REAL WORLD BLOCKCHAINS

BLOCKCHAIN HUNT 2017

INTRO

- Blockchain idea is so simple!
- Details may be complicated
- https://magoo.github.io/Blockchain-Graveyard

CRYPTOGRAPHY

CRYPTOGRAPHY: RANDOM

○ Use secure random

○ Use enough randomness: wallet dictionary, seed

○ Use enough hash iterations for passwords

○ Don't allow users to generate random

CRYPTOGRAPHY: SIGNATURE MALLEABILITY

○ Signature malleability: elliptic curve crypto only guarantees immutability of signed data, not a signature itself

○ Transaction/block id should be independent from signatures

○ Weak keys

CRYPTOGRAPHY: MORE

○ Follow the specification!

○ Combination of secure primitives may be insecure

○ Long validation → DDoS attacks

○ Do not trust — backdors are possible

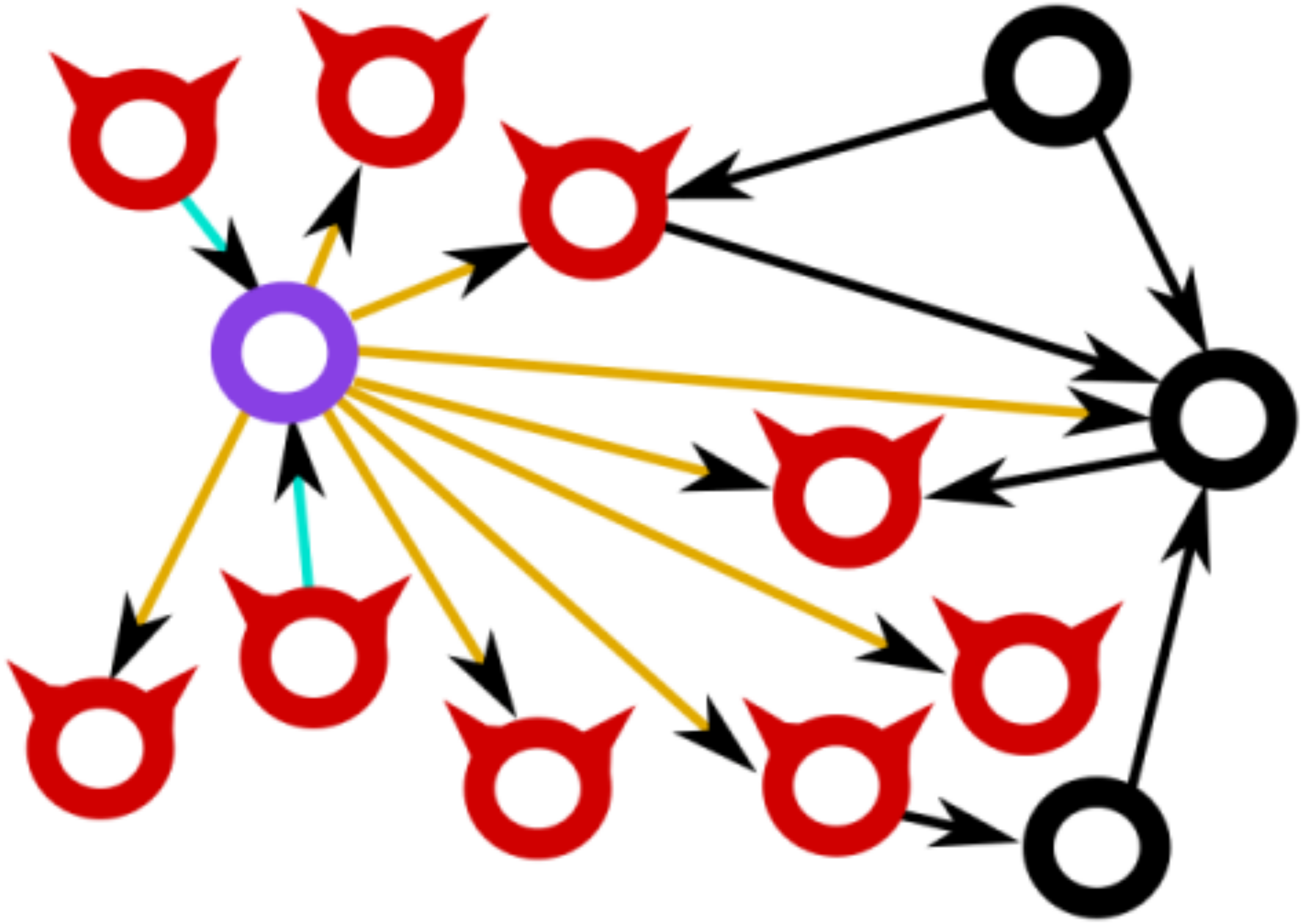
NETWORK

NETWORK: DATA CHECK

- No trusted data!
- Data size should be limited
- Data types have limits (e.g. Long)
- Easy validations first or DDoS
- Any heavy validation leads to DDoS
- Validation degradation with some parameter leads to DDoS

NETWORK

ECLIPSE ATTACKS



Bitcoin: http://ia.cr/2015/263

Ethereum: https://goo.gl/mQv58v

NETWORK THROUGHPUT

Blockchain throughput is limited!
Bitcoin 255K tx/day, Ethereum 400K tx/day

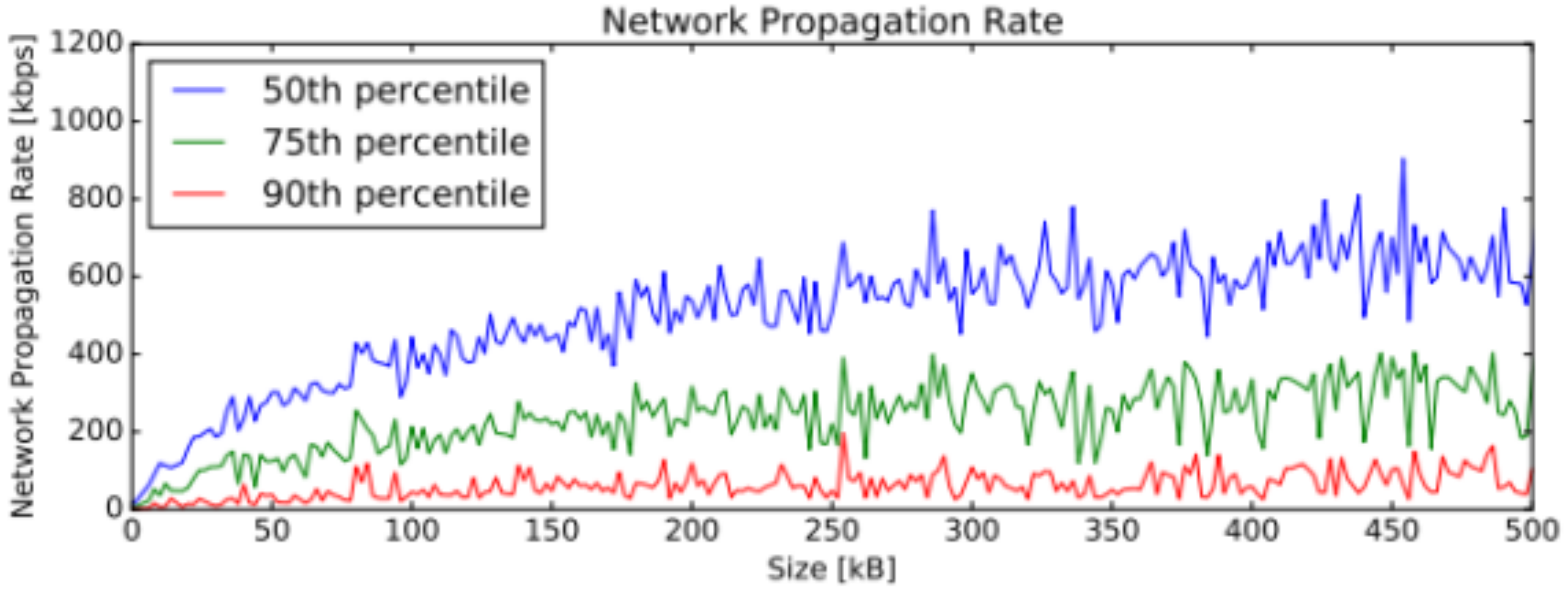
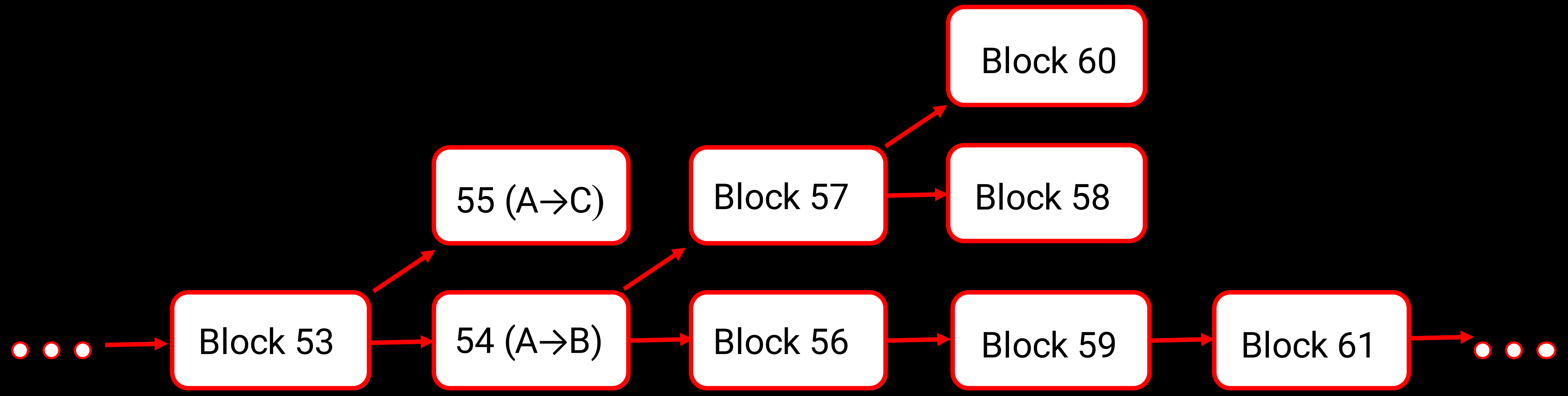


Fig. 1: Network propagation rate (capturing both latency and throughput) vs. block size.

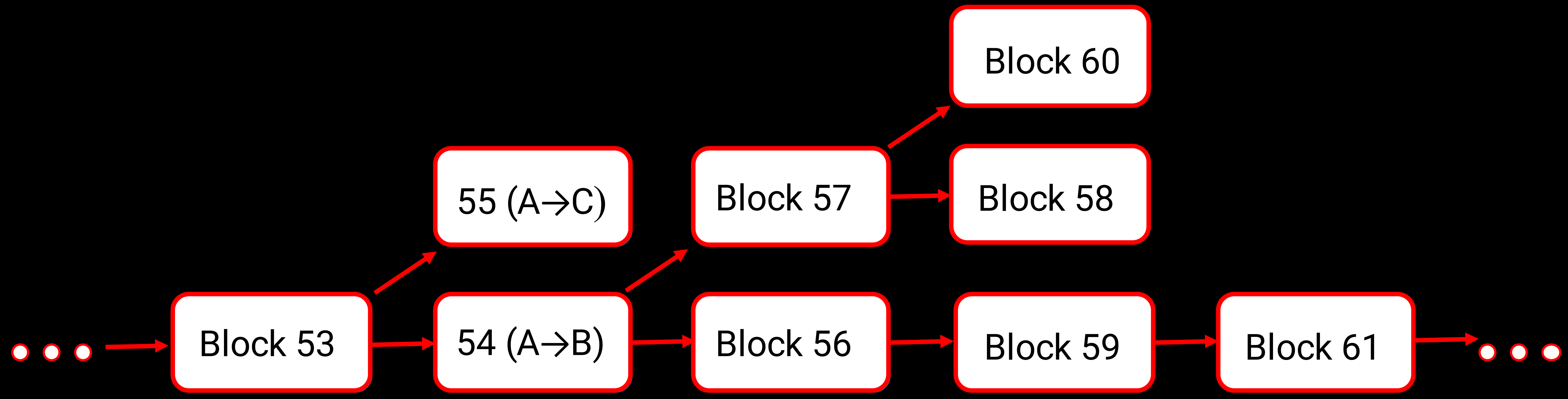
On Scaling Decentralized Blockchains”
http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

CONSENSUS



Forks

- Forks are possible!
- (Especially during protocol improvements)
- Wait for more confirmations
- Chain splits are possible!
- Define rules for such situations



Best chain discovering

HOW TO FIND THE BEST CHAIN?

Attack:

- Declare a chain with the best **score** (cumulative difficulty)
- Don't send the blocks or send just few of them

MINING

- If something is possible, it is legit
- Miners will not follow default behaviour
- ASICBOOST
- Selfish mining
- Multibranch forging
- Mine in branch with high fees
- Chain hoping

GOVERNANCE

- Still open question
- Different view of users, developers, researchers, investors, satellites, ...
- Most of them do not care about decentralization
- No one want chain split, but want his feature to be included

PROGRAMMING ERRORS

CODE BAGS

- Small code bug may lead to huge problems
- If “code is rule” how to separate bug from feature?
- Multiple implementations may help to found bugs as soon as possible
- But leads to chain split
- Even small difference in consensus rules leads to chain split

(ALMOST) NO WAY TO FIX

If something already happened it’s hard to fix it:

○ Drop blocks before exploit leads to fund loses

○ Hardfork leads to chain split

SMART CONTRACTS

BITCOIN-LIKE

○ Rich authenticated languages

○ General scheme

○ Lock funds in blockchain(s)

○ Do some work off chain

○ Unlock funds in blockchain(s)

EXAMPLES

- Atomic swap
- Payment network
- Pay-for-proof

ETHEREUM-LIKE

More freedom — do what you want*

- Within gas limit
- That may be reduced
- All nodes will run your code —> expensive + DDoS
- More freedom — more vulnerabilities

- Good examples
- Token crowdsale
- The DAO

GOING TO START YOUR SERVICE?

SERVICE

- Keep in mind blockchain limits
- Your server ~~may~~ will be hijacked
- Related centralized services ~~may~~ will be hijacked
- Keep money on cold storage, multisig addresses
- Enforce secure passwords, 2FA
- Sign messages, commits
- Start bug bounty
- Learn history
- https://magoo.github.io/Blockchain-Graveyard/advice/

Dmitry MESHKOV

Founder of ERGO Platform, researcher at IOHK.

catena@protonmail.com
https://twitter.com/DmitryMeshkov
https://ergoplatform.org
https://iohk.io
blockchaininstitute.io

Blockchain Institute.

THANKS FOR YOUR TIME!