] G. C. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, and G. Wang. Compounding of wealth in proof-of-stake cryptocurrencies. In I. Goldberg and T. Moore, editors, *Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers*, volume 11598 of *Lecture Notes in Computer Science*, pages 42–61. Springer, 2019.

[8] P. D. Filippi and B. Loveluck. The invisible politics of bitcoin: Governance crisis of a decentralized infrastructure. *Internet Policy Review*, 5(4), 2016.

[9] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. G. Sirer. Decentralization in bitcoin and ethereum networks. In S. Meiklejohn and K. Sako, editors, *Financial Cryptography and Data Security - 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26 - March 2, 2018, Revised Selected Papers*, volume 10957 of *Lecture Notes in Computer Science*, pages 439–457. Springer, 2018.

[10] D. Karakostas, A. Kiayias, C. Nasikas, and D. Zidros. Cryptocurrency egalitarianism:a quantitative approach. In *International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019)*, 2019.

[11] A. J. Kolber. Not-so-smart blockchain contracts and artificial responsibility. *Stanford Technology Law Review*, 198, 2018.

[12] L. Lamport. Proving the correctness of multiprocess programs. *IEEE Trans. Software Eng.*, 3(2):125–143, 1977.

[13] L. Lamport, R. E. Shostak, and M. C. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, 1982.

[14] C. E. Leiserson, N. C. Thompson, J. S. Emer, B. C. Kuszmaul, B. W. Lampson, D. Sanchez, and T. B. Schardl. There’s plenty of room at the top: What will drive computer performance after moore’s law? *Science*, 368(6495):eaam9744, 2020.

[15] A. Miller. *Permissioned and Permissionless Blockchains*, pages 193–204. 2019.

[16] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`, 2008.

[17] A. R. Sai, J. Buckley, B. Fitzgerald, and A. LeGear. Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing and Management*, 58(4), July 2021.

[18] D. Schwartz, N. Youngs, and A. Britto. The ripple protocol consensus algorithm. `https://ripple.com/files/ripple_consensus_whitepaper.pdf`.

[19] B. Srinivasan. Quantifying decentralization. Blockstack Summit 2017, `https://www.youtube.com/watch?v=4UXT5YVJwB4`, 2017.

[20] A. S. Tanenbaum and M. van Steen. *Distributed systems - principles and paradigms, 2nd Edition.* Pearson Education, 2007.

[21] C. Troncoso, M. Isaakidis, G. Danezis, and H. Halpin. Systematizing decentralization and privacy: Lessons from 15 years of research and deployments. *Proc. Priv. Enhancing Technol.*, 2017(4):404–426, 2017.

[22] [redacted]

[23] Q. Lin, C. Li, X. Zhao, and X. Chen. Measuring decentralization in bitcoin and ethereum using multiple metrics and granularities. In *2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW)*, pages 80–87, 2021.

[24] C. L. Reyes, N. G. Packin, and B. Edwards. Distributed governance. *William & Mary Law Review Online*, 59(1). `https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1003&context=wmlronline`.

[25] I. Amores-Sesar, C. Cachin, and J. Micic. Security analysis of ripple consensus. In Q. Bramas, R. Oshman, and P. Romano, editors, *24th International Conference on Principles of Distributed Systems, OPODIS 2020, December 14-16, 2020, Strasbourg, France (Virtual Conference)*, volume 184 of *LIPIcs*, pages 10:1–10:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

A Lists and Statistics of Validators Included in the dUNL published by Ripple, as of July 16, 2021

In this Appendix, we give lists and statistics related to validators included in the dUNL published by Ripple at `https://vl.ripple.com` (referred to as Ripple's dUNL), as of July 16, 2021 update.

Figure 2 gives the list of 19 validators belonging to entities funded by Ripple, whereas Figure 3 gives the list of all 41 validators.

Table: Validators Belonging to Entities Funded by Ripple

Entity	Domain	Connection to Ripple
Ripple	validator.ripple.com	Validator belongs to Ripple
Ripple	validator.ripple.com	
Ripple	validator.ripple.com	
Ripple	validator.ripple.com	
Ripple	validator.ripple.com	
Ripple	validator.ripple.com	
Australian National University	xrp-col.anu.edu.au	Received funding through Ripple's University Blockchain Research Initiative[1]
IIT Bombay	isrdc.in	
Korea University	blockchain.korea.ac.kr	
UC Berkeley	shadow.haas.berkeley.edu	
University College London	students.cs.ucl.ac.uk	
University of Kansas	ripple.ittc.ku.edu	
University of Nicosia	xrp.unic.ac.cy	
University of North Carolina	ripple.kenan-flagler.unc.edu	
University of Waterloo	ripplevalidator.uwaterloo.ca	
Bitso	bitso.com	Ripple led an investment round and has a Senior Executive on Bitso's Board[2]
Coil	coil.com	Ripple (via Xpring) provided initial funding of 1 billion XRP ($265 million)[3]
Towo Labs	towolabs.com	Ripple (via Xpring) is lead investor[4]
XRPL Labs	validator.xrpl-labs.com	Ripple (via Xpring) is listed as sole investor[5]

[1] https://ubri.ripple.com/
[2] https://ripple.com/insights/our-investment-in-bitso/
[3] See https://www.crunchbase.com/organization/coil-technologies/investor_financials and https://cointelegraph.com/news/ripples-xpring-gives-265-mil-in-xrp-to-content-platform-coil
[4] See https://ripple.com/insights/investing-in-towo-labs/ and https://www.crunchbase.com/organization/towo-labs/company_financials
[5] See https://ripple.com/insights/doubling-down-on-xrpl-labs/ and https://www.crunchbase.com/organization/xrpl-labs/company_financials

Figure 2: The list of 19 validators listed in the Ripple's dUNL, belonging to Ripple or entities funded by Ripple.

Table: List of 41 Validators as of July 16, 2021 dUNL Update

Entity	Domain	Public Key
Alloy Networks	alloy.ee	[redacted]
AT TOKYO	www.attokyo.com	
Australian National Univ.	xrp-col.anu.edu.au	
Bahnhof	www.bahnhof.se	
Bithomp	bithomp.com	
Bitrue	www.bitrue.com	
Bitso	bitso.com	
Blockdaemon	arrington-xrp-capital.blockdaemon.com	
Cabbit Technology	cabbit.tech	
Eminence	verum.eminence.im	
Coil	coil.com	
Coinfield	xrp.coinfield.com	
Data443	data443.com	
Individual	digifin.uk	
Flagship Solutions Group	flagshipsolutionsgroup.com	
FTSO.eu	xrpvalidator.ftso.eu	
Gatehub	validator.gatehub.net	
IIT Bombay	isrdc.in	
Individual	jon-nilsen.no	
Kompany	brex.io	
Korea University	blockchain.korea.ac.kr	
NTT Data	ripple.ntt.com	
Peer Island	peerisland.com	
Ripple	validator.ripple.com	
Ripple	validator.ripple.com	
Ripple	validator.ripple.com	
Ripple	validator.ripple.com	
Ripple	validator.ripple.com	
Ripple	validator.ripple.com	
rippleitin	rippleitin.nz	
Telindus	ripple.telinduscloud.lu	
Towo Labs	towolabs.com	
UC Berkeley	shadow.haas.berkeley.edu	
University College London	students.cs.ucl.ac.uk	
University of Kansas	ripple.ittc.ku.edu	
University of Nicosia	xrp.unic.ac.cy	
University of North Carol.	ripple.kenan-flagler.unc.edu	
University of Waterloo	ripplevalidator.uwaterloo.ca	
Worldlink	validator1.worldlink-us.com	
XRP Scan	aloha.xrpscan.com	
XRPL Labs	validator.xrpl-labs.com	

Figure 3: The list of all 41 validators in the Ripple's dUNL.

B Details of the XRP Ledger Consensus Protocol, Including Vulnerability to Single Byzantine Validator with Completely (100%) Overlapping UNLs

In the rest of this appendix, we use the following definitions.

- A validator is called *correct*, if it operates without outages and follows the unmodified XRP Ledger Consensus Protocol protocol.
- A validator is called *Byzantine*, if its local copy of the XRP Ledger Consensus Protocol protocol is modified such that the validator deviates from the XRP Ledger Consensus Protocol protocol.
- The network is called *unreliable*, if it can drop or delay messages exchanged among correct validators.
- UNLs are said to *overlap completely*, or have *100% overlap*, if all UNLs of all correct validators are identical.

In the following, we provide details and in-depth analysis of the XRP Ledger Consensus Protocol. In particular, we:

1. Give the details behind XRP Ledger Consensus Protocol necessary for the in-depth analysis (Section B.1).
2. Summarize the analysis of liveness done by Chase and MacBrough in [5] (Section B.2).
3. Present our analysis, which shows that XRP Ledger Consensus Protocol fails to guarantee liveness, even with 100% overlap across all UNLs, if one validator in the said UNL can be Byzantine and if the network is unreliable (Section B.3).

B.1 Details of the XRP Ledger Consensus Protocol

The XRP Ledger Consensus Protocol consists of 3 main steps: *Deliberation*, *Validation* and *Preferred Branch* [5].

1. **Deliberation.** In this step, a validator *Alice iteratively* proposes a transaction set to include in the current ledger (i.e., block of transactions), based on transaction proposals received from other nodes in her UNL.

   When "enough" validators in validator's UNL propose the same transaction set, a validator generates the next ledger L, applies L to the current state, issues a *validation message* for L, exits deliberation, and proceeds to the Validation step.

   The notion of "enough" validators here depends on a particular subphase of the deliberation step and can be 50%, 65%, 70% or 95% of validators [5].

   The exact percentages mentioned above are to a large extent irrelevant as the correct execution of the protocol does not depend on the outcome of the deliberation step. Namely, as stated in the paper by Chase and MacBrough [5] on page 16: *"...deliberation can terminate with an arbitrary result.*

In practice, this may require a significantly degraded network, but is nonetheless a real risk. From a theoretical perspective, deliberation is therefore completely irrelevant; it is purely an optimization . . . and it could be removed without fundamentally changing the protocol."

For illustration, Example 5 of [5] shows an example scenario where UNLs overlap completely (i.e., at 100%) and all validators are correct.In that example, due to an unreliable network, one group of validators can exit deliberation by validating ledger L and the other group of validators ledger L' different from L, at the same ledger index. We refer to this scenario, to which we will come back later, as *Network Split in Deliberation*.

In conclusion, under an unreliable network, at the end of the deliberation step, correct validators may well end up validating different ledgers and, in particular, end up in Network Split in Deliberation.

2. **Validation.** In this step a validator simply listens for validation messages coming from other validators from its local UNL. If a correct validator sees a *quorum* of validation messages for a ledger L, then it *fully validates* L.

   A quorum in XRP Ledger Consensus Protocol is defined as at least 80% of the nodes in a validator's UNL.[38]

   Once this happens, that ledger L and its ancestors are deemed fully validated and its state is authoritative and irrevocable.

3. **Preferred Branch.** In times of unreliable network or Byzantine failures of validators, it may happen that some correct validators fail to receive a quorum of validation messages for any individual ledger to fully validate.

   In short, a correct validator may see validation messages for two or more *conflicting ledgers*, which lie on different branches in the block history. In the case of conflicting ledgers, *Preferred Branch* is the step of the XRP Ledger Consensus Protocol which determines which of the ledgers and the corresponding branch of ledgers, the correct validator should switch to and consideras the "right" one.

   The details of the Preferred Branch are a fairly involved part of the XRP Ledger Consensus Protocol—we omit the details for the sake of clarity. What is important for the rest of this report is that a validator cannot switch the preferred branch from the one on which ledger L is, if that validator gets more than 50% of validations messages from the nodes in its UNL for some *descendant* of L [5].

   Here, a descendant of ledger L is recursively defined as: 1) either ledger L itself, or 2) another ledger which has L or some of L's descendants as a parent.

B.2 Liveness Analysis by Chase and MacBrough [5]

The analysis in Example 9 of [5], further shows that the XRP Ledger Consensus Protocol, under an unreliable network which causes Network Split in Deliberation, **fails to guarantee liveness (Censorship-Resistance) even with no Byzantine validators, unless the overlap of UNLs is 100%**.

Example 9 of [5] is illustrated below, in Figure 4, which is taken directly from [5].

This example considers:

[38] See `https://github.com/ripple/rippled/blob/release/src/ripple/consensus/ConsensusParms.h`, lines 73-74, in addition to [5].

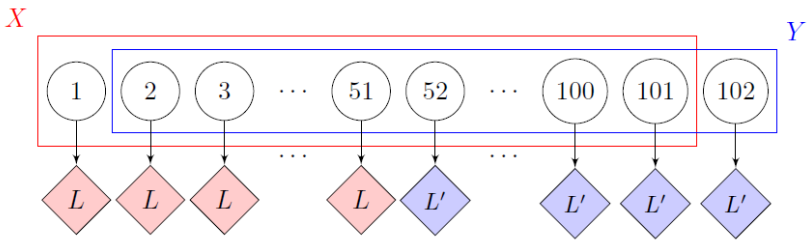


Figure 6: Example of stuck network with 99% UNL overlap and no Byzantine faults.

Example 9.

Consider a network of 102 peers drawin in figure 6. There are two UNLs, the red $X = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{101}\}$ and blue $Y = \{\mathcal{P}_2, \mathcal{P}_3, \ldots, \mathcal{P}_{102}\}$. Peers $1 - 51$ use X and peers $52 - 102$ use Y. There are two ledgers, L and L'. The nodes listening to X all validate a descendant of L, while the nodes listening to Y all validate a descendant of L'. Since $51 > 0.5|X|$ nodes in X validate a descendant of L. Thus according to the preferred branch protocol all, the nodes listening to X cannot switch branch to L'. Similarly, since $51 > 0.5|Y|$ nodes in Y all validate a descendant of L, the nodes listening to Y cannot switch branch to L'. The network cannot ever rejoin without manual intervention.

Figure 4: Example 9 and Figure 6 from [5].

1. 102 validators experiencing Network Split in Deliberation;
2. Validators 1...51 use UNL X and send validation for descendant of ledger L;
3. Validators 51...102 use UNL Y and send validation for descendant of ledger L';
4. UNL X contains validators 1...101, in total 101 validators;
5. UNL Y contains validators 2...102, in total 101 validators;
6. No validator gets a quorum of validations for the same ledger (80% of 101) and no validator fully validates any ledger;
7. The Preferred Branch step is meant to help with this situation, by allowing validators to "switch branch."
8. Nodes 1...51 (which use UNL X), cannot "switch branch" to L' as they get more than 50% of validations (51 out of 101) for a descendant of L;
9. Nodes 52...102 (which use UNL Y), cannot "switch branch" to L as they get more than 50% of validations (51 out of 101) for a descendant of L';
10. "The network cannot ever join without manual intervention" [5], i.e., it halts.

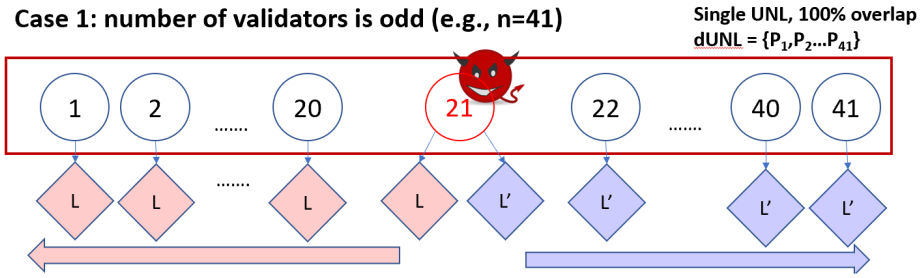


Figure 5: Attack by a single Byzantine validator with 100% UNL overlap.

B.3 Liveness Violation with 100% UNL Overlap and Single Byzantine Validator

Beyond their Example 9 illustrated in the previous section, Chase and MacBrough further argue (Theorem 11, [5]) that XRP Ledger Consensus Protocol guarantees liveness in case UNL overlap is 100%.

This is incorrect, as their analysis assumes "Byzantine accountability", i.e., limitations in potential misbehavior of Byzantine nodes which disallows a simple and standard attack by Byzantine validators in which Byzantine validators provide different information to different correct validators.

Refuting this claim of Chase and MacBrouh, we show that the XRP Ledger Consensus Protocol fails to guarantee liveness, even with 100% overlap across all UNLs, if one validator in the common UNL can be Byzantine (malicious) and if the network is unreliable.[39]

Consider the following example, which resembles Example 9 of [5] we depicted in Appendix B.2.

In this example there is a single UNL (100% overlap), and one Byzantine validator. The example uses 41 validators, as this is currently the actual number of validators in the dUNL in the XRP Ledger network, since July 16, 2021. The example is illustrated in Figure 5, only slightly modifies the Example 9 of [5] and goes as follows:

1. 41 validators experiencing Network Split in Deliberation;
2. Validators $1 \ldots 20$ send validation for descendant of ledger L;
3. Validators $22 \ldots 41$ send validation for descendant of ledger L';
4. Validator 21 is Byzantine, it sends validation for descendant of L to validators $1 \ldots 20$ and validation for descendant of L' to validators $22 \ldots 41$.
5. There is a single UNL, dUNL, containing all 41 validators.
6. No validator gets a quorum of validations for the same ledger (80% of 41) and no validator fully validates any ledger;
7. The Preferred Branch step is meant to help with this situation, by allowing validators to "switch branch."

[39] Our argument is similar to, but in its essence different from, the one presented by Amores-Sesar et al. [25] to which a short rebuttal was written by Ripple's employee Ethan Macbrough, as seen in the Twitter thread at `https://twitter.com/cczurich/status/1334153938241720322` and replies therein.

8. Nodes 1...20 cannot "switch branch" to L' as they get more than 50% of validations (21 out of 41) for descendant of L;

9. Nodes 22...41 cannot "switch branch" to L as they get more than 50% of validations (21 out of 41) for descendant of L';

10. "The network cannot ever join without manual intervention", i.e., it halts.

Exhibit 35

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, **Plaintiff,** **- against -** **RIPPLE LABS, INC., BRADLEY GARLINGHOUSE, and CHRISTIAN A. LARSEN,** **Defendants.**	**20 Civ. 10832 (AT)** **ECF Case**

EXPERT REBUTTAL REPORT OF KRISTINA SHAMPANIER, PH.D.

November 12, 2021

TABLE OF CONTENTS

I. QUALIFICATIONS

1. I am a Senior Vice President at Compass Lexecon, an economic consulting firm. I received a Ph.D. in Business and Management Science (with specialization in Marketing) from the MIT Sloan School of Management in 2007. Prior to that, I received a Master's degree in Mathematics from Moscow State University in 2001 and a Master's degree in Economics from the New Economic School (Moscow) in 2002, both cum laude. While at MIT, I conducted research on judgment, decision making, and consumer behavior.

2. At MIT, and subsequently in litigation consulting settings, I designed, conducted, and analyzed numerous laboratory, online, and field experiments and other "primary data" studies, including in survey format. I have extensive experience in survey development and administration, and analysis of data on consumer behavior in academic, consulting, and litigation settings. I have also taught outside audiences on survey design and published in academic journals and practitioner publications.

3. I have been retained as an expert witness in various matters, including matters relating to trademark infringement, false advertising, employment, and healthcare. In each of these matters, I was retained to design and field a survey, experiment, or another "primary data" study, or to evaluate such studies conducted by others.

4. My Curriculum Vitae is attached as Appendix A to this report, and includes all publications I have authored in the last ten years.

5. Appendix B lists the materials I have considered in forming my opinions. I reserve the right to update my opinions if additional information becomes available.

6. Compass Lexecon is compensated for my work on this matter at the rate of $975 per hour. I receive compensation from Compass Lexecon based on my billing and billings of staff

who have assisted me. Neither Compass Lexecon's compensation nor my compensation depends upon the outcome of this case.

II. ASSIGNMENT

7. I was retained by Kellogg, Hansen, Todd, Figel & Frederick PLLC on behalf of Ripple Labs Inc. ("Ripple") to evaluate the Expert Report of [redacted] ("[redacted] Report") in this matter.[1]

8. I reserve the right to revise my opinions if new information becomes available.

III. SUMMARY OF OPINIONS

9. Mr. [redacted] "analysis" suffers from the following fatal flaws:

   a. Mr. [redacted] provides no scientific basis for his causal conclusions regarding the effect of "Ripple's statements, actions, and product offerings" on the "perspective of a reasonable purchaser of XRP." Mr. [redacted] does not conduct an experiment, the gold standard for a causal conclusion. Neither does he conduct any other quantitative empirical analysis, such as a survey or analysis of data accumulated in the regular course of business, or qualitative empirical analysis such as focus groups. At best, his analysis can be viewed as a highly unreliable survey of a single respondent – himself.

   b. Mr. [redacted] does not evaluate whether and to what degree XRP purchasers were exposed to Ripple's statements that he "review[s] and analy[zes]." A proper analysis of the impact of such statements on potential purchasers would include such an evaluation.

[1] Expert Report of [redacted] October 4, 2021, *U.S. Securities and Exchange Commission v. Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larson*, United States District Court, Southern District of New York.

c. Mr. [redacted] "analysis" does not allow him to separate the supposed impact of Ripple's conduct on the purchaser's "perspective" from other potential influences, such as preexisting beliefs or general principles of economics.

d. Mr. [redacted] does not explain how he selected Ripple's statements that he "review[s] and analy[zes]."

e. Mr. [redacted] does not offer any market segmentation or similar analysis that would allow him to establish that the different types of XRP purchasers he describes (investment-oriented and cross-border-transfer-oriented) actually exist, or that they are the only types of XRP purchasers that exist.

f. Mr. [redacted] does not appear to possess the qualifications or experience needed to address certain aspects of the "perspective of a reasonable purchaser" or the effect of Ripple's "statements, actions, and product offerings" on those aspects of the purchaser's perspective, such as purchasers' perceptions of Ripple's at-issue statements.

IV. BACKGROUND

10. According to the operative complaint in this matter, Ripple (f/k/a Open Coin, Inc.) "is a Delaware corporation founded in September 2012, with its principal place of business in San Francisco, California, and an office in Manhattan."[2] Ripple characterizes itself as "a San Francisco-based, privately-held payments technology company that uses blockchain innovation (including XRP) to allow money to be sent around the world instantly, reliably, and more

[2] First Amended Complaint, *Securities and Exchange Commission v. Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larsen*, 20 Civ. 10832 (AT), ECF Case, United States District Court, Southern District of New York, February 18, 2021 ("Complaint"), ¶16.

cheaply than traditional avenues of money transmission."[3] The Securities and Exchange Commission ("SEC") alleges that Ripple has sold or distributed significant quantities of XRP, the digital asset at issue in this case.[4]

11. The SEC claims that XRP is an "investment contract" and thus a security.[5] According to the SEC, "[i]nvestment contracts are instruments through which a person invests money in a common enterprise and reasonably expects profits or returns derived from the entrepreneurial or managerial efforts of others."[6] The SEC claims that those "who purchased XRP . . . invested into a common enterprise with other XRP purchasers, as well as with Ripple," that the "common interest" was "in XRP's price increasing," and that Ripple "led investors to reasonably expect that they could reap a profit from their investment into XRP, derived from Ripple's and its agents' efforts into their common enterprise."[7] According to the SEC, XRP has "[n]o significant [n]on-[i]nvestment [u]se."[8] In particular, the SEC does not believe that XRP's use in cross-border payments, such as via Ripple's On-Demand Liquidity ("ODL") product, is a "use" of XRP.[9]

12. The SEC claims that Ripple sold XRP without filing a security registration statement, and therefore "never provided investors with the material information that every year hundreds of

[3] Answer of Defendant Ripple Labs, Inc. to Plaintiff's First Amended Complaint, *Securities and Exchange Commission v. Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larsen*, 20-cv-10832 (AT), United States District Court, Southern District of New York, March 4, 2021 ("Ripple's Answer"), ¶6, footnotes omitted.

[4] Complaint, ¶1; Ripple's Answer, ¶¶1, 7. According to the SEC, "[f]rom at least 2013 through the present," Ripple "sold over 14.6 billion units" of XRP. Complaint, ¶1.

[5] Complaint, ¶3.

[6] Complaint, ¶31.

[7] Complaint, ¶¶290, 302, 315.

[8] Complaint, Section V.

[9] Complaint, ¶131, Section V.A.

other issuers include in such statements."[10] Thus, according to the SEC, Ripple engaged in an "illegal securities offering from 2013 to the present."[11]

13. Ripple's position is that XRP is not a security and that it "performs a number of functions that are distinct from the functions of 'securities' as the law has understood that term for decades"; for example, "XRP functions as a medium of exchange — a virtual currency used today in international and domestic transactions — moving value between jurisdictions and facilitating transactions."[12] Among other things, Ripple contends that "holders of XRP cannot objectively rely on Ripple's efforts" because "Ripple has no explicit or implicit obligation to any counterparty to expend efforts on their behalf," "never explicitly or implicitly promised profits to any XRP holder," and in any event is not in control of the XRP Ledger.[13]

V. SUMMARY OF THE [redacted] REPORT

14. Mr. [redacted] was retained by the SEC "to independently analyze and render opinions on the perspective of a reasonable purchaser of XRP on Ripple's statements, actions, and product offerings" in connection with "purchases of XRP [that] were made . . . throughout the period that Ripple offered XRP for sale from 2013 to the filing of the SEC's Complaint on December 22, 2020."[14] Mr. [redacted] states that the purchasers he considers "primarily include individuals, institutional investors, and financial services companies."[15] Mr. [redacted] performs what he calls "review and analysis of Ripple's public statements made throughout the Issuance Period,

[10] Complaint, ¶2.

[11] Complaint, ¶3.

[12] Ripple's Answer, ¶1.

[13] Ripple's Answer, ¶¶7, 9, 10.

[14] [redacted] Report, ¶2.

[15] [redacted] Report, ¶2.

documents, and design decisions made by Ripple and/or its founders"[16] and concludes the following with respect to the "perspective of a reasonable purchaser" of XRP:

a. "[A] reasonable purchaser would have had an expectation of future profit derived from the efforts of Ripple."[17] In particular, Mr. [redacted] opines that Ripple's actions "would create the hope that a purchaser could passively earn profits by owning XRP while Ripple took steps to increase the value of the coin."[18]

b. "[T]here are certain elements in Ripple's and its founders' design of XRP, the XRP Ledger, and a variety of software products that appealed more to a purchaser of XRP interested in making a profit than to financial institutions seeking to embrace Ripple's stated vision of utilizing XRP as a bridge asset for cross-border asset transfers."[19]

[16] [redacted] Report, ¶7. In particular, Mr. [redacted] states that his "report focuses on what Ripple communicated publicly, including its assertions that usage of its products by financial institutions would ultimately lead to greater demand for XRP." [redacted] Report, footnote 25.

[17] [redacted] Report, ¶8.

[18] [redacted] Report, ¶8. In the "Summary of Findings and Conclusions" section at the end of his report, Mr. [redacted] restates this conclusion as follows, "[o]ver the course of the Issuance Period a reasonable purchaser of XRP would have had an expectation of generating profit based on the efforts of Ripple and its management to accomplish the growth strategies that Ripple advertised to the public as being already achieved or planned for the future. . . . a reasonable purchaser would have closely considered many factors that were publicized by Ripple such as disclosed partnerships with financial institutions, the quality of Ripple's management team, the target addressable market for Ripple's products, and the availability of liquidity on trading platforms for XRP." [redacted] Report, ¶89.

[19] [redacted] Report, ¶9. In the "Summary of Findings and Conclusions" section at the end of the report, Mr. [redacted] restates this conclusion as "[c]ertain aspects of the design characteristics of XRP and the promotional activity of Ripple did not appeal to a pure utility use case." [redacted] Report, ¶90. The rest of Mr. [redacted] "Summary of Findings" section and "Summary of Findings and Conclusions" section appear to list the reasons for which he holds these opinions about the "perspective of a reasonable purchaser" (or supposed logic of how a "reasonable purchaser" would arrive at these two "perspectives") rather than providing any incremental "perspectives."

VI. MR. [redacted] OPINES ON THE "PERSPECTIVE OF A REASONABLE PURCHASER" RESULTING FROM RIPPLE'S "STATEMENTS, ACTIONS, AND PRODUCT OFFERINGS" WITHOUT EMPLOYING ANY RELIABLE METHODOLOGY

15. Mr. [redacted] opinions concern the effects that Ripple's "statements, actions, and product offerings" supposedly had on the "perspectives" of reasonable purchasers of XRP. For example, he opines that actions by Ripple "would create" certain expectations for "a reasonable purchaser."[20] Conclusions of this sort are considered "causal," in the sense that he implies that Ripple's "statements, actions, and product offerings" caused changes in the "perspective of a reasonable purchaser."

16. There are scientifically grounded and reliable methodologies to assess whether causal relationships of this sort exist. Mr. [redacted] did not employ any such methodology. As a result, Mr. [redacted] has offered no legitimate and reliable basis for his opinions. Mr. [redacted] also offers no explanation as to why he failed to use such a methodology, and from the materials Mr. [redacted] provided, it does not appear that Mr. [redacted] has any experience or qualification that would enable him to use such a methodology to the extent that his opinions discuss perceptions of reasonable purchasers. Appendix C to this report lists examples of Mr. [redacted] unsupported causal propositions.

17. I describe the bases for my opinion below. Section VI.A describes reliable scientific methodologies that can be employed (but that Mr. [redacted] failed to employ) to determine whether the sort of causal relationship that Mr. [redacted] posits actually exists. Section VI.B describes in detail Mr. [redacted] "review and analysis." Section VI.C describes why the "methodology" on which Mr. [redacted] effectively relied is invalid as a matter of well-established scientific principles.

[20] [redacted] Report, ¶8.

A. The established, reliable, and supportable method for evaluating causal propositions is the experimental method

18. The gold standard for testing a causal hypothesis is an experiment. For example, Babbie (2010) states that "[e]xperiments are the primary tool for studying causal relationships"[21] and Shadish, et al. (2002) also state that "experiments are well-suited to studying causal relationships. No other scientific method regularly matches the characteristics of causal relationships so well."[22] The 2019 Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel (commonly referred to as the "Nobel Prize" in economics) was awarded to Abhijit Banerjee, Esther Duflo, and Michael Kremer for their use of experiments in the field of developmental economics[23] and, similarly, the 2021 Nobel Prize in Economics was awarded to David Card, Joshua Angrist and Guido Imbens for their work related to experiments and quasi-experiments.[24] The Royal Swedish Academy noted that "[m]ost applied science is concerned

---

[21] Babbie, Earl. *The Practice of Social Research*. Twelfth Edition. Wadsworth Cengage Learning, 2010 ("Babbie (2010)"), p. 249.

[22] Shadish, William R., Thomas D. Cook, and Donald T. Campbell. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Wadsworth Cengage Learning, 2002, pp. 7-9. Shadish, et al. (2002) further state "In many correlational studies, for example, it is impossible to know which of two variables came first, so defending a causal relationship between them is precarious. . . . The unique strength of experimentation is in describing the consequences attributable to deliberately varying a treatment."

[23] The Royal Swedish Academy of Sciences. "The Prize in Economic Sciences 2019," available at https://www.nobelprize.org/uploads/2019/10/press-economicsciences2019-2.pdf, p. 1.

[24] The Royal Swedish Academy of Sciences. "Scientific Background on the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2021 - Answering Causal Questions Using Observational Data," available at https://www.nobelprize.org/uploads/2021/10/advanced-economicsciencesprize2021.pdf ("The Royal Swedish Academy of Sciences (2021)"), pp. 1-2. "This year's Prize in Economic Sciences rewards three scholars: David Card of the University of California, Berkeley, Joshua Angrist of Massachusetts Institute of Technology, and Guido Imbens of Stanford University. The Laureates' contributions are separate but complementary. . . . The combined contribution of the Laureates, however, is larger than the sum of the individual parts. Card's studies from the early 1990s showcased the power of exploiting natural experiments to uncover causal effects in important domains. This early work thus played a crucial role in shifting the focus in empirical research using observational data towards relying on quasi-experimental variation to establish causal effects. The framework developed by Angrist and Imbens, in turn, significantly altered how researchers approach empirical questions using data generated from either natural experiments or randomized experiments with incomplete compliance to the assigned treatment. At the core, the LATE interpretation clarifies what can and cannot be learned from such experiments. Taken together, therefore, the Laureates' contributions have played a central role in establishing the so-called design-based approach in economics. This approach – aimed at emulating a randomized experiment to answer a causal question using

with uncovering causal relationships," and that in many fields, "randomized controlled trials (RCTs) are considered the gold standard for achieving this. . . . Randomized experiments can be used to answer a broad range of causal questions."[25]

19. Some of the most commonly discussed experiments are clinical trials, also referred to as randomized controlled trials, where patients are randomly assigned to a treatment group that receives the tested treatment, or a control group that receives a previously established treatment or a placebo.[26] In these experiments, if the studied health outcome of the test group (e.g., blood pressure) is statistically significantly better than in the control group, the researchers conclude that the tested treatment is effective (or more effective than the pre-existing treatment that the control group received).[27] That is, the researchers use a test group and a control group to establish whether and how a change in stimulus (tested treatment vs. control treatment) affects outcomes (e.g., blood pressure). Principles of this sort can be applied to measure causation in other fields as well, including economics as discussed above. Experiments are also common in marketing and consumer behavior and can be used to test whether receiving certain information affects consumers' views about a particular product.[28]

---

observational data – has transformed applied work and improved researchers' ability to answer causal questions of great importance for economic and social policy using observational data."

[25] The Royal Swedish Academy of Sciences (2021), pp. 1, 8.

[26] "In the medical sciences . . . randomized experiments are often used for determining the effects of a treatment. For example, a drug and a placebo may be randomly given to patients and the health effects then compared between those receiving the drug and those given a placebo." The Royal Swedish Academy of Sciences (2021), p. 7.

[27] "If we observe statistically significant differences among the groups after a comparative randomized experiment, we have good evidence that the treatments actually caused these differences." Yates, Daniel, David Moore, and George McCabe. *The Practice of Statistics*. First Edition. W.H. Freeman, 1999 ("Yates, et al. (1999)"), p. 276.

[28] See, for example, Assael, Henry. *Consumer Behavior, A Strategic Approach*. Houghton Mifflin Company, 2004, pp. 18-19. "Researchers try to determine the effects of marketing stimuli such as alternative product characteristics, advertising themes, or price levels (the cause) on consumer responses (the effect). In trying to establish such cause-and-effect relationships, the researcher must try to control all factors except the marketing stimulus being tested so that consumer responses can be attributed to that stimulus. Frito-Lay ran experiments under controlled conditions and found it could reduce oil in its light chip line (the stimulus or cause) by one-third without a decrease in consumer taste ratings (the response or effect)."

20. Here, a proper experimental methodology to support Mr. [redacted] opinions – which Mr. [redacted] did not use – would test whether the particular information he points to (i.e., Ripple's "statements, actions, and product offerings") actually caused the effects he ascribes to that information (e.g., creating particular beliefs or expectations among reasonable purchasers of XRP). To do that, a well-designed experiment would compare outcomes ("perspective of a reasonable purchaser") in the actual world in which Ripple engaged in the at-issue "statements, actions, and product offerings" with outcomes in the but-for world in which the at-issue "statements, actions, and product offerings" were not present. This experiment would directly compare the "perspective of a reasonable purchaser" in the actual and the but-for worlds.

21. Academics and experts in litigation conduct similar experiments and experiment-like studies using a variety of methods involving either data accumulated in the regular course of business or by conducting new "primary data" studies.[29]

22. Because one of the key outcomes of interest here is the beliefs held by potential XRP purchasers (e.g., whether or not the potential XRP purchasers had "an expectation of future profit"), the most direct way of measuring that outcome is through a survey of actual and potential XRP purchasers. For example, Jacoby (2013) notes surveys are "the methodological tool most often used by social scientists to probe states of mind," and are "routinely used" in litigation contexts for that reason.[30]

---

[29] See, for example, Diamond, Shari, S. "Reference Guide on Survey Research." *Reference Manual on Scientific Evidence*. Third Edition. Federal Judicial Center, 2011, pp. 359-423 ("Diamond (2011)"), at pp. 397-401. Jacoby (2013) noted that in "[a] study of trademark cases (including applications for interim injunctions) that went to final judgment reported during a 10-year span from the mid-1990s through the mid-2000s revealed more cases where survey evidence was submitted (57.4 percent) than where surveys were not submitted." Jacoby, Jacob, and Lynda Zadra-Symes. "Legal Issues That Can Be Examined via Surveys." *Trademark Surveys: Volume 1: Designing, Implementing, and Evaluating Surveys*. Jacob Jacoby. ABA Book Publishing, 2013 ("Jacoby (2013)"), p. 7.

[30] Jacoby (2013), p. 6. Diamond (2011) explains that surveys "are used to describe or enumerate the beliefs, attitudes, or behavior of persons or other social units. Surveys typically are offered in legal proceedings to establish or refute claims about the characteristics of those individuals or social units (e.g., whether consumers are likely to be

23. There are multiple types of surveys that can be conducted. A traditional survey may ask respondents for information without trying to measure any causal effects. For example, a survey could simply ask respondents which political candidate they intend to vote for, or whether they have ever purchased a particular type of product, or how they understand a particular advertisement. However, as Diamond (2011) explains, "[s]urveys that merely record consumer impressions have a limited ability to answer questions about the origins of those impressions. The difficulty is that the consumer's response to any question on the survey may be the result of information or misinformation from sources other than the trademark the respondent is being shown or the commercial he or she has just watched."[31] Surveys of this sort can be appropriate when the goal is to learn about prevalent opinions or preferences (such as which candidate is likely to win an election) rather than causal relationships (such as how new information may cause people to change their beliefs or preferences). When the purpose is to investigate such a causal relationship, a survey in the experimental form would be carried out. Diamond (2011), for example, states that "[m]any surveys are designed not simply to describe attitudes or beliefs or reported behaviors, but to determine the source of those attitudes or beliefs or behaviors. That is, the purpose of the survey is to test a causal proposition."[32] Because Mr. [redacted] attempts to describe a causal relationship (i.e., whether potential XRP purchasers' "perspectives" are caused by Ripple's at-issue "statements, actions, and product offerings"), an experimental form survey

misled by the claims contained in an allegedly deceptive advertisement; which qualities purchasers focus on in making decisions about buying new computer systems)." Diamond (2011), at p. 361.

[31] Diamond (2011), at p. 397.

[32] Diamond (2011) presents an example of how such a survey works: "For example, how does a trademark or the content of a commercial affect respondents' perceptions or understanding of a product or commercial? Thus, the question is not merely whether consumers hold inaccurate beliefs about Product A, but whether exposure to the commercial misleads the consumer into thinking that Product A is a superior pain reliever. Yet if consumers already believe, before viewing the commercial, that Product A is a superior pain reliever, a survey that simply records consumers' impressions after they view the commercial may reflect those preexisting beliefs rather than impressions produced by the commercial." Diamond (2011), at pp. 397-399.

would have been the appropriate methodology to use here. Mr. [redacted] did not conduct such a survey.

24. A well-designed experimental-form survey would simulate the actual and the but-for world for a sample of "reasonable purchasers," half of which would be randomly assigned to the "actual world" (test group) and the other half to the "but-for world" (control group). Diamond (2011) explains:

> By adding one or more appropriate control groups, the survey expert can test directly the influence of the stimulus. In the simplest version of such a survey experiment, respondents are assigned randomly to one of two conditions. For example, respondents assigned to the experimental condition view an allegedly deceptive commercial, and respondents assigned to the control condition either view a commercial that does not contain the allegedly deceptive material or do not view any commercial. Respondents in both the experimental and control groups answer the same set of questions about the allegedly deceptive message. The effect of the commercial's allegedly deceptive message is evaluated by comparing the responses made by the experimental group members with those of the control group members. If 40% of the respondents in the experimental group responded indicating that they received the deceptive message (e.g., the advertised product has fewer calories than its competitor), whereas only 8% of the respondents in the control group gave that response, the difference between 40% and 8% (within the limits of sampling error) can be attributed only to the allegedly deceptive message. Without the control group, it is not possible to determine how much of the 40% is attributable to respondents' preexisting beliefs or other background noise (e.g., respondents who misunderstand the question or misstate their responses).[33]

25. Similarly, Yates, et al. (1999) state that a great advantage of experiments is that "they can produce data that give good evidence for a cause-and-effect relationship between the explanatory

[33] Diamond (2011), at p. 398.

and response variables. We know that in general, a strong association does not imply causation. A strong association in data from a well-designed experiment does imply causation."[34]

26. In this case, a well-designed experimental survey would involve the following steps:[35]

a. The survey should be designed, conducted, and analyzed by an expert who is "[a]ppropriately [s]killed and [e]xperienced," which Mr. [redacted] is not.[36]

b. Actual and potential purchasers of XRP (the target population) would be recruited to participate in a survey. Those could be drawn, for example, from the three types of purchasers that Mr. [redacted] highlighted, "individuals, institutional investors, and financial services companies."

c. The "[i]dentification of the proper target population or universe is recognized uniformly as a key element in the development of a survey."[37]

---

[34] Yates, et al. (1999), p. 275. Yates, et al. (1999) describe the "logic behind a randomized comparative design" as: "• Randomization produces groups of experimental units that should be similar in all respects before the treatments are applied. • Comparative design ensures that influences other than the experimental treatments operate equally on all groups. • Therefore, differences in the response variable must be due to the effects of the treatments. That is, the treatments not only are associated with the observed differences in the response but must actually cause them."

[35] A survey would be preceded by exploratory research, which may include other "primary data" collection, and a pretest. The exploratory research and the design stage would include numerous decisions such as which at-issue statements to test, and how to instrumentalize the targeted population.

[36] Diamond (2011), at p. 375. "Experts prepared to design, conduct, and analyze a survey generally should have graduate training in psychology (especially social, cognitive, or consumer psychology), sociology, political science, marketing, communication sciences, statistics, or a related discipline; that training should include courses in survey research methods, sampling, measurement, interviewing, and statistics. In some cases, professional experience in teaching or conducting and publishing survey research may provide the requisite background. In all cases, the expert must demonstrate an understanding of foundational, current, and best practices in survey methodology, including sampling, instrument design (questionnaire and interview construction), and statistical analysis. Publication in peer-reviewed journals, authored books, fellowship status in professional organizations, faculty appointments, consulting experience, research grants, and membership on scientific advisory panels for government agencies or private foundations are indications of a professional's area and level of expertise," (footnotes omitted). While Mr. [redacted] may have some training in statistics, he does not appear to have any training (e.g., in marketing or psychology) that would allow him to ask questions in an unbiased fashion.

[37] Diamond (2011), at p. 376, footnote 76.

Diamond (2011) further states that "One of the first steps in designing a survey or in deciding whether an existing survey is relevant is to identify the target population (or universe). The target population consists of all elements (i.e., individuals or other units) whose characteristics or perceptions the survey is intended to represent. Thus, in trademark litigation, the relevant population in some disputes may include all prospective and past purchasers of the

d. Respondents who qualify would be randomly assigned to a test group or a control group.

e. Test group respondents would be exposed to a set of tested statements and actions by Ripple: specifically, the "statements, actions, and product offerings" that Mr. [redacted] describes in his report. These could be presented in a form of a vignette accompanied by news articles, video interviews, or other stimuli approximating the marketplace realities.[38] The names "Ripple" and "XRP" could be anonymized to control for prior knowledge.

f. The control group would be exposed to the same procedure, except that the at-issue elements of the statements, actions, and product offerings would be replaced

plaintiff's goods or services and all prospective and past purchasers of the defendant's goods or services…. The definition of the relevant population is crucial because there may be systematic differences in the responses of members of the population and nonmembers. For example, consumers who are prospective purchasers may know more about the product category than consumers who are not considering making a purchase. The universe must be defined carefully. For example, a commercial for a toy or breakfast cereal may be aimed at children, who in turn influence their parents' purchases. If a survey assessing the commercial's tendency to mislead were conducted based on a sample from the target population of prospective and actual adult purchasers, it would exclude a crucial relevant population. The appropriate population in this instance would include children as well as parents." Diamond (2011), at pp. 376-377.

Jacoby (2013) also notes the importance of selecting the correct survey universe in the context of trademark cases: "The rationale relied upon for identifying the relevant buyer class (the 'survey universe,' see chapter 5) is important, as courts may find the universe of relevant buyers too broad or too narrow. … Using the wrong universe can result in the survey being given little weight or even deemed inadmissible." Jacoby (2013), pp. 11-12.

[38] Yates, et al. (1999) state that the "most serious potential weakness of experiments is lack of realism. The subjects or treatments or setting of an experiment may not realistically duplicate the conditions we really want to study.… Lack of realism can limit our ability to apply the conclusions of an experiment to the settings of greatest interest. Most experiments want to generalize their conclusions to some setting wider than that of the actual experiment. Statistical analysis of the original experiment cannot tell us how far the results will generalize… A convincing case that an experiment is sufficiently realistic to produce useful information is based not on statistics but on the experimenter's knowledge of the subject matter of the experiment. The attention to detail required to avoid hidden bias also rests on subject matter knowledge. Good experiments combine statistical principles with understanding of a specific field of study." Yates, et al. (1999), pp. 278-279.

by "placebo" versions that lack the content that is hypothesized to have an effect on reasonable purchasers' "perspective."[39]

g. "In designing a survey-experiment, the expert should select a stimulus for the control group that shares as many characteristics with the experimental stimulus as possible, with the key exception of the characteristic whose influence is being assessed."[40]

h. Both groups will then be evaluated on a "dependent measure" which would aim at gaining the unbiased "perspective of a reasonable purchaser." For example, respondents could be asked in open-ended and closed-ended formats about their perception of the digital asset described to them, whether they would expect its price to grow because of the efforts of the company discussed in the study, whether they would expect the digital asset to be usable in transactions, including cross-border transactions, and what their own intentions would be with respect to

[39] For example, Mr. [redacted] claims that in a certain passage in an interview with Bloomberg Technology, Ripple's CEO Brad Garlinghouse contributed to certain underrating of XRP potential purchasers about XRP. [redacted] Report, ¶¶25-26.

The passage called out by Mr. [redacted] reads, "[w]hen Ripple uses XRP we're solving a payments problem. I believe that the more utility you draw, the more demand you're going to drive. And for most of these digital assets you have fixed supply. If you have fixed supply and increasing demand it's going to drive price up." Mr. [redacted] believes that because of this statement, "[p]otential purchasers of XRP would have understood [that] XRP, as designed, provided a mechanism for passive XRP owners to benefit financially from Ripple's success as a provider of financial service products built on the XRP Ledger, as a developer of the XRP ecosystem, and as a driver of demand for XRP" (footnote omitted).

In the experiment, respondents in the test group could be exposed to the interview the way it occurred, while the control group respondents could be exposed to the same interview but where the passage identified by Mr. [redacted] would be removed or replaced by a "placebo."

In addition to testing the causal proposition, such an approach would account for whether potential purchasers who viewed the interview would even pay attention to the passage highlighted by Mr. [redacted] Additional empirical research would be needed to further investigate what percentage of the potential or actual XRP purchasers was even exposed to the interview. Mr. [redacted] addressed neither of these topics.

[40] Diamond (2011), at p. 399.

the asset discussed (e.g., whether they would consider purchasing it, and what they would potentially do with it afterwards).

i. After data are collected, statistical analysis would be carried out to assess whether the perspectives of the test and control groups differ. If the perspectives are *not* statistically significantly different, one can conclude that the perspective of a reasonable purchaser is *not* caused by the statements and actions tested in the experiment (i.e., those elements that differ in the stimuli presented to the test and control group).[41] (Strictly speaking, when a researcher finds no statistically significant difference in the outcomes between the test and control groups, the researcher "fails to reject the null hypothesis" of no causal relationship.)

j. The study would also allow a researcher to assess whether different groups respond to inputs differently. In particular, Mr. [redacted] opines that Ripple's actions and the design of XRP and the XRP Ledger "appealed more to a purchaser of XRP interested in making a profit than to financial institutions seeking to . . . [use] XRP as a bridge asset for cross-border asset transfers."[42] Differences in effects observed among various subsamples in the study (e.g., individual investors vs. representatives of financial institutions) can be tested. Alternatively, data can be examined for whether participants respond in a way that makes them naturally fall into two distinct groups of "investors for profit" and "cross-border transfer users," and whether the share of "investors for profit" is statistically significantly different in the test group than in the control group. Mr. [redacted] makes no effort to

[41] "If we observe statistically significant differences among the groups after a comparative randomized experiment, we have good evidence that the treatments actually caused these differences." Yates, et al. (1999), p. 276.

[42] [redacted] Report, ¶9.

establish that the two groups of XRP purchasers he purports exist actually exist, or to measure their relative sizes. He appears to assume that "[i]nvestment-[o]riented" purchasers are prevalent.[43]

27. Mr. [redacted] does not appear to have any training or experience in designing and performing such a study. In any event, he did not carry it out in connection with offering his opinion in this case.

28. Other, non-experimental options are also available to evaluate perceptions and expected behavior, although they are less effective in isolating causal effects than the gold-standard methodology of conducting an experiment. For example, someone interested in how reasonable purchasers understand certain information could conduct a simple survey, without a control group, or carry out a qualitative study such as focus groups or qualitative phone interviews. While these methods would not allow a researcher to test a particular causal hypothesis, they are used to develop such hypotheses for subsequent experimental testing.[44]

29. Mr. [redacted] does not appear to have any training or experience in designing and performing such a study, and he did not carry out such a study in connection with offering his opinion in this case.

---

[43] For example, in his Section 7 titled "Ripple Communications and Promotional Statements," Mr. [redacted] includes Subsection 7.1, titled "Promotional Factors Considered by an Investment-Oriented Purchaser." However, he does not include a parallel subsection that would address promotional factors presumably considered by the other group of XRP purchasers that he claims exists, "[p]urchasers of XRP for cross-border payments." [redacted] Report, ¶86.

[44] Assael, Henry. *Consumer Behavior, A Strategic Approach*. Houghton Mifflin Company, 2004, p. 17. "Qualitative research is designed to learn more about consumers' underlying motives by asking them questions in an unstructured manner. It allows researchers to form hypotheses regarding consumer actions and to better define research areas so as to know the kinds of questions to ask in more structured surveys or experiments. The two most frequently used qualitative approaches are focus groups interviews and projective techniques."

Hague, et al. (2016) state that focus groups can be used to "identify and explore behaviour, attitudes and processes" and can be used "to enhance alternative means of data collection. Typically this would be as a precursor to a quantitative stage – determining the issues to be covered in the structured interviewing and giving insights into the problems or opportunities that are being researched." Hague et al. *Market Research in Practice*. Kindle Edition, Third Edition. Kogan Page, 2016, p. 69.

30. It is also possible to conduct quasi-experiments using preexisting data. In fact, the 2021 Nobel Laureates in Economics received the Nobel Prize for their use of quasi-experimental designs and for their development of a "general [causal inference] framework applicable to both quasi-experimental and experimental work."[45] In the current case, someone interested in testing whether the "statements, actions, and product offerings" at issue in Mr. [redacted] report affected the "perspective" of "reasonable purchasers" could compare actual historical trading data for XRP (the real world) against that of other digital assets, which would serve as a proxy for the but-for world assuming that they are not affected by Ripple's "statements, actions, and product offerings." The critical element of such a study on preexisting data would be "controlling" for all other differences that are not related to the at-issue conduct. Shadish, et al. (2002) discuss that because "quasi-experimental control groups may differ from the treatment condition in many systematic (non-random) ways other than the presence of the treatment," researchers have to worry about ruling out alternative explanations for the observed effect (e.g., by controlling for all other differences) "in order to get a more valid estimate of the treatment effect."[46]

31. It is not clear to me whether Mr. [redacted] possesses the qualifications to conduct such a study on preexisting data, but he certainly did not carry it out.

[45] The Royal Swedish Academy of Sciences (2021), pp. 4, 27-28.

[46] Shadish, William R., Thomas D. Cook, and Donald T. Campbell. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Wadsworth Cengage Learning, 2002, p. 14. Specifically, "[i]n quasi-experiments, the cause is manipulable and occurs before the effect is measured. However, quasi-experimental design features usually create less compelling support for counterfactual inferences. For example, quasi-experimental control groups may differ from the treatment condition in many systematic (non-random) ways other than the presence of the treatment. Many of these ways could be alternative explanations for the observed effect, and so researchers have to worry about ruling them out in order to get a more valid estimate of the treatment effect."

See also Meyer, Bruce D. "Natural and Quasi-Experiments in Economics." *Journal of Business & Economic Statistics* 13(2): 151-161, April 1995, at pp. 153-156.

B. Mr. [redacted] does not evaluate whether and to what degree XRP purchasers were exposed to the at-issue communications and does not attempt to empirically evaluate the causal effect, if any, of Ripple's public communications on perceptions or purchase decisions of actual or potential purchasers of XRP

32. Mr. [redacted] conducts his "analysis" in three sections of his report, 5, 6, and 7.[47] The three sections have a similar structure, where initial subsections lay out Ripple's alleged conduct and theoretical discussions, while a final subsection jumps to conclusions about the "perspective of [a] reasonable purchaser" without offering any empirical support for such conclusions (some conclusions about "perspective" are also weaved into the initial subsections).

33. As a preliminary matter, I note that Mr. [redacted] does not distinguish between conclusions he makes on the basis of basic economic principles and those he makes based on Ripple's communications. In his logic, it is impossible to distinguish where potential or actual purchasers would have arrived at a particular perception or purchase decision based on basic economic principles regardless of anything Ripple said or did (e.g., such as principles of demand and supply) or whether Ripple's public communication or other at-issue conduct contributed to those perceptions and purchase decisions. The experimental method discussed above would allow an expert to distinguish between these potentially confounding influences. Such distinction is generally impossible when an "expert" does not apply the experimental method, as is the case with Mr. [redacted] "analysis."

34. I address each of the three "analysis" sections of the [redacted] Report in the corresponding subsections below.[48]

[47] Other sections include introduction, summaries of findings and conclusions, background, Ripple platform overview, and a note on right to supplement.

[48] I discuss in more detail section 5 of the [redacted] Report. The issues with sections 6 and 7 are largely similar.

a. [redacted] Report Section 5 "Features of XRP Coin Economics and Suitability as a Bridge Asset"

35. In Section 5.1 of his report, Mr. [redacted] explains that "[a]ll else equal, for any digital asset with a fixed-supply cap, increased demand for the coin increases the price of the coin. This is a basic economic result of supply and demand."[49] Then he mentions that "Ripple directly and publicly made the case for this relationship between increased demand for XRP and the future price of XRP" and offers as an example Mr. Garlinghouse's interview with Bloomberg Technology in 2017.[50] Mr. [redacted] then concludes: "Potential purchasers of XRP would have understood the simple economics behind the message being promoted by Ripple on this subject: XRP, as designed, provided a mechanism for passive XRP owners to benefit financially from Ripple's success as a provider of financial service products built on the XRP Ledger, as a developer of the XRP ecosystem, and as a driver of demand for XRP."[51]

36. The critical flaw of this "analysis" is that Mr. [redacted] does not investigate whether any XRP purchasers were exposed to the interview, paid attention to it, understood it in the way consistent with Mr. [redacted] interpretation (i.e., did XRP purchasers believe that increased demand for XRP would increase its price, and if so, was that belief due to the particular statement in the interview or due to some other source), or were impacted by it in their purchase decisions (e.g., purchased XRP due to the particular statement in the interview). Nor does he acknowledge that XRP had been offered for several years (since 2013) before this interview took place.

---

[49] [redacted] Report, ¶23.

[50] [redacted] Report, ¶25.

[51] [redacted] Report, ¶26, footnote omitted.

37. Similarly, in section 5.2 of his report, Mr. [redacted] describes advantages of "stablecoin" over variable-price assets (e.g., XRP) for cross-border currency transfers.[52] In this theoretical discussion, he states that Ripple's CTO mentioned in 2016 one such supposed "shortcoming" of XRP "in a post on XRP Chat."[53] Mr. [redacted] then concludes that the relationship between the success of the platform and price of the coin "is fantastic for investment-oriented purchasers of XRP, but not for the purchasers who are exclusively interested in the utility use of the cross-border payment product."[54]

38. This section is flawed for similar reasons as section 5.1. Mr. [redacted] does not investigate whether it is the general theoretical logic that he offers that would lead to the supposed perspective of the two types of potential XRP purchasers he identifies, rather than the CTO's statement, which only touches upon one of two supposed "shortcomings." Mr. [redacted] does not investigate whether any prospective purchasers were exposed to the CTO's statement, paid attention to it, understood it in the way consistent with Mr. [redacted] interpretation (i.e., do XRP purchasers believe that XRP is a good investment but not a good instrument for cross-border transfers, and if so, did that belief come about due to the CTO's chat statement), or were impacted by it in their purchase or post-purchase decisions (i.e., purchased XRP as investment and not for cross-border transfers because of the CTO's chat statement). Mr. [redacted] also does not acknowledge that XRP had been offered for several years before the CTO's statement. Neither does he offer any market segmentation or similar analysis to allow him to establish that the two types of purchasers he describes are actually distinct or that there are only two types of purchasers.

---

[52] [redacted] Report, ¶¶27-29.

[53] [redacted] Report, ¶28.

[54] [redacted] Report, ¶31.

39. In section 5.3 of his report, Mr. [redacted] summarizes the "Perspective of a Reasonable Purchaser with Respect to XRP's Fixed-Supply Model," again splitting the purchasers into "investment-oriented purchasers of XRP" and "purchasers who are exclusively interested in the utility use of the cross-border payment product." Again, he does not explain whether these two types of purchasers were exposed or paid attention to the specific Ripple statements, whether the perspectives (perceptions and purchase behaviors) of these two types of potential purchasers were affected by those statements or by general economic logic, why these two types of customers represent a relevant market segmentation, and whether there is any basis to say these two are the only types of potential purchasers that should be considered.

b. [redacted] Report Section 6 "XRP Sale and Escrow Mechanics"

40. In sections 6.1-6-5 of his report, Mr. [redacted] discusses "XRP Sale and Escrow Mechanics," again intermingling theoretical logic, statements made by Ripple, and actions taken by Ripple.[55] This intermingling is flawed for the reasons I explain above. Then, in section 6.6, Mr. [redacted] describes the supposed "Perspective of a Reasonable Purchaser with Regards to Ripple's XRP Sales and Escrow," again discussing separately the perspective of "a potential investment-oriented purchaser of XRP" and "a reasonable purchaser of XRP that is exclusively considering the utility use of the coin."[56] Again, he does not explain why his segmentation into these two types of purchasers is valid, or whether these two types of purchasers were exposed or

[55] [redacted] Report, ¶¶32-47. Occasionally, Mr. [redacted] would interject these descriptions with what appears to be his take on purchaser "perspective." For example, he states that various aspects of institutional purchasing of XRP, "repeatedly communicated by Ripple in the XRP Markets Reports," "would appeal to an individual purchaser with a long-term investment mindset." [redacted] Report, ¶37. He does not identify any basis for distinguishing between subsets of potential XRP purchasers (for example, his "individual purchaser with a long-term investment mindset" versus an individual purchaser with a short-term investment mindset, or an individual purchaser with no investment mindset, or an entity purchaser) but also makes no attempt to argue that his conclusions hold as to all subsets of potential XRP purchasers.

[56] [redacted] Report, ¶¶48-49.

paid attention to the specific Ripple statements, whether they interpreted the statements the same way as Mr. [redacted] or whether the perspectives (perceptions and purchase behaviors) of these two types of potential purchasers are affected by those statements or by general economic logic. Each of these omissions is a critical flaw in Mr. [redacted] reasoning.

c. [redacted] Report Section 7 "Ripple Communications and Promotional Statements"

41. In Sections 7.2 to 7.7 of his report, Mr. [redacted] discusses various Ripple communications.[57] Then, in Section 7.8, he outlines the "Perspective of a Reasonable Purchaser with Respect to Ripple Communications," again splitting the purchasers without explanation or support for his categorization of those purchasers into "Investment-oriented purchasers" of XRP and "Purchasers of XRP for cross-border payments." For example, Mr. [redacted] states, without any empirical evidence, that "Ripple's extensive public comments and reports about these topics likely served to inform and persuade investment-oriented purchasers about the potential reward of purchasing XRP for the purpose of generating a profit. Indeed, the use of terms such as 'traction,' 'market fit,' 'total addressable market,' and even 'investors' when describing Ripple's

[57] These sections also occasionally include comments about purchasers' "perspective," such as "Such communications [by Ripple executives, linking the company's efforts to increases in the price of XRP] would have appealed to potential purchasers who were interested in XRP as an investment." [redacted] Report, ¶53. Similarly, Mr. [redacted] occasionally infuses these sections with theoretical logic like this statement: "[o]ne of the key aspects for evaluating whether a company or project has a viable business model is whether it has 'traction', i.e., to what extent is there is 'product/market-fit' where actual customers have signed up to use the company's product or service such as to demonstrate that it solves a real problem." [redacted] Report, ¶61. In another such instance, Mr. [redacted] explains, "[w]hen investment-oriented purchasers evaluate a company or project as a potential investment, they want to understand how the funds collected will be deployed by management to grow the venture." [redacted] Report, ¶76. Some statements appear to be somewhere in between theoretical logic and conclusions on purchaser "perspective." For example, Mr. [redacted] states, "Ripple's ongoing replacement of released XRP into new escrows reinforced the positive effect of this reduction in circulating supply by showing a commitment to keeping those coins away from trading platforms for even longer." [redacted] Report, ¶43. Another example is the statement that "Although the buyback activity would not have mattered to purely utility-oriented purchasers of XRP, buybacks are very important signals for investment-oriented purchasers. Open market purchases, and the public communications about those purchases, alter the potential risk and reward of an investment in XRP by increasing buying pressure on the coin and by reducing the probability and severity of a possible crash in the price of XRP. Like the escrow accounts described in Section 6.3, the buyback activities executed by Ripple would also have the effect of reducing the effective float of the coin." [redacted] Report, ¶47.

progress and growth potential are words typically understood by market participants to mean that they should view buying XRP as a potentially profitable investment."[58] He concludes, "[i]t is my opinion from carefully following the digital asset space that many of Ripple's public communications conveyed to reasonable purchasers of XRP an expectation of future profit derived from the efforts of Ripple."[59]

42. Mr. [redacted] supposedly supports this conclusion in part by section 7.1, where he describes which factors "a reasonable investment-oriented purchaser of XRP would consider" based on his own "experience as an investor in digital assets as well as [his] close observation of the digital asset space."[60] Thus, as with the other sections of his report, the entirety of section 7 does not include any empirical analysis (e.g., survey) that would actually evaluate whether these are the appropriate segments of purchasers, whether purchasers of either type were exposed to or paid attention to the Ripple statements, whether they interpreted them the same way as Mr. [redacted] or whether the statements had any effect on their perspectives. And, as with the other sections, he offers no support for distinguishing between the two purchaser types he chose to focus on, and no support for assuming that no other types of purchasers exist. He offers no empirical support for his opinions in this section; at most, Mr. [redacted] offers the perspective of a single such purchaser or potential purchaser, Mr. [redacted] himself, which is akin to conducting a survey of a single person, an egregious methodological error (discussed in greater detail in the next section).[61]

[58] [redacted] Report, ¶85.

[59] [redacted] Report, ¶87.

[60] [redacted] Report, ¶50.

[61] It is not clear if his perspective is solely of an "investment-oriented" purchasers or also a cross-border payment purchaser.

d. Other Flaws in Mr. [redacted] "Analysis"

43. In addition to the flaws discussed above, Mr. [redacted] does not explain how he made the selection of Ripple's statements that he "review[s] and analy[zes]" or how he identified the passages that he considers likely to have affected the perspectives of actual or potential XRP purchasers. I note that the statements Mr. [redacted] discusses are not the same as the ones that the SEC alleged formed the basis of XRP purchasers' beliefs about Ripple's conduct. For example, the complaint identifies a statement made by Mr. Garlinghouse in 2018 in an interview with Bloomberg News as one that was likely to create expectations among XRP purchasers, while Mr. [redacted] does not address it:

> "[W]e have found that part of the reason why XRP has performed well, is because people realize. . . if we work with the system to solve this problem and we can solve that problem at scale, a problem measured in the trillions of dollars, then there is a lot of opportunity to create value in XRP." Garlinghouse also speculated in the December 14, 2017 interview that, if a company created "utility" for a digital asset like XRP, "then there will be demand for the tokens, [and] the price of the tokens will go up."[62]

Similarly, Mr. [redacted] identifies Mr. Garlinghouse's interview with Bloomberg Technology in 2017, discussed above, as one that was likely to create expectations among XRP purchasers, while the complaint does not address it:

> When Ripple uses XRP we're solving a payments problem. I believe that the more utility you draw, the more demand you're going to drive. And for most of these digital assets you have fixed supply. If you have fixed supply and increasing demand it's going to drive price up.[63]

[62] Complaint, ¶348. This statement is mentioned as part of Section IV.C "Ripple Led Investors to Reasonably Expect a Profit from Their Investment Derived from Defendants' Efforts."

[63] [redacted] Report, ¶25.

44. Mr. [redacted] also highlights certain terms Ripple used, such as "investor"[64] to imply that Ripple itself treated purchasers of XRP as investors (even though he does not establish that a single XRP purchase was made for the purposes of investing as a result of the alleged conduct). However, Mr. [redacted] elsewhere acknowledges that jargon used in a given industry or setting does not necessarily align with traditional word uses; in particular, he points out that when he uses words like "coin" and "token" in his report, he does not imply "currency."[65] Mr. [redacted] offers no explanation as to why he applies this understanding selectively throughout his report.

45. It is also worth noting that in section 7.2 of his report, Mr. [redacted] states, "[t]he most popular forum, by number of posts, on XRP Chat is the 'XRP Trading and Price Speculation' forum which currently has over 200,000 posts discussing issues related to the trading and investment case for XRP, as noted in its sub-header: 'Speculation about trading and price of XRP. Technical trading tips, fundamental analysis.' "[66] This is the closest Mr. [redacted] gets to actual empirical analysis of the XRP purchaser "perspective" in the entire report. He does not, however, articulate what percentage of actual or potential XRP purchasers contribute to the chat or read it, whether this sample is representative of all the XRP actual and potential purchasers (including institutional ones), whether any of the 200,000 posts mention using XRP for transactions (or any other systematic analysis of the content), or whether it is feasible to establish a causal relationship between the content of the posts and the alleged conduct (or whether the posts are based entirely on pre-existing beliefs and general economic principles). There is a

[64] [redacted] Report, ¶¶52, 81.

[65] [redacted] Report, footnote 2.

[66] [redacted] Report, ¶54.

reliable analytical method that could have been applied to these posts to answer these questions;[67] Mr. [redacted] did not use it.

C. Mr. [redacted] "review and analysis" does not evaluate any actual or potential XRP purchaser's perspective except for his own

46. One way of characterizing Mr. [redacted] analysis is that he conducted a survey of one actual or potential XRP purchaser – himself. This interpretation highlights the inadequacy of his method. To the best of my knowledge, no test of a causal proposition would be published in an academic journal or accepted by a court in litigation with a sample size of one.[68] For example, Yates, et al. (1999) state that such a study would not be trusted:

> You would not trust the results of an experiment that fed each diet to only one rat. The role of chance is too large if we use two rats and toss a coin to decide which is fed the new diet. The more rats we use, the more likely it is that randomization will create groups that are alike on the average. When differences among the rats are averaged out, only the effects of the different treatments remain. Here is a third principle of statistical design of experiments, called *replication*: repeat each treatment on a large enough number of

[67] "[C]ontent analysis is a method of collecting social data through carefully specifying and counting social artifacts such as books, songs, speeches, and paintings. Without making any personal contact with people, you can use this method to examine a wide variety of social phenomena.… [C]ontent analysis is the study of recorded human communications. Among the forms suitable for study are books, magazines, web pages, poems, newspapers, songs, paintings, speeches, letters, e-mail messages, bulletin board postings on the Internet, laws, and constitutions, as well as any components or collections thereof. … Content analysis is particularly well suited to the study of communications and to answering the classic question of communications research: 'Who says what, to whom, why, how, and with what effect?'… Common units of analysis in content analysis include elements of communications—words, paragraphs, books, and so forth. Standard probability-sampling techniques are sometimes appropriate in content analysis." Babbie (2010), pp. 229, 333, 359.

[68] Hibberts, et al. (2012) note that a key decision when conducting a research study is "deciding the appropriate sample size. The simplest answer is that the bigger the sample the better, but this assumes the sampling method is appropriate and implemented correctly. In inferential statistics, bigger is better because it results in smaller standard errors, greater statistical power or fewer Type II errors in hypothesis testing, and tighter or narrower confidence intervals in estimation. A Type II error occurs when a researcher fails to reject a false null hypothesis. (In contrast, a Type I error occurs when a researcher rejects a true null hypothesis; the null hypothesis typically states that there is no relationship in the population)." Hibberts, Mary, R. Burke Johnson, and Kenneth Hudson. "Common Survey Sampling Techniques." *Handbook of Survey Methodology for the Social Sciences*. Ed. Lior Gordon. Springer, 2012, p. 69.

See also Yates, et al. (1999), p. 276. "One important point should be made immediately, however: *experiments with many subjects are better able to detect differences among the effects of the treatments than similar experiments with fewer subjects*." (emphasis in original).

> experimental units or subjects to allow the systematic effects of the treatments to be seen." (emphasis in original)

Babbie (2010) also discusses in a general example of sample size selection how "[o]bviously, it wouldn't be a very good idea to select a sample of only one, because the chances are great that we'll miss the true mean [] by quite a bit… The progression of sampling distributions is clear. Every increase in sample size improves the distribution of estimates of the mean.… The larger the sample selected, the more accurate it is as an estimation of the population from which it was drawn."[69]

47. Certain statements in the [redacted] Report make clear that Mr. [redacted] has effectively taken this unsupportable approach, akin to a survey of himself. For example, Mr. [redacted] states, "*[b]ased on my experience investing in digital assets*, a reasonable purchaser of XRP would understand that if Ripple's ambitious cross-border payment business were successful, the ensuing demand for XRP would tremendously increase the price of XRP."[70] That opinion is not grounded in any scientifically recognized methodology.

48. Evaluating Mr. [redacted] approach in this way demonstrates that it is unreliable and unscientific for a variety of reasons, some of which include:

a. Mr. [redacted] is aware of the purpose and sponsor of the study as well as the desired outcome for the sponsor, thus the "survey" is "double-non-blind," as opposed to the gold-standard "double-blind" approach. The importance of double-blindness of a study has been well-documented in the literature:

> One way to protect the objectivity of survey administration is to avoid telling interviewers who is sponsoring the survey.

[69] Babbie (2010), pp. 201-202.

[70] [redacted] Report, ¶24, emphasis added. See also [redacted] Report, ¶88. "*Based on my professional experience in the blockchain space, in part as an investor and trader in digital assets*, as well as my analysis of the public statements, documents, and design decisions of Ripple, I am able to reach the following findings and conclusions" (emphasis added).

> Interviewers who know the identity of the survey's sponsor may affect results inadvertently by communicating to respondents their expectations or what they believe are the preferred responses of the survey's sponsor. To ensure objectivity in the administration of the survey, it is standard interview practice in surveys conducted for litigation to do double-blind research whenever possible: Both the interviewer and the respondent are blind to the sponsor of the survey and its purpose. Thus, the survey instrument should provide no explicit or implicit clues about the sponsorship of the survey or the expected responses. Explicit clues could include a sponsor's letterhead appearing on the survey; implicit clues could include reversing the usual order of the yes and no response boxes on the interviewer's form next to a crucial question, thereby potentially increasing the likelihood that no will be checked.[71] (Diamond (2011))
>
> A double-blind experiment guards against experimenter bias, because neither the experimenter nor the subject knows which subjects are in the control group(s) and which in the experimental group(s).[72] (Babbie (2010))
>
> Experimenters must take great care to deal with all experimental units or subjects in exactly the same way, so that the treatments are the only systematic differences present. Unequal conditions introduce bias . . . . [An] experiment should therefore be double-blind.[73] (Yates, et al. (1999))
>
> With double blinding, neither the study object (e.g., a patient) nor the implementer of the treatment is aware of which group the study object is assigned to. If participants in the experiment know which treatment was given to the subjects, their behavior may be affected, which may bias the estimate of the treatment effect from the experiment.[74] (The Royal Swedish Academy of Sciences (2021))

b. The sample size of one is insufficient as discussed above.[75]

---

[71] Diamond (2011), at pp. 410-411.

[72] Babbie (2010), p. 250.

[73] Yates, et al. (1999), pp. 277-278.

[74] The Royal Swedish Academy of Sciences (2021), p. 7, footnote 7.

[75] See, for example, Yates, et al. (1999), p. 276; Babbie (2010), pp. 201-202.

c. As discussed above, the target population consists of "all elements (i.e., individuals or other units) whose characteristics or perceptions the survey is intended to represent."[76] It is not clear whether Mr. [redacted] is in the relevant target population, which based on Mr. [redacted] report would be "individuals, institutional investors, and financial services companies,"[77] for two reasons:

   i. First, he does not specify whether he ever purchased or considered purchasing XRP or sufficiently similar digital assets personally;

   ii. Second, even if Mr. [redacted] did have that experience, he provides no basis to suggest that he has any experience on which to describe how "institutional investors" or "financial services companies" would view at-issue "statements, actions, and product offerings."

d. There is no control group in Mr. [redacted] approach, *not* exposed to the at-issue conduct, thus it is impossible to separate the impact of the conduct on purchaser "perspective" from preexisting beliefs and other potential influences.[78] Mr. [redacted] "analysis" does not allow him to separate the supposed impact of Ripple's conduct on the purchaser "perspective" from other potential influences such as preexisting beliefs (e.g., based on general principles of economics).

e. Mr. [redacted] does not mention whether he was exposed to any of the alleged Ripple conduct prior to being retained as an expert in this matter and whether he purchased XRP as an "investment" as a result of such exposure.

---

[76] Diamond (2011), at p. 376. (See also footnote 37 above).

[77] [redacted] Report, ¶2.

[78] For example, Diamond (2011) notes that "[w]ithout the control group, it is not possible to determine how much of the [outcome] is attributable to respondents' preexisting beliefs or other background noise (e.g., respondents who misunderstand the question or misstate their responses)." Diamond (2011), at pp. 397-399.

49. Each of these defects is independently fatal to Mr. [redacted] analysis from a scientific perspective. Accordingly, it is my opinion that Mr. [redacted] report lacks any valid methodology, rendering its conclusions unreliable.

I declare under penalty of perjury that the foregoing is true and correct. Executed on November 12, 2021

Kristina Shamp anier

Appendix A – Curriculum Vitae

KRISTINA S. SHAMPANIER, PH.D.
Senior Vice President

T: +1 617 372 4928
kshampanier@compasslexecon.com

55 South Lake Avenue, Suite 650
Pasadena, CA 91101

Dr. Shampanier is an expert in consumer behavior and survey and experiment design. She has over 15 years of experience in designing, conducting, and analyzing lab, field, and online studies in academic, consulting, and litigation settings, as well as evaluating studies carried out by others. She has worked on class action, false advertisement, consumer safety, trademark, trade dress, and patent infringement cases, as well as antitrust and healthcare matters. These cases span a wide variety of industries, including consumer products, banking, high tech, online retail, entertainment, hospitality, luxury, and auto industries. Dr. Shampanier has published in peer-reviewed journals in the fields of mathematics and marketing.

EDUCATION

2007	Ph.D., marketing (management science), MIT Sloan School of Management *Dissertation*: "Essays in Behavioral Decision Making"
2002	M.A., economics (*cum laude)*, New Economic School, Moscow, Russia *Thesis*: "Branding"
2001	M.S., mathematics (*cum laude*), Moscow State University *Specialization*: Algebra *Thesis*: "Ranks of Subalgebras of Free Non-Associative Algebras"

EXPERIENCE

2005–2021	Compass Lexecon *Senior Vice President (2021–Present)*
2005–2021	Analysis Group Inc. *Consultant (2020–2021)* *Vice President (2016–2020)* *Manager (2009–2015)* *Associate (2007–2009)* *Intern Associate (2005)*

2003–2007 MIT Sloan School of Management
Research Assistant, Professor Dan Ariely (2003–2007)
Teaching Assistant, Consumer Behavior, Professor Yehoshua Tsal (2005–2006)
Teaching Assistant, Managerial Psychology Laboratory, Professors Tom Allen and Dan Ariely (2003–2005)

2002 New Economic School, Moscow, Russia
Teaching Assistant, Econometrics III, Professor Stanislav Anatoliev

SELECTED EXPERT CASEWORK

- **Household chemicals false advertising class action**
  Conducted conjoint analysis survey and market simulations to evaluate the price premium associated with a challenged advertising claim on behalf of the defendants. Submitted a letter to counsel and expert declaration describing the methodology and results. The findings were used by counsel at mediation negotiations to evaluate potential range of damages. The case settled after one day of mediation.
  Conducted similar analysis for a related case involving an allegedly omitted warning. Submitted a letter to counsel and expert declaration.

- **Beauty products trademark infringement**
  Designed an experiment/survey to test for consumer confusion in a trademark infringement matter involving a beauty product for the defendant (applicant) before the Trademark Trial and Appeal Board of the US Patent and Trademark Office. Filed an expert report, after which the opposer withdrew all oppositions.

- **Banking false advertising class action**
  Conducted an online survey in the choice experiment format on behalf of the defendant to evaluate whether the allegedly misleading omission had an impact on consumer purchase decisions.

- **Fast food employment litigation**
  Evaluated the possibility of interviewing class members and reviewed the opposing expert's approach on behalf of the defendant, a fast-food chain.

- ***A.R., by and through Her Next Friend, Susan Root, et al., v. Elizabeth Dudek, in Her Official Capacity as Secretary of the Agency for Health Care Administration, et al.*** **and** ***United States of America v. The State of Florida***
  US District Court, Southern District of Florida
  Evaluated on behalf of the defendant a set of unscripted interviews conducted by the plaintiffs' expert in a health care case involving preferences of patients' families. Submitted rebuttal expert report and was deposed.

- **Hospitality business trademark infringement**
  Designed and fielded an "Eveready" experiment/survey to test for consumer confusion in a trademark infringement matter in the hospitality business for the defendant (registrant) before the Trademark Trial and Appeal Board of the US Patent and Trademark Office.

- **Electronics false advertising**
  Submitted three reports on behalf of the challenged party in a case considered by the National Advertising Division of the Council of Better Business Bureaus. Opined on the merits of the design of a consumer electronics product test conducted for advertising claims.

SELECTED CONSULTING EXPERIENCE

Intellectual Property

- **Trademark and trade dress infringement matters**
  Developed numerous online experimental design surveys in the "Eveready" and "Squirt" format and rebuttal analyses of "Eveready" surveys testing consumer perception and confusion with respect to wordmarks, design marks, trade dress, and an advertising slogan in a variety of cases, including in clothing, compliance, food, fashion, auto, luxury goods, entertainment, outdoor activities, and music industries. Addressed issues of materiality (via a choice experiment survey and open-ended purchase driver survey), dilution, and secondary meaning. Assisted experts in survey design, implementation, and analysis of surveys, as well as in drafting reports and preparations for depositions. Assisted counsels with preparation for depositions of opposing experts. Such cases include:

  - ***Denimafia Inc. v. New Balance Athletic Shoe, Inc. et al.*** **and** ***New Balance Athletic Shoe, Inc. v. Denimafia Inc.***
    US District Court, Southern District of New York
    Supported Professor Joel Steckel, who was retained by New Balance, the defendant and counter-claimant in a trademark infringement mater involving the "less is more" <=> symbol used on New Balance Minimus footwear. Assisted Professor Steckel in designing, fielding, and analyzing an "Eveready" survey/experiment testing for reverse confusion (i.e., confusion with respect to the source, sponsorship, or affiliation of Denimafia products), drafting report, and preparation for deposition. In its summary judgment in favor of New Balance, the court credited Professor Steckel's survey with showing "a zero percent rate of reverse confusion with respect to the source of jeans bearing the <=> mark" and discounted Denimafia's objections to the survey design. Denimafia appealed the summary judgment decision, but ultimately did not pursue the appeal and the appellate court dismissed it.

  - **Luxury goods trademark infringement and dilution matter**
    Developed an online experimental design survey to test whether consumers noticed and how they perceived a logo briefly appearing in a TV commercial. Evaluated opposing expert's survey. Assisted expert in survey design, implementation, and analysis of survey; developing rebuttal points for opposing expert's survey; drafting reports; and preparation for depositions; assisted counsel in preparation for deposition of opposing expert.

- **Smartphone and tablet patent infringement matters**
  Assisted experts in survey design, report drafting, and preparation for deposition and trial testimony. Evaluated opposing expert's surveys (including a conjoint-style survey) aimed at isolating the value to consumers of the patented features in smartphones. Assisted counsel with preparation for and at depositions of opposing expert and data witnesses. Assisted at trial.

  - ***Hitachi Maxell, Ltd. v. ZTE Corp. and ZTE USA Inc.***
    US District Court, Eastern District of Texas, Texarkana Division
    Supported Tülin Erdem, Professor of Business and Marketing at the NYU Stern School of Business, from case inception to trial on behalf of Maxell and Mayer Brown. Assisted in designing and implementing a survey of smartphone and tablet owners to assess the awareness and relative importance of a feature disclosed in one of the asserted patents: automatic GPS map orientation. The damages expert used the survey results to inform her

analysis of reasonable royalty damages. The jury found that the asserted patents were valid and infringed by ZTE, and awarded Maxell damages of $43.3 million.

False Advertising

- ***Kenneth Hobbs v. Brother International Corporation***
  US District Court, Central District of California
  Supported Professor Joel Steckel of New York University Stern School of Business in conducting two surveys on behalf of Brother International Corporation, the defendant in a consumer class action false advertising case. The plaintiff claimed that the printers at issue did not scan complete pages, causing the edges of images to be truncated. One survey evaluated consumer awareness of a printer's alleged malfunctioning. The other, a survey/experiment, addressed the materiality of this limitation to consumers. In its order denying class certification, the court cited the experiment involving more than 450 people who had purchased or planned to purchase a printer close to the time of the survey, which found that "consumers chose the Brother printer with nearly identical frequency regardless of whether they were made aware of the unscannable margin at the time of their selection." The plaintiff agreed to dismiss his case with prejudice and waive his right to appeal. Assisted Professor Steckel with design, implementation, and analysis of the studies; drafting reports and declarations; and preparation for deposition.

- **E-Retailer false advertising matter**
  Supported Professor Joel Steckel in conducting two experiments on behalf of a major e-retailer accused of using misleading reference price terms (e.g., "Compare at"). In the first study, groups of consumers visiting the defendant's website were randomly assigned to view the reference price labels as either "MSRP" (manufacturer's suggested retail price) or "Compare" throughout their shopping session and subsequent website visits. No difference in the sales conversion rate was found. Further, a survey of consumers who made purchases during the study period showed no difference in recall of the product price, the reference price, or the term used with the reference price. The second study, conducted with an online consumer panel, found that consumers' understanding of reference prices did not depend on the label used (e.g., "was," "compare at," "compare," and "MSRP"). Assisted in design, implementation, and analysis of both studies, and in preparation of deposition and trial testimony.

- **Online services false advertising matter**
  Evaluated opposing experts' surveys testing consumer perception of charges for an online service. Assisted in drafting report and counsel's briefs, as well as in preparation for depositions. Assisted counsel in preparation for depositions of opposing experts.

- **Cigarette false advertising matter**
  Evaluated opposing counsel's survey-like methodology to evaluate consumer perception of cigarette packaging. Assisted expert in drafting declarations and report.

Corporate Acquisitions

- **AT&T's acquisition of DIRECTV – survey of consumer preferences**
  Supported Professor Ravi Dhar of the Yale School of Management in developing, conducting, and analyzing a survey examining consumer attitudes toward bundled Internet and television services, in a case widely covered by the media. AT&T and DIRECTV cited the outcome of the study in their applications to the Federal Communications Commission (FCC), pointing to the benefit to consumers

when Internet and television services are delivered by the same provider. The FCC and the Department of Justice approved the acquisition. Assisted Professor Dhar in survey design, implementation, and analysis, as well as report drafting.

Antitrust

- **Microsoft antitrust matters**
  - ***Jim Hood, Attorney General ex rel. State of Mississippi v. Microsoft Corporation***
    Chancery Court of Hinds County, Mississippi
  - ***Pro-Sys Consultants Ltd. and Neil Godfrey v. Microsoft Corporation and Microsoft Canada Co./Microsoft Canada CIE***
    Supreme Court of British Columbia

  Developed affirmative damages analysis and rebuttals of the plaintiffs' damages analysis and class certification arguments in the cases involving allegations of Microsoft's overcharging consumers for its operating systems, word processors, and spreadsheet products.

- **Credit cards antitrust matter**
  Developed an online experimental design survey to expose issues with opposing expert's survey testing consumer reaction to retailers' potential credit card policies. Assisted expert in survey design, implementation, and analysis preparation of report; and in preparation for and at deposition. Assisted counsel in preparation for deposition of opposing expert.

- **High tech antitrust matters, including *Advanced Micro Devices, Inc. v. Intel***
  US District Court, District of Delaware
  Analyzed incremental costs for price/cost analysis. Assisted in data production and analysis, drafting reports, deposition preparation, and at deposition.

PUBLICATIONS

"Choice Experiments," with Joel Steckel, Rebecca Kirk Fair, and Anne Cai in *Legal Applications of Marketing Theory*, Cambridge University Press, Jacob Gersen and Joel Steckel, eds., 2021, forthcoming

"Patient Quality of Life and Benefits of Leptin Replacement Therapy (LRT) in Generalized and Partial Lipodystrophy (GL, PL)," with Omer Ali, Keziah Cook, Edward Tuttle, Charles Gerrits, and Rebecca Brown, *Diabetes*, Vol. 61, Supplement 1, 1331-P, 2018

"How To Interpret A Contract? Ask Those Who'd Sign It," with Omri Ben-Shahar, Lior Strahilevitz, Duo Jiang, and Rebecca Kirk Fair, *Law360*, March 21, 2018

"Survey And Real-World Data: A Winning Combination," with Peter Simon, Riddhima Sharma, and Rebecca Kirk Fair, *Law360*, July 2017

"What Consumers Really Think about Reference Price Labels," with Rebecca Kirk Fair, Laura O'Laughlin, Jesse Shea, and Joel Steckel, *Law360*, May 2017

"Probabilistic Price Promotions – When Retailing and Las Vegas Meet," with Dan Ariely and Nina Mazar, *Management Science,* Vol. 63, No. 1, pp. 250-266, 2016

"Zero as a Special Price. The True Value of Free Products," with Dan Ariely and Nina Mazar, *Marketing Science*, Vol. 26, No. 6, pp. 742-757 (lead article), 2007

"How Small Is Zero Price? The True Value of Free Products," *Advances in Consumer Research,* Vol. 33, pp. 254-255, 2006

"Algorithms Realizing Rank and Primitivity of Systems of Elements of Free Non-Associative Algebras," *Fundamental and Applied Mathematics*, Vol. 6, No. 4, pp. 1229-1238, 2000

SELECTED PRESENTATIONS, POSTERS, AND SPEAKING ENGAGEMENTS

"Discrete Choice and SF-36 Estimates of Patient Quality of Life and Benefits of Leptin Replacement Therapy (LRT) in Generalized and Partial Lipodystrophy (GL, PL)," poster with Omer Ali, Keziah Cook, Don Lee, and Edward Tuttle, 21st European Congress of Endocrinology, Lyon, France, May 2019

"Surveying the Truth: False Advertising and Trademark Litigation," with August Horvath and Joel Steckel, first webinar in the series, *Deceit and Denial: The Role Surveys Play in False Advertising and Trademark Litigation*, American Bar Association's Section of Antitrust Law Advertising Disputes & Litigation Committee, February 2016

"Listening to Customers – How to Ask the Right Question, Surveys in Litigation," recurrent lecture at Professors Jiwoong Shin and Aniko Oery's M.B.A. classes*, Listening to the Customer*, Yale School of Management, 2012, 2013, 2015, and 2016

"How Small is Zero Price? The True Value of Free Products," Association for Consumer Research, North American Conference, San Antonio, TX, and London Business School, 2005

PROFESSIONAL ASSOCIATIONS AND MEMBERSHIPS

- American Marketing Association
- *Marketing Science* "Ambassador" (until 2018)

ACADEMIC HONORS

2005–2006	The Zannetos Fund Fellow, Massachusetts Institute of Technology
2005–2006	The Stuart Fund Fellow, Massachusetts Institute of Technology
2006	AMA-Sheth Foundation Doctoral Consortium Fellow
2004–2005	MasterCard Fellow, Massachusetts Institute of Technology
2003	The Russell Sage Summer Institute, Trento, Italy
2002–2003	DuPont Fellow, Massachusetts Institute of Technology

LANGUAGES

Russian (native), French (intermediate)

Appendix B – Materials Considered

Court Documents

- Answer of Defendant Ripple Labs, Inc. to Plaintiff's Complaint, *Securities and Exchange Commission v. Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larsen*, 20-cv-10832 (AT), United States District Court, Southern District of New York, January 29, 2021.
- Answer of Defendant Ripple Labs, Inc. to Plaintiff's First Amended Complaint, *Securities and Exchange Commission v. Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larsen*, 20-cv-10832 (AT), United States District Court, Southern District of New York, March 4, 2021.
- First Amended Complaint, *Securities and Exchange Commission v. Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larsen*, 20 Civ. 10832 (AT), ECF Case, United States District Court, Southern District of New York, February 18, 2021.
- Expert Report of [redacted] October 4, 2021, *U.S. Securities and Exchange Commission v. Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larson*, United States District Court, Southern District of New York.
- *Securities and Exchange Commission v. W. J. Howey Co. et al*, No. 328 U.S. 293, Supreme Court of the United States, 1946.

Academic Articles and Books

- Assael, Henry. *Consumer Behavior, A Strategic Approach*. Houghton Mifflin Company, 2004.
- Babbie, Earl. *The Practice of Social Research*. Twelfth Edition. Wadsworth Cengage Learning, 2010.
- Diamond, Shari, S. "Reference Guide on Survey Research." *Reference Manual on Scientific Evidence*. Third Edition. Federal Judicial Center, 2011, pp. 359-423.
- Hague, et al. *Market Research in Practice*. Kindle Edition, Third Edition. Kogan Page, 2016.
- Hibberts, Mary, R. Burke Johnson, and Kenneth Hudson. "Common Survey Sampling Techniques." *Handbook of Survey Methodology for the Social Sciences*. Ed. Lior Gordon. Springer, 2012.
- Jacoby, Jacob, and Lynda Zadra-Symes. "Legal Issues That Can Be Examined via Surveys." *Trademark Surveys: Volume 1: Designing, Implementing, and Evaluating Surveys*. Jacob Jacoby. ABA Book Publishing, 2013.
- Meyer, Bruce D. "Natural and Quasi-Experiments in Economics." *Journal of Business & Economic Statistics* 13(2): 151-161, April 1995.
- Shadish, William R., Thomas D. Cook, and Donald T. Campbell. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Wadsworth Cengage Learning, 2002.
- Yates, Daniel, David Moore, and George McCabe. *The Practice of Statistics*. First Edition. W.H. Freeman, 1999.

Other Publicly Available Materials

- The Royal Swedish Academy of Sciences. "Scientific Background on the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2021 - Answering Causal Questions

Using Observational Data," available at https://www.nobelprize.org/uploads/2021/10/advanced-economicsciencesprize2021.pdf.

- The Royal Swedish Academy of Sciences. "The Prize in Economic Sciences 2019," available at https://www.nobelprize.org/uploads/2019/10/press-economicsciences2019-2.pdf.

Appendix C – Examples of Mr. [redacted] Unsupported Causal Propositions

¶	[redacted] Statement (Unsupported conclusion bolded)	Section
8	Based on my experience in the digital asset space, I conclude that a **reasonable purchaser would have had an expectation** of future profit derived from the efforts of Ripple. Specifically, **purchasers would have expected or hoped to profit by later re-selling their XRP at a higher price on a secondary market** after XRP substantially increased in value […]Although **Ripple's development of the blockchain and broader XRP ecosystem, along with its promotion of the bull case for buying XRP**, would not guarantee a profit, it **would create the hope that a purchaser could passively earn profits by owning XRP** while Ripple took steps to increase the value of the coin.	2. Summary of findings
9	there are certain elements in Ripple's and its founders' design of XRP, the XRP Ledger, and a variety of software products that **appealed more to a purchaser of XRP interested in making a profit than to financial institutions seeking to embrace Ripple's stated vision of utilizing XRP as a bridge asset for cross-border asset transfers**	2. Summary of findings
24	Based on my experience investing in digital assets, a **reasonable purchaser of XRP would understand that if Ripple's ambitious cross-border payment business were successful, the ensuing demand for XRP would tremendously increase the price of XRP**.	5. Features of XRP Coin Economics and Suitability as a Bridge Asset
26	**Potential purchasers of XRP would have understood the simple economics behind the message being promoted by Ripple on this subject: XRP, as designed, provided a mechanism for passive XRP owners to benefit financially from Ripple's success** as a provider of financial service products built on the XRP Ledger, as a developer of the XRP ecosystem, and as a driver of demand for XRP.	5. Features of XRP Coin Economics and Suitability as a Bridge Asset
31	The correlation between the success of the platform and price of the coin is fantastic for investment-oriented purchasers of XRP, but not for the purchasers who are exclusively interested in the utility use of the cross-border payment product. **From the perspective of a reasonable investment-oriented purchasers, the fixed-supply and variable-price model provides a direct link between 1) the success of Ripple's efforts to build the XRP ecosystem and stimulate demand for XRP and 2) the financial performance of the purchaser's investment in XRP. From the perspective of a utility-oriented purchaser, as discussed above, the fixed-supply and variable price model of XRP presents significant disadvantages**	5. Features of XRP Coin Economics and Suitability as a Bridge Asset

37	These points would **appeal to an individual purchaser with a long-term investment mindset,** and were repeatedly communicated by Ripple in the XRP Markets Reports.	6. XRP Sale and Escrow Mechanics
43	Although Ripple continued to sell XRP into the open market on a regular basis, this **significant restriction of the XRP supply would have greatly encouraged potential investment-oriented purchasers of XRP to earn a speculative investment profit with their purchase**.	6. XRP Sale and Escrow Mechanics
47	**Although the buyback activity would not have mattered to purely utility-oriented purchasers of XRP, buybacks are very important signals for investment-oriented purchasers**.	6. XRP Sale and Escrow Mechanics
48	The manner and mechanism of Ripple's ongoing sales, distribution, escrow, and **buybacks of XRP would have been extremely important to a potential investment-oriented purchaser of XRP**	6. XRP Sale and Escrow Mechanics
49	On the other hand, a **reasonable purchaser of XRP that is exclusively considering the utility use of the coin would be less concerned with some of these heavily promoted sales and distribution mechanisms.**	6. XRP Sale and Escrow Mechanics
65	Another type of partnership that **would have appealed to a purchaser interested in the investment use case for XRP** was solidified by an agreement between Ripple and a provider of retirement investment accounts. Ripple announced that purchasers could buy XRP through Bitcoin IRA's retirement accounts.	7. Ripple Communications and Promotional Statements
85	Ripple's extensive public comments and reports about these topics likely served to **inform and persuade investment-oriented purchasers** about the potential reward of purchasing XRP for the purpose of generating a profit. Indeed, the **use of terms such as "traction," "market fit," "total addressable market," and even "investors" when describing Ripple's progress and growth potential are words typically understood by market participants to mean that they should view buying XRP as a potentially profitable investment**.	7. Ripple Communications and Promotional Statements
86	Purchasers of XRP for cross-border payments would also be **interested in some of these topics, but not all**. For example, a money transmitter **likely cares deeply** about specific topics like the liquidity of the digital asset trading platforms it needs to rely on to complete an ODL transaction, but **is less interested** in Ripple's communications about the bull case for the price of XRP.	7. Ripple Communications and Promotional Statements
87	It is my opinion from carefully following the digital asset space that **many of Ripple's public communications conveyed to reasonable purchasers of XRP an expectation of future profit derived from the efforts of Ripple**.	7. Ripple Communications and Promotional Statements

89	Over the course of the Issuance Period a **reasonable purchaser of XRP would have had an expectation of generating profit** based on the efforts of Ripple and its management to accomplish the growth strategies that Ripple advertised to the public as being already achieved or planned for the future.	8. Summary of Findings and Conclusions
89	Given this relationship between Ripple's performance and the price of XRP, a **reasonable purchaser would have closely considered many factors** that were publicized by Ripple such as disclosed partnerships with financial institutions, the quality of Ripple's management team, the target addressable market for Ripple's products, and the availability of liquidity on trading platforms for XRP.	8. Summary of Findings and Conclusions
90	**Certain aspects of the design characteristics of XRP and the promotional activity of Ripple did not appeal to a pure utility use case.**	8. Summary of Findings and Conclusions