Ripple ($XRP) Analysis

Myles Snider, Kyle Samani, and Tushar Jain
August 31, 2017

Intro

Note: In this analysis, we will refer to Ripple in several contexts:

Ripple Inc. - a California-based, venture-backed C corporation
Ripple protocol/network - a design specification for inter-bank communication
XRP - the native, but not exclusive, currency of the Ripple protocol

We will distinguish between these throughout this analysis.

Ripple is a blockchain protocol for inter-bank settlements. Unlike many other blockchains, Ripple is designed to work with existing institutions to facilitate the ability to quickly transact *any asset* globally. The Ripple protocol's native currency, XRP, is only required to pay fees for transactions on the Ripple network. It can be used in other instances, but banks have the option to transact IOUs in any asset, including USD, EUR, and other fiat currencies. Ripple Inc. builds an infrastructure protocol that facilitates decentralized exchange of assets between banks.

The Ripple protocol utilizes a novel consensus mechanism called the "Ripple Protocol Consensus Algorithm," or RPCA. This is different from Bitcoin's proof-of-work or Ethereum's proposed proof-of-stake consensus model. The stated goal of RPCA is to provide increased scalability and faster confirmation times.

The Ripple protocol is developed and maintained by Ripple Inc., a United States C-corporation that's raised over $93 million in venture capital. Currently, Ripple, Inc. exercises unilateral control over the Ripple network. This arrangement, and the company's plans to democratize control in time, will be discussed below.

We recognize that the Ripple protocol has an opportunity to displace legacy inter-bank networks, but we must distinguish between a good use for a blockchain and a good investment opportunity. We believe that the Ripple protocol satisfies the former, but that XRP does not satisfy the latter. The Ripple protocol can impact trillions of dollars of economic activity, but this commerce is unlikely to be conducted in XRP. The XRP token has little core utility beyond nominal fee payment and is unlikely to grow in value proportional to Ripple network usage. We will not conduct a quantitative valuation because we do not believe that XRP presents a compelling investment in qualitative terms.

Summary

Background

The original Ripple design is a modern, digital interpretation of age-old IOU networks. To dive into the mechanics of Ripple, we must first understand some basics of the modern banking system.

When I deposit money into my bank account, I essentially loan that money to the bank. The bank incurs a liability: my bank owes me my money, all or part of which I can request at any time. Each time I make a deposit, I am essentially extending a credit line to the bank— I trust that the bank will repay me for all of my deposits.

It's easy to send $100 to a friend who uses the same bank. The bank internally shifts its liabilities from one creditor to another. Specifically, the bank reduces its liabilities to me by $100, and increases its liabilities to my friend by $100.

This system works because both my friend and I have extended a line of credit to the bank and we have confidence that the bank will pay us what we are owed when we request it. The transaction is manifested as a change in the bank's internal ledger, which keeps track of how much money it owes to each client.

This process becomes more complex when I want to pay someone who uses a different bank. In some instances, our banks may have a trusted relationship such that the bank of the receiving party is willing to accept an IOU from my bank, but this is not always the case. If I bank with Chase and my friend banks with Bank of America, a transaction between us is not just a matter of one bank updating its internal ledger; rather, those banks must actually exchange money (at some point). Because these types of inter-bank transactions happen frequently, banks often exchange IOUs, settling these periodically with actual monetary transfers. The IOU system allows transactions to happen more quickly.

However, this only works because the banks (Chase and Bank of America in our example) trust one another to fulfill their mutual IOU obligations. If our banks do not have a trusted relationship, then we

must wait for the money to actually be transferred, or the transaction must be routed through a mutually trusted third party. Both of these processes are slower and more costly than simple IOU issuance. These transfers are more complex across borders, where banks are less likely to have trusted relationships.

Chase and Busan (a South Korean bank) may not have a trusted relationship. If I want to send money from my account at Chase to my friend's account at Busan, the payment must route through multiple parties. Each transaction has a cost and takes time. Thus, international payments are slow and expensive.

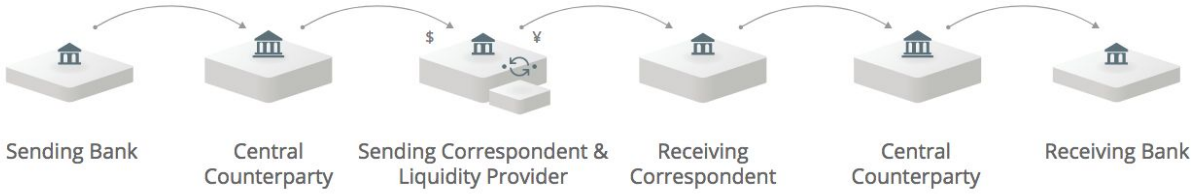


Image Source

The Ripple Ledger Solution

The Ripple network replaces the system described above with a blockchain-- eliminating friction, speeding up transaction and settlement times, and greatly reducing costs. In many ways, this is a perfect use case for blockchain technology. The legacy system is slow, expensive, and error-prone; banks must coordinate transfers of value across different internal databases, making it extremely difficult to settle transactions quickly. Not only is this process slow, it adversely impacts a bank's balance sheet by increasing working capital requirements. Banks often have to open accounts with other foreign banks and fund them with local currency (these are known as nostro accounts).

This money sits idle until banks need to make a payment in that currency, creating inefficiencies. Banks that can't afford to fund many nostro accounts, or that need to make a payment in a currency for which they don't have an account, must rely on third-party liquidity providers for that currency. Not only does this subject the banks to counterparty risk, but it often requires that their capital be tied up in transit for days at a time.

Ripple allows banks to move from a system of disjointed, trust-based databases to a single distributed database, the Ripple ledger. This gives transactions a fluidity and speed that can't be achieved in the legacy system, and it greatly frees up working capital. Ripple solves real problems for banks.

The Ripple network is essentially a map of trust lines. When two parties wish to exchange value, but do not have a direct line of trust, Ripple routes the transaction through the fastest and shortest possible

path of trusted parties, enabling global parties to transact instantly without establishing new trust lines. The network provides a distributed ledger that logs all of these transactions.

Perhaps the most interesting feature of the inter-bank Ripple protocol is the fact that these transactions do **not** have to be denominated in the network's native currency, XRP. The network manages inter-bank IOUs that themselves can be denominated in any asset. A USD-USD IOU example follows. This gets a little complex, so here's a quick primer on terminology:

- *BankX-USD* refers to USD assets issued by BankX on the Ripple protocol
- *BankY-USD* refers to USD assets issued by BankY on the Ripple protocol
- While these two assets are nominally the same (both are for USD), they may be valued differently, since each entails a different counterparty risk; e.g. what if BankX is Lehamn Brothers in August 2008 and BankY is JP Morgan Chase? Generally speaking, assets issued by more trusted entities will be worth slightly more on the Ripple protocol, even if they should nominally be valued equally.

A consumer (User A) may deposit 100USD through a gateway, such as BankX. If User A wishes to send 50USD to User B in another country, BankX will issue 50 *BankX-USD* on the Ripple platform. This is simply another form of IOU from BankX to the party that owns or receives the *BankX-USD*; rather than existing only in the bank's internal database, this IOU now exists and can be transacted on the Ripple ledger.

While User B does not have an account with BankX, User B may have an account with BankY, which can issue its own *BankY-USD* on the Ripple network.

User A can initiate a transaction to User B's account at BankY for 50USD. BankX will automatically submit a transaction to convert 50 *BankX-USD* to 50 *BankY-USD* to an order book, where it can be filled by anyone acting as a market maker. The market maker, who holds both *BankX-USD* and *BankY-USD*, converts the 50 *BankX-USD* into 50 *BankY-USD* and sends that to User B's account at BankY. Transaction complete.

In this way, the Ripple network also acts as a decentralized exchange. Because BankX may be a more trusted institution than BankY, *BankX-USD* are slightly more valuable than *BankY-USD*. As a result, there exists an opportunity for the market maker to make a slight profit on the exchange, which provides the incentive to act as a market maker.

This transfer could play out another way without IOUs, but with XRP instead. This opportunity would exist if both BankX and BankY were willing to exchange USD for XRP. After User A initiates a transaction, BankX would convert the USD to XRP, send the XRP to BankY, and BankY would convert the XRP back into USD. Then User B could withdraw USD from BankY.

We find it important to note that the 2nd option presented is not exclusive to XRP. Banks and financial institutions could perform the same transfer using BTC, ETH, DASH, or any other cryptoasset as the

bridge currency. In those cases, the transfers would take place on their respective blockchains, rather than on the Ripple ledger.

Ripple Protocol Value Proposition

The Ripple consensus protocol, known as RPCA, relies on a unique algorithm for determining a single truth that is agreed upon by all nodes in the Ripple network. Like any distributed, cryptographic consensus mechanism, RPCA is a complex system that involves many different types of actors and interactions. An overview follows:

At its core, RPCA is a group of servers, each of which maintains its own Unique Node List (UNL). A UNL is a list of other nodes to which a server has extended a line of trust. The server will only consider proposals about the state of the shared ledger from its UNL. Servers exchange “candidate sets,” which are sets of transactions that may be added to the final ledger. The process of consensus requires that nodes continuously exchange candidate sets until 80% of the nodes in the server’s UNL agree on the same set and order of transactions. Only after this threshold is reached can a candidate set be added to the ledger.

Nodes within a given UNL will continue to exchange candidate sets until the 80% threshold is reached. However, unless there is sufficient overlap among all UNLs on the entire network, then different UNLs could reach 80% consensus individually with different sets of transactions. This would mean that the network-wide ledger (which includes all UNLs) would not have a single consensus, creating a fork. Thus, the Ripple protocol relies on sufficient overlap of UNLs (a minimum of 40%) in order to reach network-wide consensus.

RPCA Issues

The primary challenge in this arrangement, as mentioned before, is that different servers have different UNLs. Unless there is sufficient overlap among *all* UNLs on the network, the network could fork. While there is a theoretical motive for servers to have different UNLs (to achieve decentralization), there’s also motive to converge on UNLs to avoid hard forks.

To further complicate this issue, there exists a default UNL, curated by Ripple Inc., to which new servers automatically subscribe. Each server can opt out of this UNL at any time and select a new one, but there are two problems with this. First, there exists little public data on which servers are most trustworthy, so new servers would have a difficult time deciding which other servers to include on their own UNLs. Secondly, because increased divergence among UNLs leads to greater possibility of a fork, and since a fork is bad for all users of the network, enterprise clients will be motivated to choose the UNL that minimizes the probability of a fork. Both of these factors mean that new nodes will most likely choose the UNL recommended by Ripple Inc.

Ripple Inc. has made attempts to assuage these concerns. First, Ripple Inc. will gradually add more third-party validators to its default UNL, replacing those operated by Ripple Inc. Second, Ripple Inc. has

indicated that there are 55 unique validator nodes (as of July 2017) on the Ripple network, many of which are operated by companies and institutions other than Ripple Inc. However, it does not appear that any of these validators have yet been added to the default UNL.

A final issue that exists with the RPCA is that there does not seem to be sufficient motivation for anyone to actually run a validating node. Nodes are not compensated for any of the work they perform. According to Ripple Inc., institutional participants will run nodes for the health of the network.

> "If the Ripple network becomes successful and is widely used for interbank settlement, there will be an incentive for participants to ensure the reliability and stability of the network. If this happens, institutions will run Ripple servers to participate in the network. Once you are running a server, the additional cost and effort to operate a validator is essentially zero—it would simply involve flipping a software switch from off to on. It is the validators who decide the evolution of the Ripple network, so the primary incentive to run a validator is to preserve and protect the stable operation and sensible evolution of the network."

We believe that this is a potentially dangerous assumption and one that may affect the long term stability of the Ripple network.

These concerns have been explored previously and explained in greater detail.

- Bitcoin developer Peter Todd on technical issues with RPCA.
- IBM's Jo Lang on potential risks associated with Ripple.
- This research paper, which highlighted flaws in RPCA and disputed claims made in Ripple's white paper, prompting a response/correction from Ripple Inc.

XRP Tokens

XRP is the native token of the Ripple protocol. A few facts about the token:

- There are a total of 100 billion XRP. All have been premined, meaning they were all created at the time the protocol was deployed.
- Ripple Inc. has distributed some of the XRP to enterprise clients. Currently, Ripple Inc. holds ~62 Billion XRP.
- XRP are used to pay fees on the platform (to prevent network spam).
- XRP that are used to pay fees are burned; XRP fees are not payed to validators. XRP is a deflationary currency.
- 55 billion of the XRP held by Ripple Inc. will be placed in an escrow contract by the end of 2017; the contract will release 1 billion XRP each month, for 55 months, to be used by Ripple Inc. at its sole discretion.

XRP Value Proposition

XRP is a free floating cryptocurrency that is available to trade on a number of crypto exchanges. If XRP will build long term value, it must have utility. We'll examine that utility below.

The first value proposition for XRP is that it is required to utilize the Ripple protocol. Users cannot participate in the network unless they maintain at least 20 XRP (worth about $4 USD at time of publication) in their wallets. XRP is the only way to pay for transaction fees on the network, so all parties must have some XRP in order to perform transactions. This function serves to prevent spam on the network, since each transaction has a cost.

While these two use cases mean that XRP will hold *some* value as long as the Ripple network continues to exist, they do not necessarily mean that the token will increase in value as the network grows. According to Ripple Inc., the value proposition of XRP lies in its utility as a currency for settlement.

While banks can exchange IOUs freely on the Ripple protocol, these IOUs must eventually be settled. These settlements, if done in fiat, are still subject to the inefficiencies of the legacy banking system that Ripple aims to replace.

In the IOU example below, a liquidity provider or market maker would have to offer up to 28 different currency pairs in order to participate in all order books. Market makers must have accounts and balances with every institution, and for every asset, for which they are offering to perform transactions. In some instances, these transactions may have to trade through several different liquidity providers or market makers, which increases total transaction costs and decreases speed.

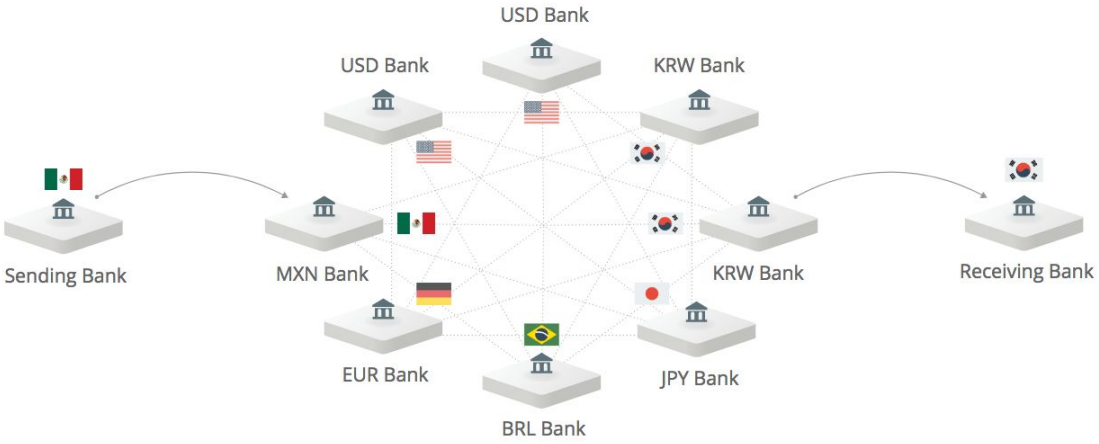


Image Source

It is important to note that this process mirrors the process already used by the banking system today. However, because Ripple moves these settlements onto a blockchain, even transactions that are routed through several different parties can happen quickly and far more inexpensively than they do in the traditional banking system.

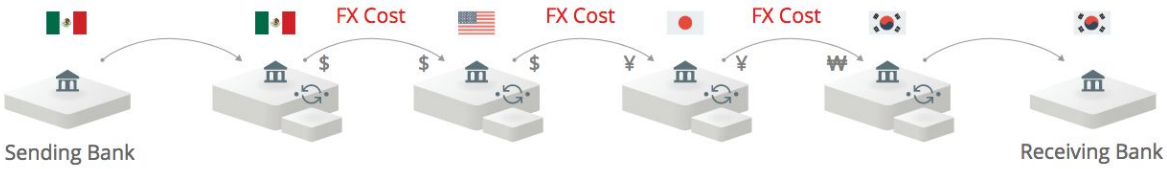
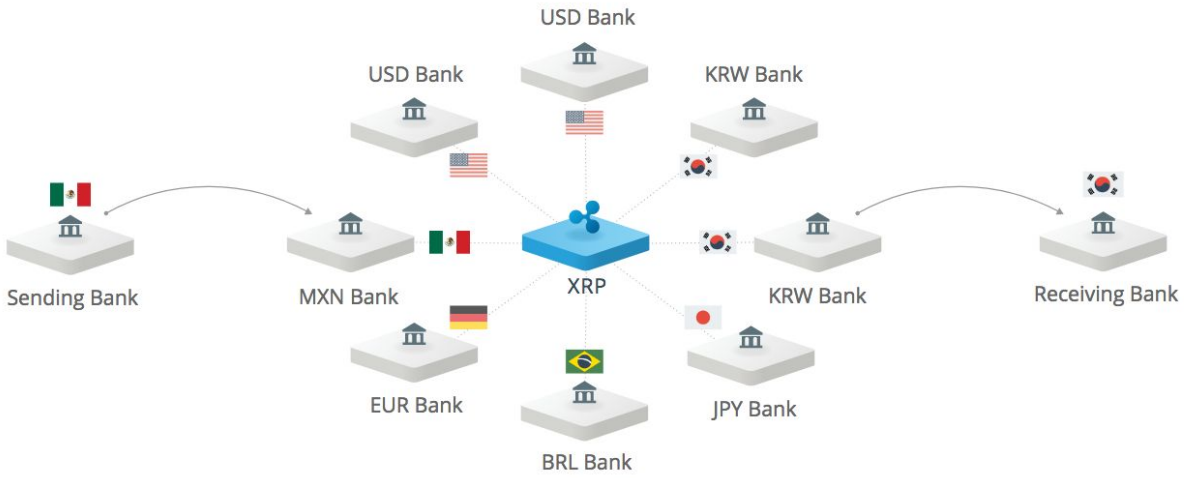


Image Source

On the other hand, transactions can be denominated in XRP, which reduces the number of network participants through which a transaction will be routed. This is shown below.



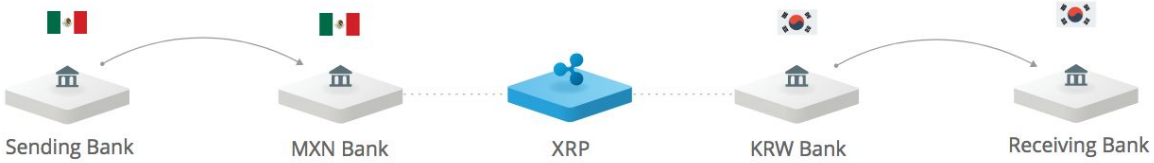


Image Source

Ripple Inc. expects that XRP will be used as a bridge currency between various asset and/or fiat currency pairs. They also expect that banks and financial institutions will choose to conduct

transactions in XRP, rather than in IOUs, because it allows for faster settlements. We remain skeptical of both of these claims.

As noted before, the settlement function of XRP is not something that is exclusive to the Ripple protocol. These international settlements could be sent using Bitcoin, Ethereum, or any other cryptocurrency. We find it probable that banks will move towards using the global reserve cryptocurrency, which will likely be Bitcoin or a fiat currency issued on a blockchain (People's Bank of China, for example, has discussed possibly putting fiat currency on-chain). Banks wishing to use XRP for settlements would need to hold large amounts of XRP in their accounts, incurring enormous price risk. They would also still be forced to use the legacy system for payments going to places where XRP rails are not currently in place.

We don't find a compelling argument for a digital currency that exists specifically for inter-bank settlements. While XRP transfers currently confirm faster than BTC or ETH transfers, this not likely to be the case for an extended period. XRP is highly unlikely to be used outside of the inter-bank settlement system (there is basically no infrastructure for it outside of the inter-bank payment system), so it will probably not become a global reserve currency in the same way that Bitcoin or Ethereum might. Any cryptocurrency that reaches global reserve status will likely be relatively stable. Banks will prefer to settle IOUs using the global over XRP. When governments eventually issue fiat currencies on a blockchain, banks will be able to instantly settle in their preferred local currencies. Financial institutions could continue to use the Ripple protocol to transact IOUs, but we find it unlikely that XRP will be widely used as a settlement currency.

If XRP isn't adopted as a settlement currency, it will not sustain its current implied network value of ~$8.5B. Investing in XRP at current prices is a bet that XRP will become the global inter-bank settlement currency. The outcome is likely to be binary, and we do not believe XRP will become the global settlement currency.

Risks

We've outlined the major risks related to the Ripple protocol and XRP tokens, which we believe make XRP a poor investment at current prices.

- The Ripple network currently faces major centralization risk:
    - Ripple Inc. controls the vast majority of tokens and has complete discretion over these tokens. As Ripple Inc. sells these tokens, the USD-denominated price of XRP will face significant downward pressure.
    - Ripple Inc. also exerts great influence over the protocol through default UNLs.
    - Ripple Inc. currently operates the majority of validating servers.

- Uncertainty around RPCA:

    - Because Ripple Inc. has maintained such a large degree of control over the network, the Ripple protocol has yet to be tested with a significant number of dishonest nodes.
    - Multiple research papers have questioned the mechanics of the consensus protocol, indicating uncertainty over its security.
    - The incentives for network actors to run a full validating node are unclear. This may lead to network instability and/or increased centralization.

- Redundancy risks:
    - The main value proposition of XRP (as a bridge/settlement currency) is something that could just as easily be done with BTC, ETH, DASH, or other layer 2 networks (e.g. Lightning, Raiden). XRP provides at best marginal benefits relative to these alternatives.
    - Ripple's current speed and scalability advantages relative to BTC and ETH will fade as these networks evolve.
    - Because XRP is designed as an inter-bank settlement currency, it will have little usage outside of the Ripple network. Banks have motivation to conduct inter-bank settlements using assets their customers deposit, which are likely in time to be BTC, ETH, or on-chain fiat currencies. Maintaining a separate currency for this purpose is counterproductive.

- XRP Transfers vs. IOU Transfers:
    - Banks and institutions will likely prefer to issue assets directly on the Ripple blockchain through IOUs to minimize working capital requirements.
    - These assets can be traded on the Ripple decentralized exchange and routed through multiple parties, meaning there will almost always be a path through which assets can flow internationally. The multi-party IOU route may incur slightly higher costs than using XRP as a global bridge currency, but these costs are still a fraction of those of the legacy systems.

- Economics of using XRP
    - Banks that hold XRP to conduct transactions would need to hold enough to cover their largest expected payment obligation-- which could be problematic as XRP rises and falls in value.

Conclusion

XRP currently has a network value of about $8.5 billion, excluding the 62 billion XRP that are owned by Ripple, Inc. We believe that most of this value is a result of speculation due to partnership and customer announcements by Ripple, Inc. The company has made major progress on several fronts and continues to sign important partnerships with banks and other financial institutions around the world. We recognize the value in the service that Ripple Inc. is providing, and we believe that inter-bank settlements are one of the best use cases for blockchain technology.

However, it is important to recognize that a good use of blockchain technology does not always justify the value of a chain's native token. In the case of XRP, we believe that the token holds little utility beyond payment of negligible fees, and thus is unlikely to maintain and build value in the long term. While we expect that XRP tokens will continue to see price spikes as Ripple Inc. makes announcements, we don't believe that the fundamentals of the protocol will build sustained value for XRP. An investment in XRP is not an investment in Ripple Inc. The company may do well offering a useful service to banks, but XRP's value is likely limited. For these reasons, we are bearish on XRP at current prices.

Please email research@multicoin.capital with any comments or questions.