chaincode

Breaking Bitcoin Core

Chaincode Residency, June 20th 2019

Introducing

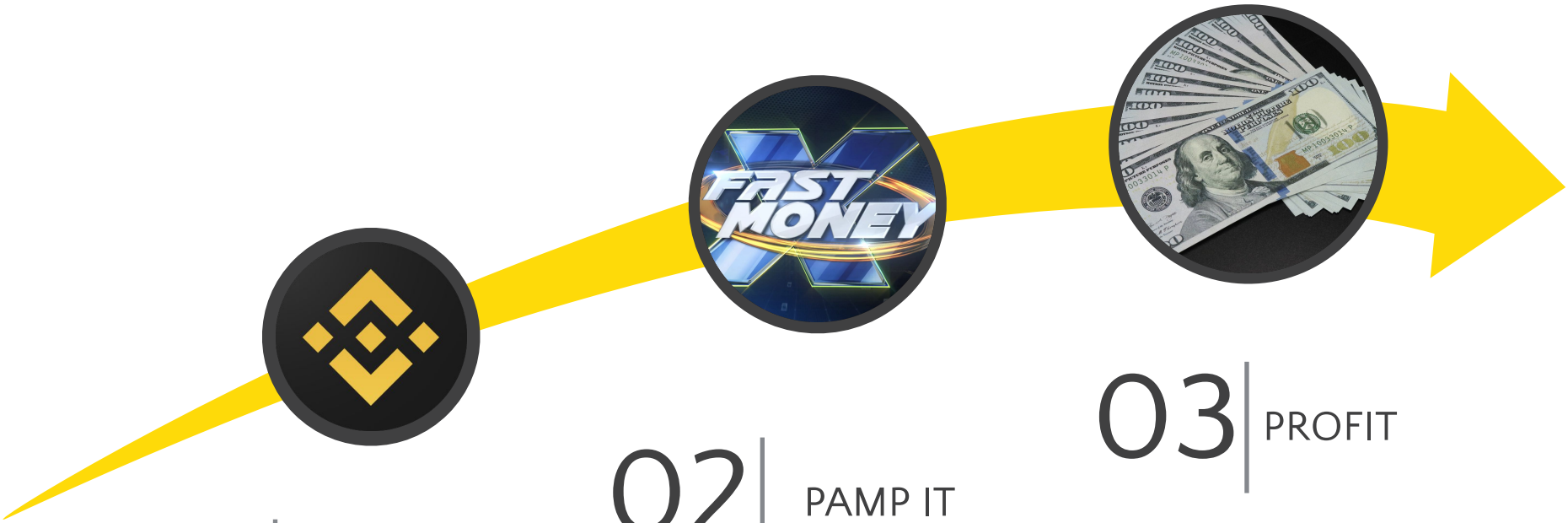
chaincode

Bitcoin Residents' Vision

chaincode

chaincode

THE PLAN



01 | LIST IT

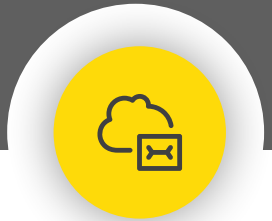
02 | PAMP IT

03 | PROFIT

chaincode

UNIQUE FEATURES

MORE OPCODEs



SATOSHI'S ORIGINAL OP_RETURN VISION

REDUCE MEMPOOL LIMITS

REMOVE UNNECESSARY CHECKS

MORE OPCODES

- Satoshi removed many of the original OPCODEs in 2010
- We've restored those OPCODEs including OP_CAT
- More OPCODEs = more features

Restore Satoshi's original OP_RETURN vision

- OP_RETURN was broken by Satoshi in 2010
- We've restored the original vision of OP_RETURN (and OP_*VERIFY)

Relax mempool limits

- CPFP package size is needlessly limited to 25 txs
- RBF can only replace 100 txs
- We’ve relaxed those limits

Less unnecessary checking

- CheckBlock() previously skipped checking for duplicate inputs in a transaction
- This optimization was removed in 2018
- We've restored the duplicate input optimization

Your job - QA testing

- Make sure that we're safu from:
  - Stealing funds
  - Denial-of-service attacks
  - Inflation
  - Attacks on miners
  - … and any other shenanigans.

Good luck!

https://github.com/jnewbery/bitcoin/tree/2019-06-breaking-bitcoin-core