



**ΣRGO**

COMPREHENSIVE CRYPTOCURRENCY DESIGN

DMITRY MESHKOV, ALEX CHEPURNOY

25 APRIL 2017

MOSCOW BLOCKCHAIN DEVELOPERS MEETUP

# Structure

- Ergo idea
- Blockchain problems
- Ergo solution

Σrgo idea

# Motivation

## Theory

- Provably secure
- New features
- Impractical

## Practice

- 1000 currencies
- Ad-hoc solutions
- Security issues

# Motivation

## Theory

- Provably secure
- New features
- Impractical



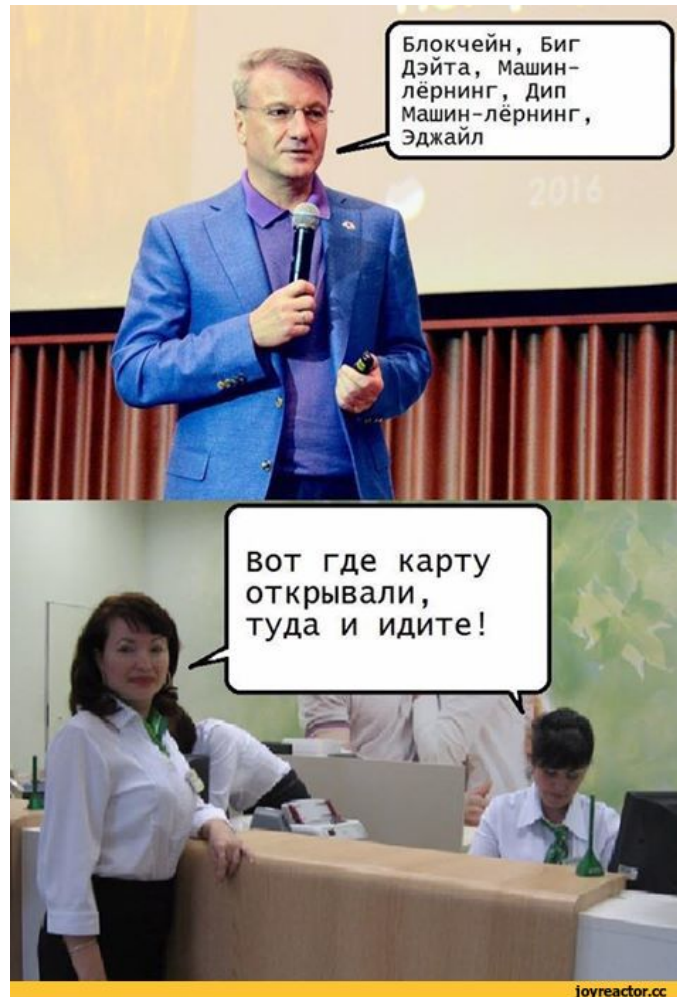
## Practice

- 1000 currencies
- Ad-hoc solutions
- Security issues

# Motivation

## Theory

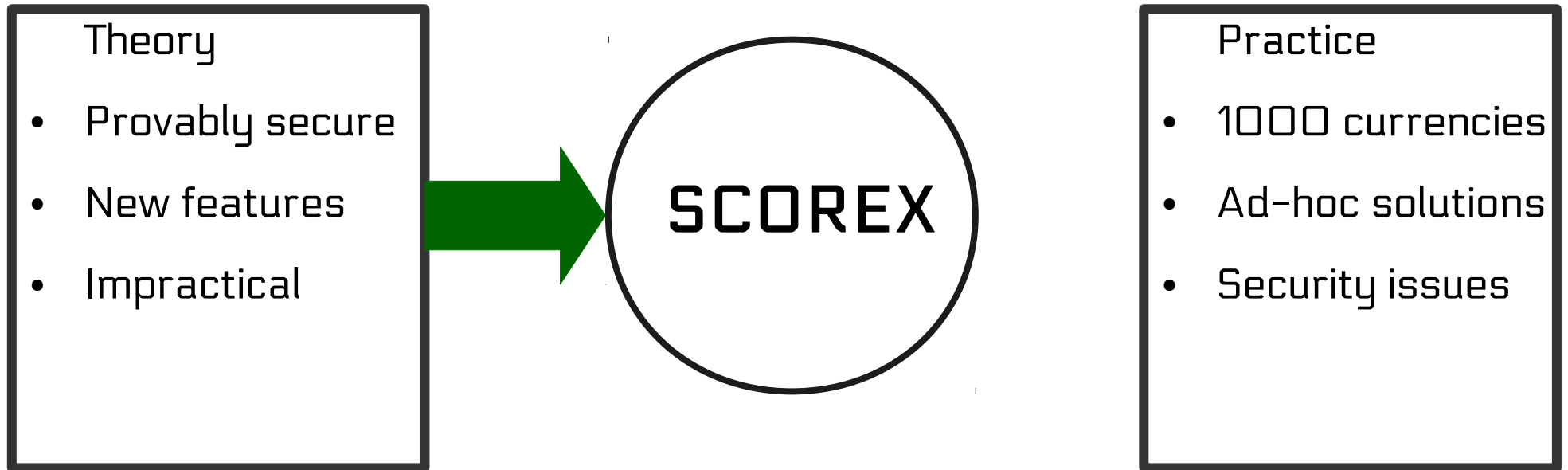
- Provably secure
- New features
- Impractical



## Practice

- 1000 currencies
- Ad-hoc solutions
- Security issues

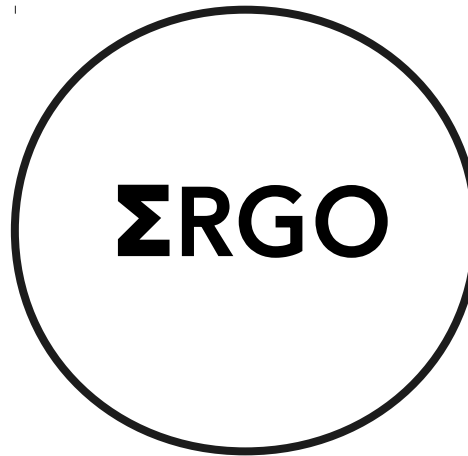
# Motivation: Scorex



# Motivation: $\Sigma$ rgo

## Theory

- Provably secure
- New features
- Impractical



## Practice

- 1000 currencies
- Ad-hoc solutions
- Security issues



# Σrgo idea

Design scalable, user-friendly  
decentralized cryptocurrency by combining  
ideas complementing each other

# Blockchain problems

# Throughput

- Bitcoin throughput: 2-3 tx/sec.
- Blocks are full
- Transaction fees are high
- Not applicable for mass adaptation

# Smart contracts

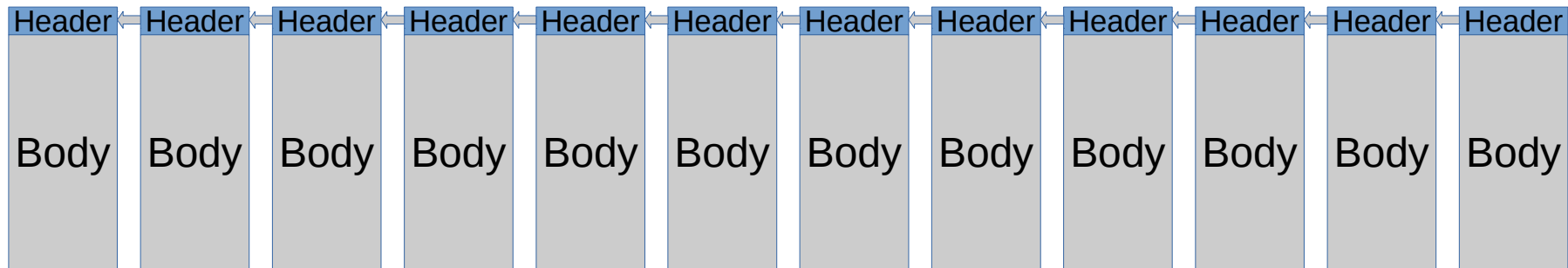
- Bitcoin script is limited
- Instructions are hard-coded

General-purpose smart contract languages:

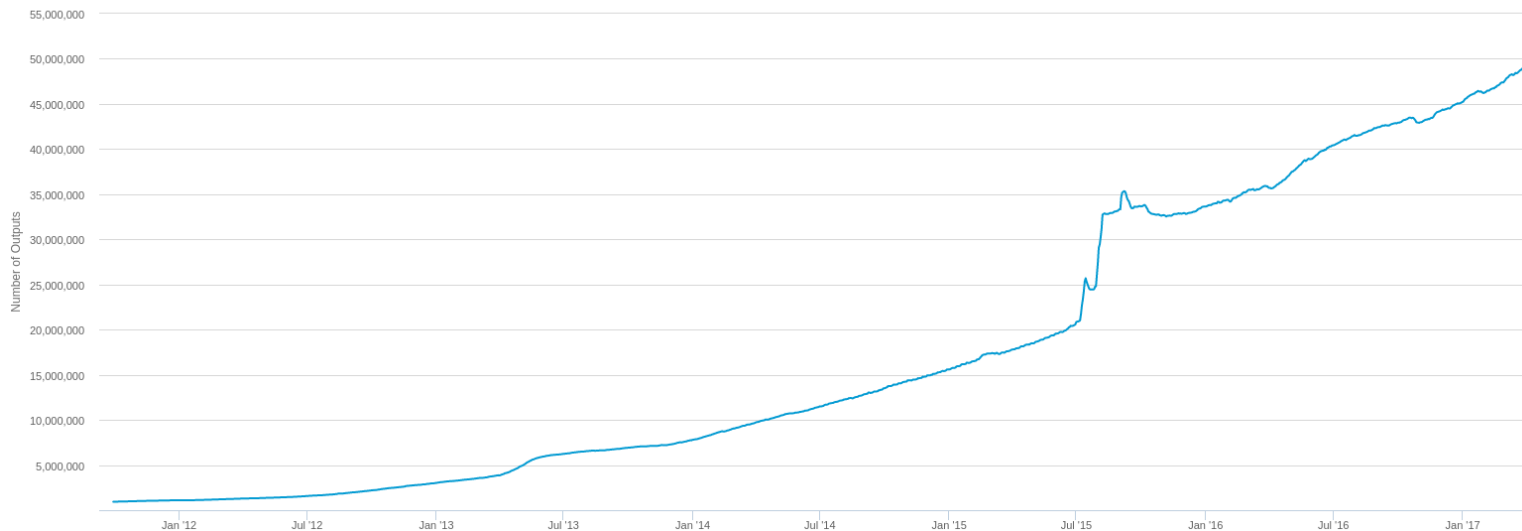
- Limited with total cost of all the operations
- Cost estimations are hard (DoS attacks)
- A lot of possibilities => a lot of vulnerabilities

# Blockchain and State

- Blockchain

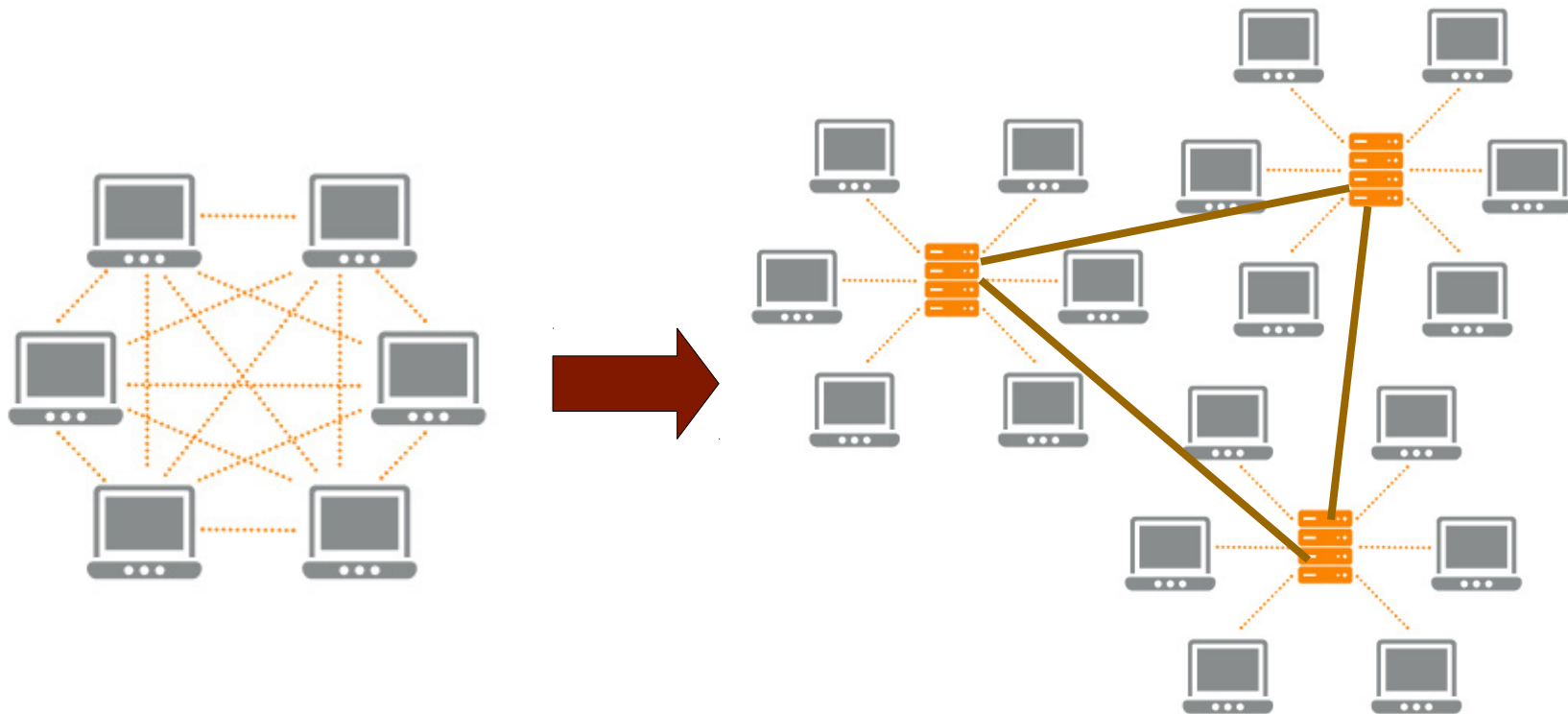


- State



# Blockchain and State

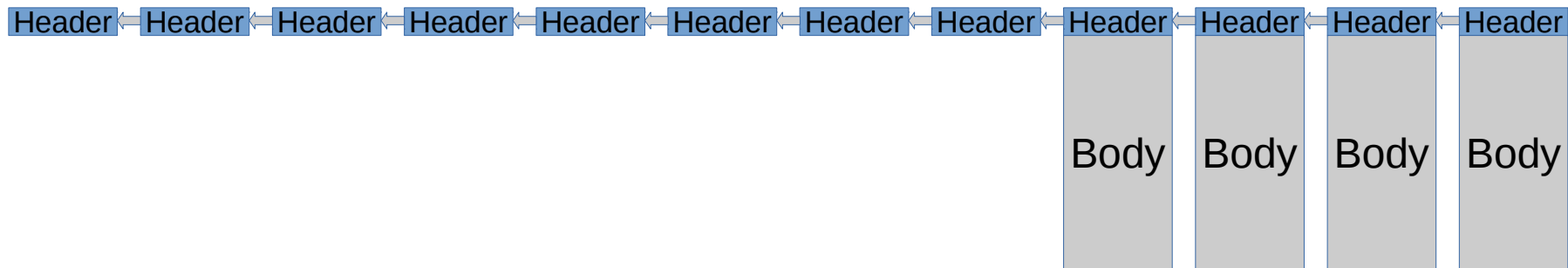
- Indefinitely growing Blockchain (100 Gb HDD)
  - Indefinitely growing State (1.6 Gb RAM)
- so
- Mining centralization or SPV mining
  - Services centralization



# Σrgo Solution

# Blockchain size: Rollerchain

## Rollerchain

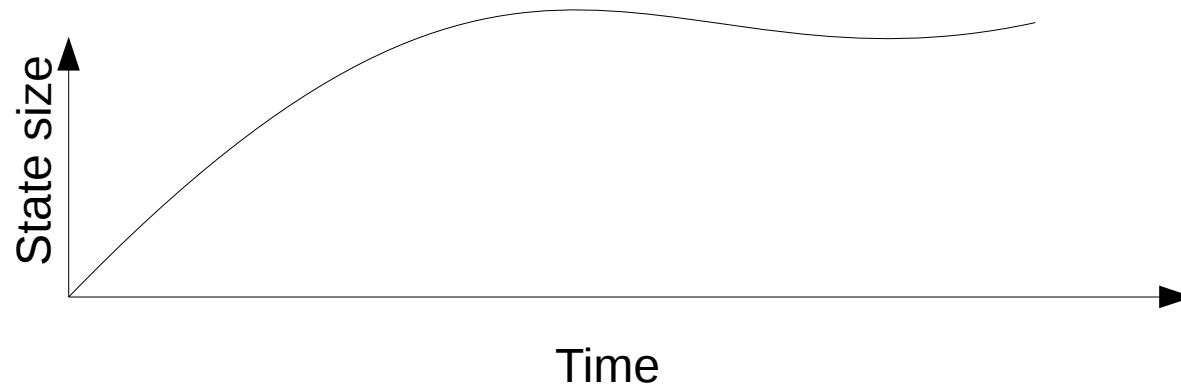


- Miners are enforce to keep fixed number of last blocks and headers (~40 Mb)
- Static storage requirements
- Fast bootstrap



# State size: Space-scarce economy

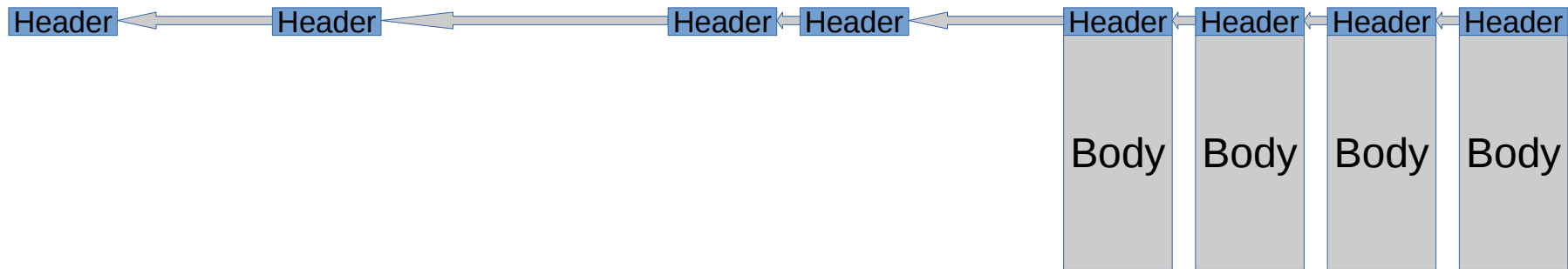
## Space-scarce economy state



- Controllable State size with upper-bound
- Incentive for active users
- Return lost coins to economy
- Predictable miner reward

# Header chain size: PoPoW

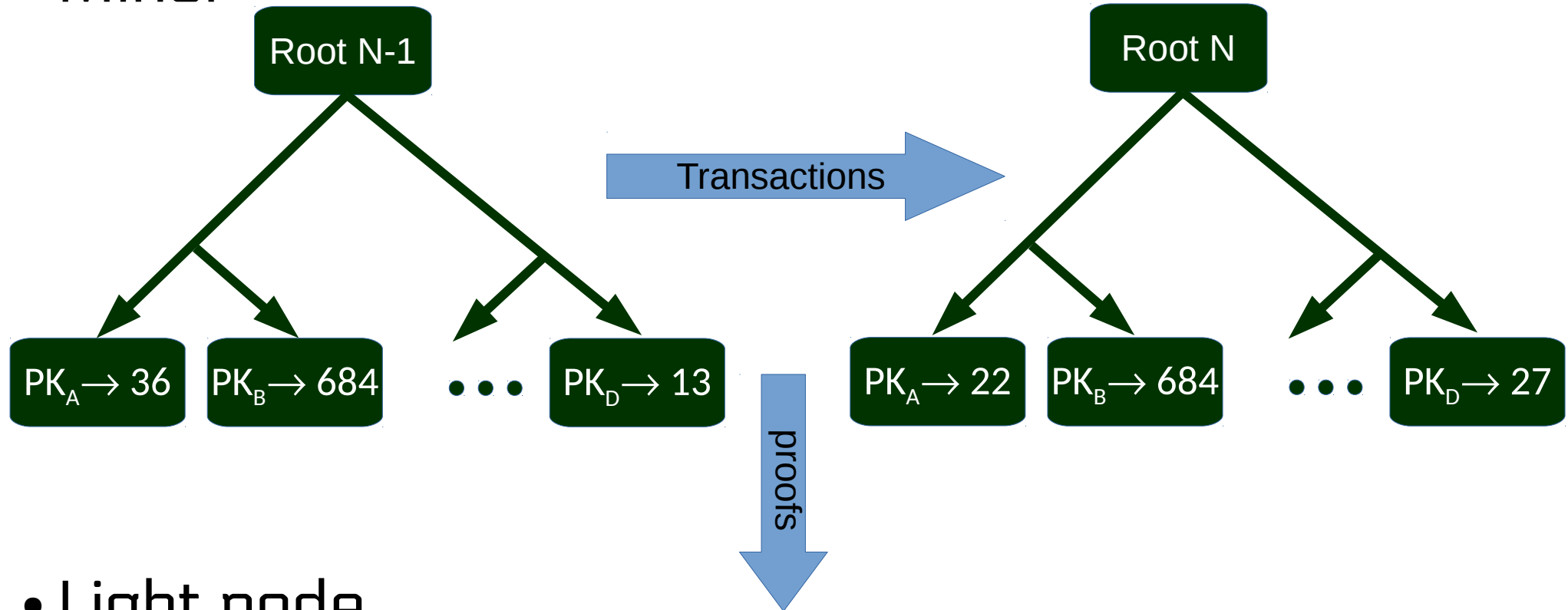
## PoPoW



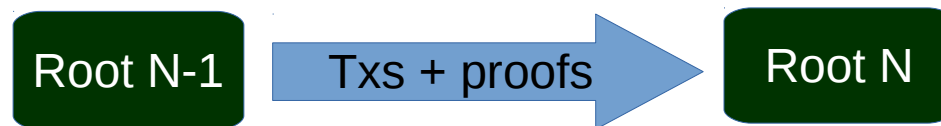
- Full nodes should keep only sublinear subset of headers (~20 Kb)
- Extremely fast bootstrap
- Cross-chain proofs (e.g. sidechains)

# Light node state size

- Miner



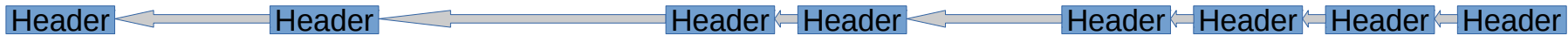
- Light node



Proofs verify balances and calculate new root hash

# Light node state size

- Light node blockchain: (~20 Kb)



- Light node state: 32 byte

Root N

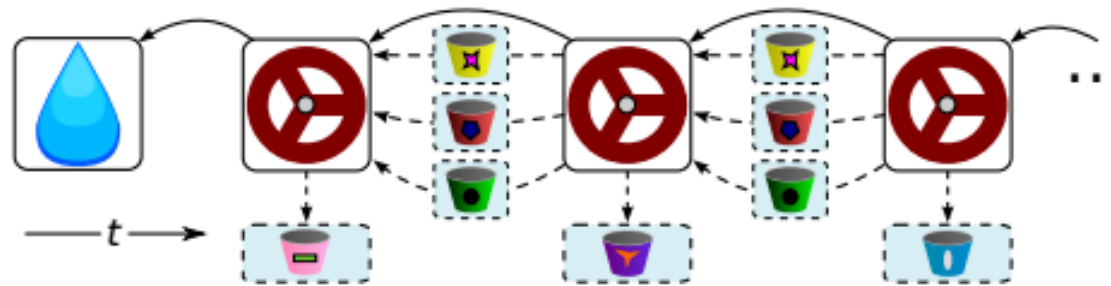
- Full node security guarantees with few Kb of data
- Decentralized user-friendly light wallet

# Smart contracts support

- Rich authenticated transaction language ( $\Sigma$ lang)
- Environment propositions + Crypto propositions
- For free: threshold signatures, ring signatures
- Ahead-of-time cost analysis
- Protocols-friendly blockchain

# $\Sigma$ rgo as database

- State as database
- Aspen blockchain structure



- Sidechains – data chain and money chain

# Throughput

- Bitcoin-ng for maximum on-chain throughput (100 tx/s)
- Off-chain protocols on top of flexible transactional language (10K tx/s)
- Multiple blockchains with sidechain token transfer between them for further research

---

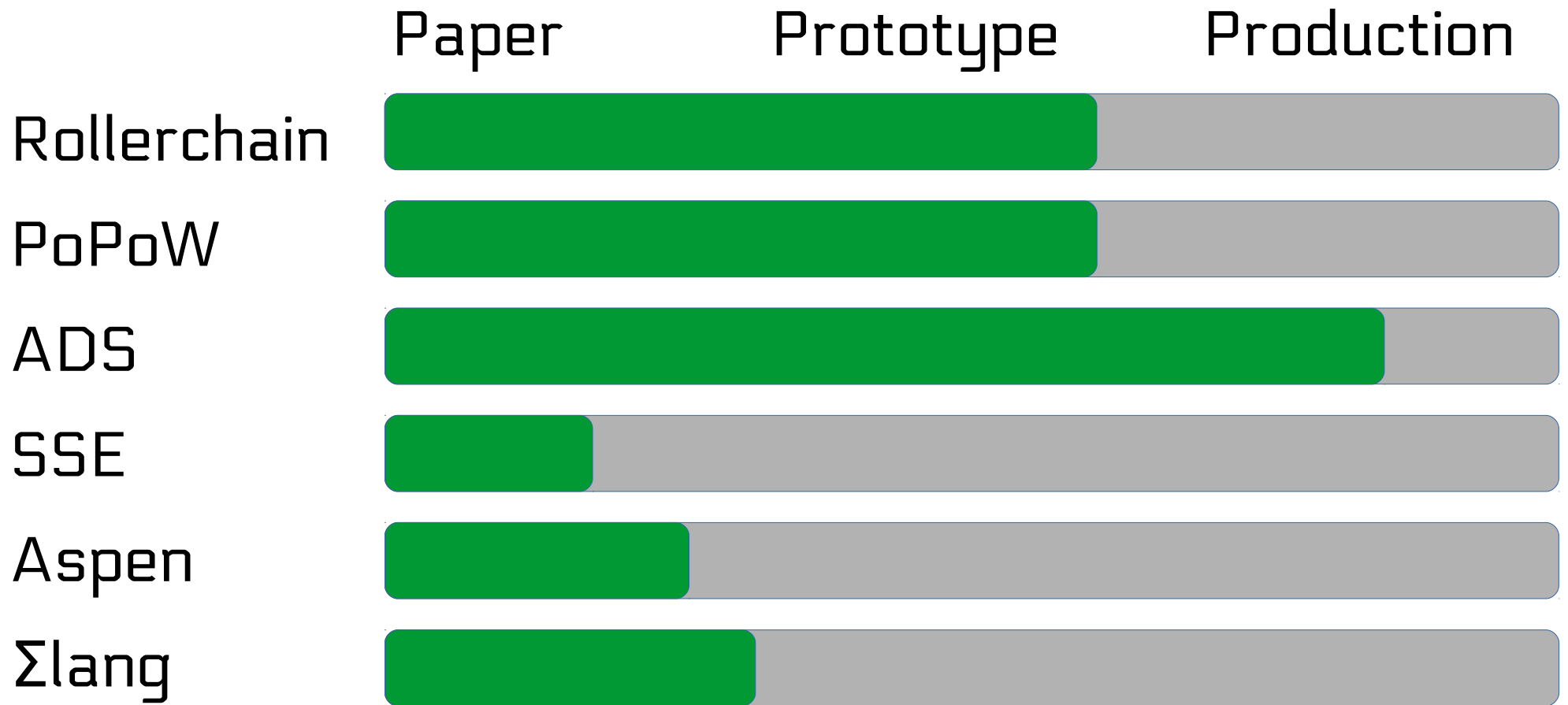
I. Eyal, et al. Bitcoin-ng: A scalable blockchain protocol

J. Poon, T. Dryja, The bitcoin lightning network: Scalable off-chain instant payments

A. Miller, et al. Sprites: Payment channels that go faster than lightning

A. Back, et al., Enabling blockchain innovations with pegged sidechains

# Status





# Conclusion

- Constant storage requirements
- Controllable state size
- Full-node security guarantees on smartphones
- Smart-contracts including cryptography
- Efficient blockchain as database
- High throughput
- Decentralized network

# Thank you!

Collaborations are welcomed!

- Site: <http://ergoplatform.org>
- Twitter: <https://twitter.com/ergoplatformorg>
- Email: [ergoplatform@protonmail.com](mailto:ergoplatform@protonmail.com)