How to build a Ƀapp?

Berat@citrea/smartContracts
@okkothejawa

What's a ฿app?

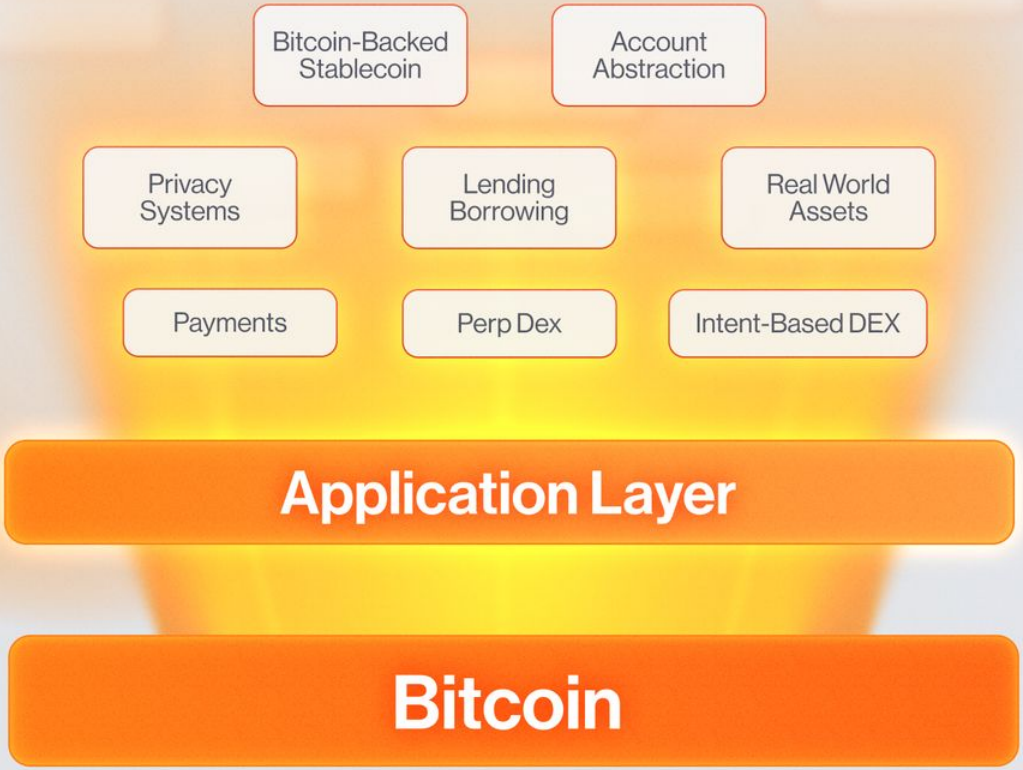
Bitcoin's (lack of) programmability

- Bitcoin's programmability is limited to specifying under which conditions Bitcoins can be spent.
- You can specify that you want your Bitcoins to be spend by someone who knows a preimage to a hash, someone who knows the answer to an arithmetic equation, or in most of the cases, holder of a private key.
- This level of programmability is not sufficient for a proper financial application.

What's a ₿app?

- Non-custodial
- Uses BTC or BTC-denominated assets
- Secured by Bitcoin network

₿apps Framework



Non-custodial applications that use BTC or BTC-denominated assets and are secured by the Bitcoin network.

Extends BTC's utility via zero-knowledge technology, atomic swaps, BitVM-based bridge and cross-chain infrastructure.

Absorbs the economic activity by supporting applications on the execution layer.

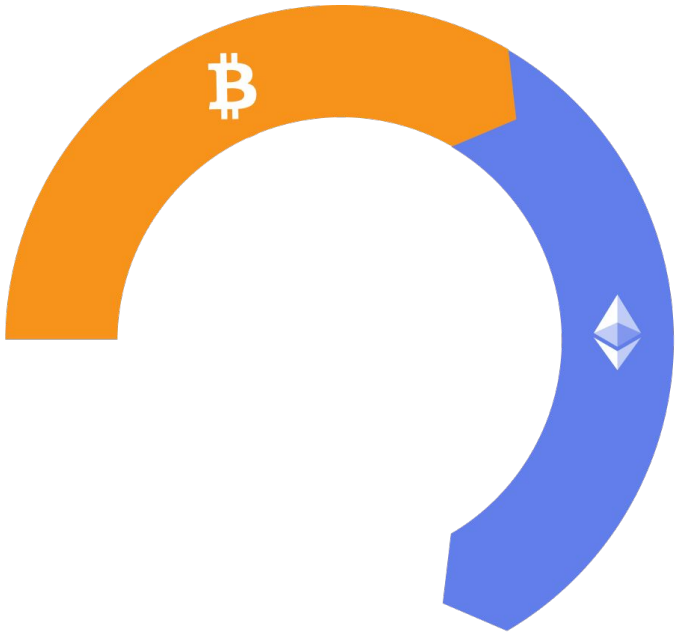
Why build a ฿app?

2.2T $

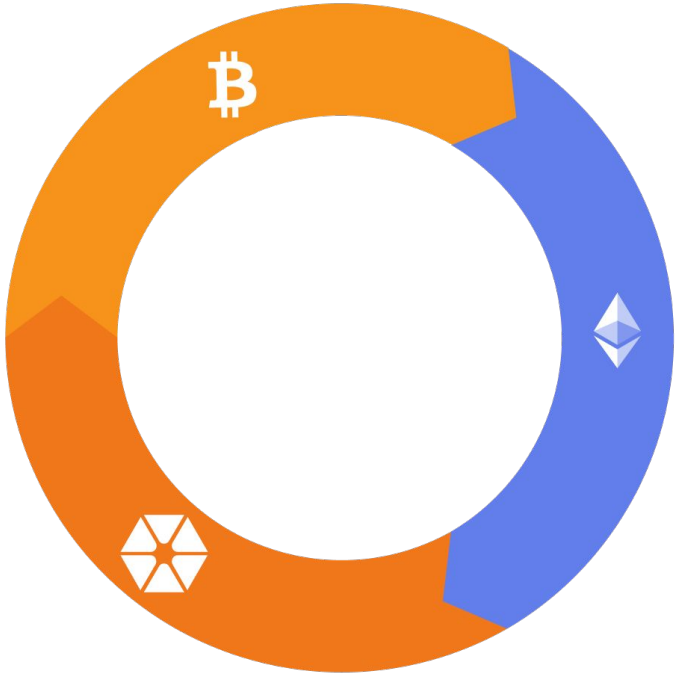
Bitcoin’s market cap

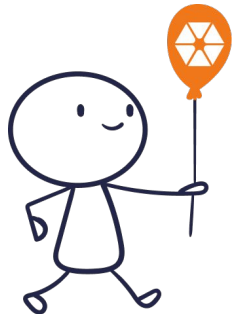
Where to build a Ƀapp?

A timeline of Bitcoin and Ethereum

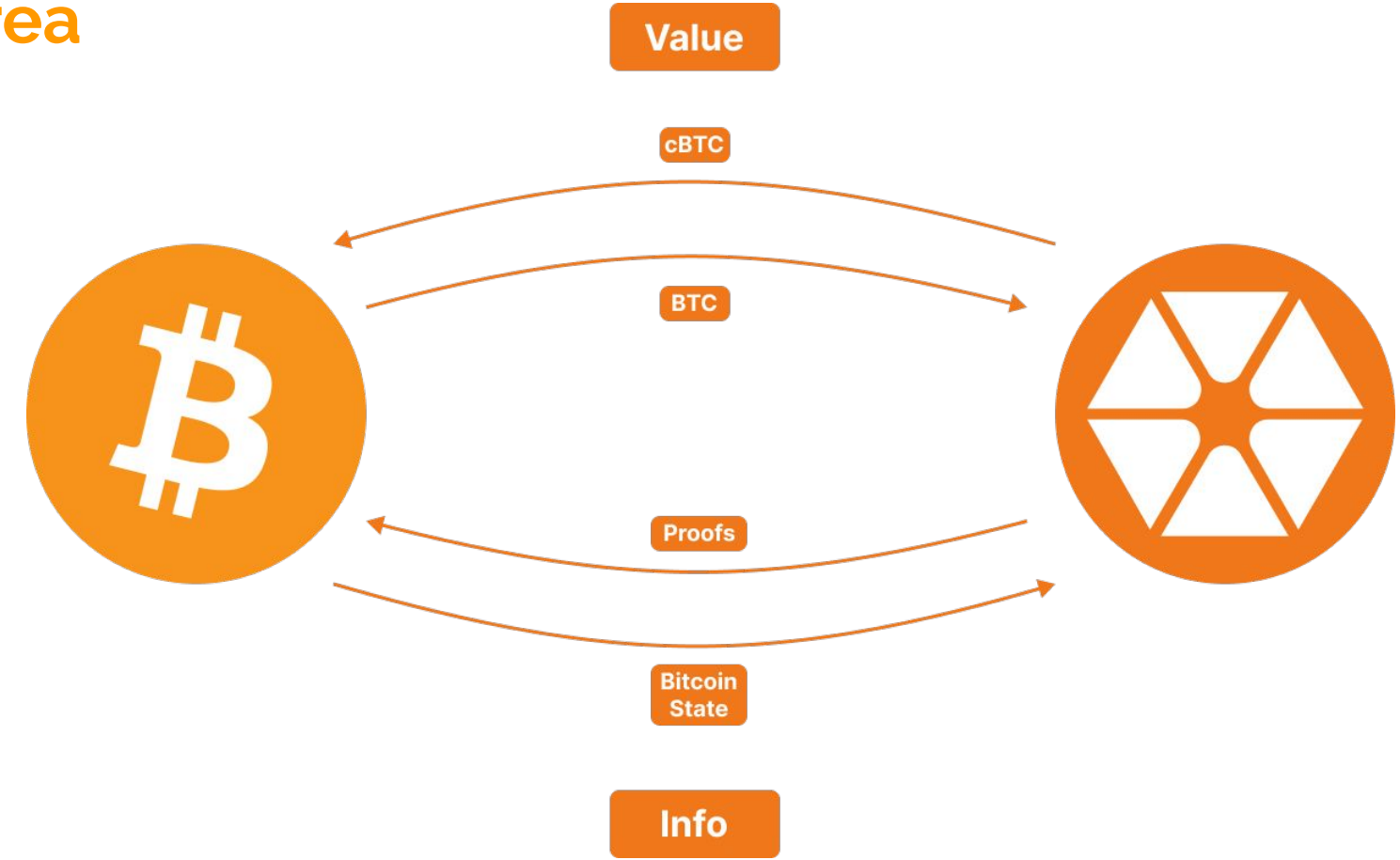


Citrea bridges the gap





Citrea



cBTC

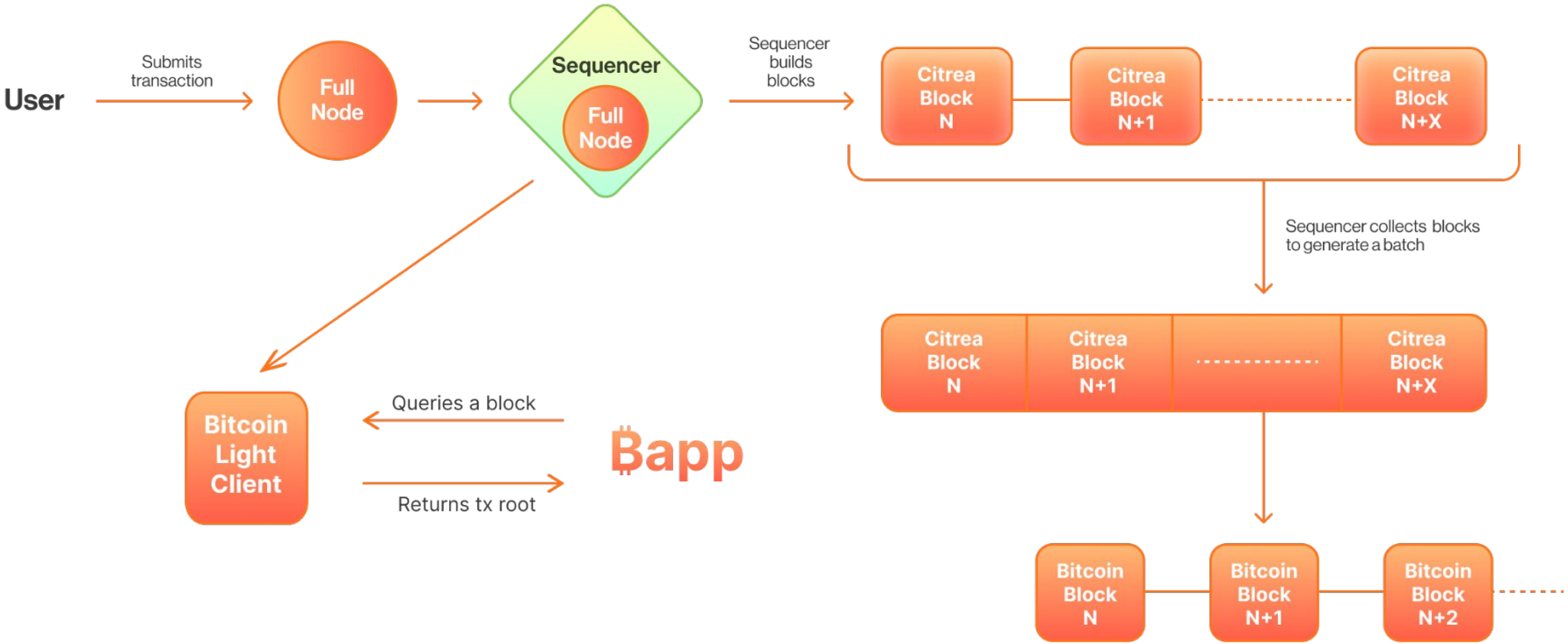
- Has a better bridge than its alternatives such as wBTC on Ethereum. wBTC is controlled by a mere multisig while cBTC is powered by Clementine, a trust-minimized bridge utilizing BitVM.
- wBTC is just a token among many, cBTC is the central asset of Citrea.

How to build a ฿app?

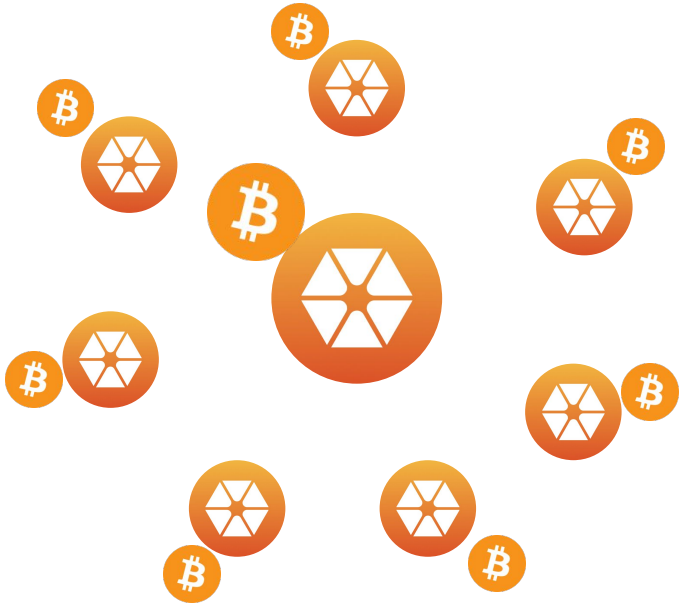
Some types of ₿apps

- Cross-chain application between Bitcoin and Citrea
- Citrea application utilizing cBTC
- Citrea application acting on external information about Bitcoin without interacting with Bitcoin directly (e.g BTC price)

Citrea's access to Bitcoin state



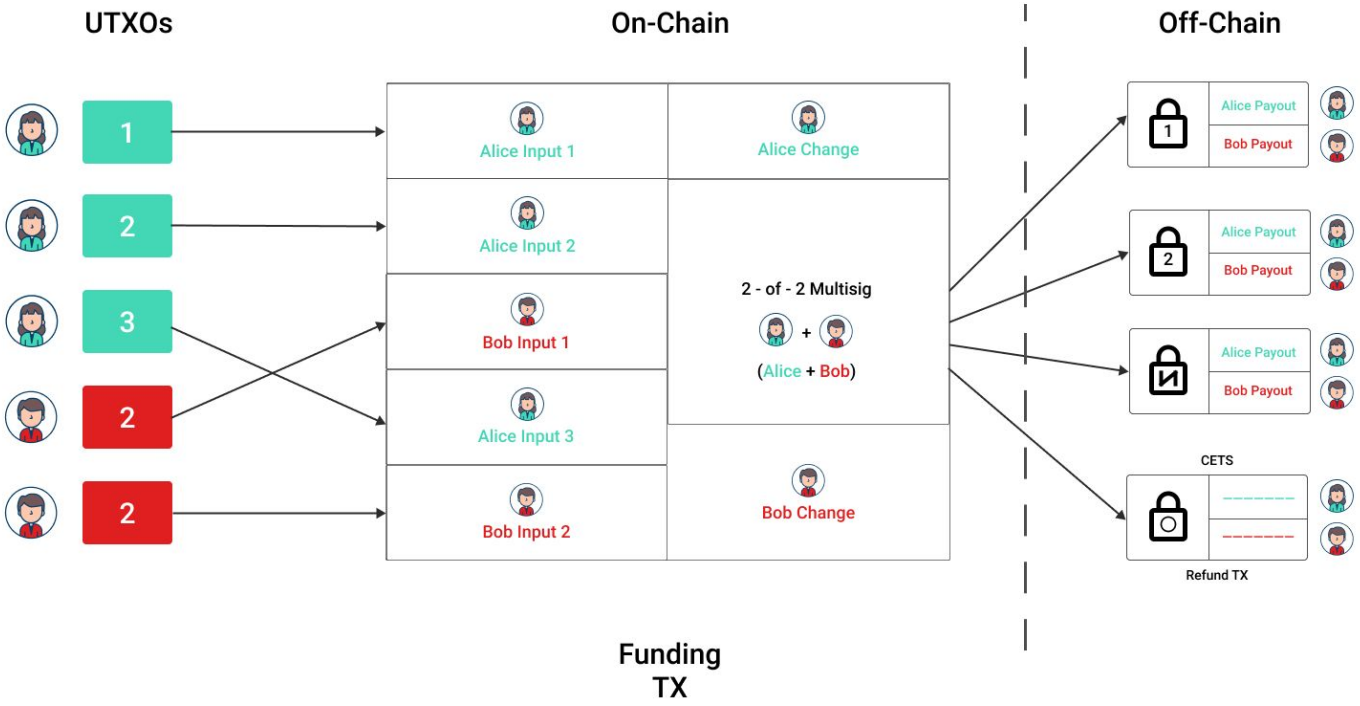
Citrea's access to Bitcoin state



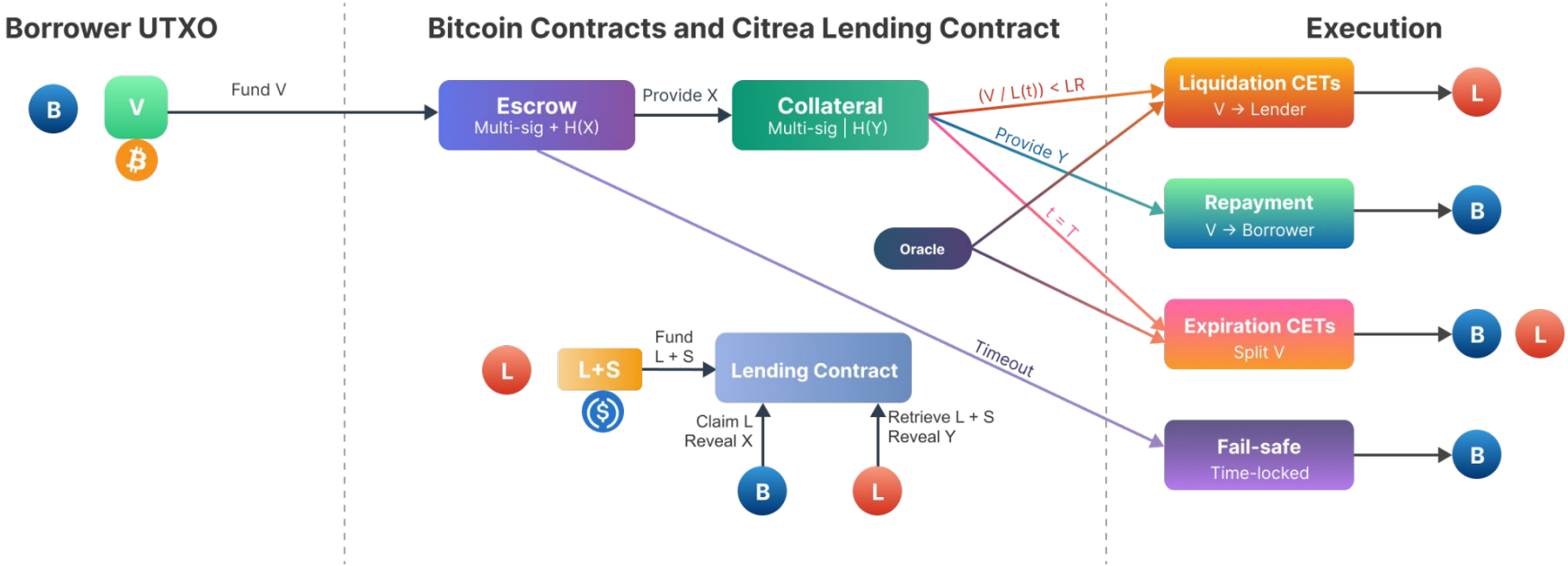
Primitives to use

- DLCs
- BitVM
- Atomic swaps

What are DLCs?



A lending app built with DLCs

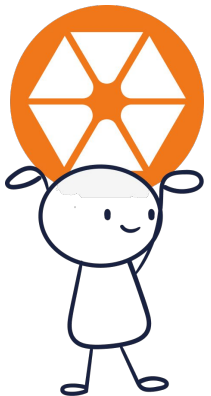


What is BitVM?

- Verify computations on Bitcoin, punish the prover if they make a false claim.
- On-chain action required only in the case of disputes, akin to optimistic rollups.
- Can be used for optimistically verified ZK proofs. (e.g. Clementine)

Building tooling

- Bitcoin related JS libraries are not very good
- Bitcoin EVM wallet aggregators
- Better testing tools for Bitcoin side
- Tenderly for Bitcoin, simulation software



An example ₿app

- Utilizes `BitcoinLightClient` to incentivize miners to include your Bitcoin tx in their blocks.

Citrea Origins