



# R3 Review: Ripple Labs

Considerations for Adoption by Large Financial Institutions (May 2015)

---

Jo Lang, Platform & Research, R3 CEV

*Companion to Peter Todd's "Ripple Protocol Consensus Algorithm Review"*



## Introduction

At R3 we are focused on building industry partnerships based on the premise that emerging technologies such as blockchains and distributed ledgers will positively transform the current industry-operating model. These technologies have the potential to deliver the benefit of improved security, controlled transparency and accessibility to both regulators and customers globally, while also substantially reducing costs and complexity for financial institutions. Conducting in-depth evaluations of the risks and benefits of existing solutions is a critical part of this approach.

Ripple Labs was a natural choice for our inaugural evaluation, as they have emerged as an early leader in the crypto-technology space, offering a production platform for lower cost global payments and settlement. Ripple has also focused on partnership rather than competition with existing financial institutions looking to improve transaction processes and gain efficiencies. As part of R3's due diligence on the public Ripple network, we partnered Peter Todd to complete a [technical review](#) of the Ripple Protocol Consensus, which has provided the foundation for the findings below.

This companion paper begins with a brief summary of the Ripple solution, including a description of the role of the native currency (XRP). The paper also highlights some areas of concern that large financial institutions should consider if they were to participate at scale on the public Ripple network. These include:

- The role of the Unique Node List (UNL) and risks to increased centralization of validation via default UNL usage
- Software conflict concerns due to the Ripple protocol not splitting out the consensus-critical codebase (validation) from the non-critical codebase (user software)
- Potential misalignment of incentives or risks with any increased reliance on the native currency (XRP)
- Unclear incentive structure for non-Ripple Labs validating nodes to join the network

Some of the above areas of concern are not unique to the Ripple consensus protocol or platform, yet they are still key considerations for financial institutions to evaluate closely. Further, when taken as a whole, the risks and indirect incentives discussed in this and the companion paper have the potential to position Ripple Labs as a new trusted third party within the global payments landscape.

## Overview of Ripple Labs

### The Solution

**Ripple Labs defines the Ripple network as a “Federated Payments System”** which leverages cryptographic methods in order to secure, validate, and record transactions.<sup>i</sup> The drivers to integrate with Ripple's solutions are the need to decrease costs per transaction, particularly cross-border transactions, and to increase transparency across the financial services industry. Unlike Bitcoin and other cryptocurrencies, Ripple is openly not trying to disrupt banking, but rather upgrade traditional payment and settlement solutions. Their focus is on building a solution that accurately represents assets and liabilities issued by identifiable issuers and enables real-time efficient transfer and settlement globally.



**Three things set Ripple apart from current settlement solutions: cost, speed, and ubiquity.** Aside from the small amount of XRP destroyed with each trade, there are no fees or added margins for currency exchanges on the Ripple protocol. This means that each trade has one buyer, one seller, and one price. The Ripple ecosystem is comprised primarily of users, asset custodians (gateways), and market makers. We have begun to see the emergence of newer payments solutions and products that have built on top of the Ripple network to leverage their settlement solution. Saldo.MX enables people in the U.S. to pay bills and buy prepaid cards in Mexico, while Shift Payments allows users to spend digital currencies, gold, and regular money - all with the Shift debit card.<sup>ii</sup>

## XRP

**Ripple defines XRP as a 'math-based currency' which represents value of assets on the ledger.** Ripple uses XRP in order to move value across the network and facilitate real-time atomic transaction settlement. This eliminates settlement risk and minimizes counterparty risk between trusted parties. In order to do this, Ripple represents counterparties' liabilities ("or IOUs") on the ledger. The network will then use XRP to facilitate the transfer of assets across the ledger.

**XRP acts as an anti-spam mechanism.** In order to initiate transaction processing on the network, which is public, a minimum amount of XRP expenditure is required. As the number of transactions on the network increases, so does the XRP requirement. This is in place to deter bad actors from flooding the network. For FX transactions, according to Ripple Labs, **XRP will act as a 'bridge currency' for illiquid currency pairs**, thereby removing the need for correspondent banking partners in order to complete a transaction.

## Identified Areas of Concern

### Unique Node List (UNL)

**In practice not all unique network participants (nodes) are guaranteed to adopt the same Unique Node List.** If more than 20% of nodes within the network do not agree with the majority, this will force a consensus split, forcing the ledger to fork, generating multiple versions of the ledger. Not only will this create issues of version control among participants but also could potentially result in Denial of Service (DoS) or theft via undetected double spending.

Even within a private network of financial institutions, there is great variability among transaction settlement requirements. Financial institutions will want to set up transaction validators that are guaranteed to meet their unique institutional standards and requirements. Even for institutions that collectively determine transaction settlement requirements, the risk for consensus split remains. Asynchronous software updates among participants will force inconsistent UNLs, this risk is exacerbated for users, such as Financial Institutions, who would host custom implementations, and do not follow standard release cycle. It must be noted that to-date, almost all cryptocurrency consensus splits have occurred unintentionally.

To minimize risk of consensus split, Ripple Labs recommends adoption of their default UNL. This creates a **highly centralized system architecture** where currently all validators are operated and maintained



internally by Ripple Labs. This model would force financial institutions to rely on a third-party for transaction validation where they have little to no visibility. This is especially risky as there is potential for incentive misalignment between institutions and Ripple Labs.

**Takeaway:** *The risks of a consensus split, whether intentional or not, are not unique to Ripple. With proper monitoring in place, the potential negative impact for most scenarios is relatively low. Users' risk tolerance and unique requirements would determine the mitigation strategy. However, the highly centralized model that the Ripple Network encourages fails to eliminate any need for a trusted third party but rather creates a new type of trusted third party. This is especially risky, as there is potential for incentive misalignment between institutions and Ripple Labs.*

## Software

**As of publication, the primary implementation of the Ripple protocol does not distinguish between the consensus-critical codebase (validation) and the non-critical codebase (user software).** In order to accommodate variable transaction types and requirements, the protocol is complex and all functionality has been coded directly into the protocol layer itself. **As a result, any upgrade to Ripple user software will alter the consensus-critical codebase.** This also means that any changes such as those made to address bugs will alter the consensus-critical codebase and as a result will alter the Unique Node List. Participants who choose to host custom implementations of the Ripple protocol must consider that they will miss out on any positive changes that Ripple makes to their protocol and will have to rely on Ripple for timely notification. Financial institutions looking to implement Ripple's solution will need to look at a custom solution in order to accommodate significant and unique user requirements.

**Takeaway:** *Distinct requirements among participating institutions heighten the probability for consensus split, generating multiple ledgers with differing transaction information. As Ripple looks to integrate with more complex financial institutions, it will be critical that they take measures to eliminate these software risks. Ripple's not-yet-released Gateway Protocol promises to begin to address these risks.*

## Reliance on XRP

**Incentive misalignment between network participant nodes (financial institutions) and Ripple Labs is a major risk factor due to the central role of XRP in performing transactions.** Ripple Labs still holds the majority of XRP, and it is in their favor for its value to increase. Ripple justifies XRP as an 'anti-spam mechanism' to deter transactions. It acts as a transaction fee where the fee amount is adjusted based on the value of XRP at that time. Theoretically, participants need to hold a minimal amount of XRP in order to pay the transaction fee required. However, as the volume of transactions increases the server load, transaction speed is slowed while the cost of the transaction and the amount of required XRP continues to increase. At a certain point, this will force validators out of the network who are unable or unwilling to pay the required fees. It is critical to note that Ripple's internal validators will never be priced out of the system. In the event of a transaction flood, Ripple is inclined to let it continue because



the **increased economic activity increases the value of their holdings**. As a result, this raises key AML concerns as Ripple would not be incentivized to report suspicious economic activity.<sup>iii</sup>

**Takeaway:** *XRP is an unregulated store of value, backed by Ripple Labs, and this generates a significant imbalance of network influence in favor of a non-bank entity. Furthermore, their business model is heavily reliant on the value of XRP, raising key questions about liability and risk tolerance of participating financial institutions.*

## Incentive Structure

**There seems to be no clearly defined validator incentive structure for non-Ripple validators.** This would include validation nodes chosen by financial institutions. Due to the lack of incentive, the number of public validators is limited, and this encourages the same highly, centralized system architecture as Ripple's default Unique Node List (UNL). A clearly defined incentive structure would not only promote honest validation but also deter bad actors from dishonest validation. Furthermore, as it stands today, the cost for validators to hijack the system is minimal but could have powerful, negative consequences on network participants. Validators could be able to block a valid transaction or simulate a ledger in order to enable double spending. The power of social consensus is another cause for concern as validators have the ability to decide to reverse monetary losses in order to undo the impact of major theft. Given that proprietary validators perform majority of validation on the Ripple Network, this **places a significant amount of decision-making power in the hands of a third-party**.

**Takeaway:** *The lack of validator incentive structure encourages a highly, centralized system architecture. Whether or not the validator incentive structure is a major risk will depend on how the participants choose their Unique Node List (UNL). If users decide to implement custom nodes, for example between trusted institutions, incentives would be defined within the context of the counterparty agreements. However, if participants choose to adopt Ripple's default UNL, they will be placing a significant amount of trust in the hands of another non-bank third party.*

## Security

*At the time of publication, information regarding Ripple Labs operational security practices is unavailable. The following points are based on publicly available information and observations.*

Currently master codebase is hosted by 3<sup>rd</sup> party (GitHub) and Ripple does not require PGP signatures for ` minimal ability to audit who wrote and committed what code. At this time, Ripple does not have a formal validator onboarding process nor do they offer a secure method to download their software, which has previously lead to significant monetary losses. Today, unless there is a validation from a trusted party, such as Ripple or Blockchain.Info, users are unable to validate that they are in fact downloading the Ripple validator software. However, this in turn means that if Blockchain's security and validation is compromised than there is no guarantee for the user that the software is legitimate. In March 2014, this resulted in users' losses totaling \$100K. The loss could have been avoided if Ripple had PGP signatures for committed code.



**Takeaway:** *We do not believe that the issues outlined above are unique to Ripple, but they do require careful consideration.*

## Conclusion

As noted in our introduction, some of the risks laid out above are not unique to the Ripple consensus protocol and may be mitigated over time by improvements to the platform. Yet, in its current form, there are unique aspects of the protocol that could lead to Ripple Labs emerging as a new trusted third party in bilateral settlement. Namely:

1. The potential for Unique Node Lists to trend to a centralized model
2. Possible misalignment of incentives or risks with any increased reliance on the native currency (XRP)

Financial institutions looking at potential adoption of Ripple's solution should evaluate the identified risks against the benefits for a new payment and settlement network, including but not limited to increased transaction processing speed, increased currency interoperability and overall decreased costs.

---

<sup>i</sup> "Federation Protocol", Ripple Labs Wiki,

<sup>ii</sup> Ripple Labs, <http://ripple.com>, 2015

<sup>iii</sup> As of May 5th, 2015, FinCen announced that they would hit Ripple Labs with a \$700,000 USD civil penalty fine and specifically cited Ripple for failure to report suspicious transactional activity.

## About R3

R3CEV LLC (“R3”) is an innovation firm focused on building and empowering the next generation of global financial services technology. We leverage our members’ decades of experience and deep networks within the financial services community to empower innovators, promote industry collaboration and affect positive market transformation on a global scale. R3 operates three primary integrated business disciplines: Crypto 2.0, Exchanges, and Ventures. R3 Crypto 2.0 focuses on intelligent applications of cryptographic technology and distributed ledger-based protocols within global financial institutions and markets. R3 Exchanges creates and introduces innovative new execution solutions which redefine the trading experience for existing and evolving asset classes. R3 Ventures makes targeted early stage investments in forward thinking companies that seek to shape the next generation of financial services.

R3’s Crypto 2.0 team is deeply integrated within the global crypto-technology ecosystem and seeks to positively transform the current industry-operating model across many lines of business, delivering the benefit of improved security, controlled transparency and accessibility to both regulators and customers globally, while also substantially reducing costs and complexity for participating banks. Our team works closely with industry experts and an impressive advisory board, which includes **Richard Gendal Brown**, noted thought leader and Executive Architect for IBM; **Tim Swanson**, industry expert and author; **Peter Todd**, Bitcoin Core Developer and **Dr. Patrick Deegan**, Chief Architect of the Open Mustard Seed Identity solution.

Led by Founder and Managing Partner **David Rutter**, the R3 team is composed of a highly specialized team of financial services industry veterans, technologists, subject matter experts and new tech entrepreneurs especially focused on rethinking and improving the modern financial markets ecosystem. Mr. Rutter is a noted creative thought leader in financial markets innovation and has played a significant role in the evolution global OTC derivatives industry, championing the change from voice to electronic trading. From 2003-2013 David served as Chief Executive Officer of Electronic Broking at ICAP Plc, the world’s largest interdealer broker. David’s primary roles included leading the BrokerTec fixed income and EBS foreign exchange platforms, two of the largest electronic OTC platforms in the world. Prior to ICAP, David was co-owner of Prebon Yamane, last serving as Chief Executive Officer, Americas. David also serves as an advisor and board member to several financial services corporations and charities. Additionally, R3 members **Todd McDonald**, **Jesse Edwards**, **Raja Ramachandran** and **Jo Lang** help lead R3’s Crypto 2.0 practice.



## About the Author

Jo Lang leads platform development and research at R3. She focuses on developing tools and resources for both financial institutions and innovative fintech companies to collaborate effectively. Her research focuses primarily on crypto-technologies, global regulatory and industry standards, and their applicability across the financial eco-system in both developed and emerging markets.

Prior to joining R3, Jo was at Epiphyte where she led business development and managed key senior relationships at major global finance and technology firms. Prior to Epiphyte, Jo was a Consultant at Capco within the Wealth & Investment Management practice. While she was there she led research initiatives primarily focused on global wealth management trends and technologies. Jo graduated cum laude from Swarthmore College with a B.A. in History and German Studies.

