Building Better Privacy Applications

&

Benefiting Miner Economy

Berat@citrea/smartContracts
@okkothejawa

Two workshops in one

- Achieving better privacy and UX than CoinJoins with cBTC Tornado Cash pools
    - Deployment steps for Tornado Cash core and UI
    - Using a Tornado Cash instance on Citrea Testnet
- Benefiting miner economy with a miner incentivization ₿app
    - Going through the code
    - Testing it via Forge test

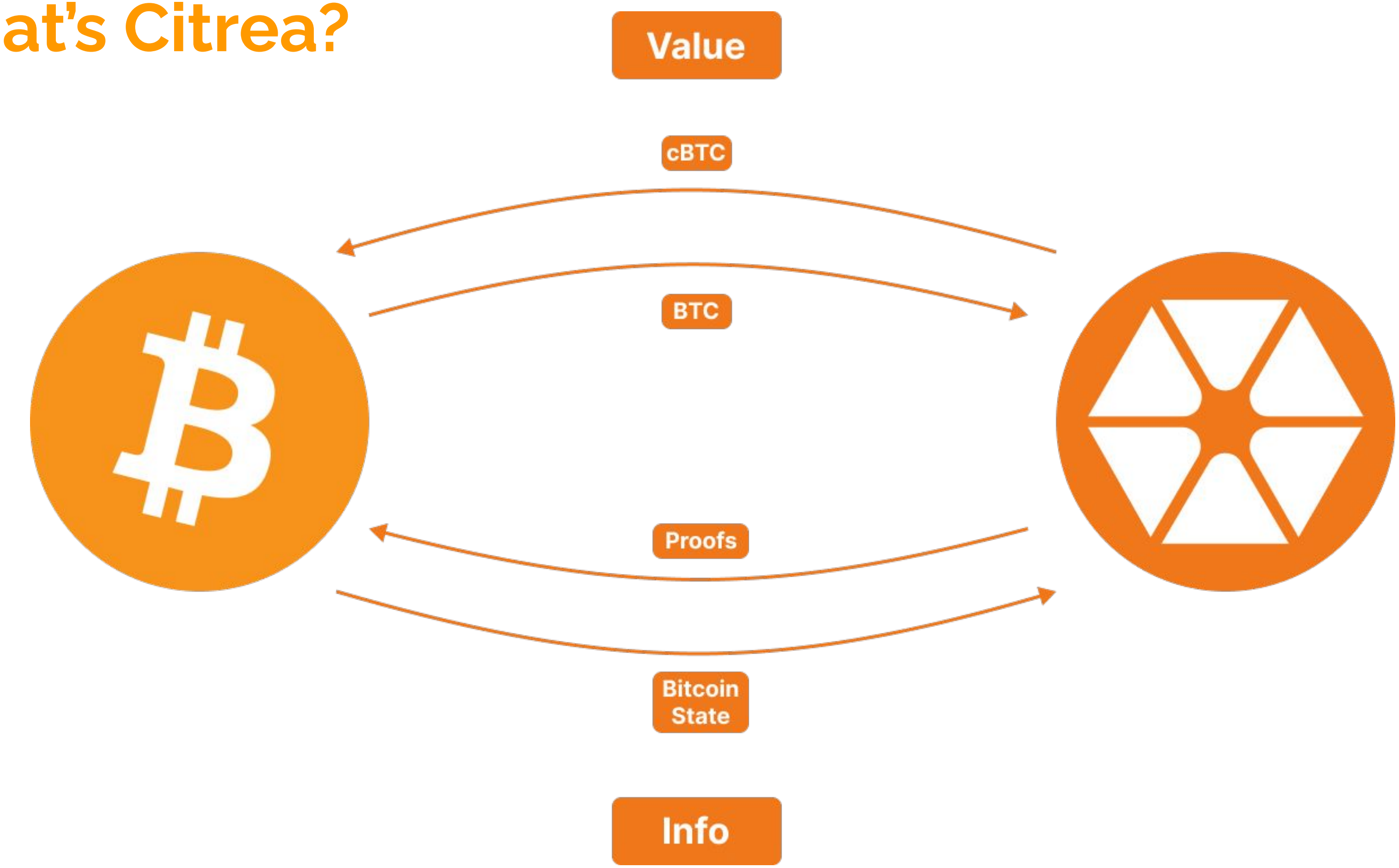
What's a smart contract?

- Immutable* software that runs on Ethereum Virtual Machine.
- If a line of code reverts, the whole call reverts (stops execution).
- Compute costs gas (money).
- No scheduled calls, so there isn't something like a cron job. All transactions must originate from external actors.

ZK?

- Privacy
- Scaling
- Assume there is a cryptographic way of verifying the result of a computation without doing the computation yourself, and the inputs of this computation can be secret.
- Prove that you made a deposit to a bank without revealing who you are.
- Verify that after applying the list of transactions *T*, Citrea's state moved from *S0* to *S1* without running *T* yourself.

What's Citrea?



Value

cBTC

BTC

Proofs

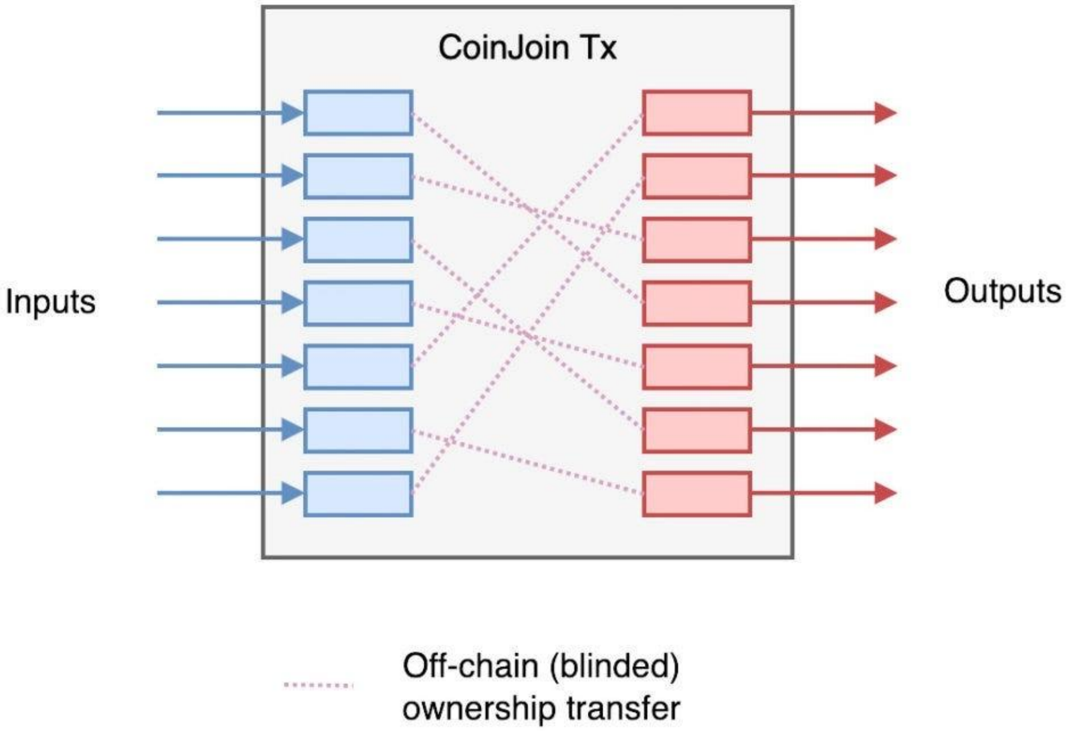
Bitcoin State

Info

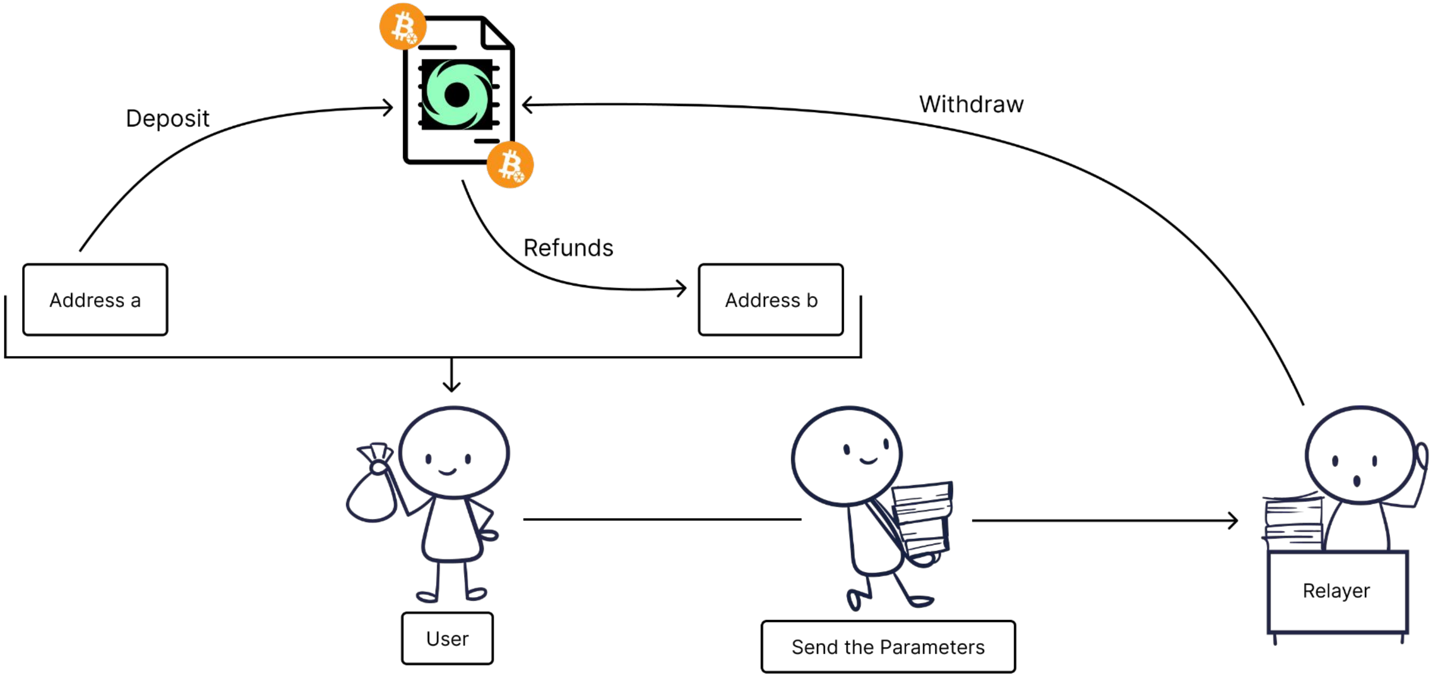
cBTC

- Has a better bridge than its alternatives such as wBTC on Ethereum. wBTC is controlled by a mere multisig while cBTC is powered by Clementine, a trust-minimized bridge utilizing BitVM.
- wBTC is just a token among many, cBTC is the central asset of Citrea.

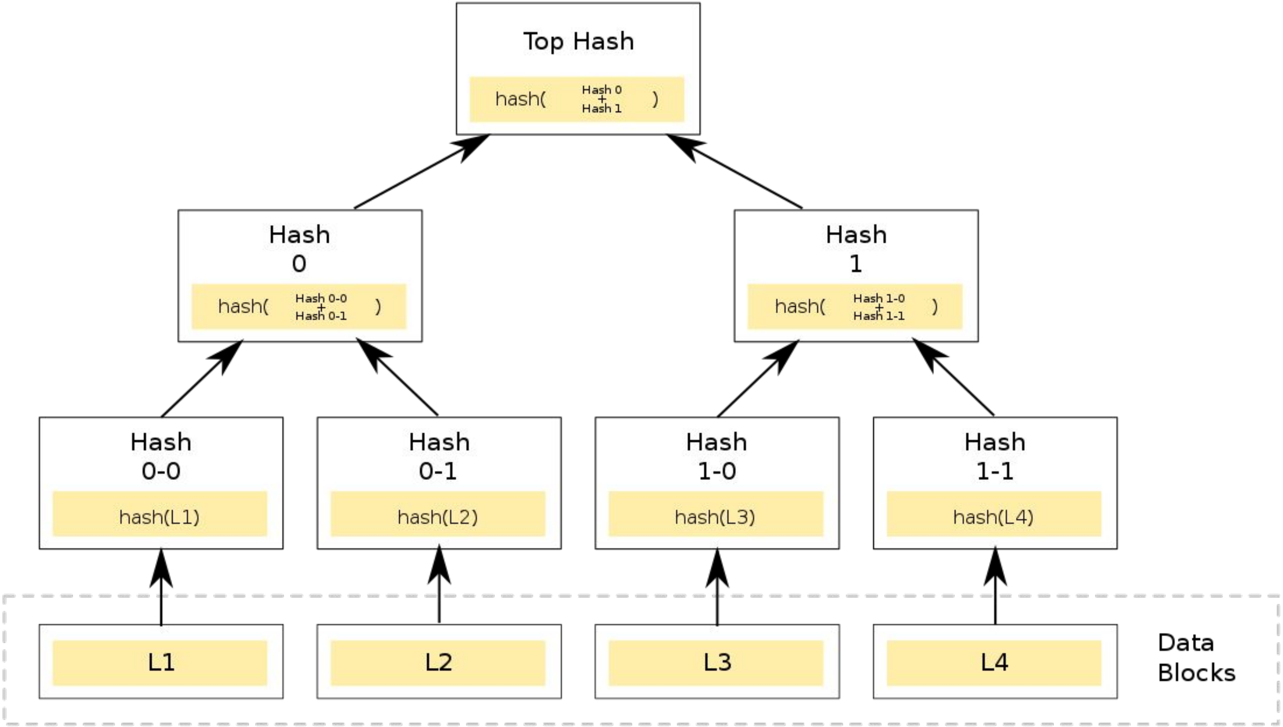
Coinjoin


CoinJoin Tx
Inputs
Outputs
Off-chain (blinded) ownership transfer

Flows of Tornado Cash



A Merkle tree



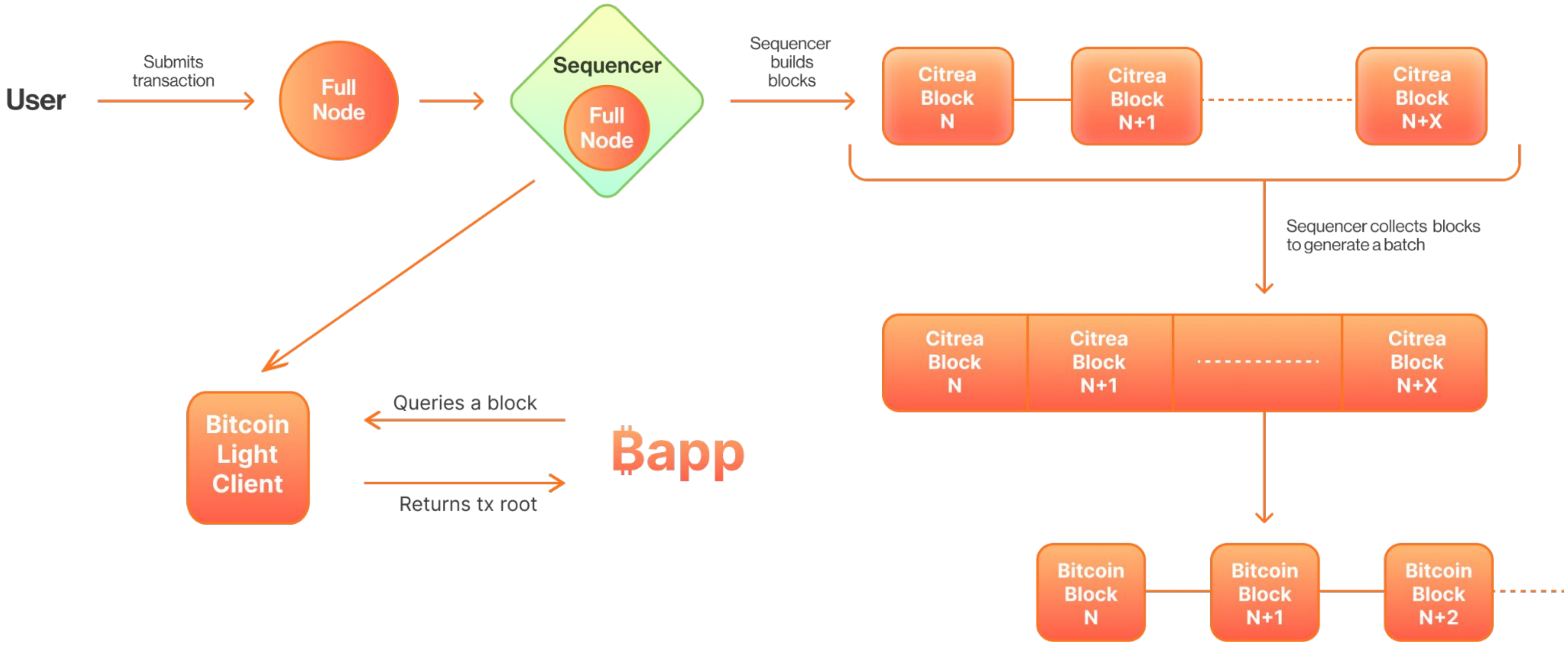
Comparing Coinjoin with Tornado Cash

- A single Coinjoin transaction’s anonymity set is practically limited to the number of participants who provided inputs during a short period of time.
- After a certain amount of time, Tornado Cash pools’ anonymity set is all the depositors. Tornado Cash depositors can wait indefinitely before withdrawing.
- Coinjoins suffer from UX problems as if any input UTXO is spent before the tx is sent, the whole process needs to start over. Wallets and protocols may mitigate this problem to a degree but Tornado Cash simply doesn’t have this problem.

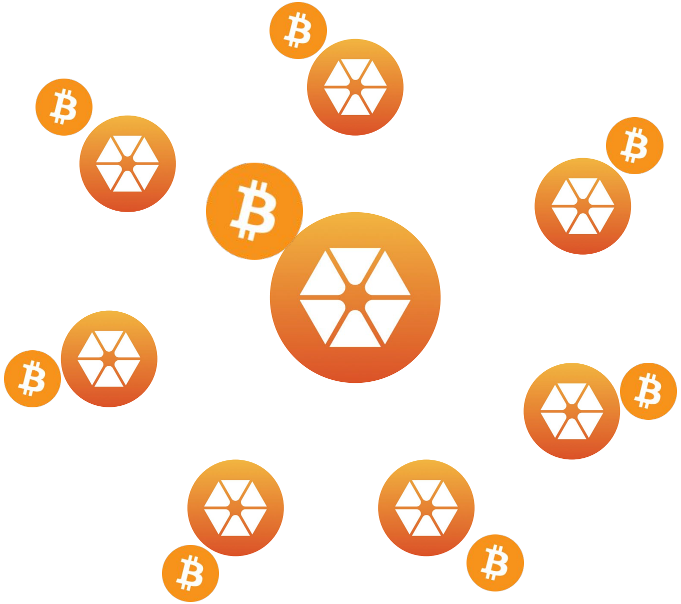
Anonymization strategy with cBTC

- Bridge BTC to Citrea via Clementine or a 3rd party bridge depending on the amount
- Deposit to Tornado Cash
- Withdraw to a fresh address after waiting a while
- Bridge cBTC back to Bitcoin

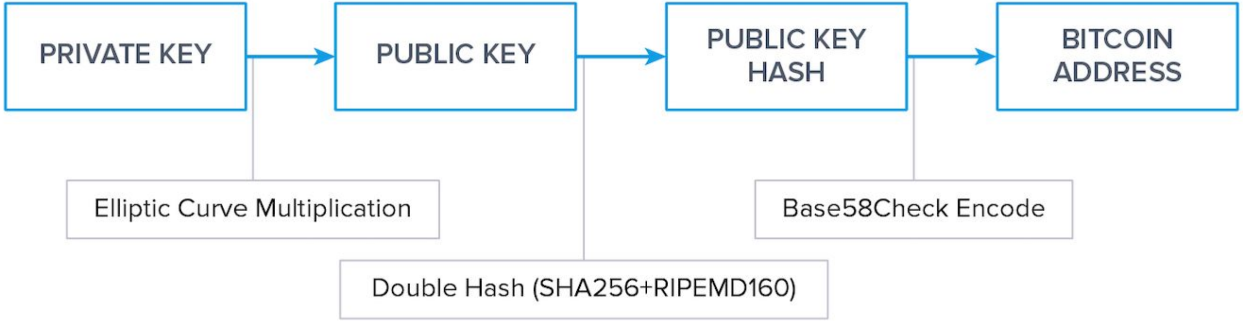
Citrea's access to Bitcoin state



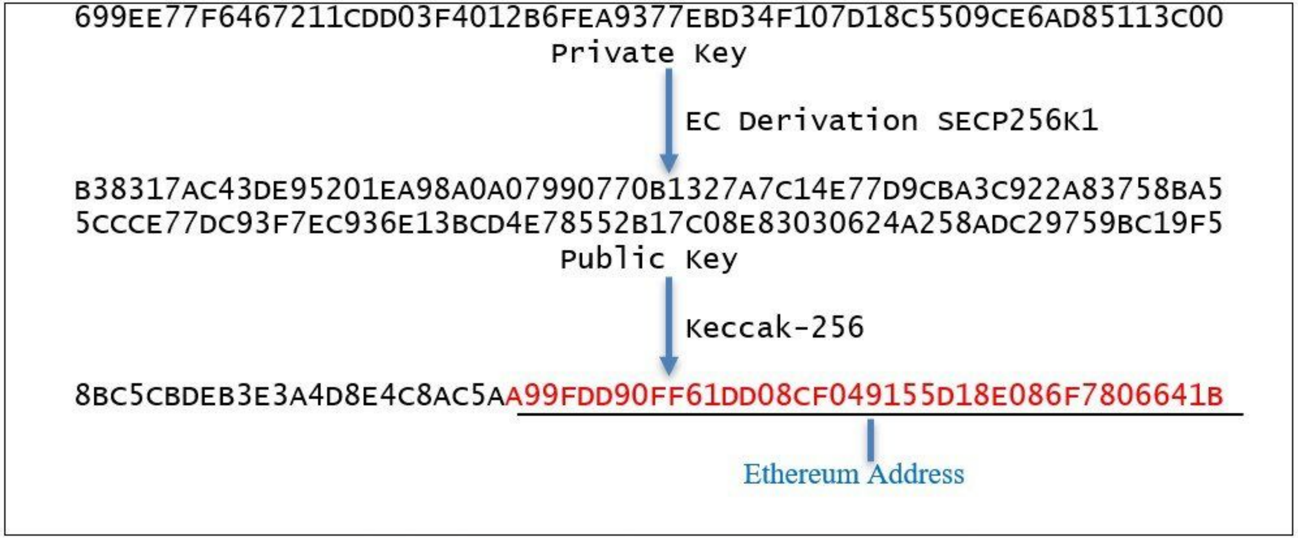
Citrea's access to Bitcoin state



Bitcoin address generation



EVM address generation



699EE77F6467211CDD03F4012B6FEA9377EBD34F107D18C5509CE6AD85113C00

Private Key

EC Derivation SECP256K1

B38317AC43DE95201EA98A0A07990770B1327A7C14E77D9CBA3C922A83758BA5
5CCCE77DC93F7EC936E13BCD4E78552B17C08E83030624A258ADC29759BC19F5

Public Key

Keccak-256

8BC5CBDEB3E3A4D8E4C8AC5AA99FDD90FF61DD08CF049155D18E086F7806641B

Ethereum Address

Incentivizing miners

- Reward miners with cBTC after mining rewards are halved to 0.
- Incentivize miners to include your tx with cBTC, could be also done for non-standard txs.