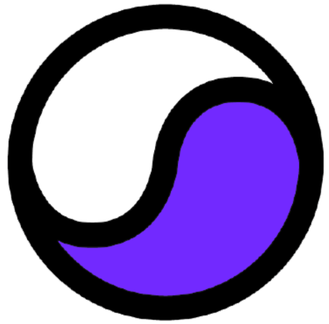


Nomic Bitcoin Sidechain

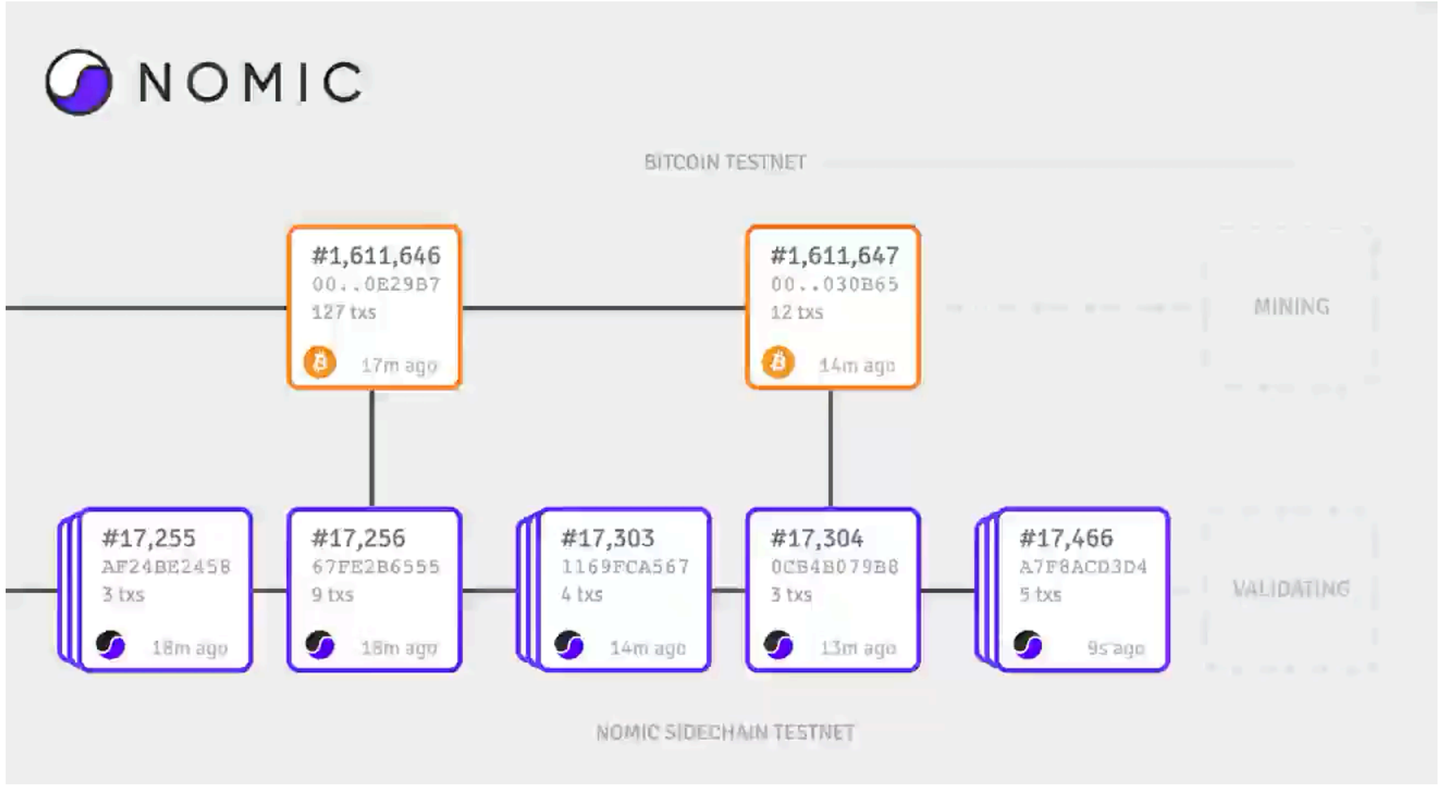
Matt Bell (@mappum), https://nomic.io

Overview

- What is Nomic?
- Our philosophies/beliefs
- Technical design walkthrough
- Possible applications

What is Nomic?

- Bitcoin sidechain network
- Secured by proof-of-stake
- Supports new functionality with BTC as the native asset (e.g. Bitcoin DeFi)



NOMIC

Philosophy

- Proof-of-stake and proof-of-work work well together
  - PoW is ideal robust base layer
  - PoS is nice for building new things on top
- We want to build on Bitcoin (DAOs, NFTs, decentralized lending, etc.)
- Focus on engineering and performance

NOMIC

Reserve Script

- Big fancy Taproot multisig based on amount of stake
- 2/3 of voting power must sign to spend
- Supports up to 1000 signers

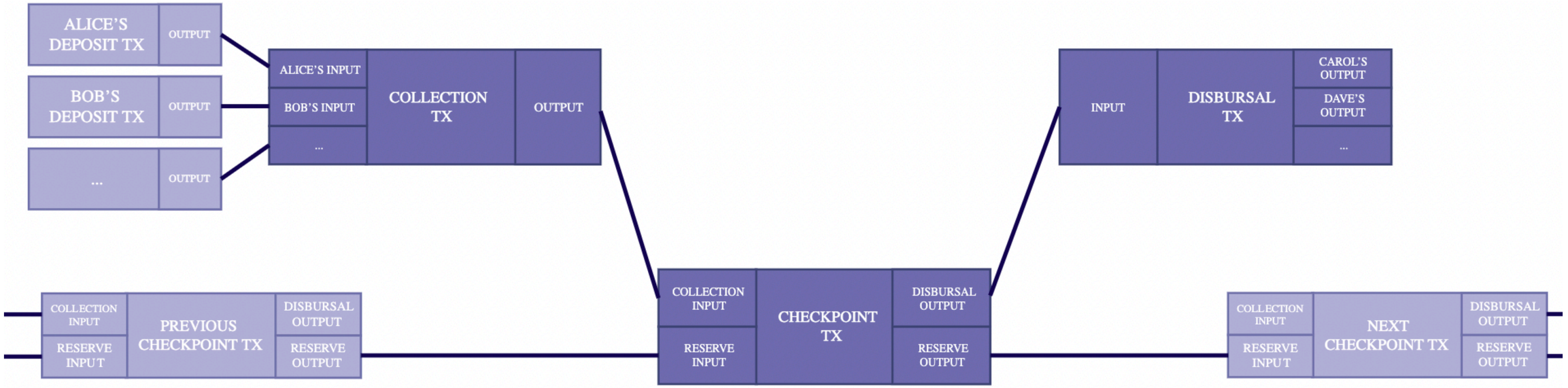
- **Key path:** MuSig of largest 2/3 of multisig
- **Script paths:**
  - **Fallback script*:*** Big linear multisig ——————->

```
<pubkey1> OP_CHECKSIG
OP_IF
  <voting_power1>
OP_ELSE
  0
OP_ENDIF

OP_SWAP
<pubkey...> OP_CHECKSIG
OP_IF
  <voting_power...>
  OP_ADD
OP_ENDIF

OP_SWAP
<pubkeyN> OP_CHECKSIG
OP_IF
  <voting_powerN>
  OP_ADD
OP_ENDIF

<two_thirds_of_total_voting_power>
OP_GREATERTHAN
```

NOMIC

Checkpoints

- Funds in reserve get spent to latest signatory set periodically (e.g. once per Bitcoin block)
- Collect deposit UTXOs, move previous reserves, pay out withdrawals



NOMIC

Proof-of-stake

- Staking token, minted to anyone who locks up their BTC
- Stakers participate in the reserve multisig and in making blocks on the Nomic blockchain
- Long-range attacks solved by anchoring to Bitcoin, light clients can SPV Bitcoin then follow the chain of checkpoints

NOMIC

Security

- **Slashing:** If signatories sign an unexpected checkpoint, they lose their stake
  - Secure even when fraudulent tx is censored
- **Emergency disbursal:** Timelocked transaction which pays everyone back BTC on the mainchain
  - Only 1/3 of voting power has to be honest

NOMIC

Comparison to Other Sidechains

- **Liquid, RSK:** Permissioned set of signers, Liquid users also require permission to withdraw
- **Drivechains:** Not possible without a soft fork, relies on honest hashrate majority
- **ETH-based solutions:** WBTC - fully custodial, tBTC - honesty assumptions
- **Stacks:** Does not have a reserve mechanism

NOMIC

Applications

- Decentralized Lightning hub
- Bitcoin-native DeFi
  - Derivatives for hashrate, fee, double-spend risk, etc.
  - Replace centralized exchanges
- Futarchy DAOs

NOMIC

Project Status

- Has been under development for 3 years
- Has run on Bitcoin testnet
- Launch scheduled for Bitcoin block 709,632
- **Twitter: @nomicbtc**
- **Telegram: https://t.me/nomicbtc**
- **https://nomic.io**

NOMIC

Thank you!

- Twitter: @nomicbtc
- Telegram: https://t.me/nomicbtc
- https://nomic.io