



The research statements below are a representative sampling of real-world problems that are top of mind for Ripple and the ILP/XRP ledger teams, as well as for the broader community working in blockchain, cryptocurrency and global digital payments. This list of topics is not intended to be prescriptive, but can be used as a resource for universities as they develop their own research strategies within the framework of the University Blockchain Research Initiative and beyond. This list is preliminary; the intent is to use it as a working document that can be modified based on university partner feedback and the introduction of new topics, both by Ripple and by university faculty and students.

Consensus

- Can consensus protocols be built with block finality and asynchronous safety with little- $o(N^2)$ communication?
- What are possible attacks on Cobalt / XRP LCP as described in respective papers? For example: frontrunning; What are possible mitigations?

Data Science

- How would you graph and analyze blockchain transactions using wallet identification, transaction clustering, etc.?

Decentralization

- What are useful ways to measure decentralization? What is the effective decentralization of the major assets in the digital space?
- Are there novel deanonymizing attacks on anonymity coins?

Digital Asset Derivatives

- Are there any novel derivative structures on digital assets that can leverage cryptography/multiparty agreement protocols?

Digital Asset Market Structure

- What are the best structures to incentivize price discovery and deep liquidity on distributed exchanges, where time-priority is poorly defined?
- What are ways of measuring the utility of digital assets in the market? How much should crypto-crypto trading volume be weighed compared with crypto-fiat volume? What are the best ways to measure the flow of fiat into and out of the digital asset ecosystem?
- What factors move or correlate with digital assets? Is the digital market a leading or trailing indicator for other asset classes?

Distributed Systems

- Are there novel attacks on various cryptocurrencies that are cheap but possibly not incentive compatible (i.e., if I'm willing to pay some cost to attack the network, how small would that cost be)?
- Given XRP's consensus mechanism, what are the most efficient ways to scale the ledger?

Game Theory

- Are tokens isolated from fiat? Is there an incentive structure for cryptocurrencies that accounts for the fact that tokens aren't isolated from one another?

Incentive Structures

- Evaluate the incentives in emerging blockchain networks (proof-of-work, Byzantine fault tolerant (XRP), etc.) on a variety of factors including: Network diversity and participation, Security, consolidation of decision making, etc.

Infosec / Opsec

- What assumptions about the adversary are reasonable for blockchain consensus protocols (e.g., how important is safety/liveness under unbounded asynchrony? Is adaptive security really needed for PoS?)

Market Liquidity

- What is the price impact of an order/execution on open order books? How does this evolve as markets become more liquid?

Network Analyses- Non-Technical

- How do adoption curves take place globally (eg: December 2017 run-up in cryptocurrencies)? What adoption models make sense for the new digital asset class and where are we in terms of these models ?
- How does Metcalfe's Law apply to global payment systems/networks? What is the strength of different digital asset ecosystems based on different network analyses?

Network Analyses- Technical

- Given the trajectory of the Internet, what network topology should be expected for Interledger connectors?
- What can be learned from TCP congestion and flow control strategies for interledger transport protocols like STREAM?
- What are the implications of sending data over the interledger as a replacement for the internet itself? Could Internet SDN controllers be repurposed for Interledger?
- Large scale testing of Interledger: How does interledger perform in large scale distributed simulations?
- How can privacy be preserved while sending micropayments through interledger (e.g. Interledger VPNs or TOR over ILP)?

Regulatory Impact on Digital Assets

- What is the overall regulatory landscape within the digital asset space and what is their impact on local/global perception of these new technologies?
- What are the potential downstream impact (on banking, exchanges, payment companies, etc.) of different regulatory stances of major economies (India, Japan, Brazil, US, etc.)?

Software Engineering

- How would offline payments be implemented for interledger? (Similar to how credit cards do offline payments)
- What architecture or tools (FPGAs) could be used to build super fast interledger connectors?