Assessing Layer-2 Blockchain Protocols in the BoLT Ecosystem

07-300, Fall 2021

Sarayu Namineni
https://www.andrew.cmu.edu/user/snaminen/

November 12, 2021

1 Project Description

I will be working with Professor Seth Goldstein in the Computer Science Department to evaluate the usability and performance of layer-2 blockchain protocols in the Building on Local Trust (BoLT) ecosystem. In particular, we will assess implementations of custom ledgers for the BoLT ecosystem using layer-2 blockchain protocols, such as Celo, Near, and Solana, on metrics such as throughput, cost, and the flexibility of the smart contract language.

BoLT is a transparent, reputation-based market in exchangeable credit, which allows people to support local businesses at low cost and with minimal risk. BoLT allows all individuals on the network to define and mint their tokens (ZUZ), unlike a conventional blockchain which operates on a single token. Furthermore, these specifications can be of variable length, such as by having multiple maturity dates or buyback options.

A significant challenge in this project will be reducing the performance overhead of the BoLT ledger, which is derived from a set of three-way trade-offs commonly-referred to as the "blockchain trilemma." The blockchain trilemma theorizes that it is only possible to achieve two out of three factors: scalability, security, and decentralization. The overhead of a consistent ledger results in poor performance, and layer-2 solutions, such as Celo, Near, and Solana, aim to bridge this gap by offloading the transactional burden to adjacent networks.

Such highly-scalable blockchain technologies are still in their nascency and do not have strong user communities. There is limited support for the development of on-chain programs and little to no precedent for a multi-token system like BoLT. Our project will build upon emerging layer-2 solutions, assessing the flexibility and performance of their smart contract languages for our application.

The significance of this project is two-fold, as it has both a socioeconomic and a technical impact. BoLT offers individuals, especially marginalized and economically disadvantaged ones, new avenues of acquiring capital, empowering communities that have been historically turned away from lending institutions. Furthermore, this project contributes to the emerging understanding of the performance of layer-2 blockchain protocols. In particular, it provides insight into the scope of smart contract languages and the viability of on-chain programs.

2 Project Goals

2.1 75% Project Goal

- Complete implementation of a custom ledger for the BoLT system on Solana's network, which includes the following primitives:
  - Creating a ZUZ specification, which is defined by an issuer, maturity date, interest, and buyback options (if any)
  - Mint ZUZ
  - Transfer ZUZ between users on the network, defined by functions to offer an exchange, accept the offer, and revoke the exchange
  - Buyback ZUZ, or swap out some amount of a specified ZUZ for an equivalent amount of another specification
  - Extend a trustline, or an agreement that a user of the system will accept a specified ZUZ issued by another user as their own until a given expiration date
  - Delegate the authority to mint, accept, and offer exchanges for a specified ZUZ to other users on the network
  - Destroy ZUZ

2.2 100% Project Goal

- Complete implementation of a custom ledger for the BoLT system on Solana's network, which includes the following primitives:
  - Creating a ZUZ specification, which is defined by an issuer, maturity date, interest, and buyback options (if any)
  - Mint ZUZ
  - Transfer ZUZ between users on the network, defined by functions to offer an exchange, accept the offer, and revoke the exchange
  - Buyback ZUZ, or swap out some amount of a specified ZUZ for an equivalent amount of another specification
  - Extend a trustline, or an agreement that a user of the system will accept a specified ZUZ issued by another user as their own until a given expiration date
  - Delegate the authority to mint, accept, and offer exchanges for a specified ZUZ to other users on the network
  - Destroy ZUZ

- Deploy custom ledgers implemented on Celo, Near, and Solana as backends to the current BoLT system for testing
- Compare the performance and usability of the custom ledgers on metrics such as throughput, cost, and the flexbility of the smart contract language

2.3 125% Project Goal

- Complete implementation of a custom ledger for the BoLT system on Solana's network, which includes the following primitives:
  - Creating a ZUZ specification, which is defined by an issuer, maturity date, interest, and buyback options (if any)
  - Mint ZUZ
  - Transfer ZUZ between users on the network, defined by functions to offer an exchange, accept the offer, and revoke the exchange
  - Buyback ZUZ, or swap out some amount of a specified ZUZ for an equivalent amount of another specification
  - Extend a trustline, or an agreement that a user of the system will accept a specified ZUZ issued by another user as their own until a given expiration date
  - Delegate the authority to mint, accept, and offer exchanges for a specified ZUZ to other users on the network
  - Destroy ZUZ
- Deploy custom ledgers implemented on Celo, Near, and Solana as backends to the current BoLT system for testing
- Compare the performance and usability of the custom ledgers on metrics such as throughput, cost, and the flexibility of the smart contract language
- Derive zero-knowledge methods for identity management as it relates to ”Know Your Customer” (KYC) and anti-money laundering (AML)

3 Project Milestones

3.1 First Technical Milestone for 07-300

I aim to familiarize myself with smart contract development on Solana's network. This includes setting up local development clusters, learning the basics of how to use Rust in on-chain programs and test suites, and getting a better understanding of the JSON RPC client API. I hope to have a strawman prototype of the BoLT ledger which implements three primitives: creating ZUZ specifications, minting ZUZ, and transferring ZUZ.

3.2 First Bi-Weekly Milestone for 07-400: February 1st

I aim to have a prototype of the BoLT ledger which implements the three primitives as listed earlier, creating ZUZ specifications, minting ZUZ, and transferring ZUZ, as well as the three primitives necessary for transactions, namely offering ZUZ for exchange, accepting an offer, and revoking the offer for exchange.

3.3 Second Bi-Weekly Milestone for 07-400: February 15th

I aim to implement the primitives for extending trust lines, buybacks, and destroying ZUZ. These operations require the most complex state management up until this point, so I expect to have gained enough familiarity with the development language in order to implement them.

3.4 Third Bi-Weekly Milestone for 07-400: March 1st

I aim to implement the primitives for delegation, which authorize permissions from the issuer of specification to another user on the network, to perform actions such as minting, accepting, and offering ZUZ for exchange.

3.5 Fourth Bi-Weekly Milestone for 07-400: March 15th

I aim to deploy the ledger from my local clusters to Solana's mainnet and connect it to the BoLT system backend for testing.

3.6 Fifth Bi-Weekly Milestone for 07-400: March 29th

I aim to collect measurements on throughput, cost, and latency by running experiments on the BoLT network.

3.7 Sixth Bi-Weekly Milestone for 07-400: April 12th

I aim to draw comparisons on the experimental metrics among the various layer-2 protocols which get deployed to the BoLT system, including implementations of Celo and Near.

3.8 Seventh Bi-Weekly Milestone for 07-400: April 26th

I intend to synthesize the results of the comparative analysis to determine a final recommendation for the design of the BoLT ledger.

4 Literature Search

In order to familiarize myself with the inciting problem and preliminary solutions for BoLT, I have read the following papers related to the use of blockchain technology in lending markets [3] [4] [5] [6]. I have also begun to survey the documentation for various layer-2 protocols, with a particular emphasis on Solana [1] [2].

5 Resources Needed

In order to implement the ledger prototype, I will need access to the ZUZ system and AWS EC2 instances, which will be provided to me through the project group.

References

[1] Solana docs. https://docs.solana.com/.

[2] Solana wiki. https://solana.wiki/docs/.

[3] Gregory S. Crawford, Nicola Pavanini, and Fabiano Schivardi. Asymmetric information and imperfect competition in lending markets. *American Economic Review*, 108(7):1659–1701, July 2018.

[4] P. Dandekar and Bryce Wiedenbeck. Strategic formation of credit networks: Preliminary report. 2011.

[5] Pranav Dandekar, Ashish Goel, Ramesh Govindan, and Ian Post. Liquidity in credit networks: A little trust goes a long way. In *Proceedings of the 12th ACM Conference on Electronic Commerce*, EC '11, page 147–156, New York, NY, USA, 2011. Association for Computing Machinery.

[6] Joseph Stiglitz and Andrew Weiss. Credit rationing in markets with imperfect information. *American Economic Review*, 71(3):393–410, 1981.