Drivechain and Blind Merged Mining

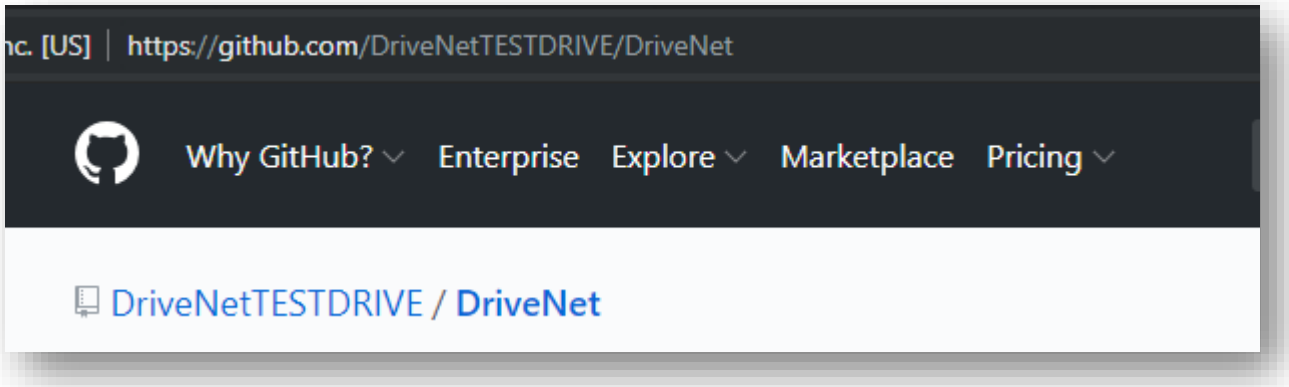
Paul Sztorc
Research Director, Tierion
May 15th, 2019

About Me

- 2012 -- Bitcoiner
- 2014 -- Truthcoin.info Blog
- 2015-Present – Scaling Bitcoin 1,2,3,4; TabConf and BoB
- Currently: Research Director at Tierion
- Previously: Statistician at Yale Econ Department

Topic: Drivechain

- A Bitcoin Layer-2 (… or, a “Layer 1.5”)
- Scaling AND Interoperability
- Soft Fork -- BIPs 300 and 301
- www.drivechain.info



GitHub

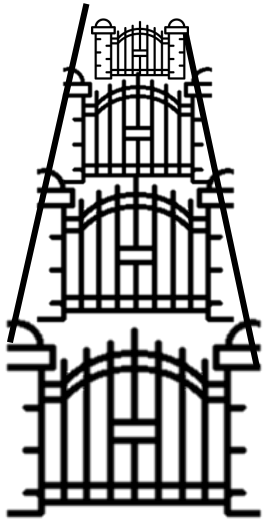
Original Nov 2015 Post

In One Slide

Problem	**Meta-Consensus** (Altcoins, Hard Forks, and Contentious Features)
Solution	**Interoperability** **(**One Token, traveling among many blockchains)
Goal	Don’t compete to win -- instead just play all the hands (so you can’t lose).

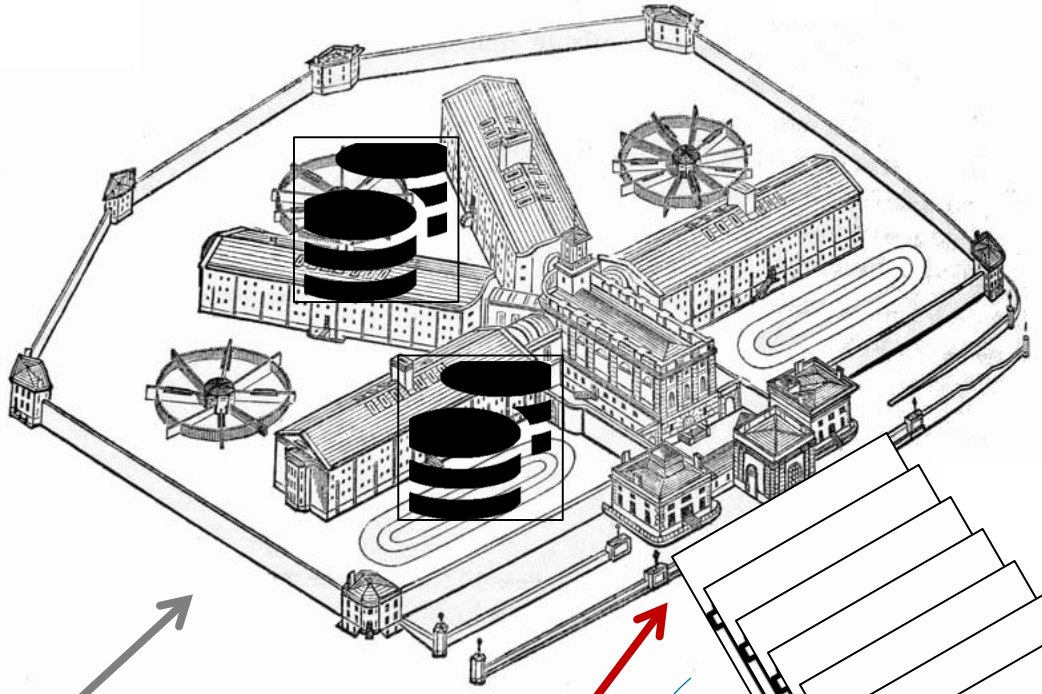
How it Works

- New Kind of Output: “Hashrate Escrow”
- Anyone can *<u>deposit to it</u>* at any time.
- But *<u>withdrawals</u>* are very slow.



Series of gates.

Prison Metaphor



Prison

Only way out.

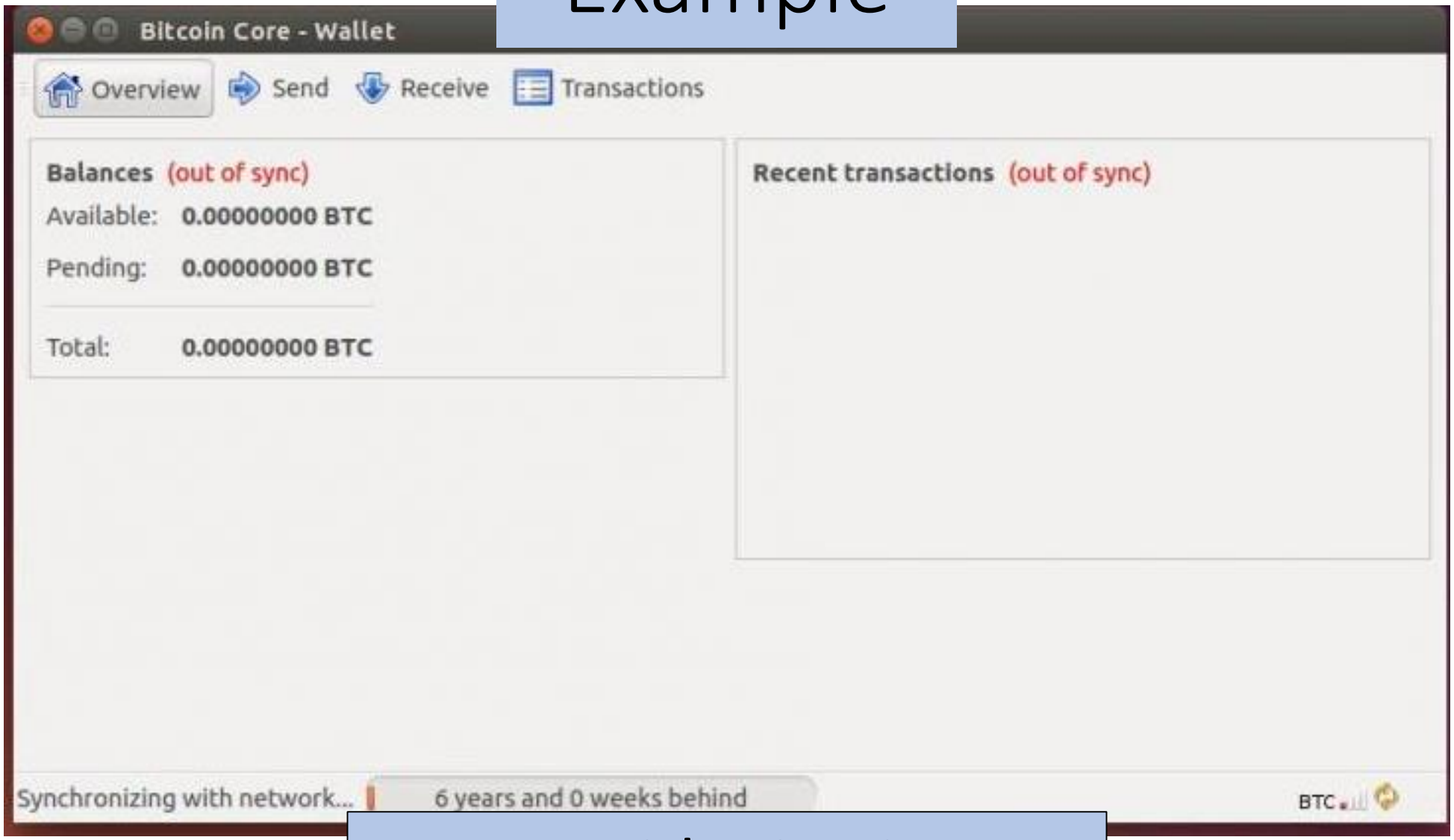
13,150 Gates

...

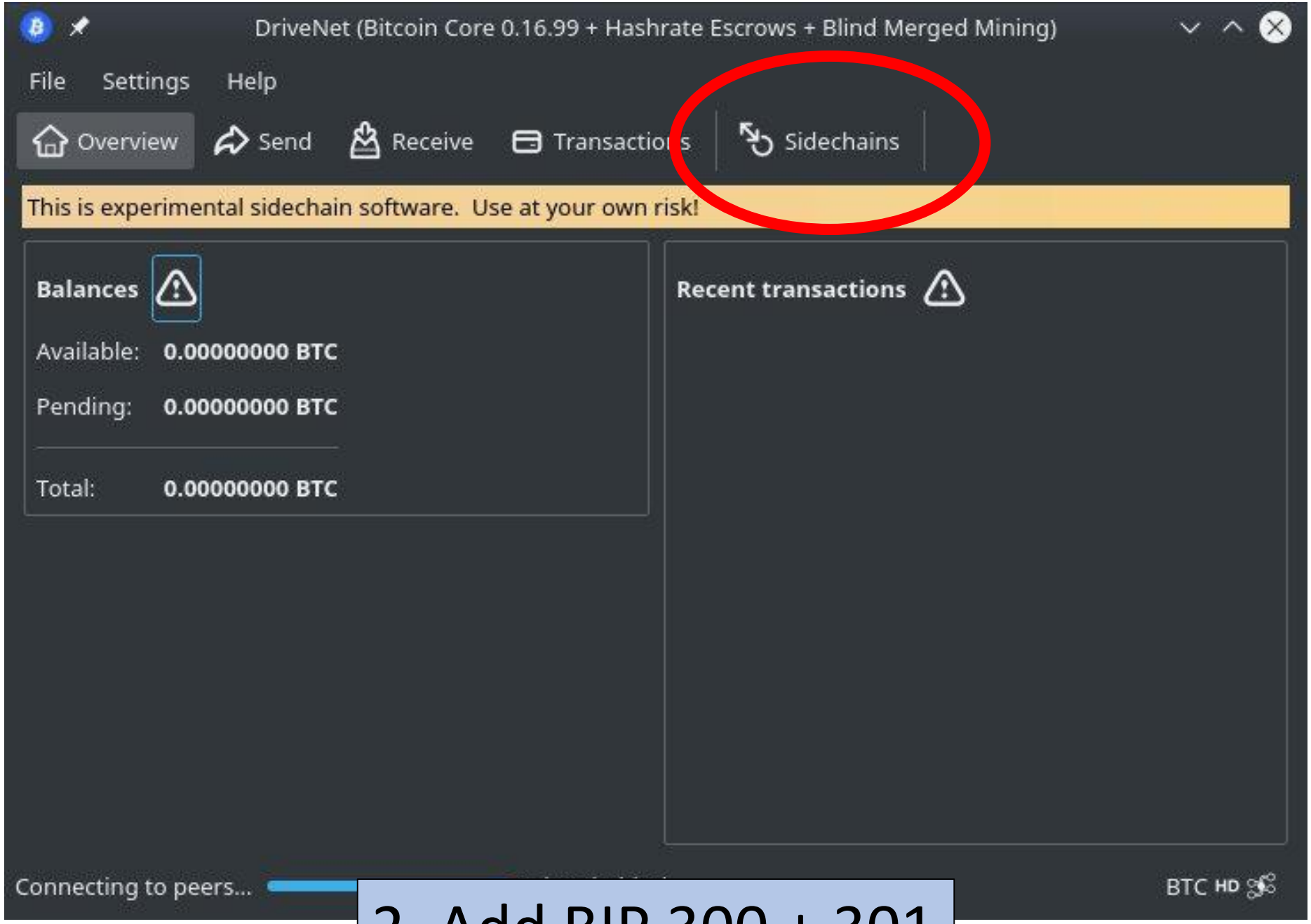
BTC

Example

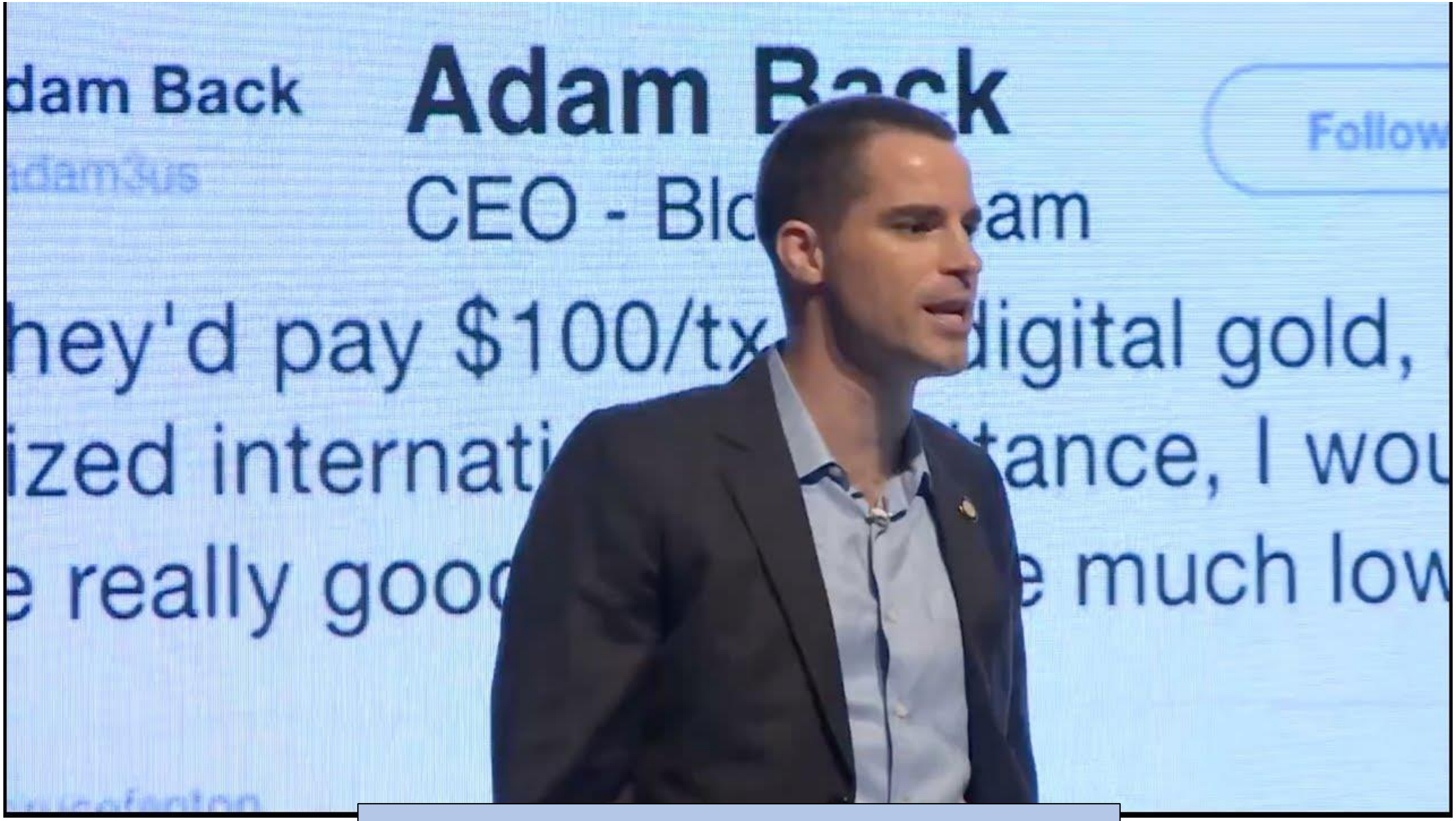
Example



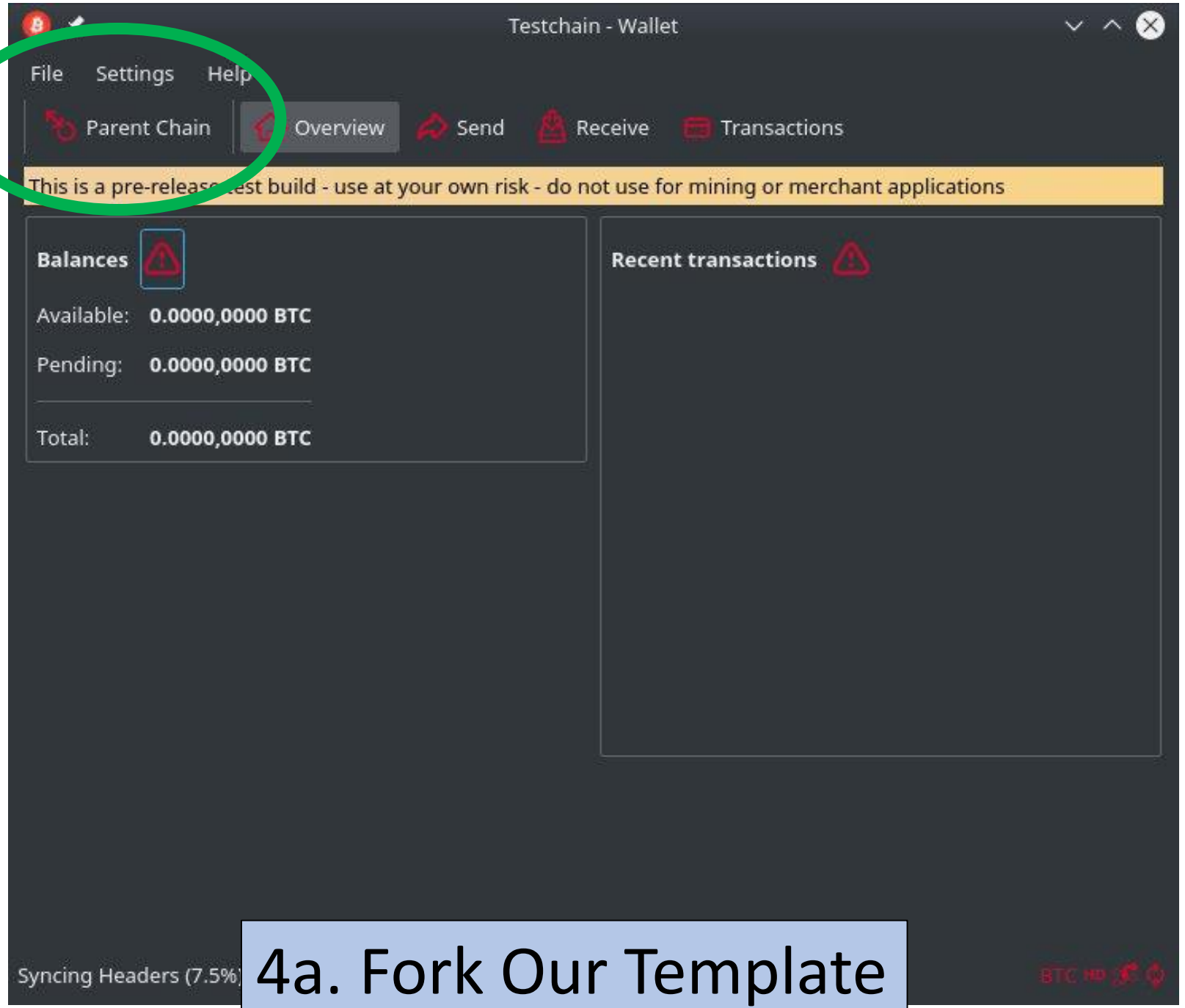
1. Start with Bitcoin Core



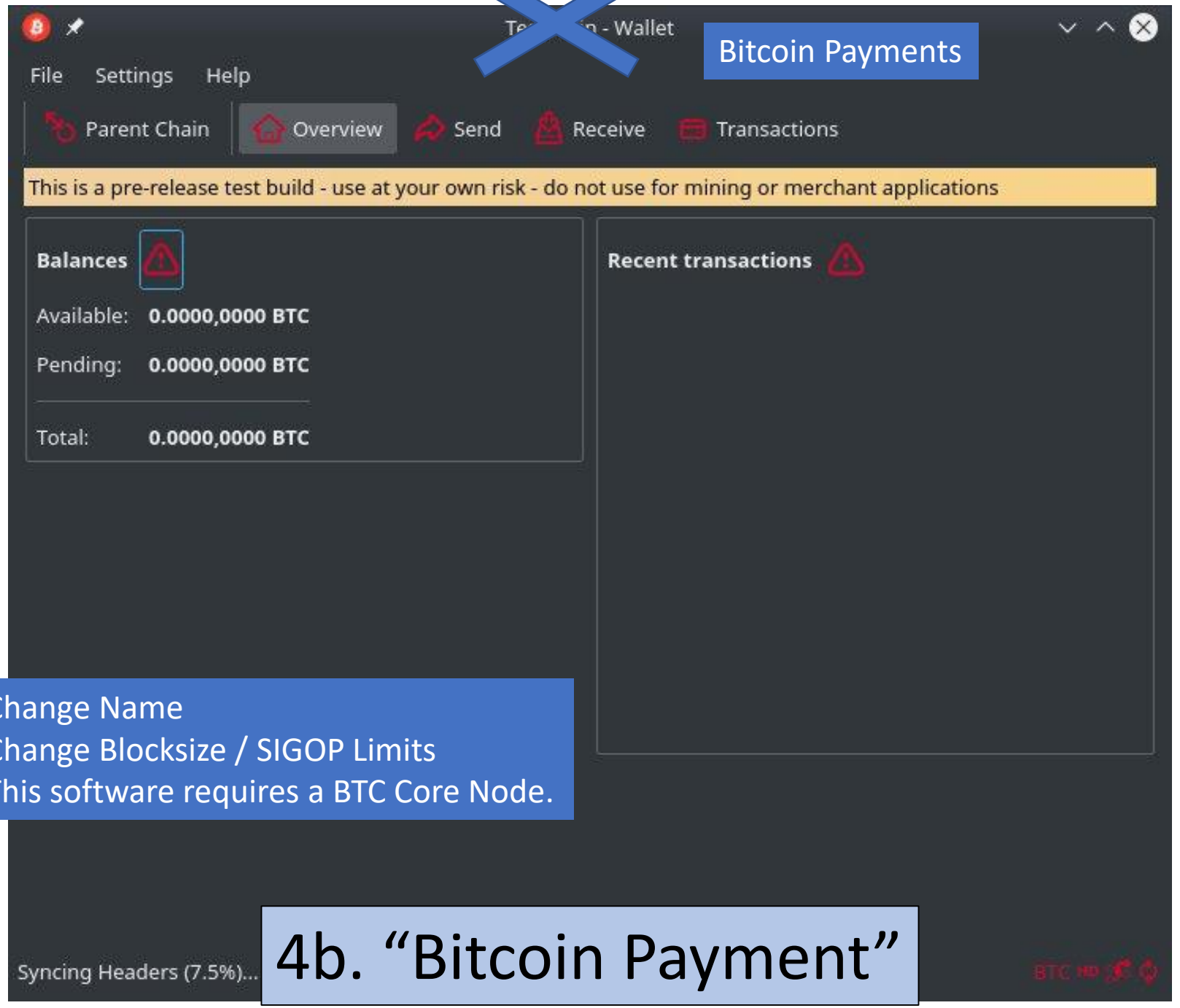
2. Add BIP 300 + 301



3. Meta-Consensus Problem



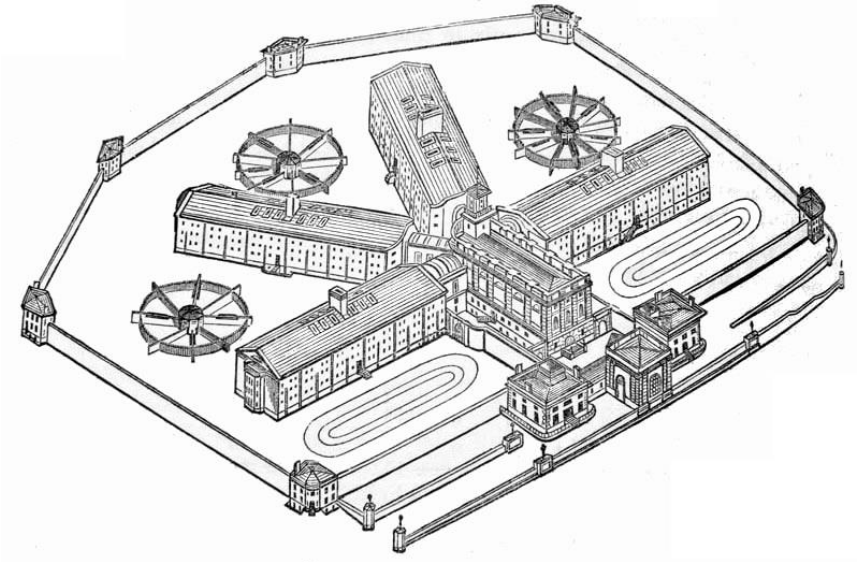
4a. Fork Our Template



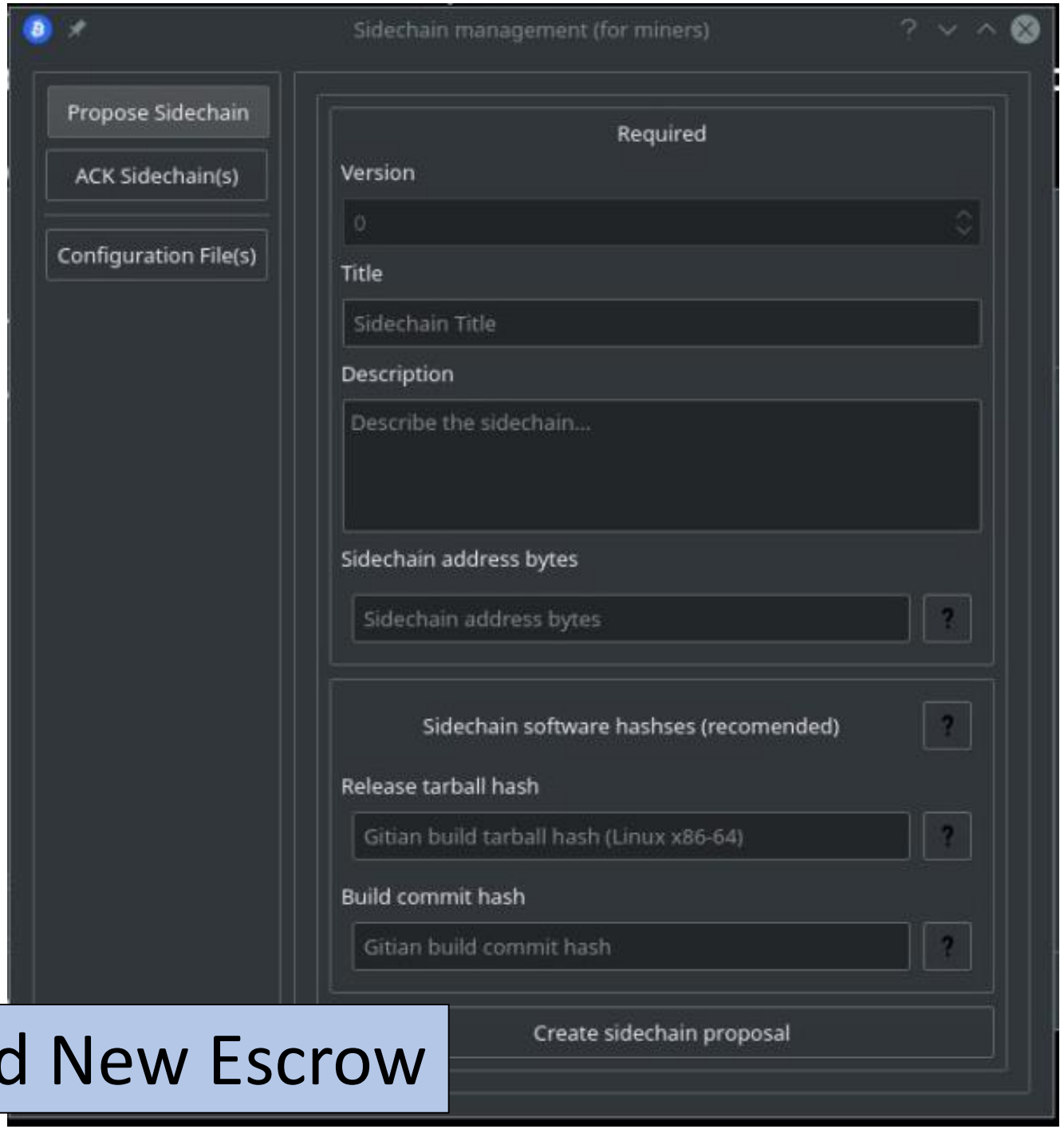
- Change Name
- Change Blocksize / SIGOP Limits
- This software requires a BTC Core Node.

4b. “Bitcoin Payment”

“Bitcoin Payments”

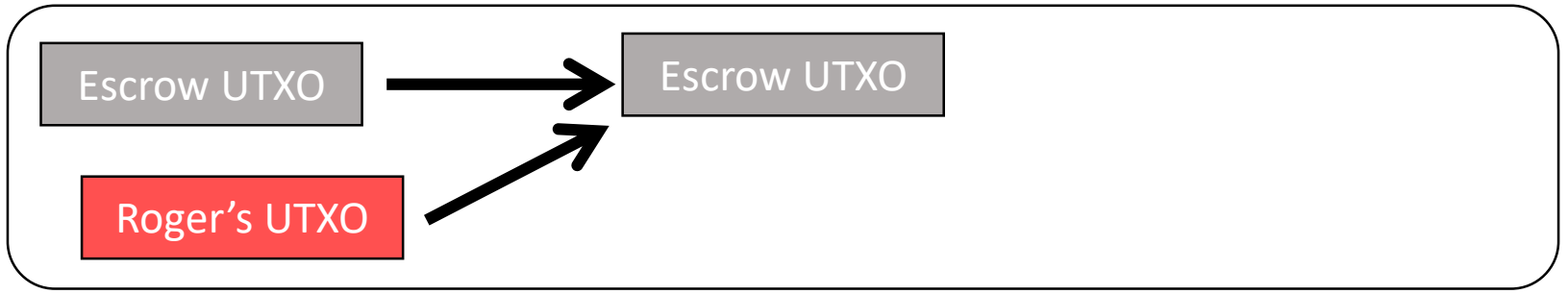


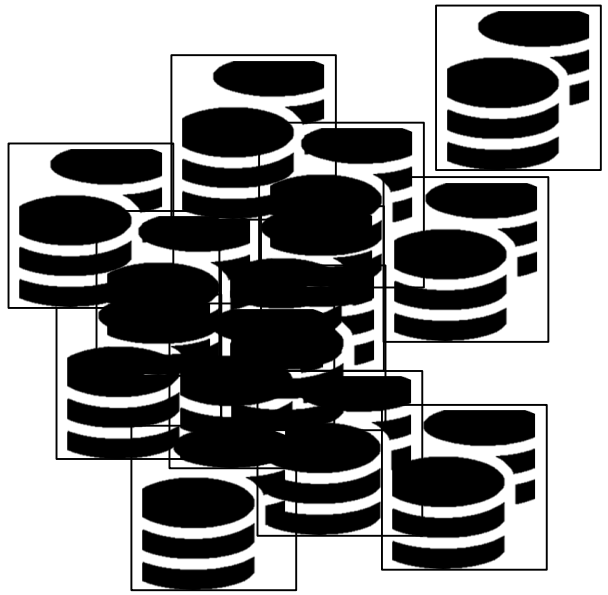
Now Open For Business

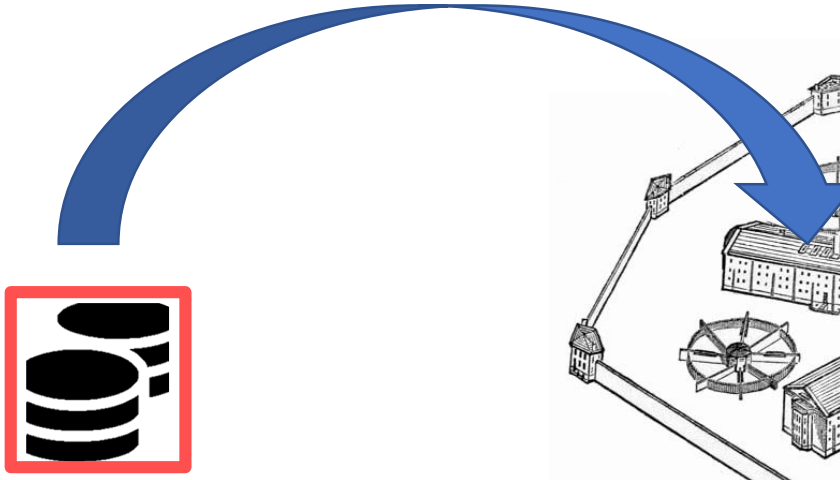


5. Add New Escrow

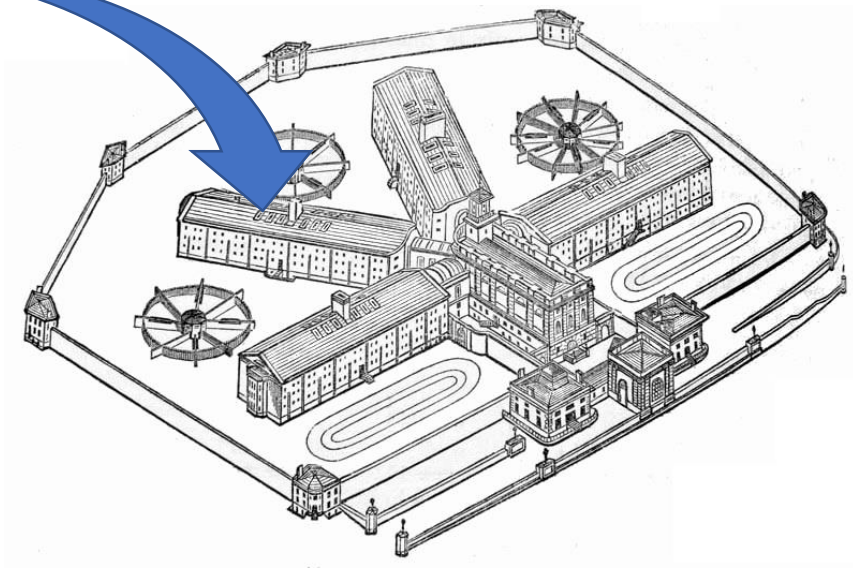
On layer-1:







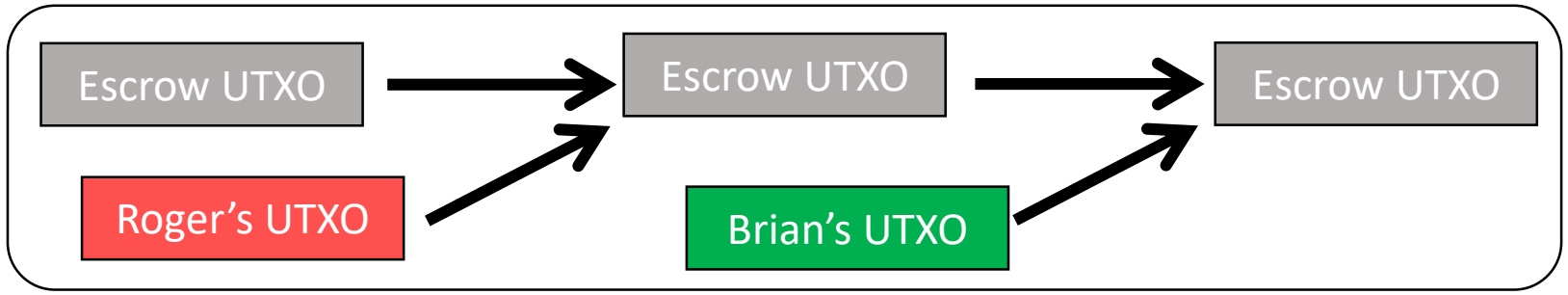
Roger's 50,000 BTC

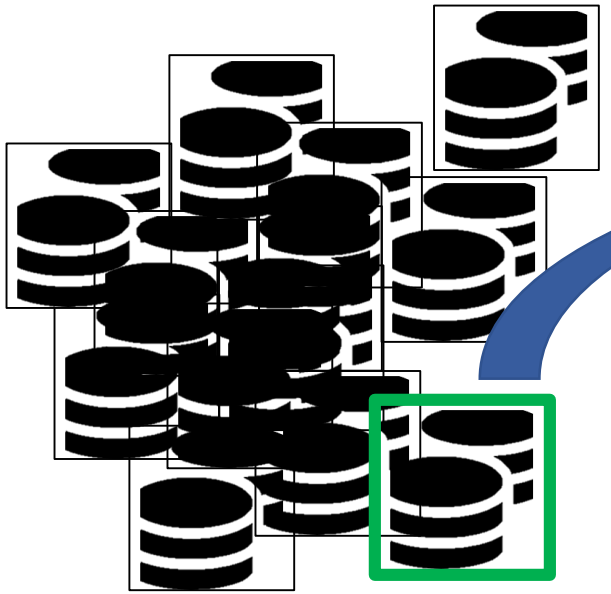


"Bitcoin Payments"

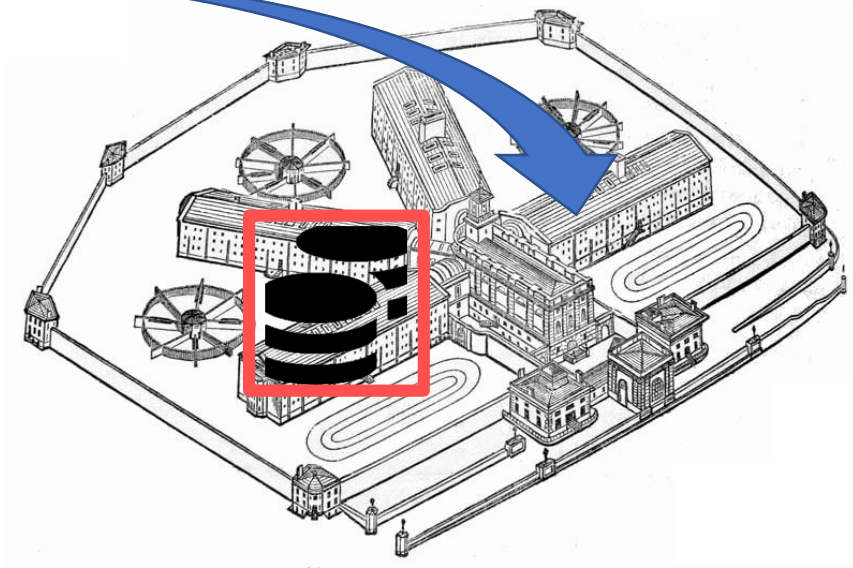
6a. Spend from Layer-1 to Layer-1.5

On layer-1:





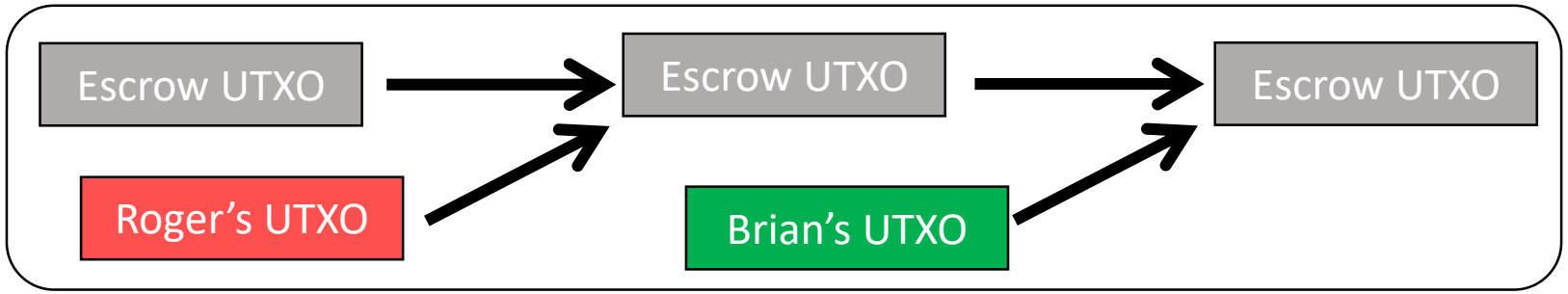
Brian's 7,000 BTC

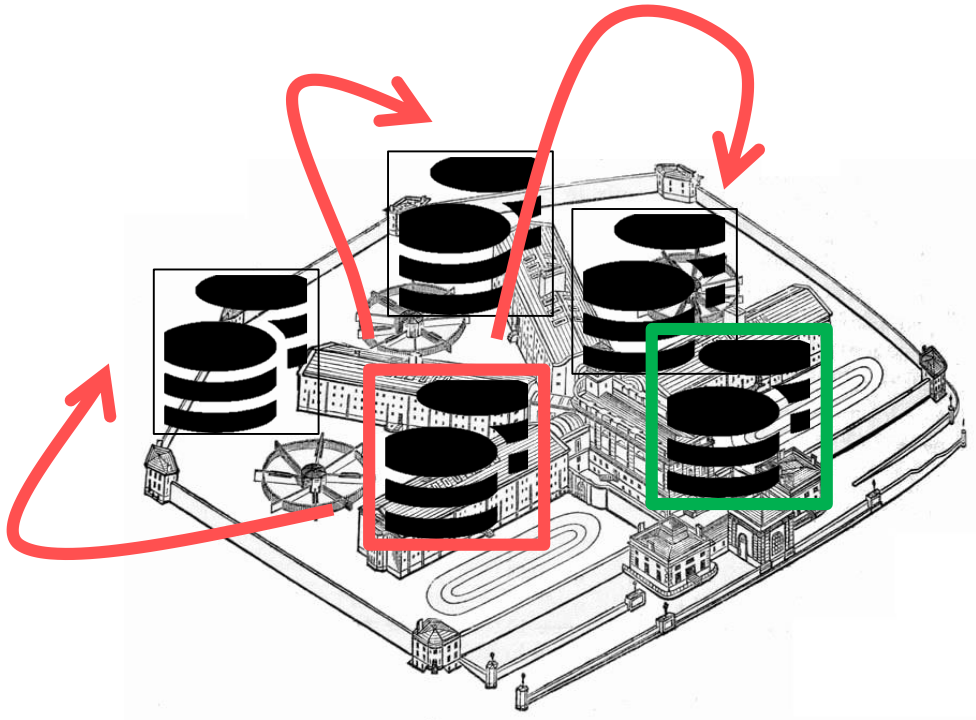


"Bitcoin Payments"

6b. Spend from Layer-1 to Layer-1.5

On layer-1:





"Bitcoin Payments"

7. Spend within the Escrow

Generates txn fee revenues for miners

Sideshift, Shapeshift, Atomic Swaps, Etc

SIDESHIFT.AI

TEST PILOT STAGE

Become An Affiliate: Shill friends, get money

Choose conversion

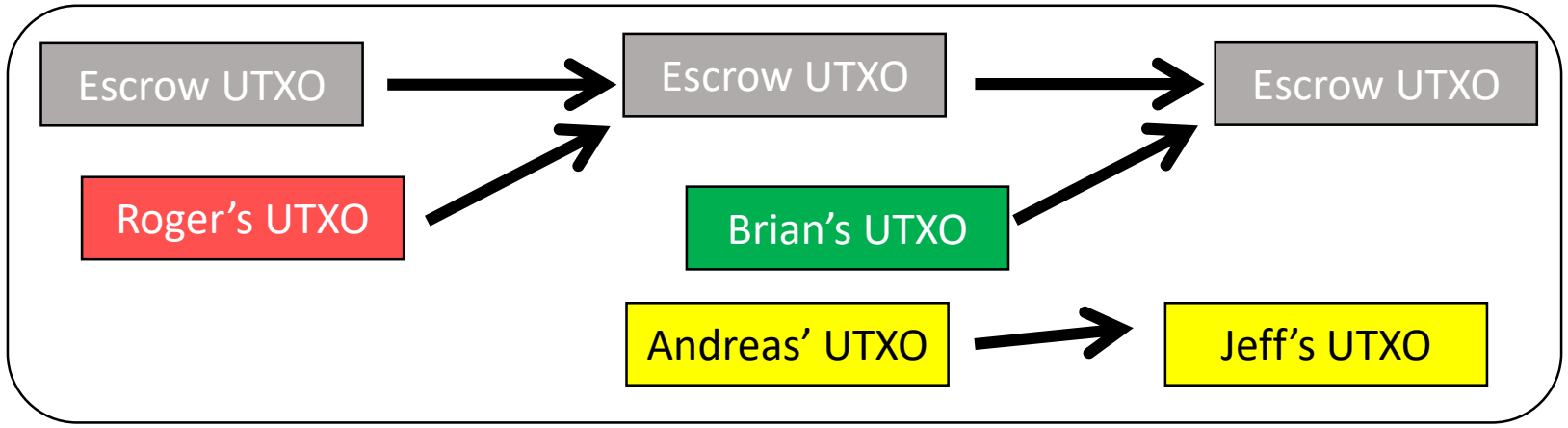
Bitcoin (Lightning) → Tether USD

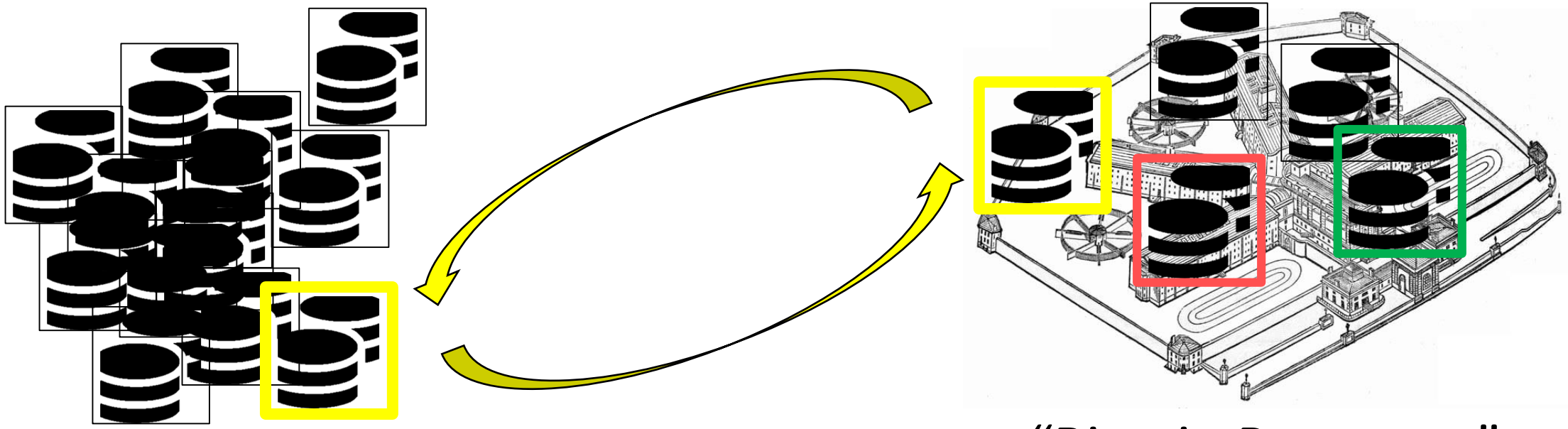
SHIFT

Time	From	To
7 hours ago	⚡0.0003 BTC	0.008601 ETH
16 hours ago	0.0149022 BTC	0.9805 ZEC
17 hours ago	⚡0.00001 BTC	0.03671 USDT
17 hours ago	⚡0.00001 BTC	
17 hours ago	0.00868722 BTC	

8a. Swapping to Instant Freedom

On layer-1:

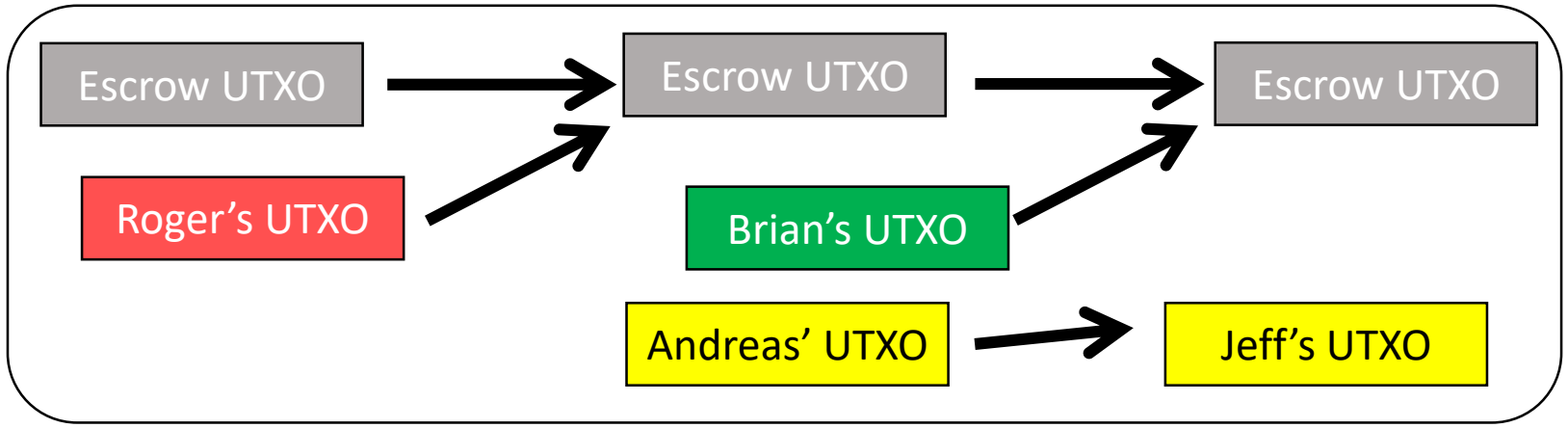


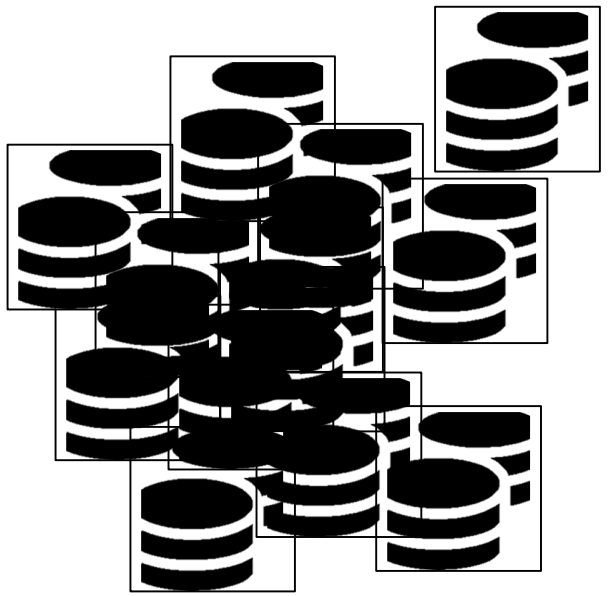


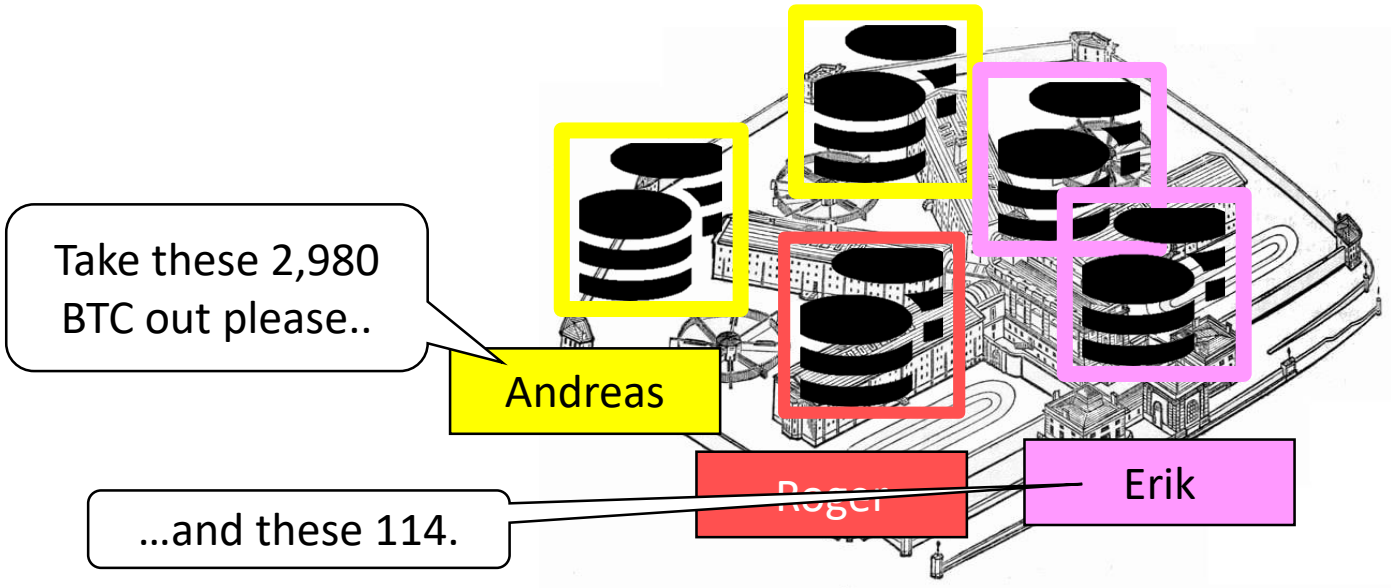
"Bitcoin Payments"

8b. Prisoner Exchange

On layer-1:

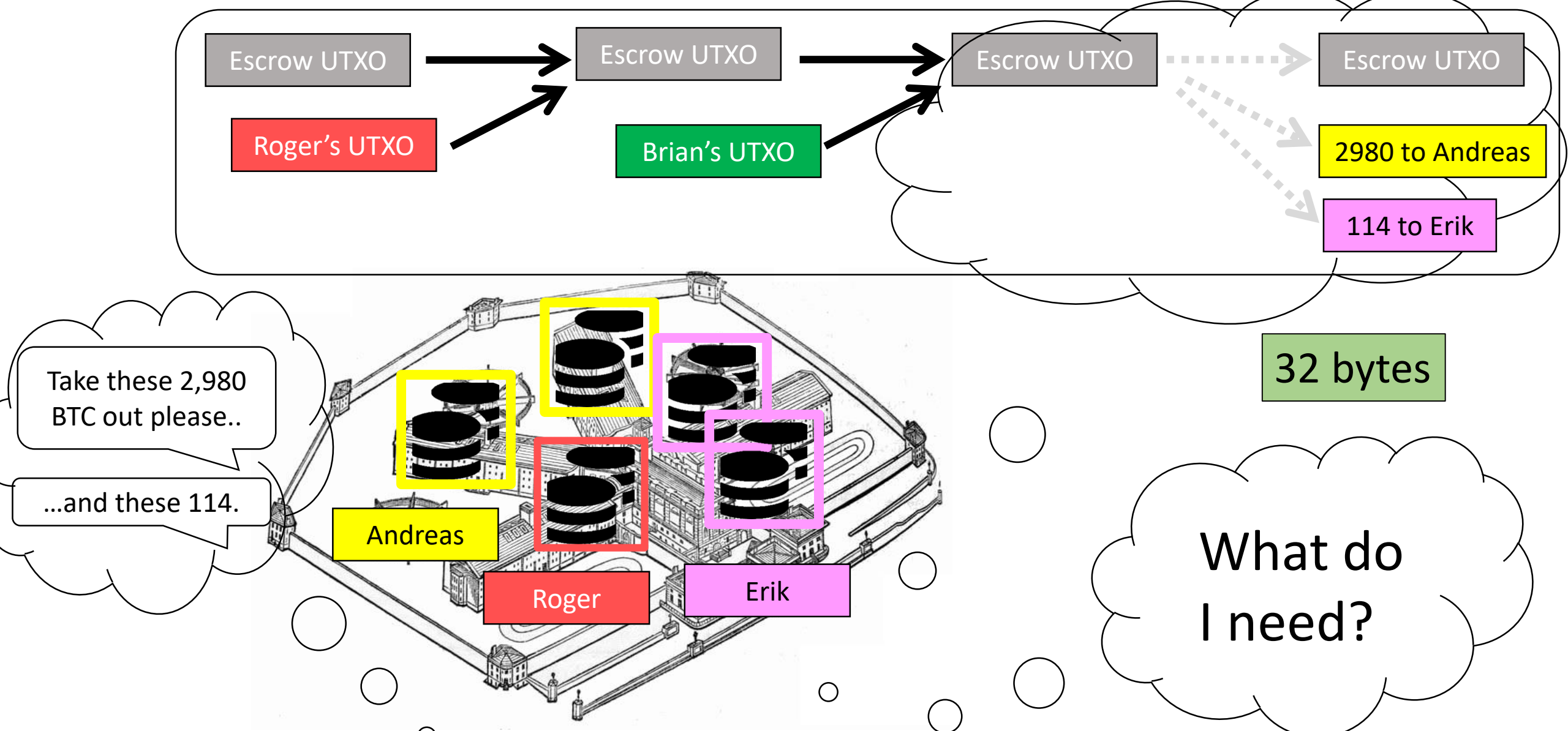






"Bitcoin Payments"

9. Leaving Prison

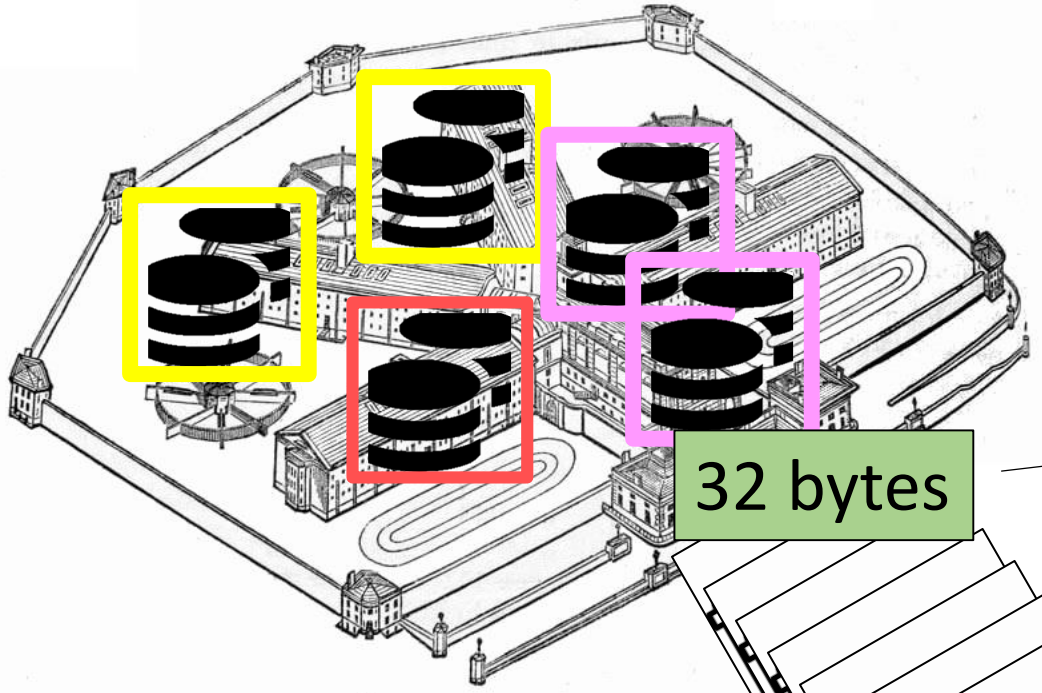


@"Bitcoin Payments"

10. The Withdrawal Txn

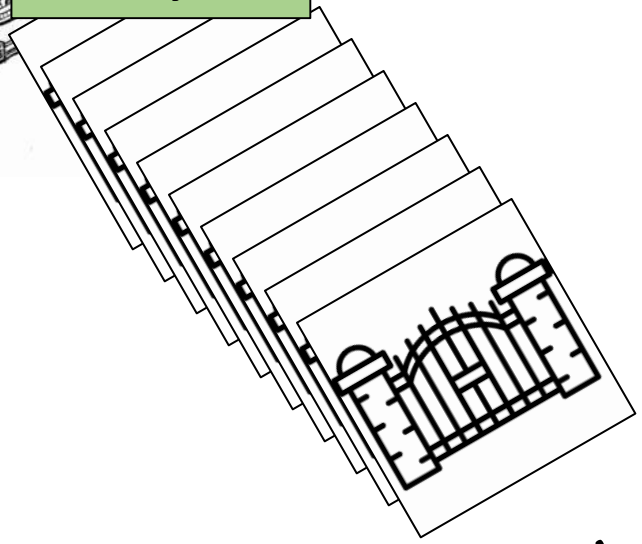
Debug window
Information
Console
Network Traffic
Peers
getblockheader
00:27:47
getblockheader
00:27:47
{
"hash":
"84e51e142b7410dad573e0b63225cc935c27a29ca3fd1c1fe147d9b03e89a5ce",
"confirmations": 1,
"height": 83,
"version": 536870912,
"versionHex": "20000000",
"merkleroot":
"6fb20a8389a1442abd4b7d540e9c68c0e7bbb9bdb42b2d243c5d40d33deed605",
"time": 1556522344,
"mediantime": 1556522316,
"nonce": 0,
"bits": "207fffff",
"difficulty": 4.656542373906925e-10,
"chainwork":
"hashwtprime":
"0000000000000000000000000000000000000000000000000000000000000000",
"previousblockhash":
"4fb9bd41b134fda5638a4c9da2f8419eefb7dae5ab9e70c621c5fe1dc86115cf"
}
32 bytes
10. The Withdrawal Txn

Prison Metaphor



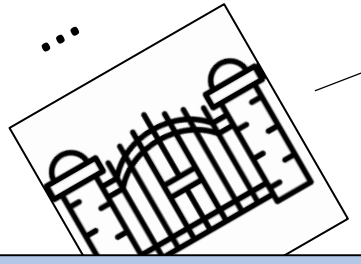
32 bytes

1st gate



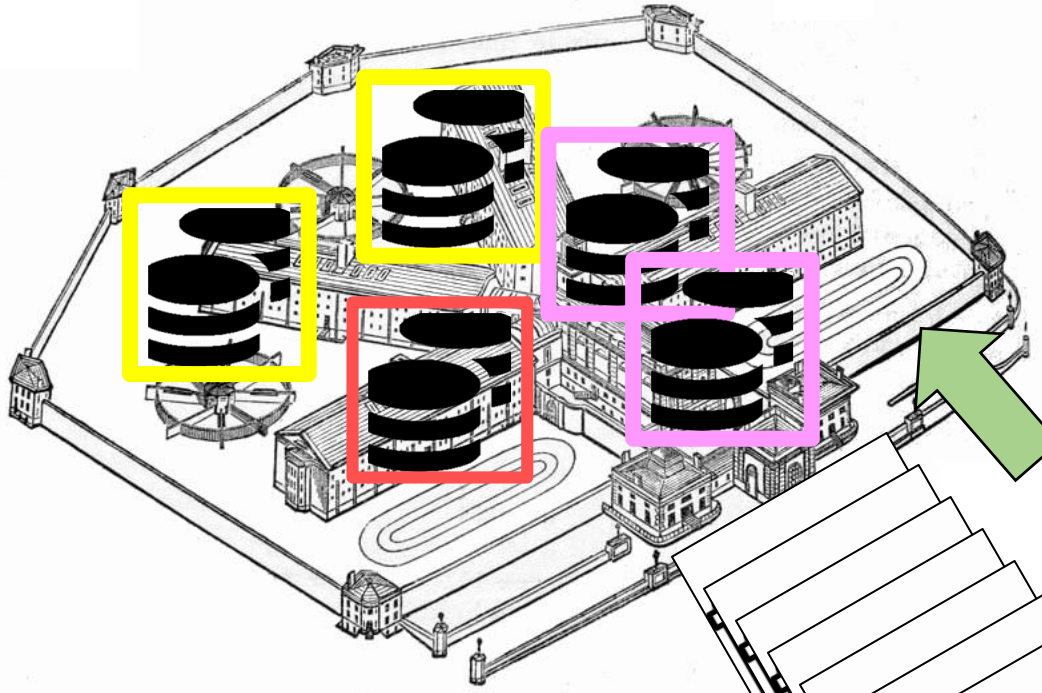
...

13150th gate



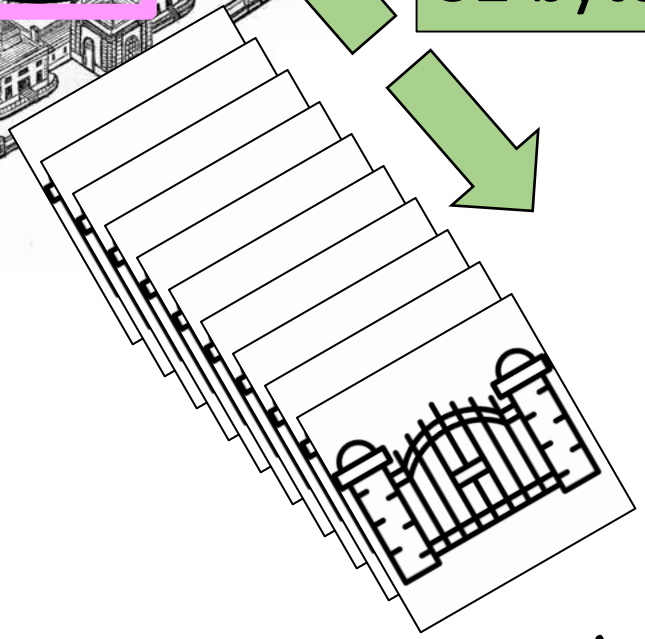
11. Starting Off…

Prison Metaphor

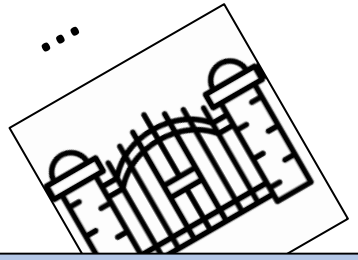


32 bytes

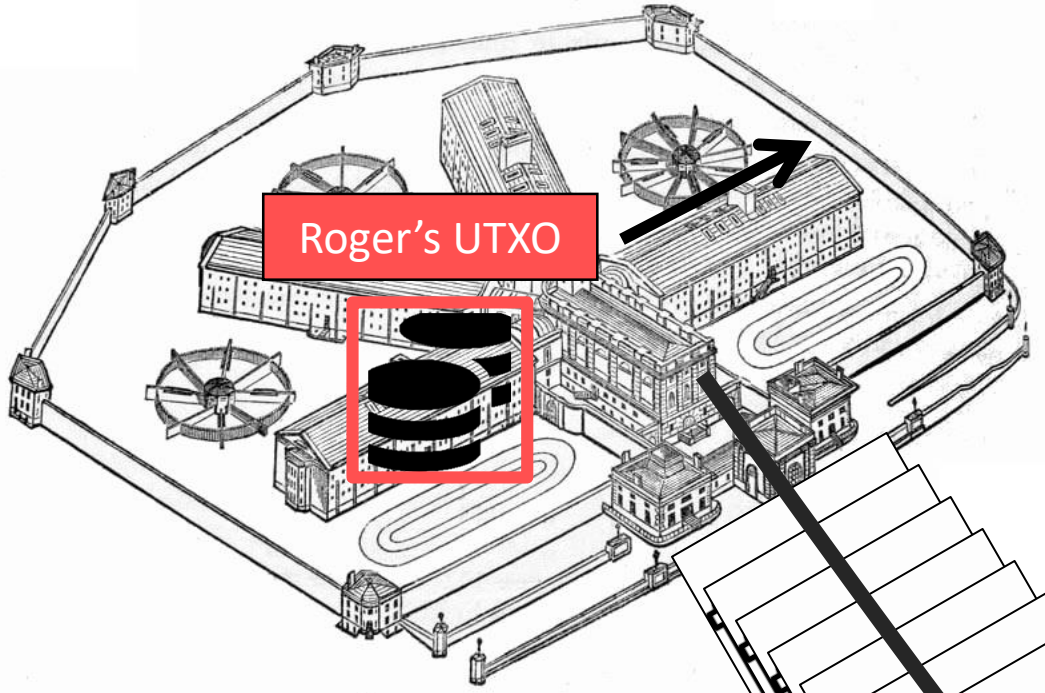
Miners



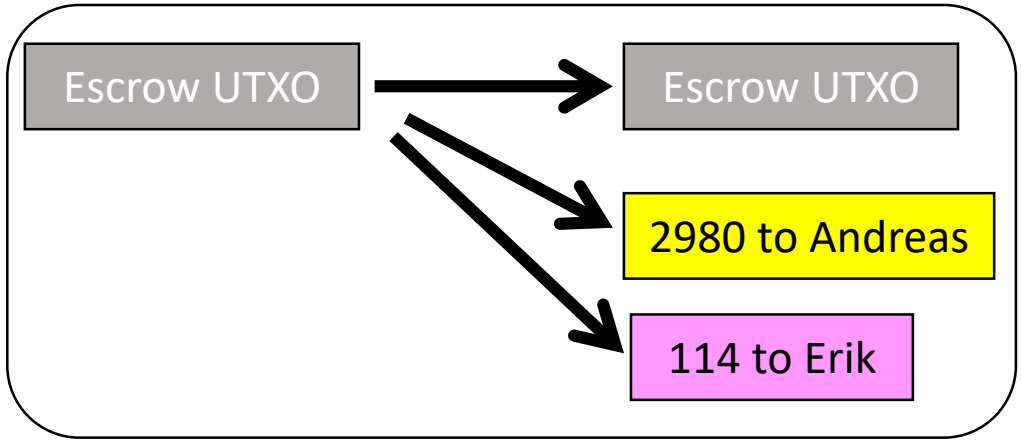
...

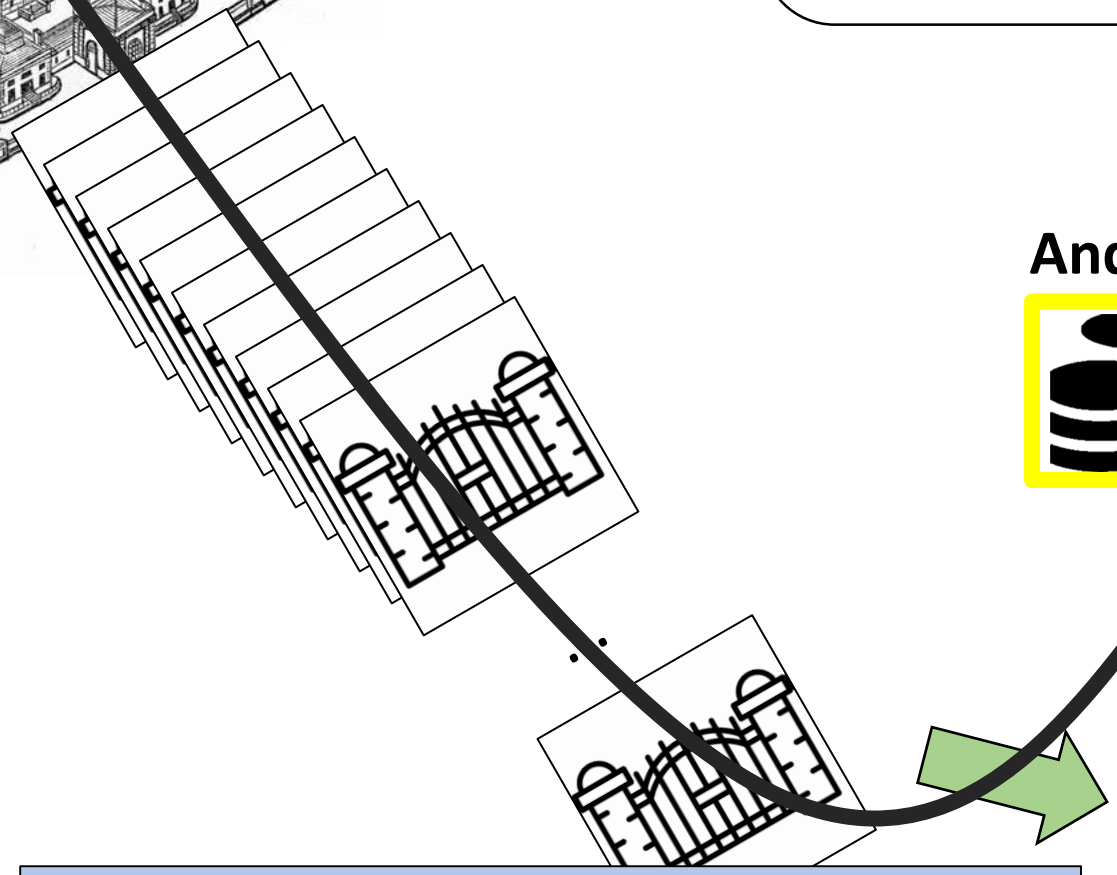


12. Making Progress…



On layer-1:





Andreas

Erik

32 bytes

13. Withdrawal Complete

Costs and Risks

Using any escrows?	No	Yes
Costs	A soft fork.	A soft fork + ***New security considerations*** for the layer-1.5 coins.

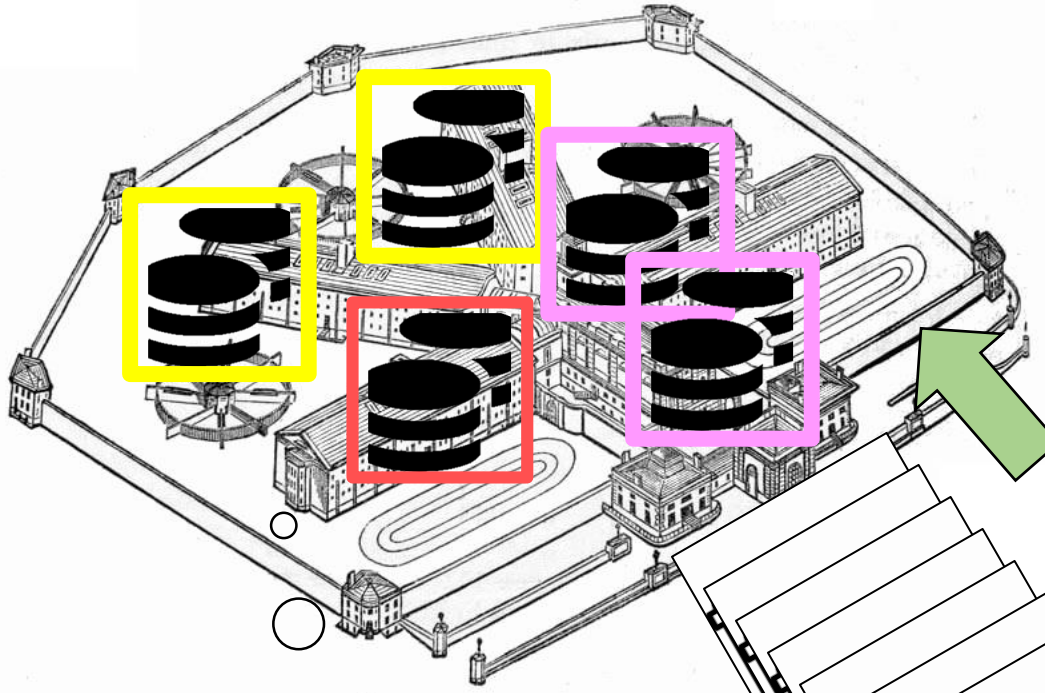
Upper Layers = Different Threat Models

Upper Layer:	Lightning Network	Hashrate Escrow
New Security Considerations	• Notice fraud in time. • Emergency Broadcast to Layer-1 • Shrug off custodial period.	…

Upper Layers = Different Threat Models

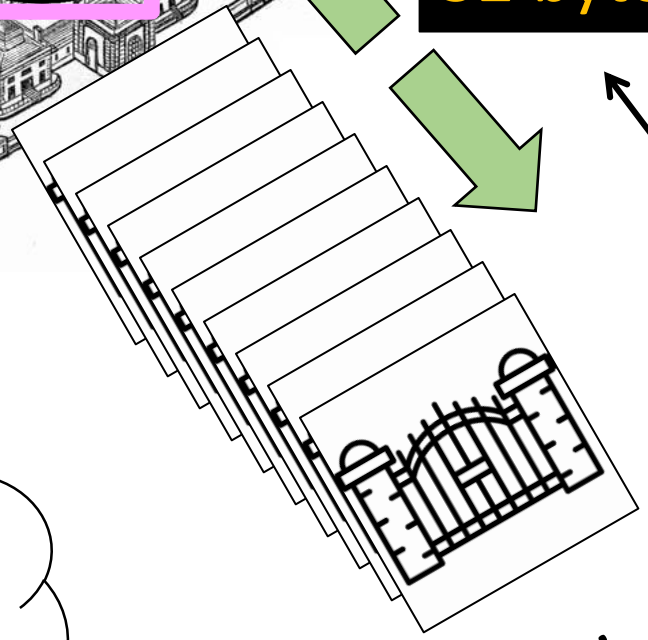
Upper Layer:	Lightning Network	Hashrate Escrow
New Security Considerations	• Notice fraud in time. • Emergency Broadcast to Layer-1 • Shrug off custodial period.	Are these escrows making miners wealthier? Are they ***popular***?

Miner Theft

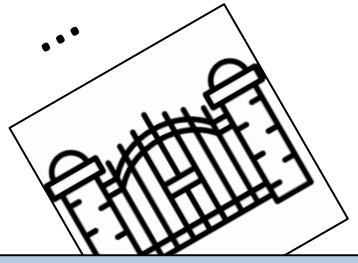


(Evil 32 Bytes)

32 bytes



...



Escrow UTXO → Escrow UTXO

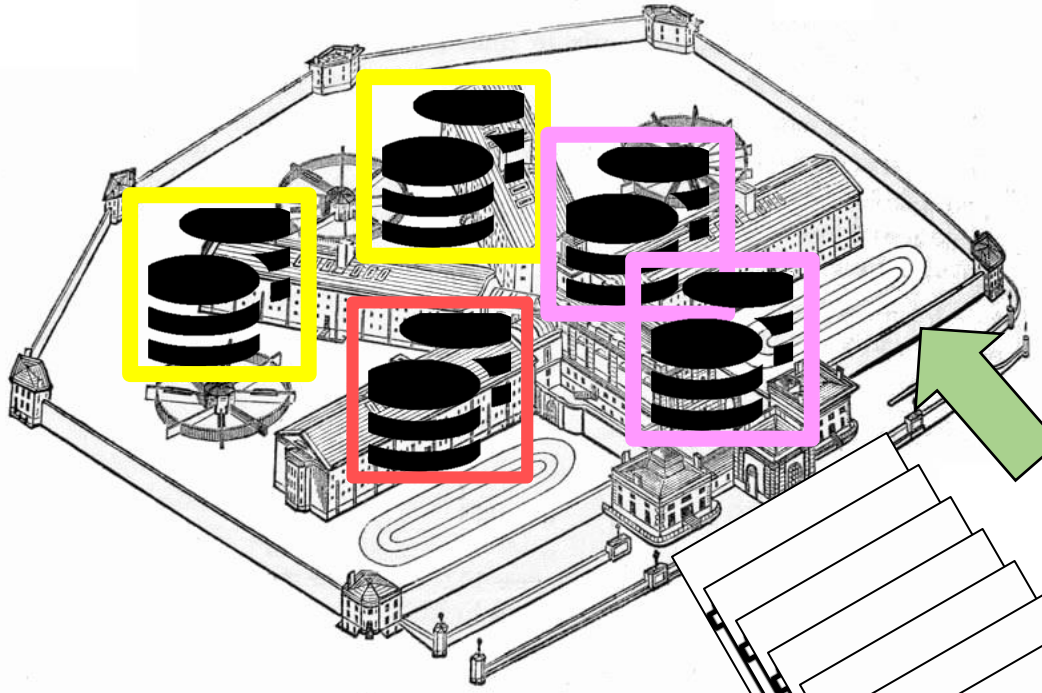
50,000 to Jihan Wu

32 bytes

Oh no…

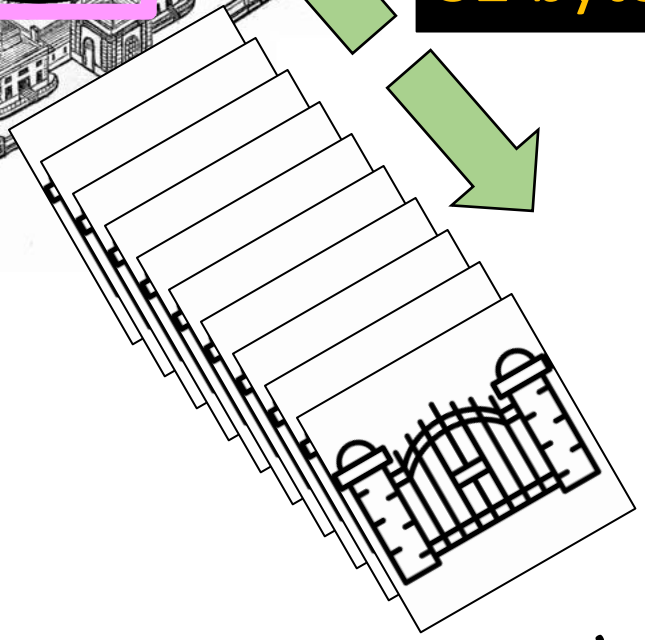
11. Starting Off…

3 Awkward Months…

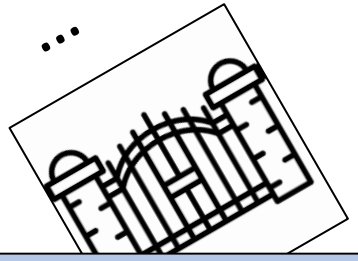


32 bytes

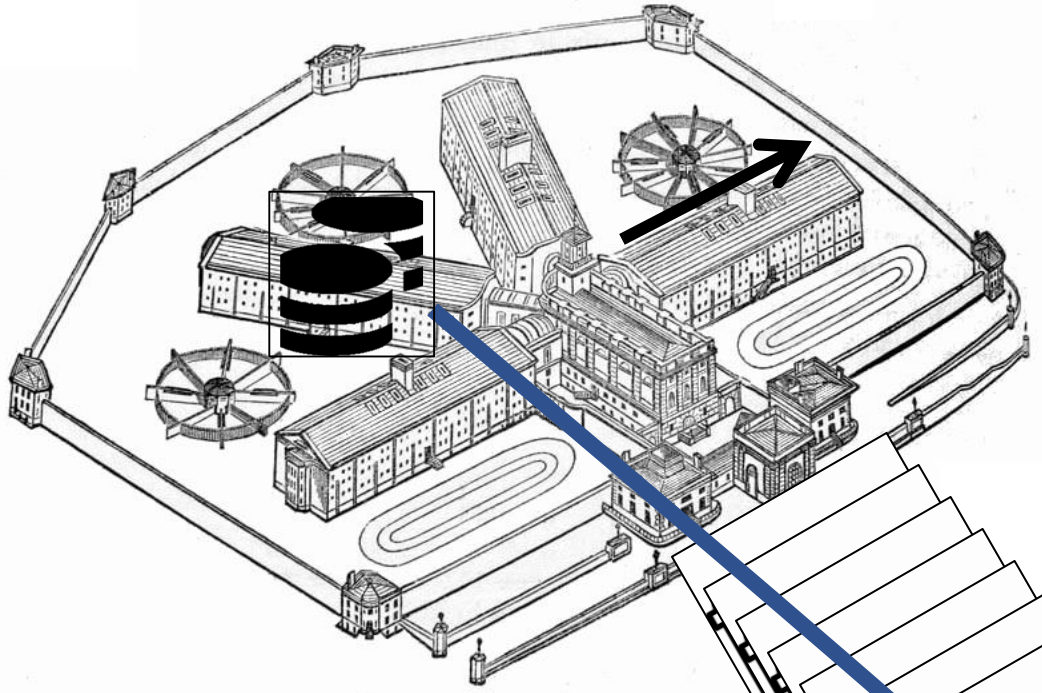
Miners



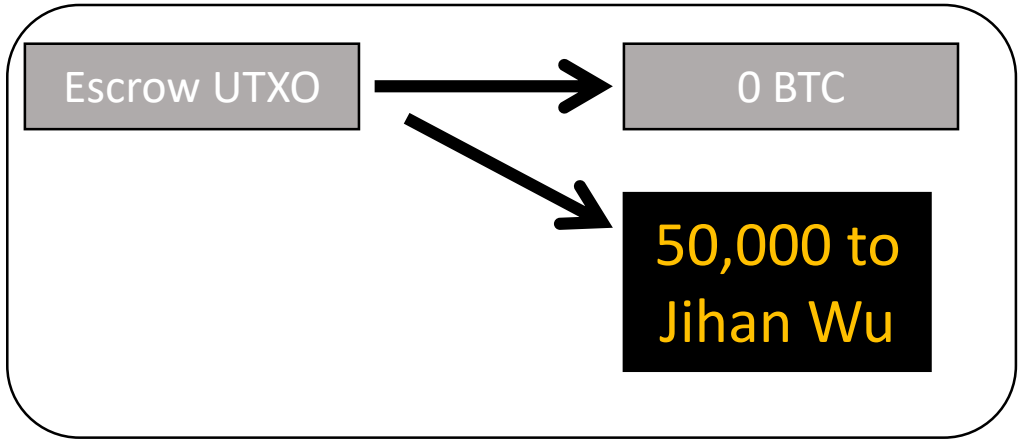
…

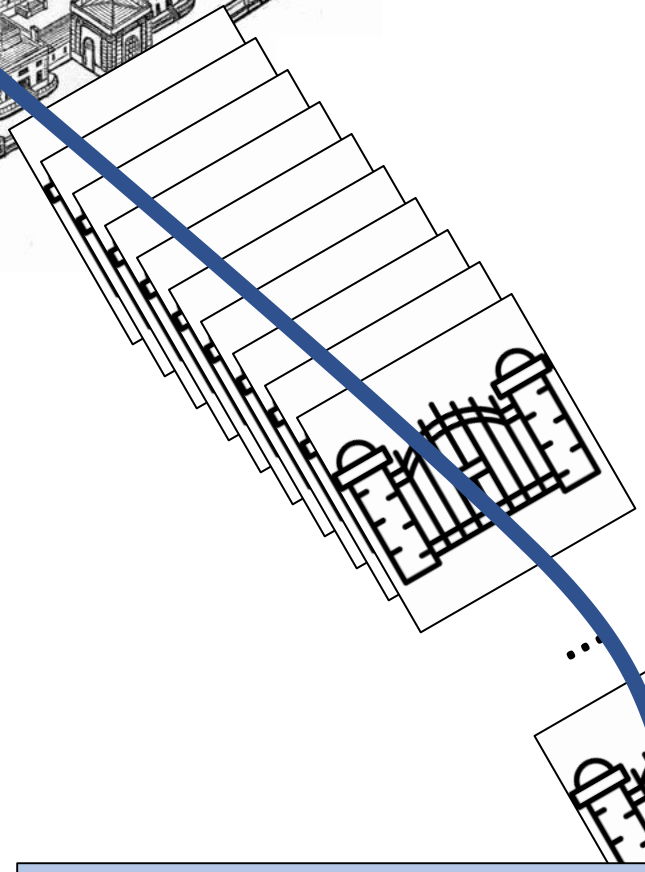


12. Making Progress…



On layer-1:



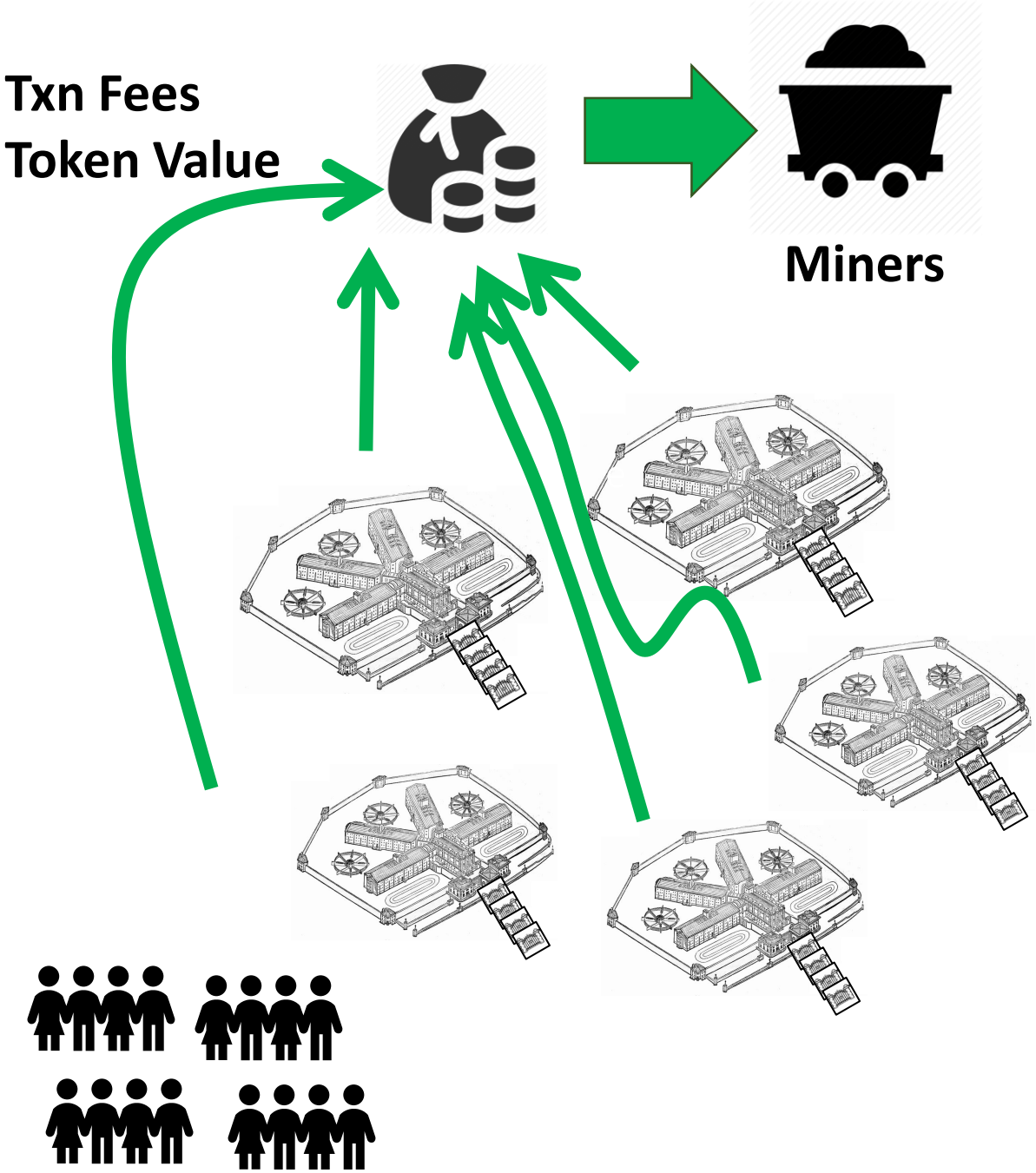


32 bytes

13. Withdrawal Complete

Summary

1. New source of miner-profits.
2. Miners choice: claim this revenue, or destroy it.
3. High-Auditability:
   a) Reducing “all txns” down to “net transfers”.
   b) Crunching all xfers down to 32 bytes.
   c) One transfer at a time.
   d) Transfers take 3 months to settle.



Good News: 100% Optional

- Layer-1 Full nodes: track coins as they enter/exit prisons.
- “Vanilla” Layer-1 contains everything that is needed…
  - …to validate Drivechain txns.
  - …to maximize mining-revenues.

Retail Payments – Comparing the Process
1) Onboard; 2) Make n payments; 3) Settle

You know it. You love it.

Aka “Largeblock Sidechain”
(a **hashrate escrow**; a **prison**)

	Lightning Network	“Bitcoin Payments”
Extra Software	LN Node	SC Node (SPV option)
Onboard a User	Layer-1 txn	Layer-1.5 txn
Preparation	1 channel-open txn	--
N Payments	..on LN	..on L-1.5
Settle to Layer-1	1 channel-close txn	1 “sideshift” out

Total Transaction Fees

	L.N.	B.P.
%-based (LN or SS)	n	1
Layer-1 (larger)	3	1
Layer-1.5 (smaller)	0	n

So, LN is only cheaper when there are many low-value payments. Ie, LN is cheaper than BP, for ***micropayments***.

User Experience

* I assume that an automated hot-wallet is out of the question!

If you are willing to swallow the new security consideration…

	Lightning N.	BTC Payment
Onboard without Layer-1	No	Yes
Receive Payments while Offline*	No	Yes
Recover Wallet From Seed	No	Yes
Immune to Greif-ing / Routing	No	Yes
Option to use SPV Mode	No	Yes
Reckless	Yes	Yes
Txn Settles Instantly	Yes	No

…then we see that the primary advantage of LN is **fast settlement**, especially when both buyer and seller are online. So, LN probably best for in-person retail; SC better for online shopping, perhaps.

Goals

1. Neutralize Meta-Consensus Threats – Altcoins, Hard Forks
2. Boost Hashrate Security In the Long Run
3. Bring Cool New Features to BTC
    1. Payments Sidechain (Just Explained)
    2. New, Risky Crypto (Liquid / MimbleWimble / zCash)
    3. BitAssets (see truthcoin.info/blog/BitAssets)
    4. Identity (see truthcoin.info/blog/codex-identity-sidechain)
    5. Prediction Markets (BitcoinHivemind.com)

Hivemind Endorsements

Please watch my other (short) talks:
BitcoinHivemind.com

Endorsements

"Hivemind may be the most important invention since Bitcoin itself."

- **Roger Ver** (Jun 2015), Bitcoin evangelist and seed investor (Blockchain.info, The Bitcoin Foundation, Ripple, BitPay, ShapeShift, Purse.io)

"I'd give it a low chance of success, but at least it's clever crazy rather than stupid crazy. :)"

- **Peter Todd** (Oct 2015), Bitcoin core developer, notable skeptic (Coinkite "Chief Naysayer"), inventor of Treechains

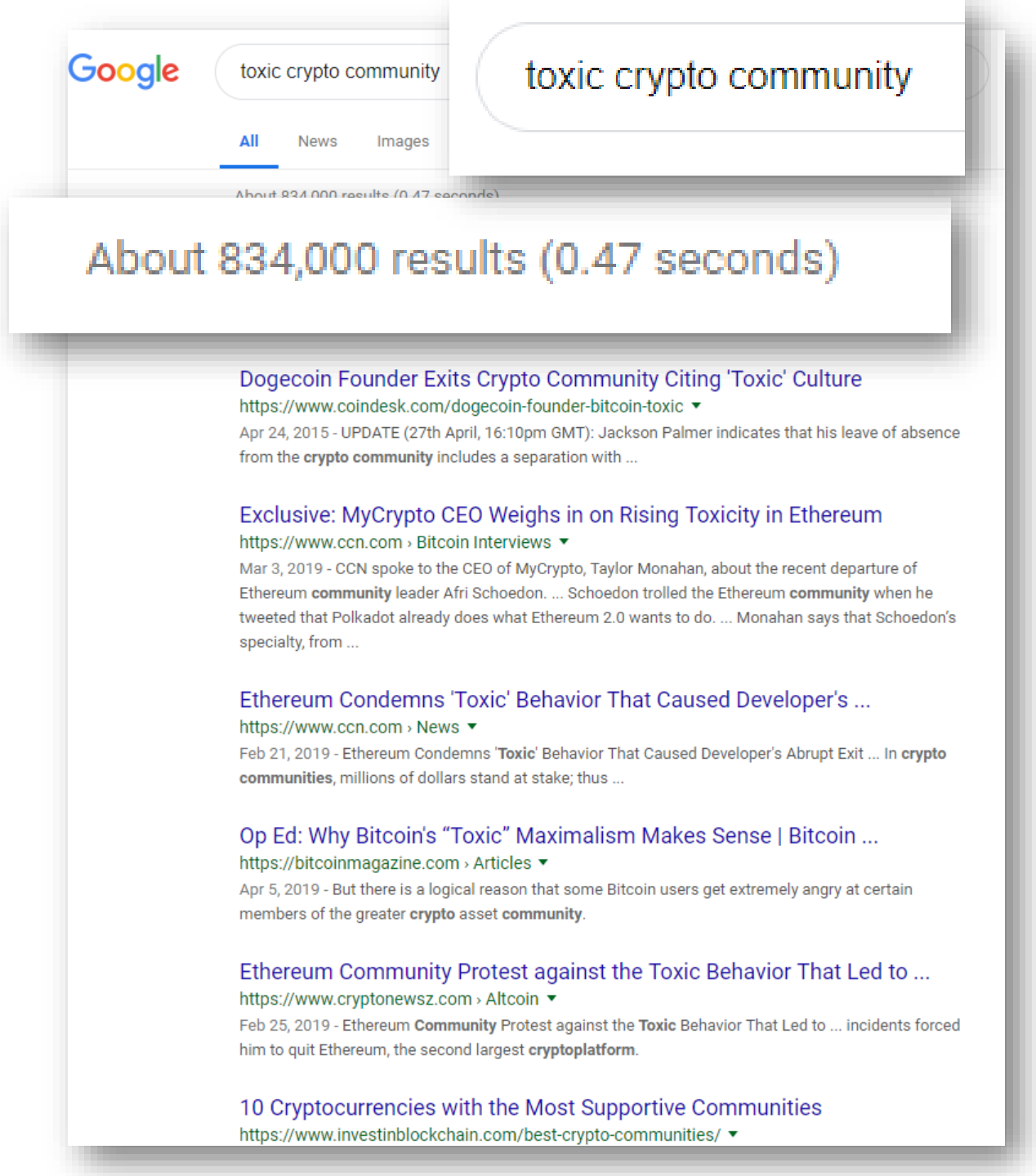
"Hivemind is a real project with interesting use cases. It's great to see them using sidechains - anyone with Bitcoin can participate in their markets."

- **Dr. Adam Back** (Dec 2015), Notable Cypherpunk, inventor of Hashcash Proof-of-Work, Blockstream Co-Founder and President

"I'm very optimistic about the feasibility of this project."

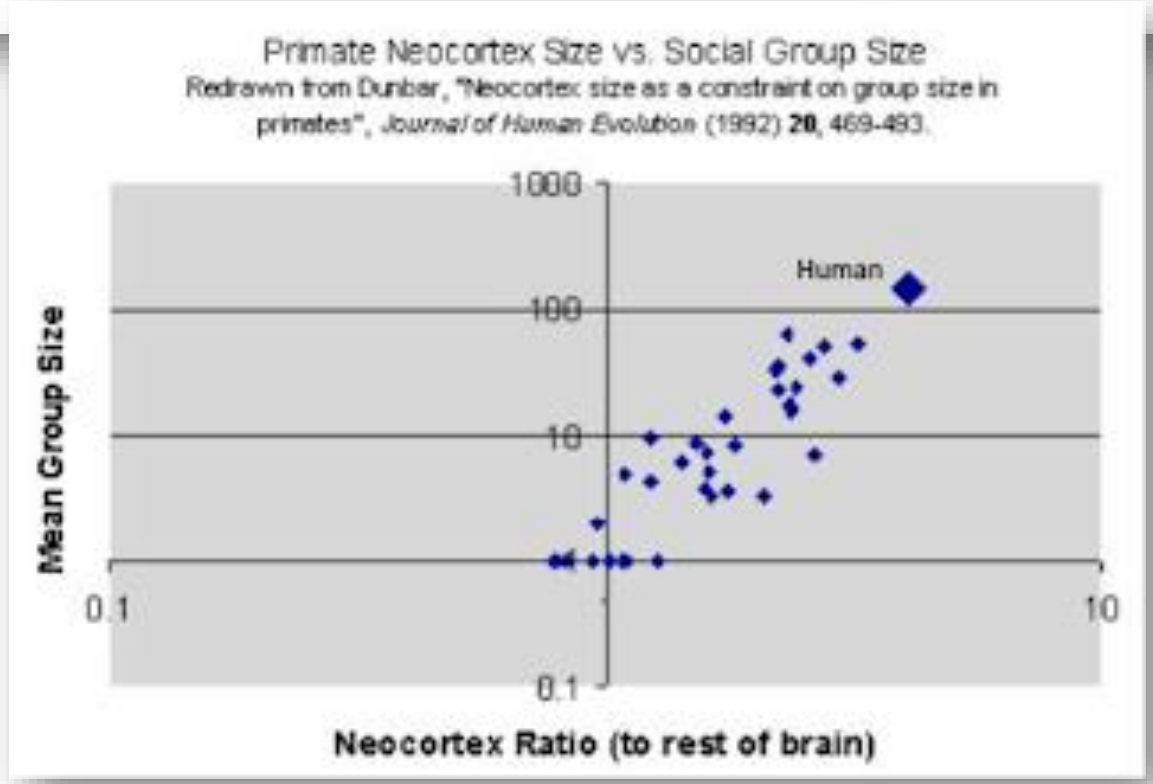
- **Andrew Poelstra** (May 2015), author of A Treatise on Altcoins, On Stake and Consensus, co-author of the Sidechains Whitepaper

“Toxicity”


Google
toxic crypto community
All
News
Images
toxic crypto community
About 834,000 results (0.47 seconds)
Dogecoin Founder Exits Crypto Community Citing 'Toxic' Culture
https://www.coindesk.com/dogecoin-founder-bitcoin-toxic
Apr 24, 2015 - UPDATE (27th April, 16:10pm GMT): Jackson Palmer indicates that his leave of absence from the crypto community includes a separation with ...
Exclusive: MyCrypto CEO Weighs in on Rising Toxicity in Ethereum
https://www.ccn.com › Bitcoin Interviews
Mar 3, 2019 - CCN spoke to the CEO of MyCrypto, Taylor Monahan, about the recent departure of Ethereum community leader Afri Schoedon. ... Schoedon trolled the Ethereum community when he tweeted that Polkadot already does what Ethereum 2.0 wants to do. ... Monahan says that Schoedon's specialty, from ...
Ethereum Condemns 'Toxic' Behavior That Caused Developer's ...
https://www.ccn.com › News
Feb 21, 2019 - Ethereum Condemns 'Toxic' Behavior That Caused Developer's Abrupt Exit ... In crypto communities, millions of dollars stand at stake; thus ...
Op Ed: Why Bitcoin's “Toxic” Maximalism Makes Sense | Bitcoin ...
https://bitcoinmagazine.com › Articles
Apr 5, 2019 - But there is a logical reason that some Bitcoin users get extremely angry at certain members of the greater crypto asset community.
Ethereum Community Protest against the Toxic Behavior That Led to ...
https://www.cryptonewsz.com › Altcoin
Feb 25, 2019 - Ethereum Community Protest against the Toxic Behavior That Led to ... incidents forced him to quit Ethereum, the second largest cryptoplatform.
10 Cryptocurrencies with the Most Supportive Communities
https://www.investinblockchain.com/best-crypto-communities/

Thursday, February 09, 2017

Money, blockchains, and social scalability



Thank You