Sidechain Scaling
“Bitcoin Fission”
Scaling via strategy, not physics

Paul Sztorc

paul.sztorc@blog.com

Saturday Oct 8, 2016

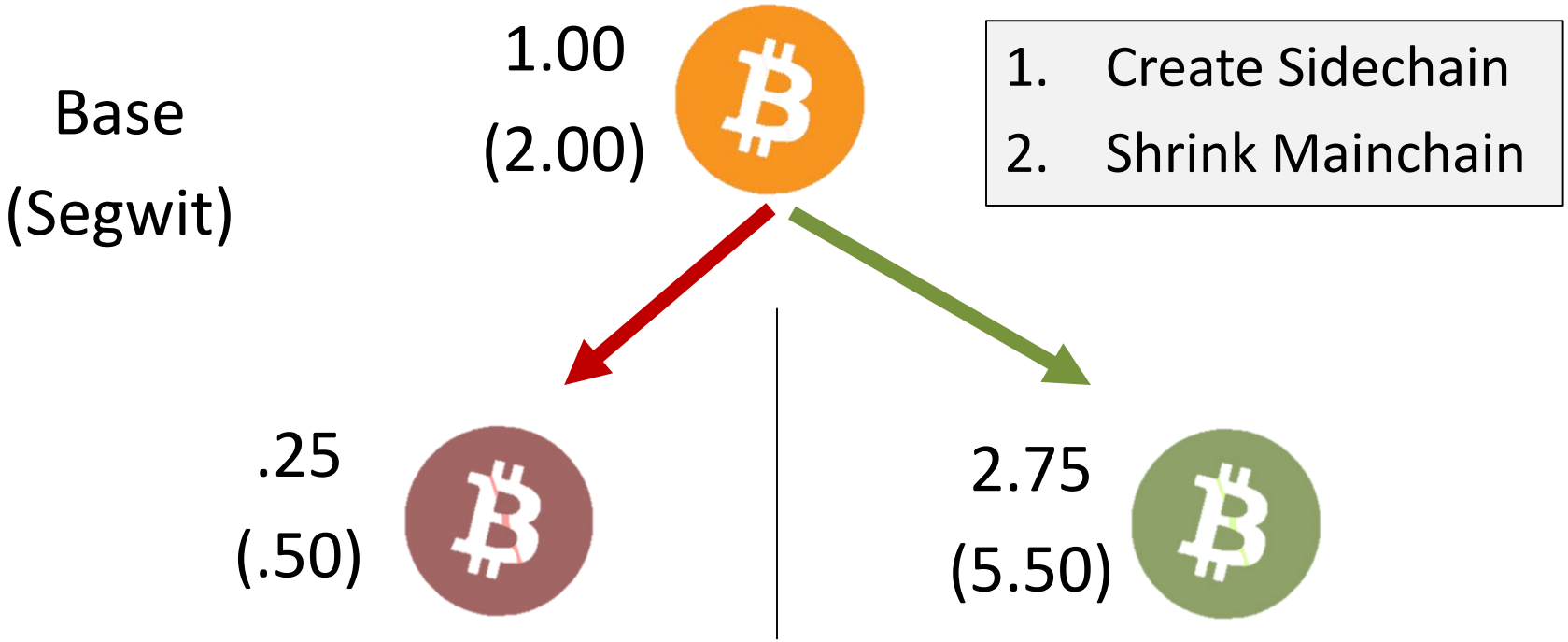
Pizza

- If we cut a pizza into more slices, does it weigh any less?

Agenda

1. Overview & Problem
2. Basics & Definitions
3. Inter-Chain Harms (Are Negligible)
4. Chain II is More Secure Than It Appears
5. Benefits of Fission

The Concept: Teamwork, Not Copies



	Small BTC (Main)	Large BTC (Side)
Nodes:	Many, Cheap, Private	Few, Expensive, Public
Tx Fees:	Higher	Lower
Mode:	Money / settlement	VISA / Payment network

Insecure…intentionally… (diff security).

Problem(s) This Talk Addresses

1. Declining Node Count
   - *Complaints* about disk space, time to sync, bandwidth hogging, risk, reduced privacy.

What motivates people to run full nodes?

2. Loss of Permissionless Innovation!
   - Bitcoin is conservative by design, but this goes against ethos of open source / individual freedom.
   - Misallocation of Dev Resources
3. Throughput (it increases)

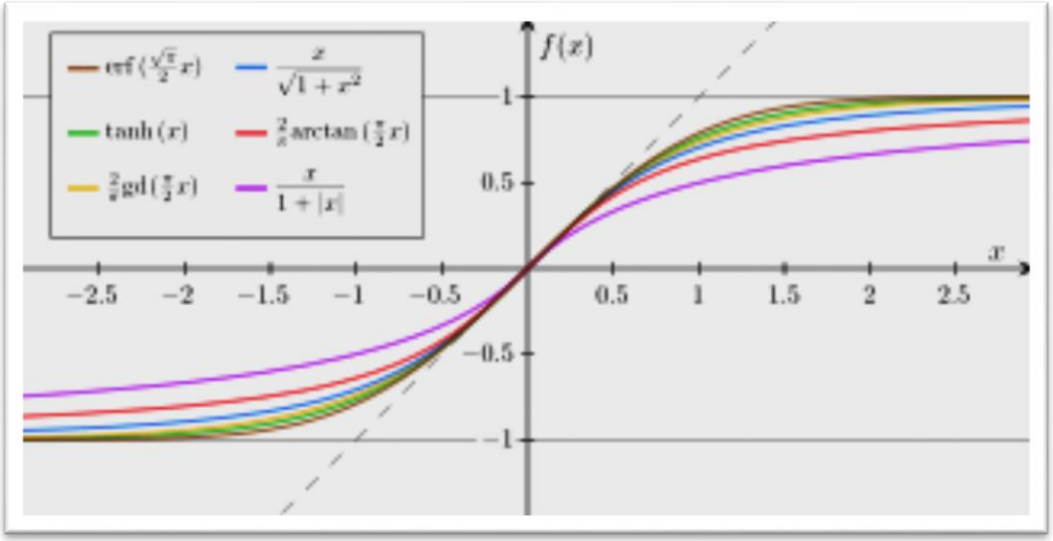
- Does Not Improve:
  - Physics of Info-Xfer
  - "Miner Centralization" (abil. censoring, 51% attack)

Fungibility

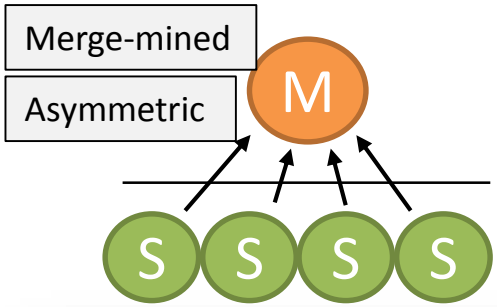
Lightning

What are sidechains?

- An "alt-chain" is a blockchain with "alt" rules and abilities. (Different cost/benefit tradeoff.) :)
  - "alt-coin" = alt-chain + new ***monetary network***.
  - "sidechain" = alt-chain + inherits ***monetary network***.
  - (Note that ***mone. networks*** are *inherently adversarial.*) : (
- Open Questions
  - Is a sidechain "Bitcoin"? Essentialism
  - To what extent are "we" responsible for them?



What is Drivechain?



www.truthcoin.info/blog/drivechain/

Drivechain - The Simple Two Way Peg

24 Nov 2015

Main-to-Side

(Much Earlier)

Transaction 1: 96e08e333304dad95d10...
17bAY2JM37he7t.. OP_RETURN 1MFWbAqkcA6Pjz... → 4HftNSm282A3rG..

Transaction 2: ff44d9cdda857a902cf698...
14e4o4b5yibp4w.. OP_RETURN 1QAtLEPrxddW9D... → 4HftNSm282A3rG..

Transaction 3: 653cbe17844eba9df26ad...
1WEZNFsw5trRJU.. OP_RETURN 1teQsVXAXxrCtTT... → 4HftNSm282A3rG..

Three deposits, from Bitcoin (orange) to an address (green) on a Bitcoin sidechain (bold green). The Mainchain BTC are trapped "in 4HftNSm282A3rG.."

Contracts, Payments, Services

Sidechain

(Very Recent Past)

17bAY2JM37he7t.. OP_WITHDRAW 96e08e333304dad95d10... OP_RETURN 1ExTxQbQrdXXJM... → 1BitcoinEater000..

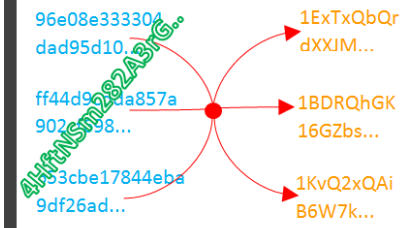
14e4o4b5yibp4w.. OP_WITHDRAW ff44d9cdda857a902cf698... OP_RETURN 1BDRQhGK16GZbs... → 1BitcoinEater000..

1WEZNFsw5trRJU.. OP_WITHDRAW 653cbe17844eba9df26ad... OP_RETURN 1KvQ2xQAiB6W7k... → 1BitcoinEater000..

...ividual withdrawals (WTs), from a Sidechain ...to the Mainchain (orange). Software selects ...txns (blue) to match the desired amounts.

Side-to-Main

(At Present)



The assembled WT^, whose ID will be included in the Sidechain header for a while. On the Bitcoin Mainchain, it eventually moves BTC "from 4HftNSm282A3rG.." to their new owners.

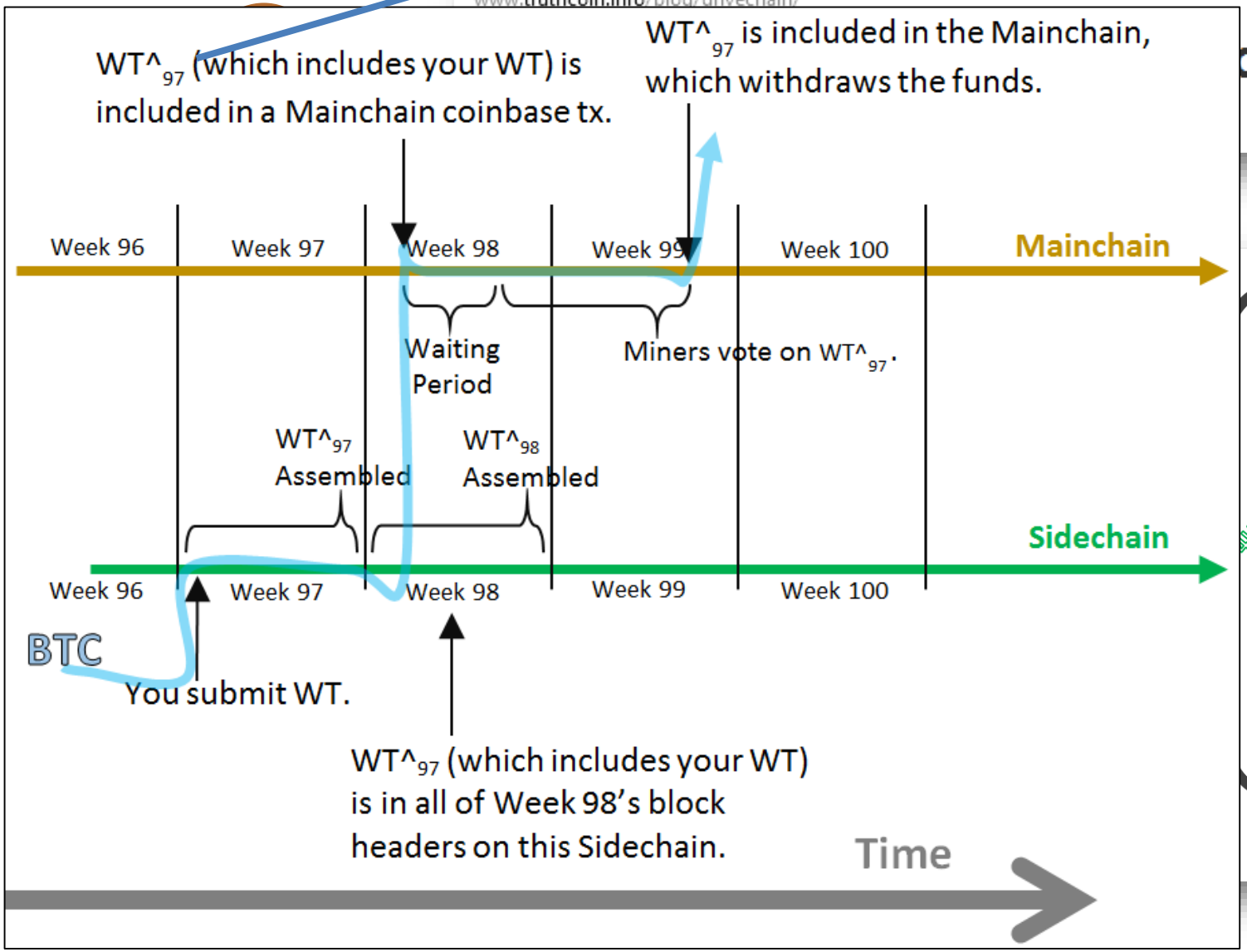
For simplicity, I assume that all addresses/transactions contain exactly 1 BTC (except for the WT^ which contains 3 BTC).

What is Dr

04B4697D5319B8B0E461BE624EAD61331
CA613216F061D2533490ABBB71616A0

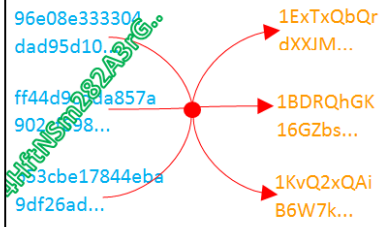
www.truthcoin.info/blog/drivechain/

o Way Peg



Side-to-Main

(At Present)



The assembled **WT^**, whose ID will be included in the Sidechain header for a while. On the Bitcoin Mainchain, it eventually moves BTC "from **4HftNSm282A3rG..**" to their new owners.

What is Dr

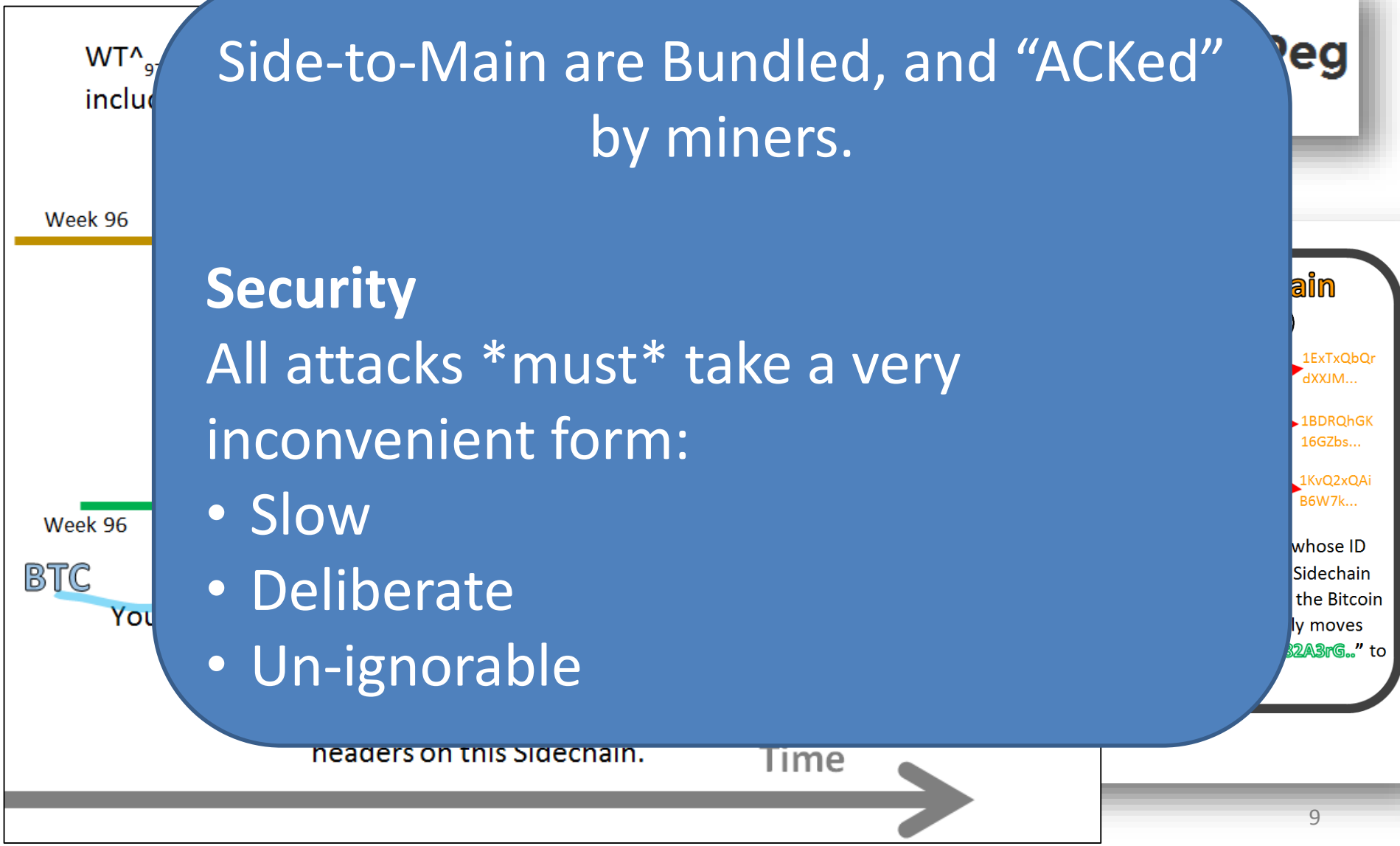
04B4697D5319B8B0E461BE624EAD61331
CA613216F061D2533490ABBB71616A0

Side-to-Main are Bundled, and “ACKed” by miners.

Security

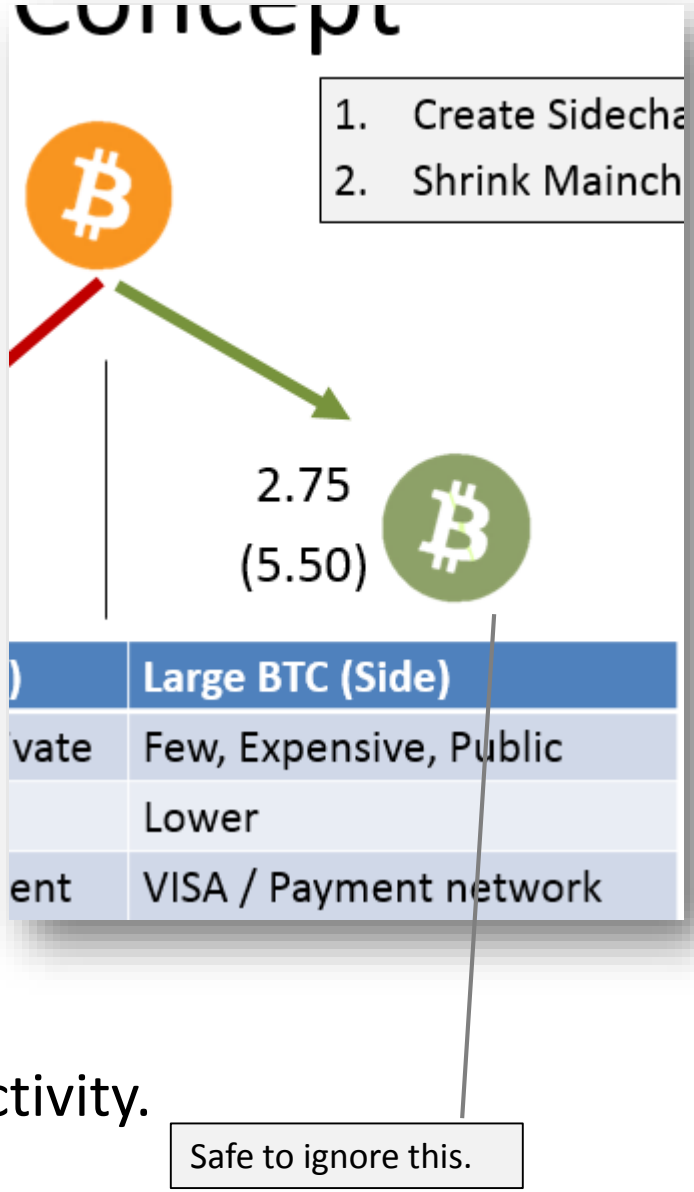
All attacks *must* take a very inconvenient form:

- Slow
- Deliberate
- Un-ignorable



Great News: Costs are "Opt In"

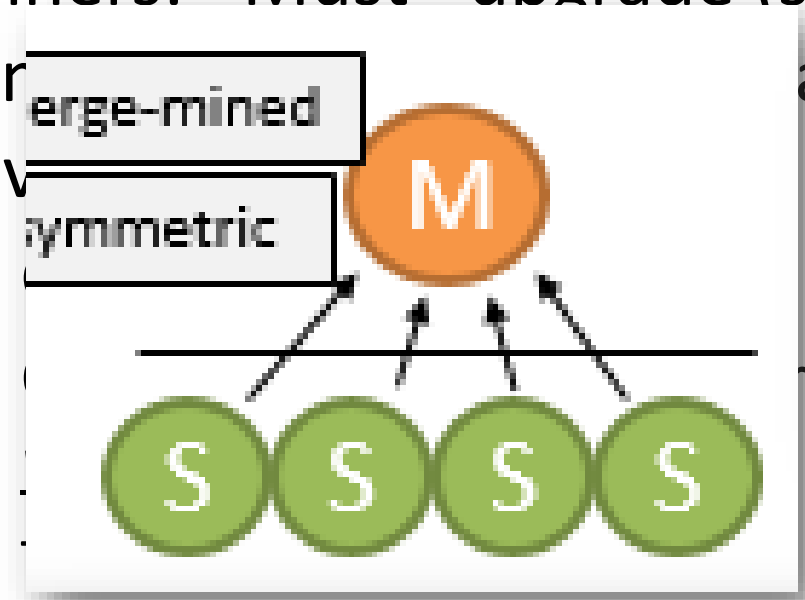
- Network: "Opt-In" Soft Fork
- Users: ***Option*** to use Sidechain
  - "checkbox", if want cheaper txns & higher node costs.
- Miners: *Must* upgrade (sf + mm.sc – if sidechain generates tx fee revenues).
  - Cost is tiny. Pays for itself.
  - Other centralization pressures *way* more relevant (spv, spy, smp).
  - Talk on sidechain risks / miner interactivity.

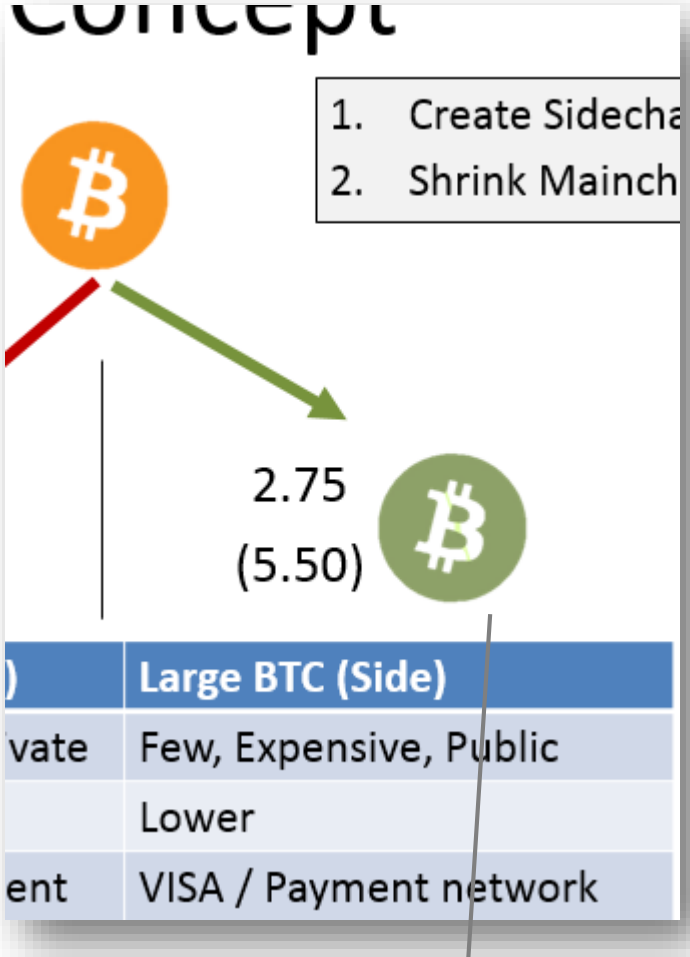


Great News: Costs are “Opt In”

- Sidechain used as a large, lightning hub…
  …that is itself a BTC blockchain.

  Slowly syncs to settlement layer.
- Miners: *Must* upgrade (sf + mr… ates rev…
  - …
  - …res
    …smp).
  - … interactivity.





Safe to ignore this.

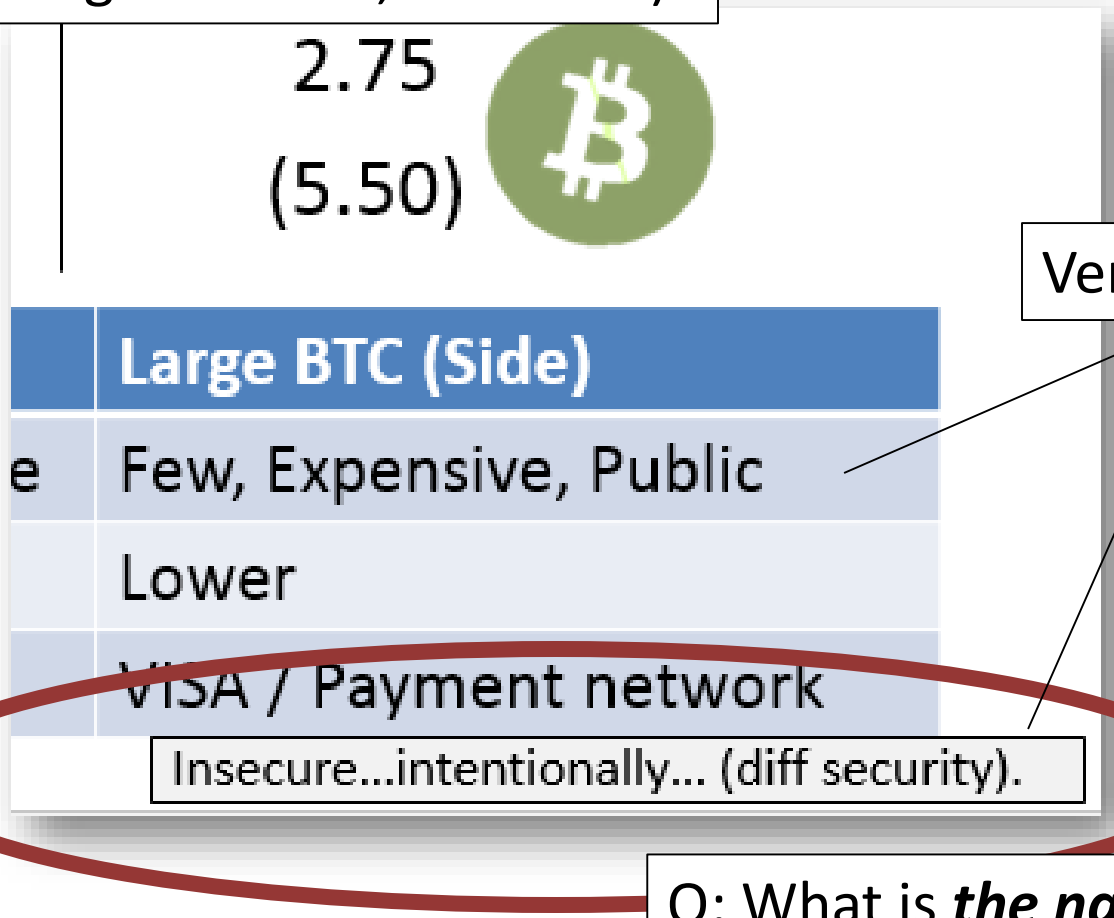
End of 1st Half

Agenda

1. Overview & Problem
2. Basics & Definitions
3. Inter-Chain Harms (Are Negligible)
4. Chain II is More Secure Than It Appears
5. Benefits of Fission

What about this?

If risks = 0, but what if benefits = 0?!
(Pointless if Large BTC dies, or breaks)!



Very Un-Bitcoin like

Q: What is ***the nature of our weakness*** to having few nodes?

Is this "just" PayPal, Venmo, etc?

Sidechains + Lightning Network

Lightning Network

Scalable, Instant Bitcoin/Blockchain Transactions

Transactions for the Future

Instant Payments. Lightning-fast blockchain payments without worrying about block confirmation times. Security is enforced by blockchain smart-contracts without creating a on-blockchain transaction for individual payments. Payment speed measured in milliseconds to seconds.

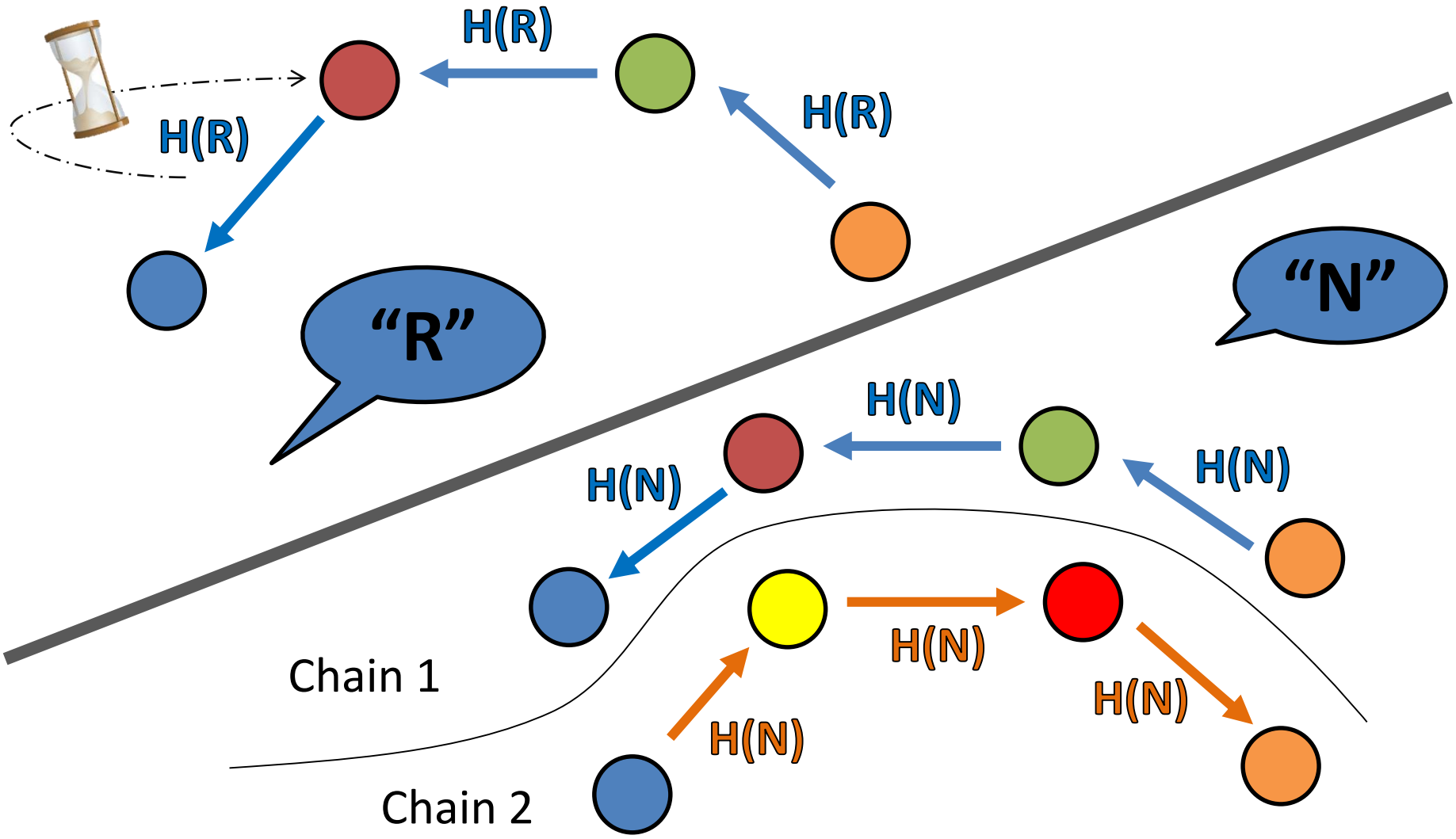
Scalability. Capable of millions to billions of transactions per second across the network. Capacity blows away legacy payment rails by many orders of magnitude. Attaching payment per action/click is now possible without custodians.

Low Cost. By transacting and settling off-blockchain, the Lightning Network allows for exceptionally low fees, which allows for emerging use cases such as instant micropayments.

Cross Blockchains. Cross-chain atomic swaps can occur off-chain instantly with heterogeneous blockchain consensus rules. So long as the chains can support the same cryptographic hash function, it is possible to make transactions across blockchains without trust in 3rd party custodians.

Point 1: The BTC on “small” are instantaneously interchangeable for the BTC on “large”.

Sidechains + Lightning Network



Why Do We Want Many/Cheap Nodes?

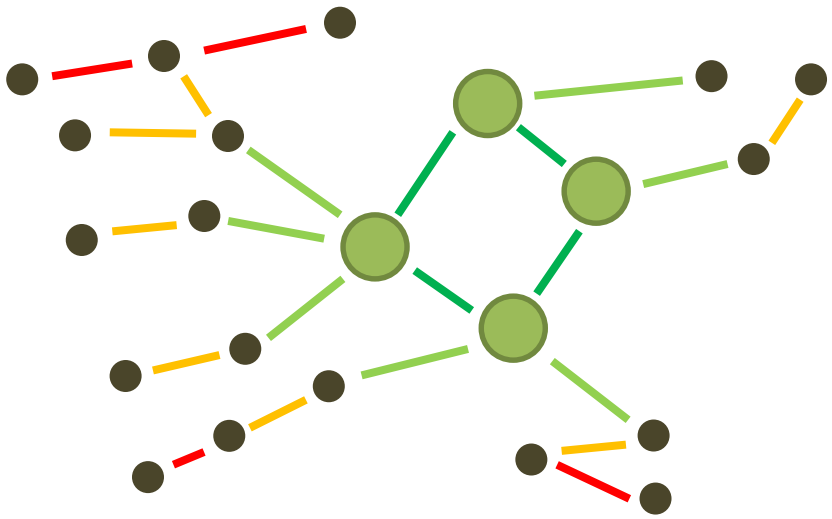
What is ***the nature of our weakness*** to having few/expensive nodes?

1. Redundancy – Avoid a central point of failure.
2. Security – Discourage / overwhelm attackers ("Where should I aim?")
3. Sovereignty – "your" money, "your" contracts ..."your" node.

How can { **SmallBTC** + **BigBTC** + LN } help with this?

Surviving a Fatal Attack

- Say an attack disables all of the nodes.
  - Typically: existential
- OK, say an attack disables the *large nodes* only.
  - Worst case: All “Large BTC” are paused.
  - Best case: Full refund on “small BTC”

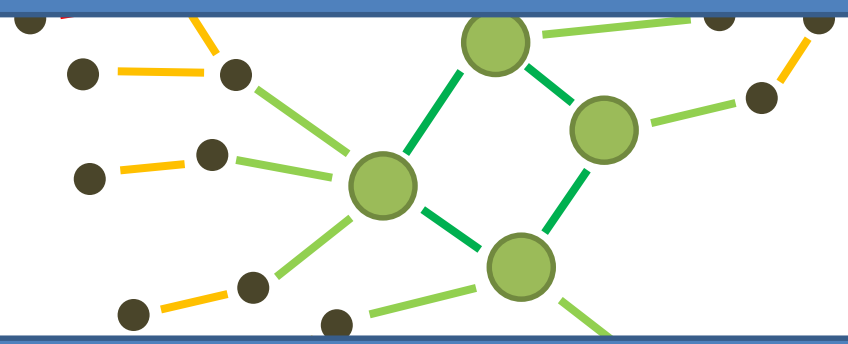


- Channels are off-chain.
- [1] miners buy BTC with btc.
- [2] miners pay themselves
- Possible “emergency blocks”
  - ultra-small
  - Within Mainchain coinbase

Surviving a Fatal Attack

- Say an attack disables all of the nodes.
  - Typically: existential
- OK, say an attack disables the *large nodes* only.
  - Worst case: All “Large BTC” are paused.
  - Best case: Full refund on “small BTC”

-- Realistic case: (Probably) 95% of users get a refund, at cost 1-2%.

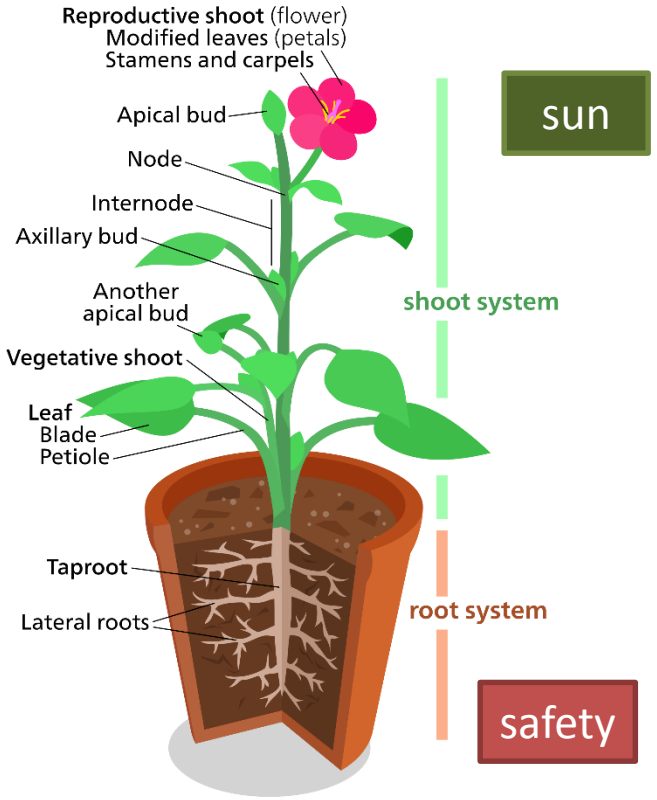


- [1] miners sell BTC for btc.
- [2] miners pay themselves
- Possible “emergency blocks”

Result: Attack is pointless, largely no point in bothering with attacking.

(Potential) Synergy

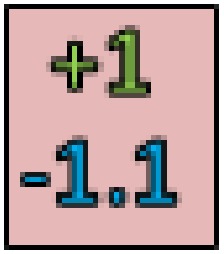
- "Weighing the pizza" -- static and solitary, ignores *strategic interaction* . Need Reactive / Organic metaphor.
- Better metaphor: weed that won't die.



- Small BTC + Large BTC (+ Lightning) = **Regeneration**
- Regeneration = Attack's Wont Succeed = Attacks costly, and embarrassing.
- Conclusion: can take "large" risks, but only pay "small costs"

Game Changer – Metaphors

- US Legal
  - Global **BitTorrent** (VPN allows sophisticated consumers to breach copyright laws, therefore non-VPN unsophisticated breaches are often tolerated).
  - Alcohol **Prohibition** (opposite – total ban was attempted, but it backfired resulting in large black market sales, rise of mafia, etc)
- Biology
  - Dominance Hierarchies
  - Costly Signaling (Handicap Principle)



- Psychology
  - Learned Helplessness (saving effort, in situations which are perceived as hopeless).

Conclusion: Benefits

1. Scale by factor of 3 (2 → 6).
2. Laboratory for “Scale Experiments”.
3. Only hope for decreasing size (recovering nodes).
4. Improvements in tech increase *both* security & scale simultaneously.
5. My Ulterior Motives
    1. Sidechains (Anti-Scam)
    2. Hivemind

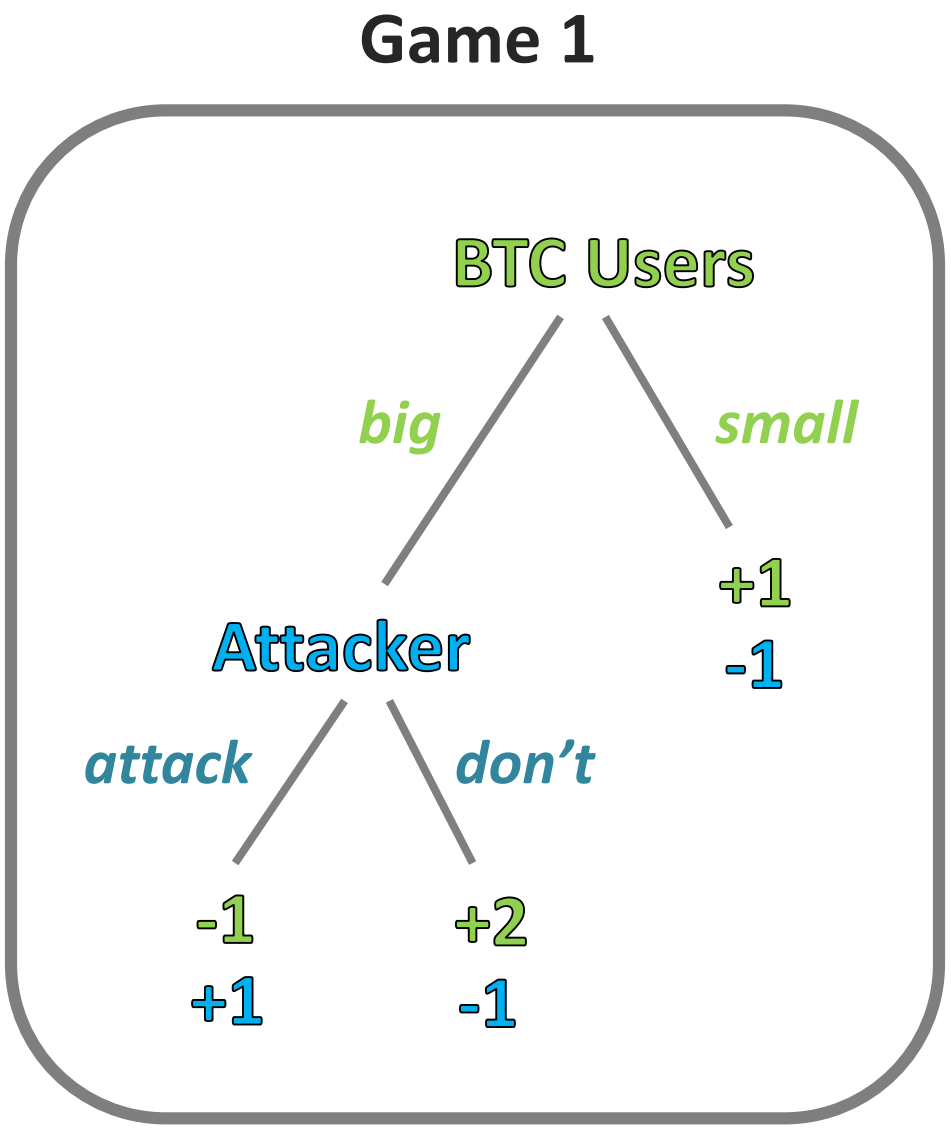
Thank You!!

Paul Sztorc

bloq

Appendix

Game Changer



BTC Users

+2 = more BTC

+1 = some BTC

-1 = BTC Dead :-(

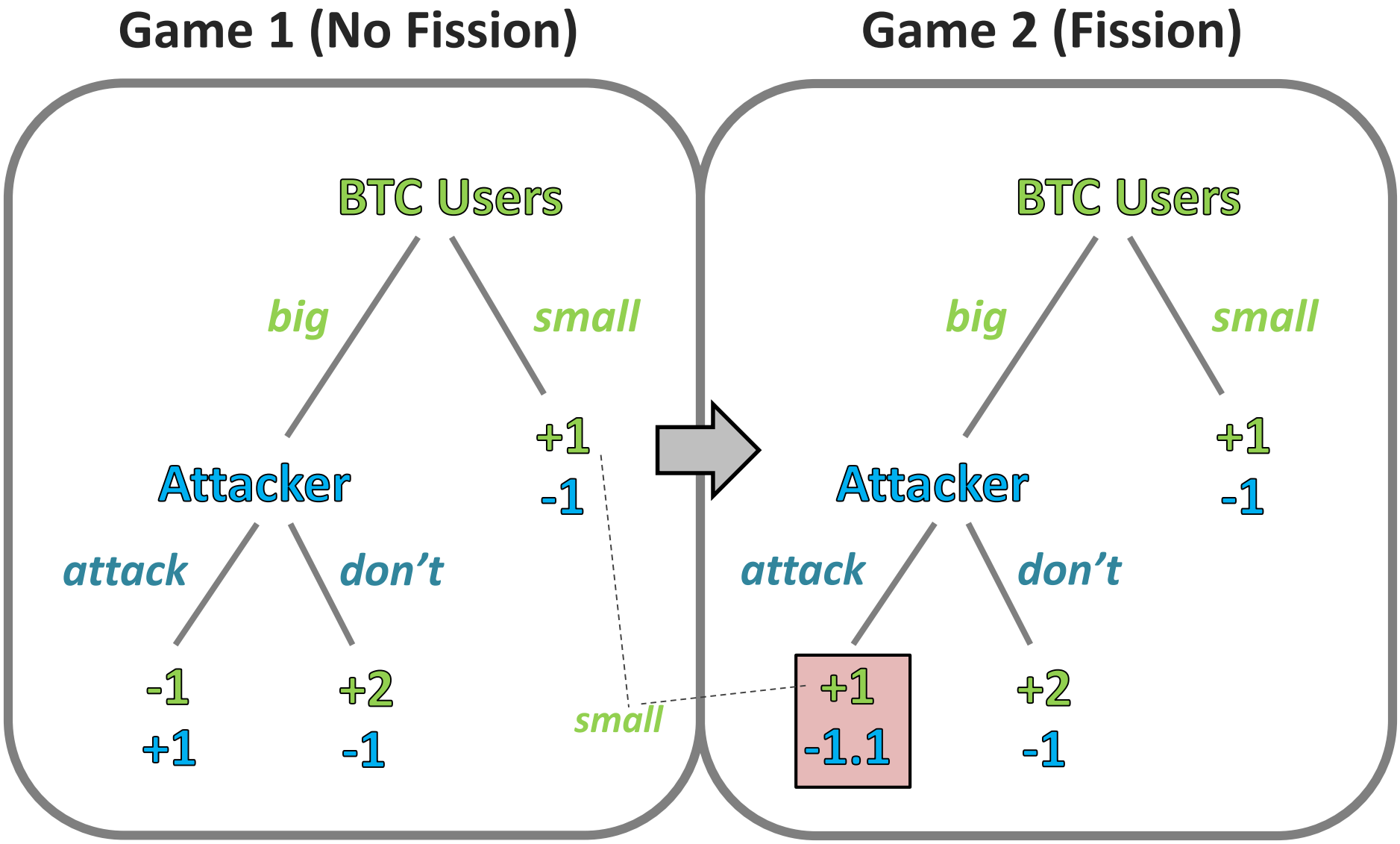
Attacker

+1 = BTC Dead >-)

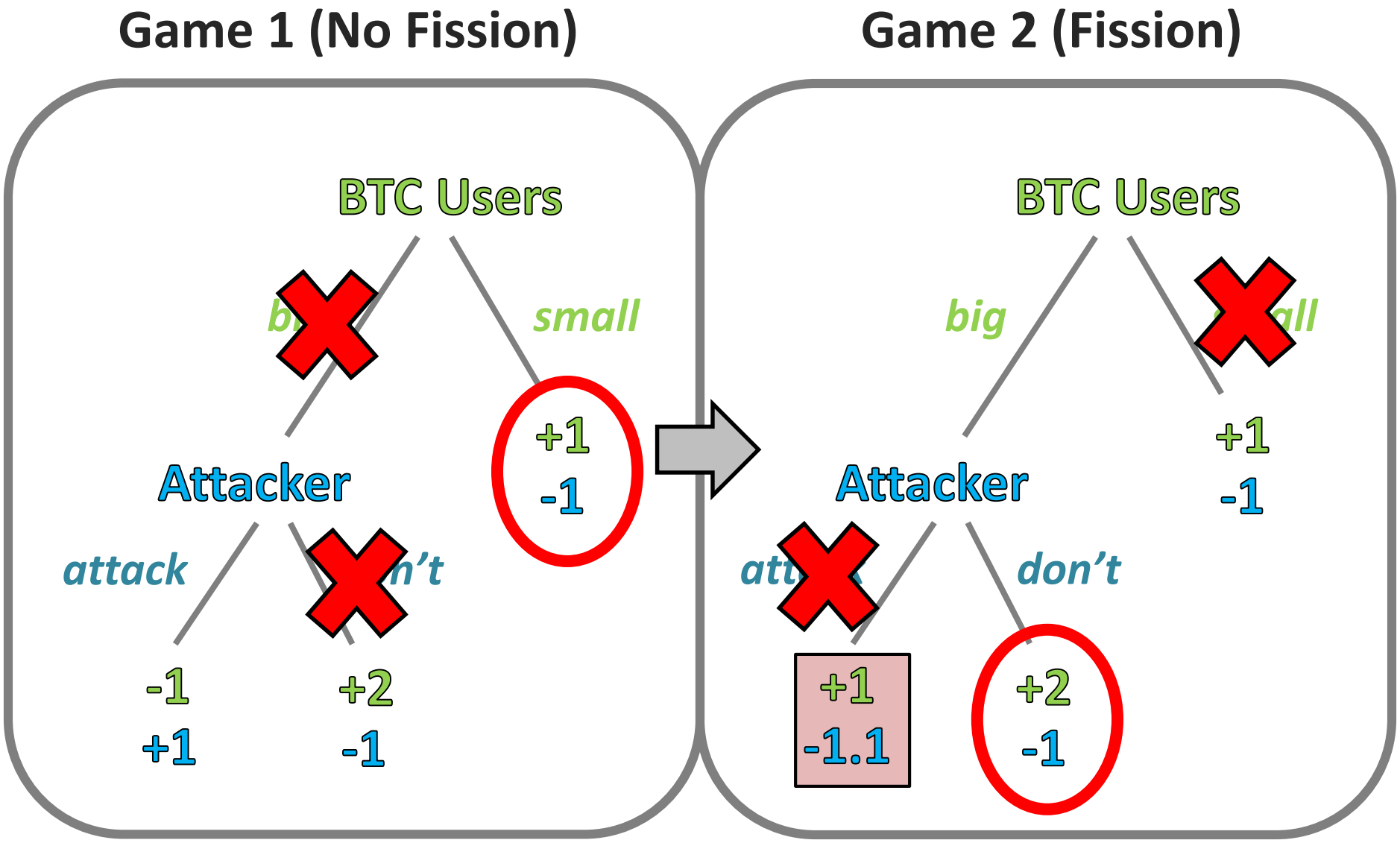
-1 = BTC Alive :-(

-1.1 = failed attack : /

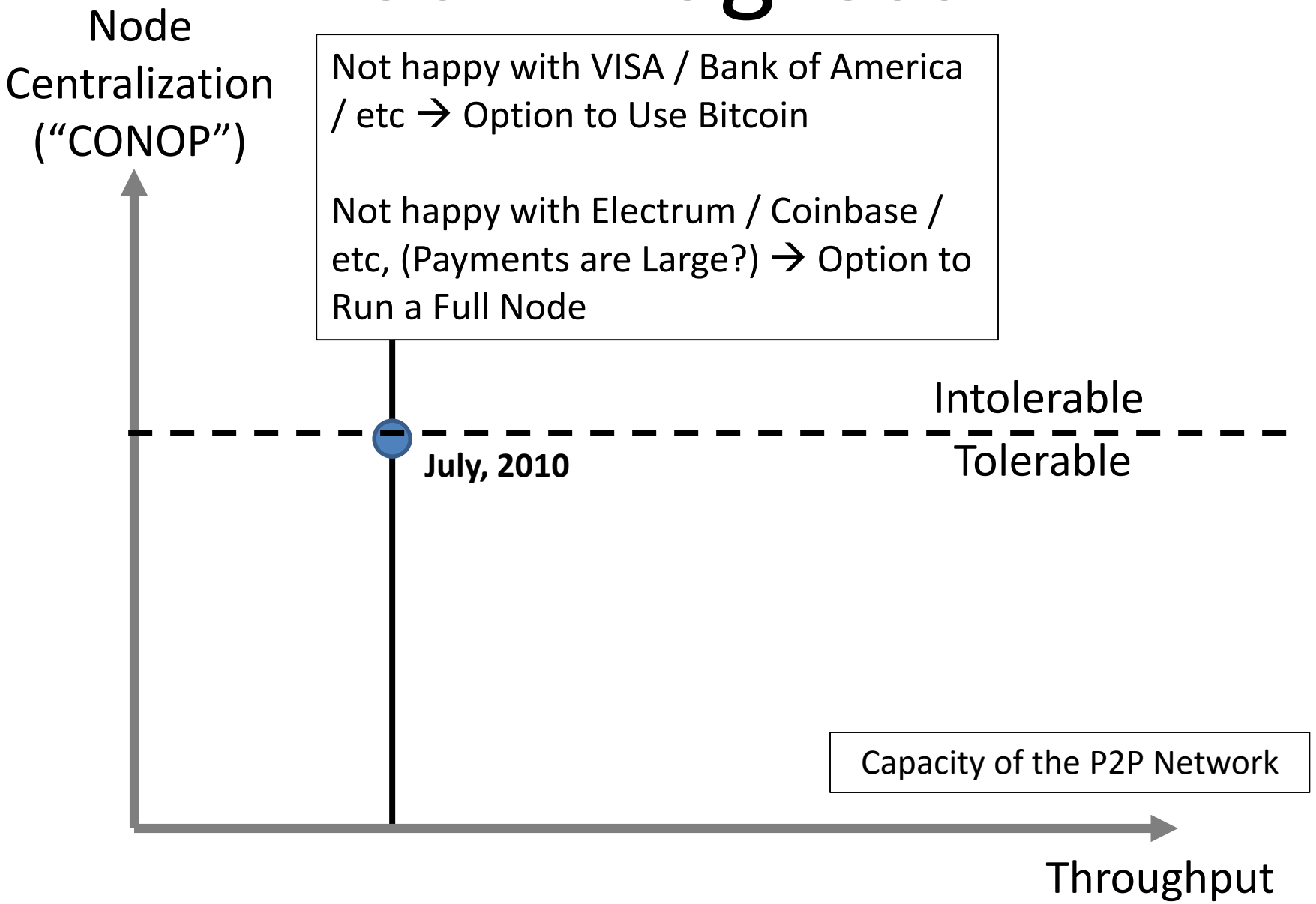
Game Changer



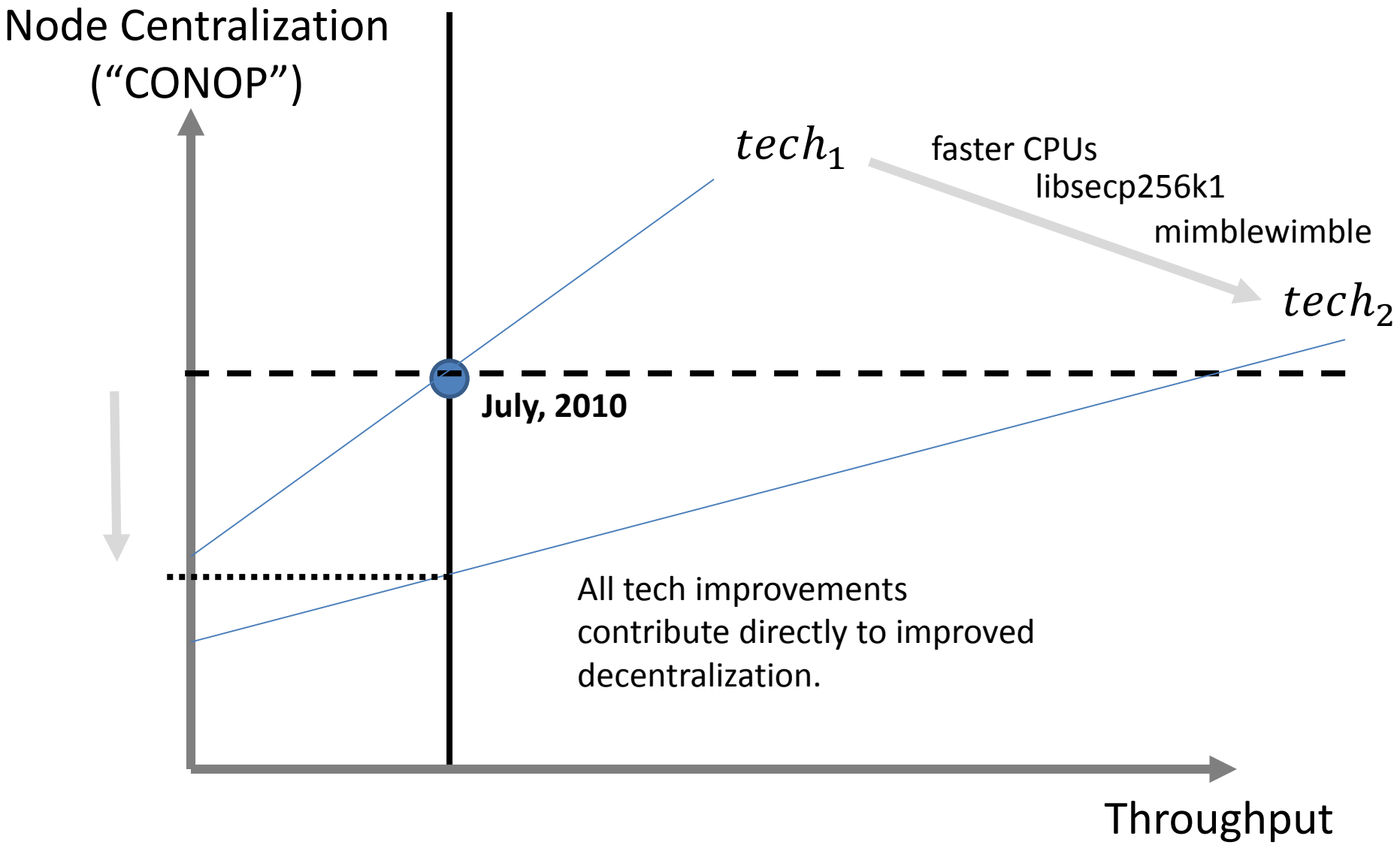
Game Changer



Tech Progress



Is min(y) optimal…or should we tradeoff…



…or take min(Y) AND max(X).

- Keep “Small BTC” the same size.
- Keep “Large BTC” as large as possible.

	Benefits	Costs
Small:	Small	Small
Large:	Large	Large
Both:	Large	Small