This is a followup post on “A DEX on plasma” from Apr’18. We have gone through many iterations and have what we believe is a production quality spec. Note that ours is designed for trading and not UTXO payments like almost all other specs here.

Our focus is weighted with UX, Scaling and Security in that order.

UX is the primary driver since we are building a business, not just engaging in technical research. Most of our choices were based on pragmatic conditions of the market and user base today. For example, we realized that exit games are a non-starter because although they work, even many tech-savvy users would avoid such exchanges at the current time. Our users were also confused why they have to deposit a heavy bond to take out their own money.

Scaling was the next primary driver. We aimed for sub-linear cost in terms of gas, storage and computational load with increasing volume. Without this, the platform becomes self-limiting as gas costs drive traders elsewhere. Scaling also feeds into security since super-linear cost would make it practical to overwhelm any validators with long chains of transactions, dust trades and other attacks whose impact is amplified by high activity.

Security is last but not the least. It is intertwined with the two needs above. We needed a security model and proof so that the model could be examined and any gaps speedily addressed.

Read the full Gluon Plasma paper to understand our motivations and drivers.

Top features:

1. Offline Recipient
2. Instant finality on plasma chain
3. Fast withdraws (< 1 hour)
4. Fungible
5. Unlimited number of coins
6. Unlimited trades per block
7. Light nodes
8. Compact fraud proofs
9. Ethereum Network Congestion tolerant
10. Security Model/Proof
11. Watchtower-free
12. Exit Game-free
13. Challenge/Response-free

Ok, so what’s the catch?

Data Unavailability is not yet eliminated. A governance token is used to vote for a chain halt if the operator turns maleficent. SEE UPDATE BELOW

Security Proof Outline

A payment network is secure if the following constraints hold for every transaction:

1. The recipient can receive the payment directly.
2. The sender’s provable intention is required to send the payment.
3. The amount received is exactly the amount sent.
4. Network participants can verify validity according to consensus rules.

If it can be shown that every state change enforces the above, then the network is safe. The above needs to be enforced at 3 levels:

1. All steps of the protocol, which is the interface between the main chain and plasma chain
2. Plasma ledger entries
3. Plasma chain, which is the arrangement of plasma ledger entries.

I ask the reader to read the full paper since the protocol and the fraud proofs together make the system, so listing just the protocol here would be a disservice.

Guide to reading the paper: What each chapter speaks about

3: Deriving account model from UTXO model

4: How Exchange security models work

5: Why we needed a different plasma flavor

6: Gluon Plasma fundamentals

7: Gluon Plasma characteristics (is this flavor suitable for your project?)

8: Gluon Plasma Protocol

9: Fraud Proofs

Appendix A,B and C: Proofs of safety and custody

Your improvements and critical feedback is highly appreciated!

UPDATE:

Joey Krug suggested we replace the POA with tendermint consensus POS. We realized that if we decouple the exchange and consensus (ie block committer) roles, we can eliminate data unavailability:

1. Exchange(s) creates transactions.
2. Tendermint POS committers create blocks from transactions.
3. If exchange withholds data, POS validators will simply not commit any more blocks.
4. If at least 1/3 of the POS validators collude with the exchange and duplicitously commit a block while withholding data, other POS validators can slash their deposit (which needs to be hefty).

Regarding 3. Chain is abandoned and halts when there is a single exchange on the plasma chain. On a multi-exchange chain, the byzantine exchange is ejected and trades in its block are effectively rolled back. Other exchanges can continue to operate. Multi-exchange feature is not yet finalized.

A single exchange Tendermint POS can probably be implemented without much impact.