Twister

Private cryptocurrency transactions using rollups

rollup: a way to store some data off-chain in a blockchain setting, while still providing same security guarantee as the blockchain

– *how to make private transactions on a rollup?*

method:

– survey possible implementations for rollups

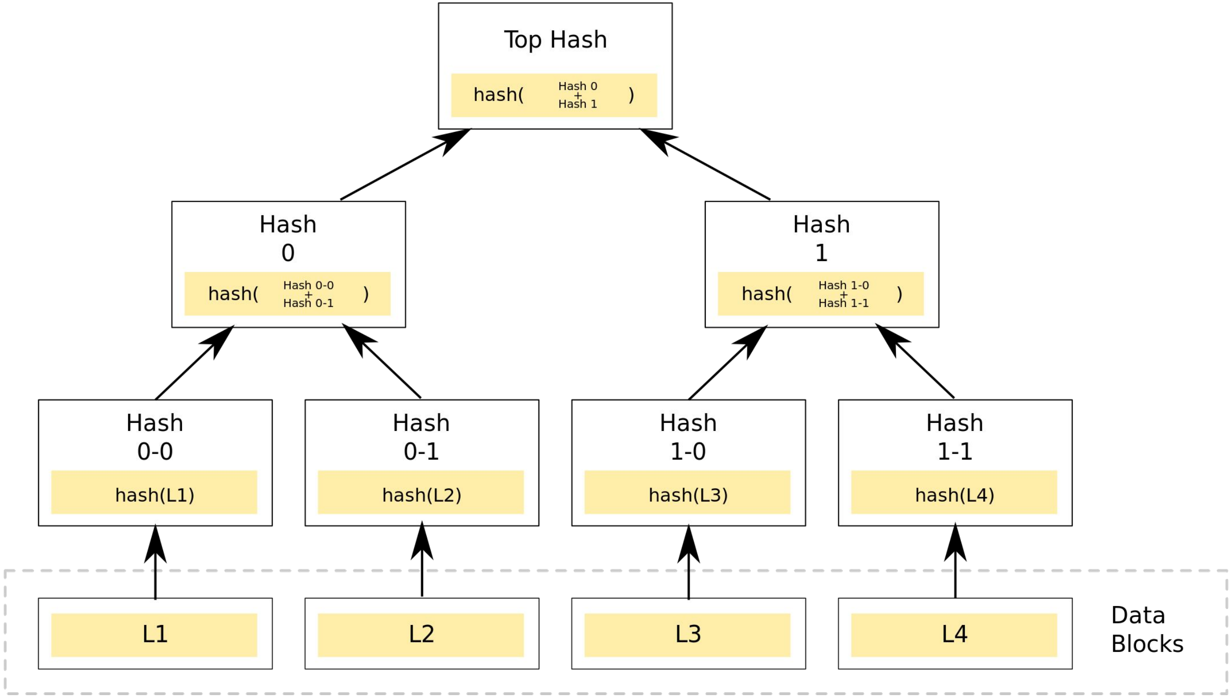
– fork open-source zk-SNARK-based private transaction code

conclusion:

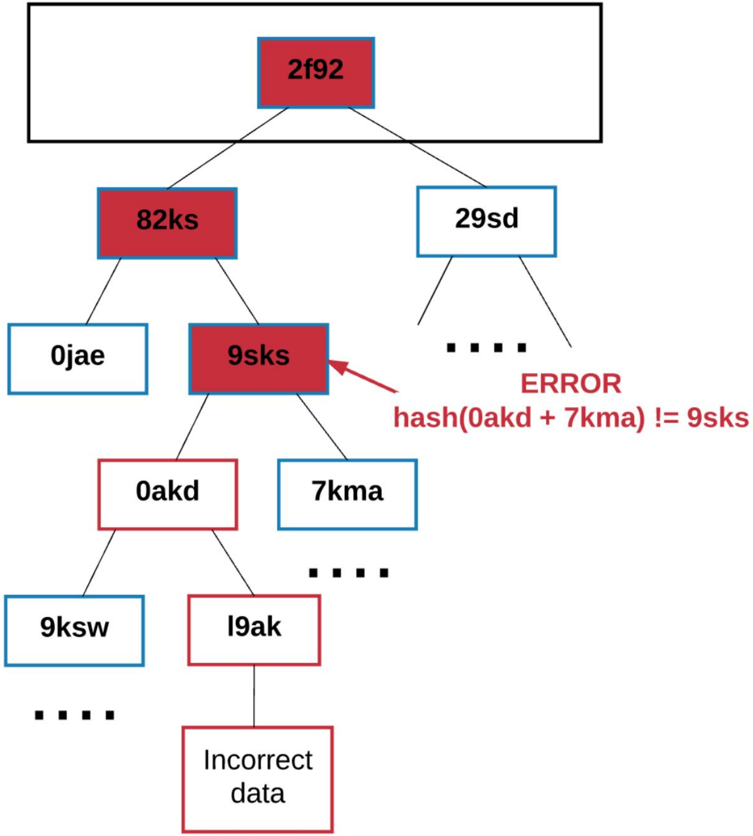
– Implemented working private transactions on Ethereum rollup testnet: Arbitrum

– next: keep surveying zk-SNARKs

Merkle Proof (Bitcoin)



Merkle Proof – Verification



Layer 1

– In our blockchain setting, we can abstract the current consensus layer as "Layer 1" (L1)

- – holds proof of transactions (merkle roots)
- – holds transaction data itself
- – not zero-knowledge
  - – anyone can connect to the p2p network, download history of all previous transactions

Rollups

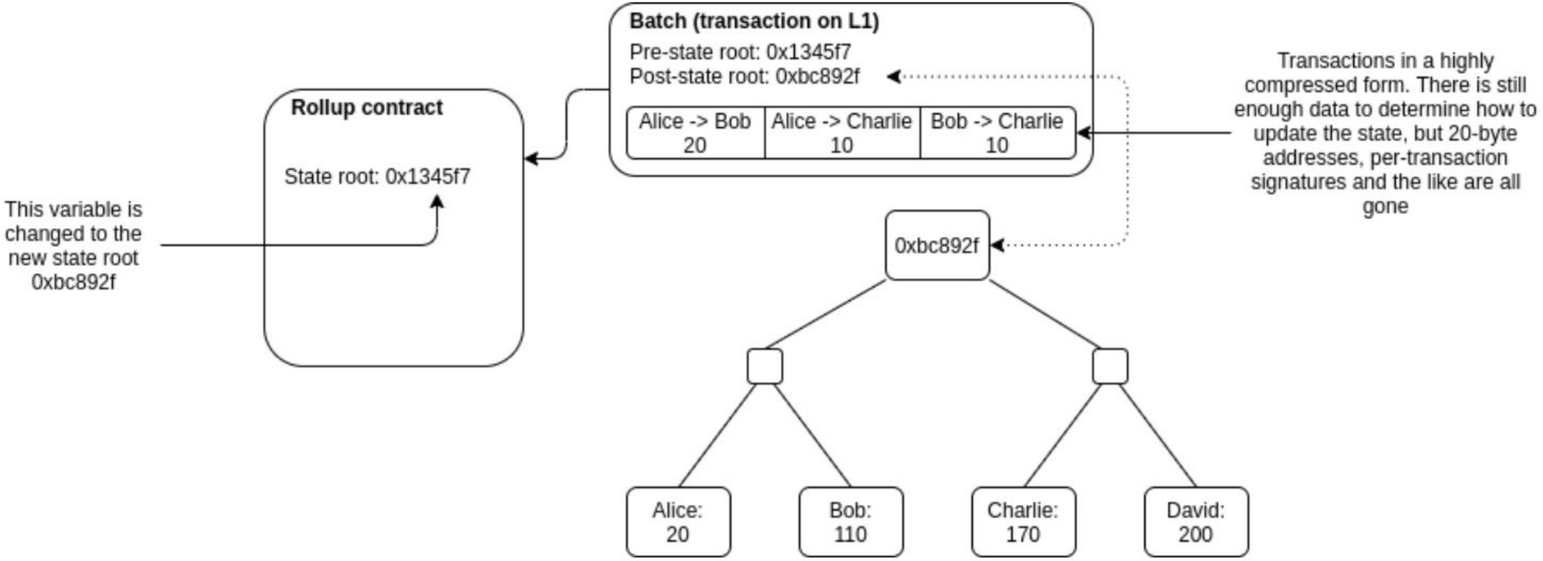
– Rollups move computation (and state storage) off-chain, but keep some data per transaction on-chain

– Result is a system where scalability is still limited by the data bandwidth of the underlying blockchain, but at a very favorable ratio

– Use compression tricks to replace data with computation wherever possible

Rollups

– Anyone can transaction with funds inside of the rollup, which are batched to exit be used onto regular L1

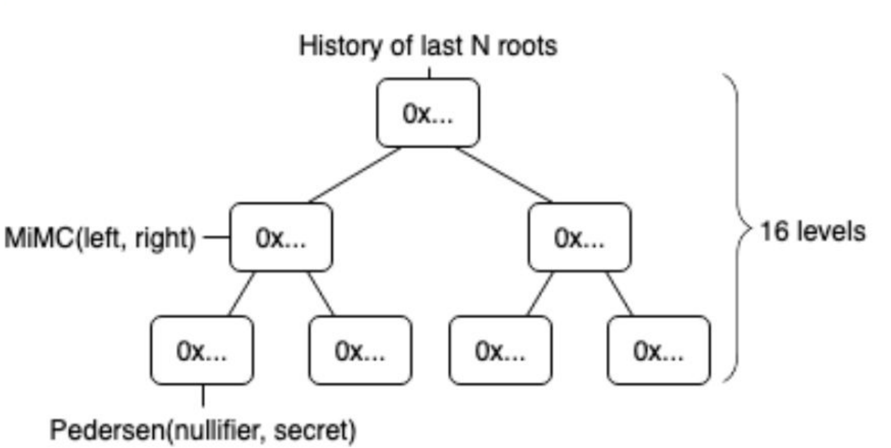


This variable is changed to the new state root 0xbc892f

Transactions in a highly compressed form. There is still enough data to determine how to update the state, but 20-byte addresses, per-transaction signatures and the like are all gone

zk Deposit / Withdrawal

- On Deposit
  - generate random **secret** and **nullifier**
  - compute commitment using **secret** and **nullifier**



- On Withdrawal
  - prover provides merkle path and preimage (**nullifier**) to commitment
  - verifier checks SNARK proof provided by spender (zero-knowledge proof of **secret**), releases funds

Resources

- Open-source zk-SNARK private tx's: https://app.tornado.cash/
- Arbitrum Rollups testnet: https://explorer.offchainlabs.com/#/
- Twister repo: https://github.com/technicallyty/tornado-frax-ui