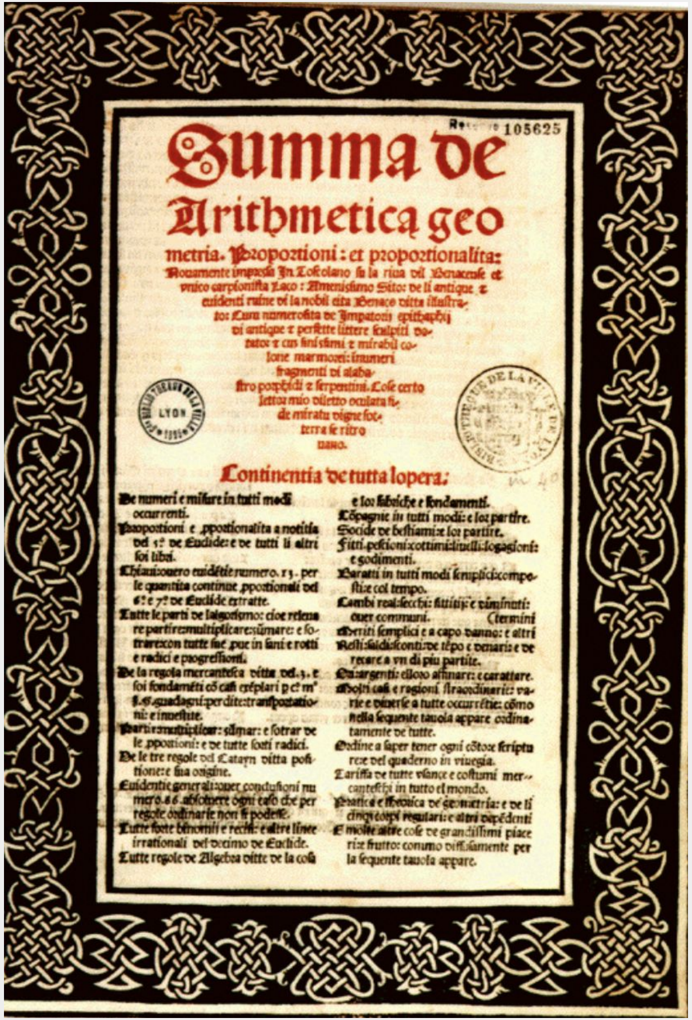
Summa

HCMC - 6/4/2022

Enrico & Jin



Summa de Arithmetica geometria. Proportioni: et proportionalita:

Novamente impressa In Toscolano su la riva dil Benacense et unico carpionista Laco: Amenissimo Sito: de li antique e evidenti ruine di la nobil cita Benaco ditta illustrata: Cum numerosita de Impatori epithaphii di antique e perfette littere sculpiti dotato e cum finissimi e mirabil colone marmorei: inumeri fragmenti di alabastro porphidi e serpentini. Cose certo lettor mio diletto oculata fide miratu digne sotterra se ritrovano.

Continentia de tutta lopera:

De numeri e misure in tutti modi occurrenti.
Proportioni e pportionalita a notitia del 5.° de Euclide: e de tutti li altri soi libri.
Chiavi: overo evidentie numero. 13. per le quantita continue pportionali del 6.° e 7.° de Euclide extratte.
Tutte le parti de lalgorismo: cioe relevare partire: multiplicare: summare: e sotrare: con tutte sue pve in sani e rotti e radici e progressioni.
De la regola mercantesca ditta del. 3. e soi fondamenti co casi exemplari p c.° m° f. e guadagni: perdite: transportationi: e investite.
Partir multiplicar: summar: e sotrar de le pportioni: e de tutte sorti radici.
De le tre regole del Catayn ditta positione: e sua origine.
Evidentie generali: over conclusioni numero. 66. absolvere ogni caso che per regole ordinarie non si podesse.
Tutte sorte binomii e recisi: e altre linee irrationali del decimo de Euclide.
Tutte regole de Algebra ditte de la cosa e lor fabriche e fondamenti.
Copagnie in tutti modi: e lor partire.
Socide de bestiami: e lor partire.
Fitti: pesioni: cottimi: livelli: logagioni: e godimenti.
Baratti in tutti modi semplici: composti: e col tempo.
Cambi reali: secchi: fittitii: e diminuti: over communi.
Termini: Meriti semplici e a capo danno: e altri Resti: saldi: sconti: de tepo e denari: e de recare a un di piu partite.
Oro: argenti: e loro affinare: e carattare.
Molti casi e regioni straordinarie: varie e diverse a tutte occurretie: como nella sequente tavola appare ordinatamente de tutte.
Ordine a saper tener ogni cōto e scripture del quaderno in vinegia.
Tariffa de tutte usance e costumi mercanteschi in tutto el mondo.
Pratica e theorica de geometria: e de li cinqi corpi regulari: e altri depēdenti
E molte altre cose de grandissimi piacer: e frutto: comumo diffusamente per la sequente tavola appare.

Chapter 7

The Manner in Which All Business Books Are to be Authenticated, Why, and by Whom.

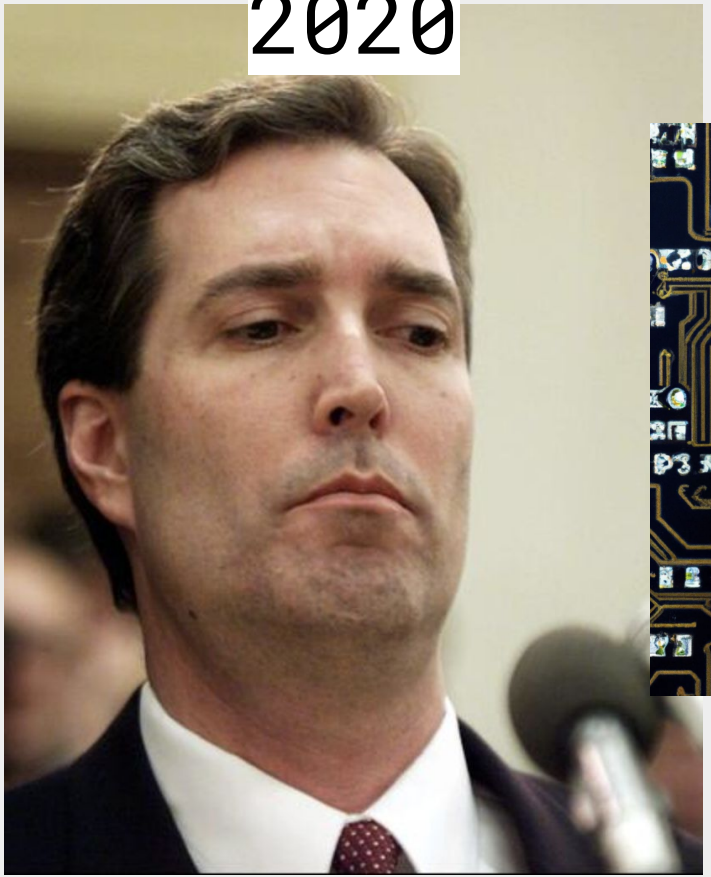
transactions.

In the name of his officer, the clerk will write all this on the first page of your books and will attest to its truth. He will then attach the seal of the pertinent officer which will make them authentic for any situation in which their presentation might be required. This custom should be fully commended, as should the places where it is observed.

Book authentication

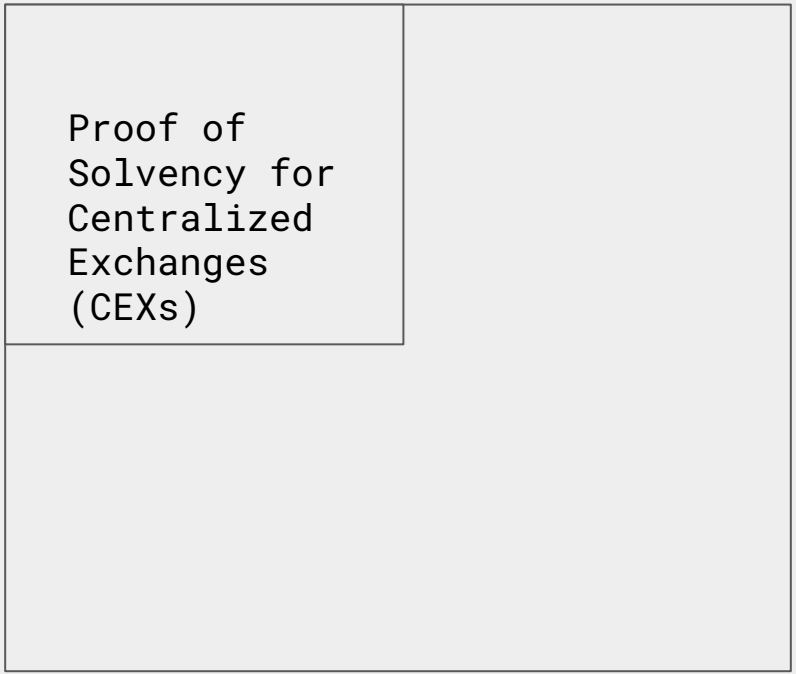
1400

2020



2023

Book Authentication

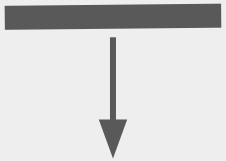


Proof of Solvency

- Cryptographic proof that a CEX is solvent at a specific moment in time

Proof of Solvency

- Cryptographic proof that a CEX is solvent at a specific moment in time



Assets >= Liabilities

LIABILITIES

- Deposits of the users
- Denominated in ETH, BTC, USDC …
- Do not live on-chain, live in the CEX’s DB

ASSETS

- Cryptographic assets (ETH, BTC, USDC…) controlled by the CEX
- Live on-chain
- Should map 1:1 the deposits of the users

LIABILITIES

- Deposits of the users
- Denominated in ETH, BTC, USDC …
- Do not live on-chain, live in the CEX’s DB

Proof Of Solvency

- Cryptographic proof that a CEX is solvent at a specific moment in time

Summa: ZK Proof of Solvency

Why ZK?

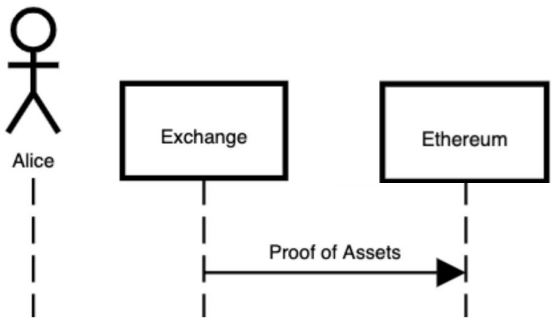
ZK of what?

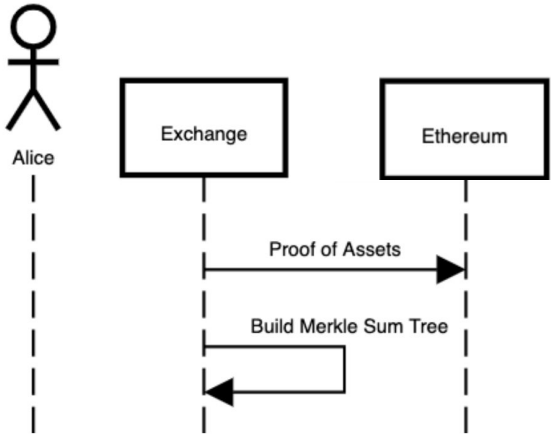
- Other users information such as their balances and usernames
- Total number of users
- Total amount of liabilities
- Total amount of assets
- The addresses of the wallets controlled by the CEX

ZK of what?

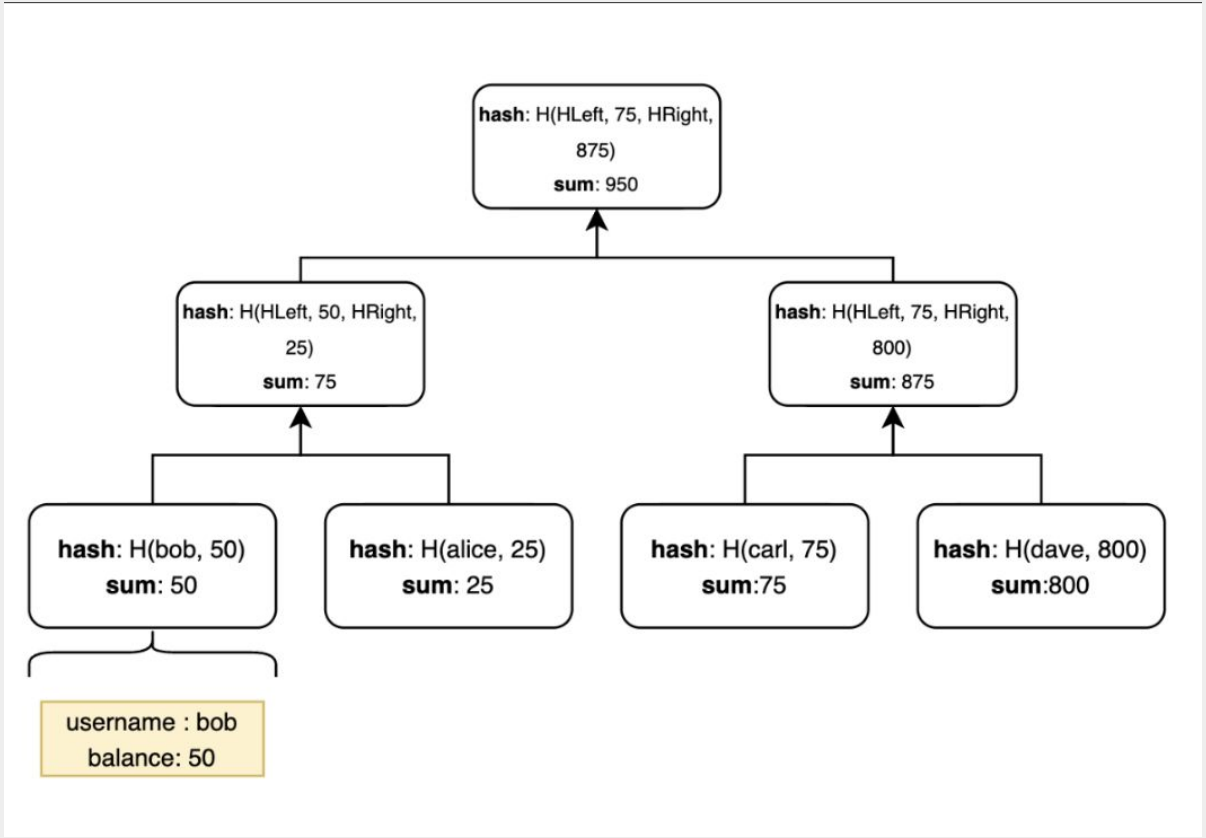
- Other users information such as their balances and usernames
- Total number of users
- Total amount of liabilities
- Total amount of assets (WIP)
- The addresses of the wallets controlled by the CEX (WIP)

How?

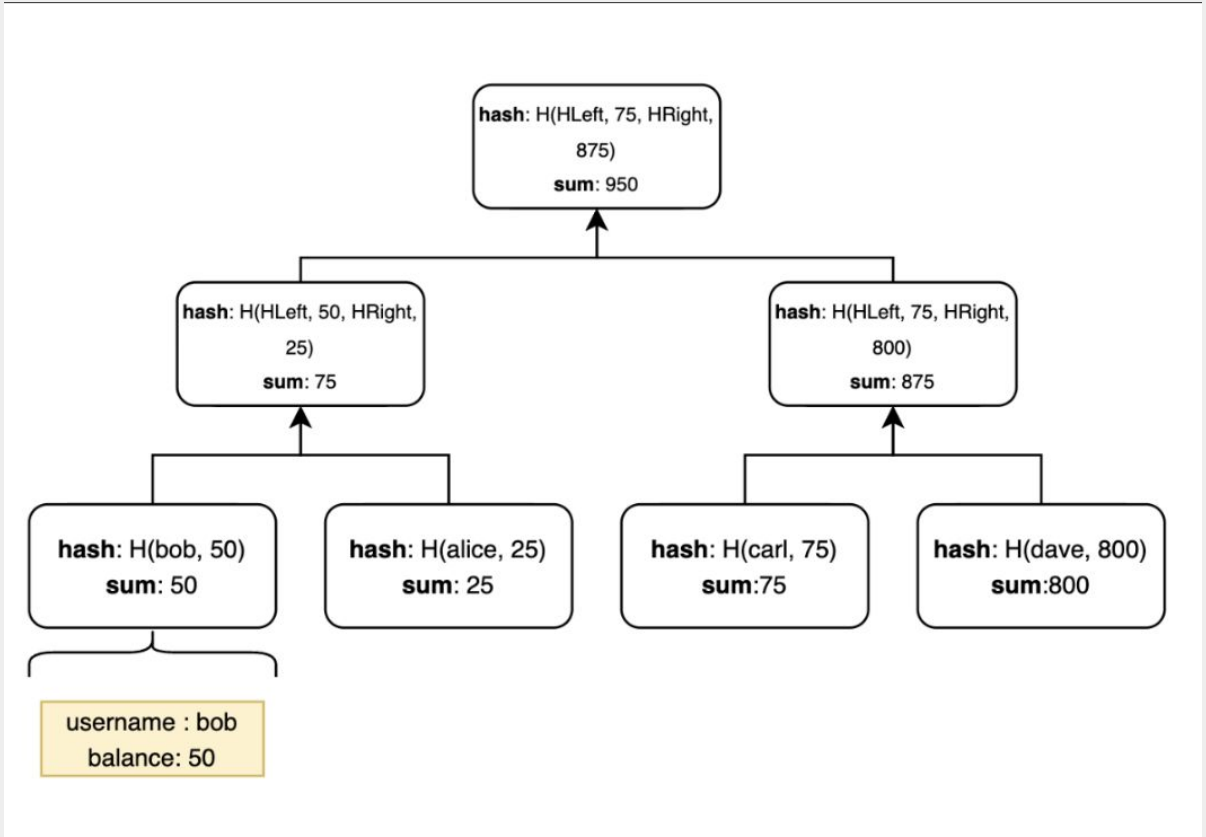

Alice
Exchange
Ethereum
Proof of Assets


Alice
Exchange
Ethereum
Proof of Assets
Build Merkle Sum Tree

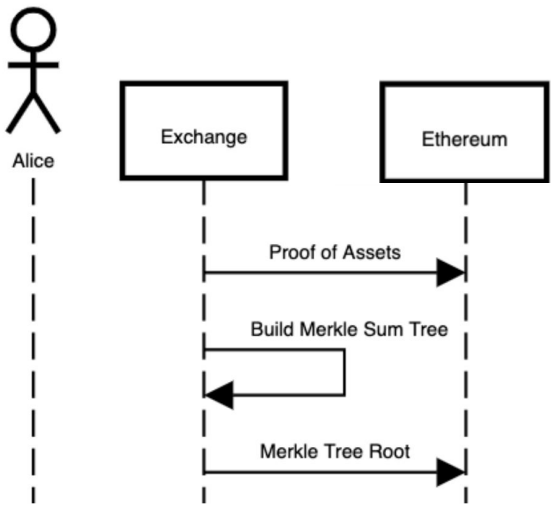
Merkle Sum Tree

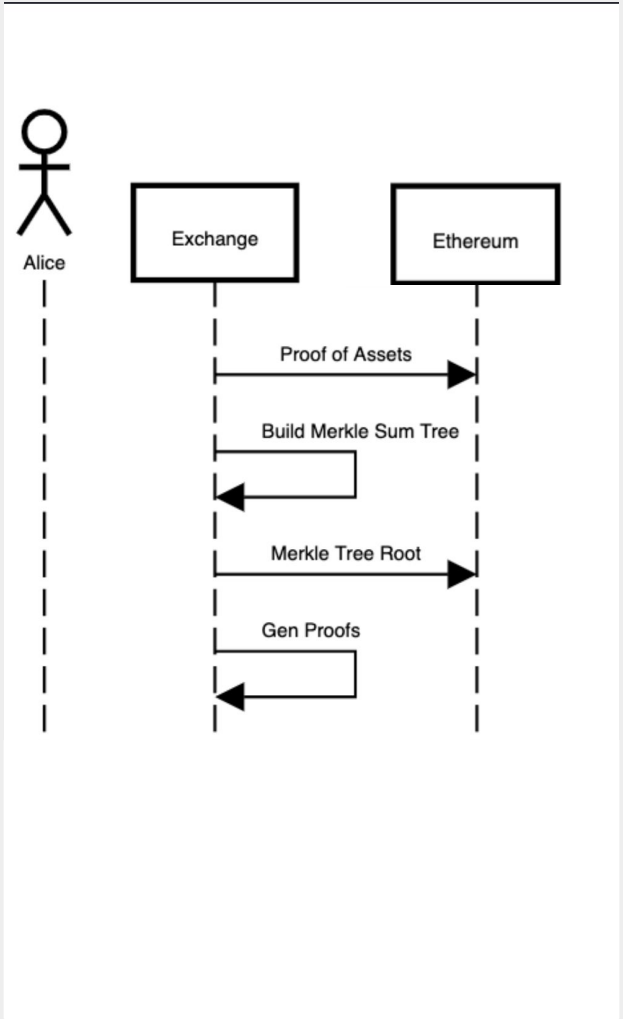


Merkle Sum Tree



- The entries are the users' data (= liabilities)
- Lives off-chain
- Only the root-hash gets published on-chain


Alice
Exchange
Ethereum
Proof of Assets
Build Merkle Sum Tree
Merkle Tree Root


Alice
Exchange
Ethereum
Proof of Assets
Build Merkle Sum Tree
Merkle Tree Root
Gen Proofs

Zk Proofs

- Individual Proof for each user

Zk Proofs

- Individual Proof for each user
- Attest that the user is included in the MST with the correct balance

Zk Proofs

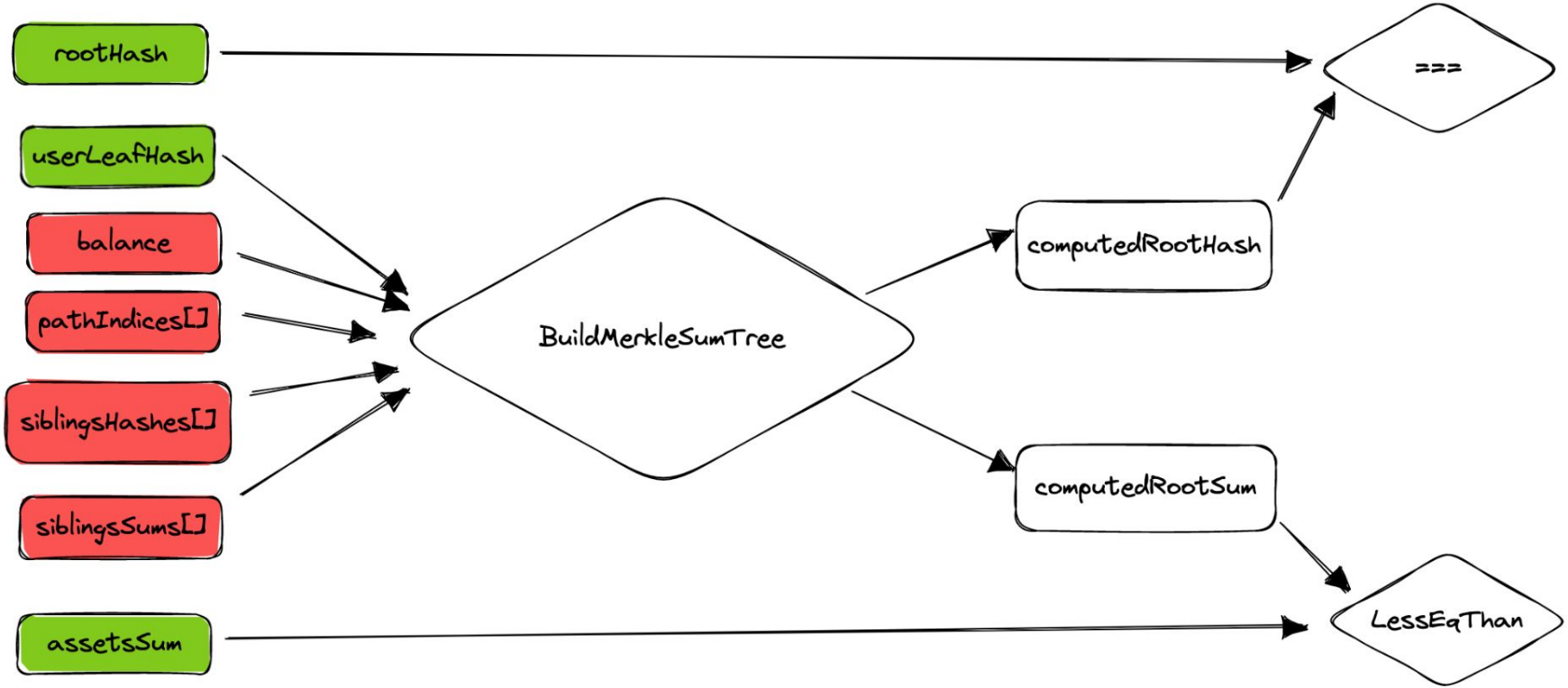
- Individual Proof for each user
- Attest that the user is included in the MST with the correct balance
- Attest that hash of the MST matches the one committed

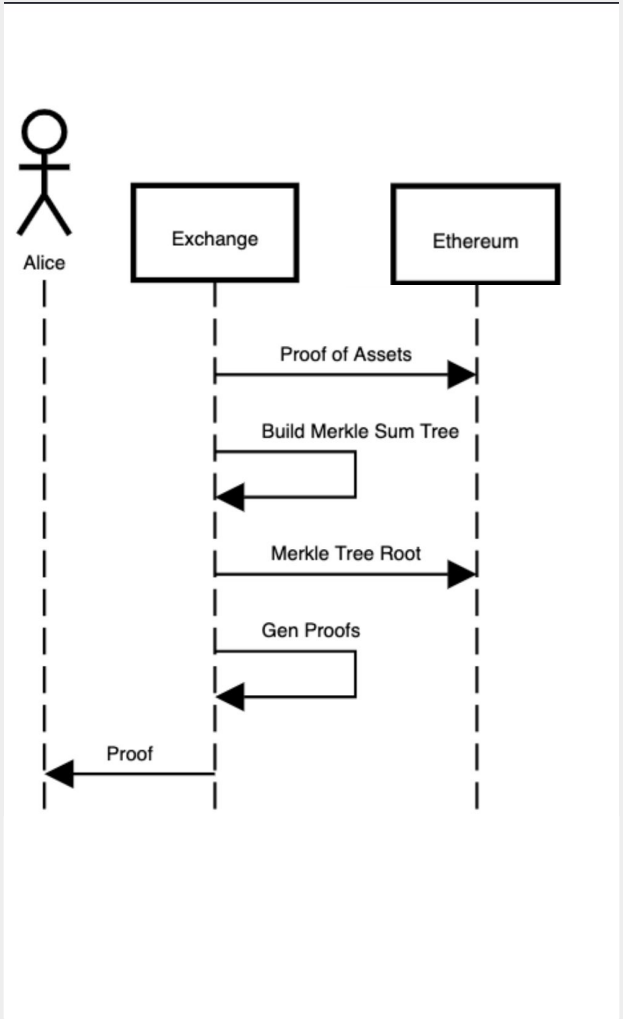
Zk Proofs

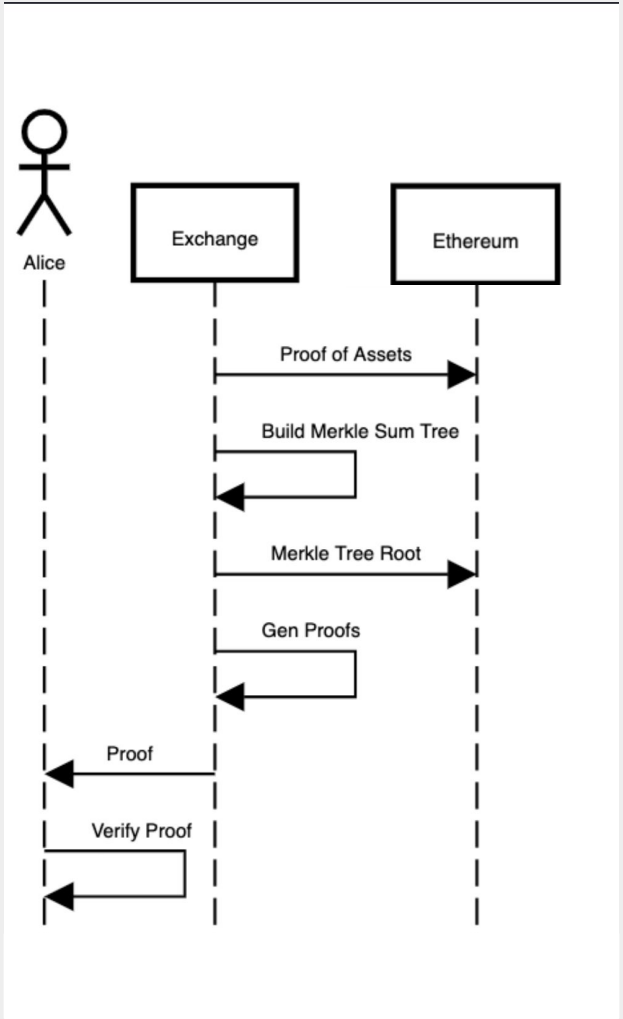
- Individual Proof for each user
- Attest that the user is included in the MST with the correct balance
- Attest that hash of the MST matches the one committed
- Attest that sum of liabilities is Less Than the assets of the exchange (as committed in step 1)

Zk Proofs

- Individual Proof for each user
- Attest that the user is included in the MST with the correct balance
- Attest that hash of the MST matches the one committed
- Attest that sum of liabilities is Less Than the assets of the exchange (as committed in step 1)
- Attest that no sum overflow happened in the merkle sum tree computation


rootHash
userLeafHash
balance
pathIndices[]
siblingsHashes[]
siblingsSums[]
assetsSum
BuildMerkleSumTree
computedRootHash
computedRootSum
===
LessEqThan

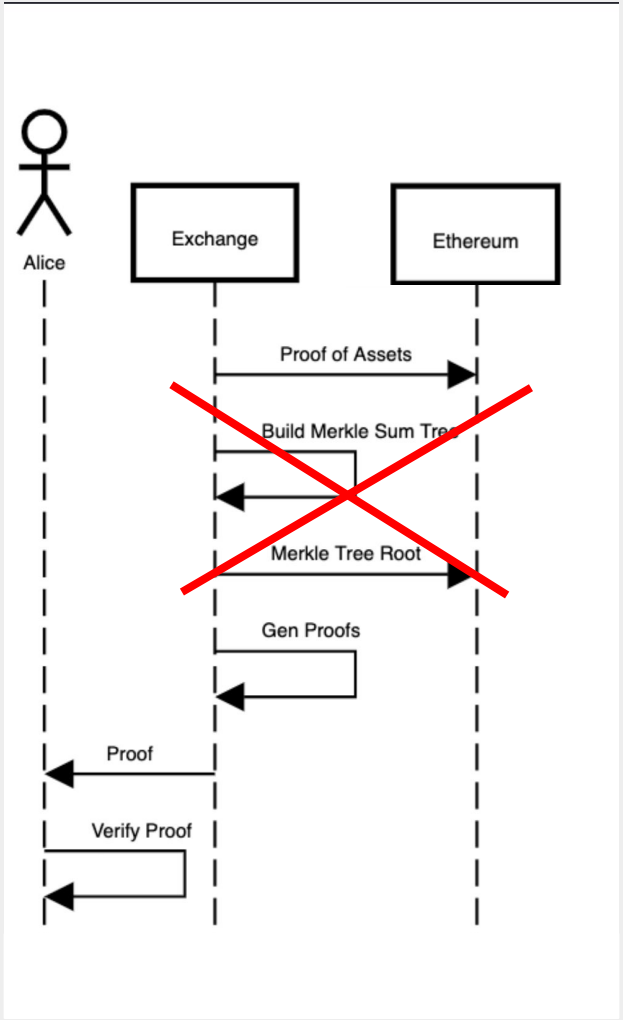

Alice
Exchange
Ethereum
Proof of Assets
Build Merkle Sum Tree
Merkle Tree Root
Gen Proofs
Proof


Alice
Exchange
Ethereum
Proof of Assets
Build Merkle Sum Tree
Merkle Tree Root
Gen Proofs
Proof
Verify Proof

Proof Verification

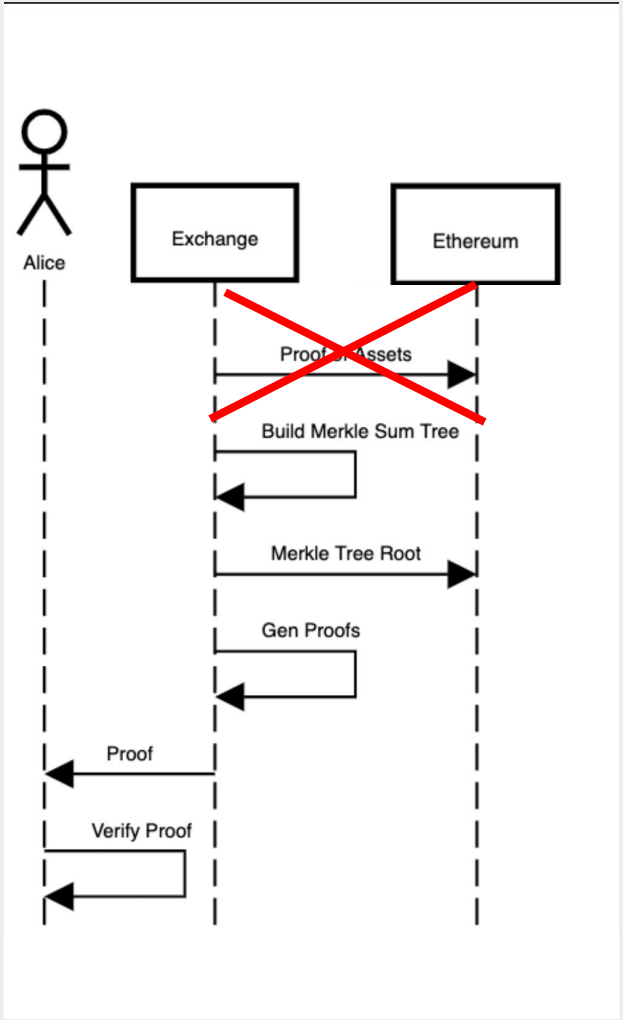
F(proof, username, balance, assets, root)

Next Steps


Alice
Exchange
Ethereum
Proof of Assets
Build Merkle Sum Tree
Merkle Tree Root
Gen Proofs
Proof
Verify Proof

Polynomial Commitment

- Replace the merkle sum tree commitment with a polynomial commitment
- Proving that (username, Balance) is included in that commitment


Alice
Exchange
Ethereum
Proof of Assets
Build Merkle Sum Tree
Merkle Tree Root
Gen Proofs
Proof
Verify Proof

idea #1 Ethereum State Proof

- Prove that Cex own a wallet using ECDSA Signature
- Prove the balance of that wallet using account proofs from the ethereum state Trie
- Prove that this balance is >= liabilities

idea #2 Recursion for privacy

- Recursively verify inside a snark that:
  - an Axiom proof attesting the balance of a wallet is valid
  - the CEX controls that wallet (ECDSA signature)
  - the balance of that wallet is >= total liabilities

idea #2 Recursion for privacy

- Recursively verify inside a snark that:
  - an Axiom proof attesting the balance of a wallet is valid
  - the CEX controls that wallet (ECDSA signature)
  - the balance of that wallet is >= total liabilities

The recursed proof hides a public input from the original proof

Open issues

Open issues

- Dispute resolution

Open issues

- Dispute resolution
- Interactive protocol

Thank you!

Merkle Sum Tree - Rust

Halo2 Circuits