ΣERGO
COMPREHENSIVE CRYPTOCURRENCY DESIGN

DMITRY MESHKOV
26 MAY 2017
GENESIS MOSCOW CONFERENCE
• Ergo idea
• Blockchain problems
• Ergo solution
Σ ergo idea
Motivation

Theory
- Provably secure
- New features
- Impractical

Practice
- 1000 currencies
- Ad-hoc solutions
- Security issues
Motivation: Scorex

Theory
- Provably secure
- New features
- Impractical

Practice
- 1000 currencies
- Ad-hoc solutions
- Security issues
Motivation: Σrgo

Theory
- Provably secure
- New features
- Impractical

Practice
- 1000 currencies
- Ad-hoc solutions
- Security issues
Design scalable, user-friendly decentralized cryptocurrency by combining ideas complementing each other
Blockchain problems
Throughput

- Bitcoin throughput: 2–3 tx/sec.
- Blocks are full
- UTX size: 200K tx
- 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**
Miners should validate transactions efficiently. They can:
1. Keep State in RAM => Mining centralization
2. Do not keep State => SPV mining
Problems for users:
- Can’t validate blocks on low-end hardware
- Long validation on commodity hardware

=>
- Users move to centralized services
Σ ergo Solution
Multi-mode Cryptocurrency

- Asymmetric design – miners how generate blocks and proofs for them
- Light nodes that check miner proofs
- No trust between miners and light nodes!
Blockchain size: Rollerchain

Rollerchain

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

Chepurnoy, A., et al. Rollerchain, a Blockchain With Safely Pruneable Full Blocks
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

D. Meshkov, A. Chepurnoy, On space-scarce economy in blockchain systems.
Light node state size

- Miner
  - Root N-1
  - $PK_A \rightarrow 36$
  - $PK_B \rightarrow 684$
  - $PK_D \rightarrow 13$
  - Root N
  - $PK_A \rightarrow 22$
  - $PK_B \rightarrow 684$
  - $PK_D \rightarrow 27$

- Light node
  - $Root_{N-1}$
  - $Txs + proofs$
  - $Root_N$

Proofs verify balances and calculate new root hash

Reyzin, L., Meshkov, D, Chepurnoy, A. & Ivanov A. Improving Authenticated Dynamic Dictionaries, with Applications to Cryptocurrencies
PoPoW

- Nodes should keep only sublinear subset of headers (~20 Kb)
- Extremely fast bootstrap
- Cross-chain proofs (e.g. sidechains)
Light node state size

- Light node blockchain: (~20 Kb)
- Light node state: 32 byte
- Full node security guarantees with few Kb of data
- Decentralized user-friendly light wallet
• State as database
• Aspen blockchain structure

• Sidechains – data chain and money chain

A. E. Gencer, R. van Renesse, E. G. Sirer, Service-oriented sharding with aspen
Smart contracts support

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

Chepurnoy A. Σ-State Authentication Language, an Alternative to Bitcoin Script
Throughput

- Bitcoin-ng for maximum on-chain throughput (1K tx/s)
- Off-chain protocols on top of flexible transactional language (1M tx/s)
- Multiple blockchains with sidechain token transfer between them for further research

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

- Rollerchain
- PoPoW
- ADS
- SSE
- Aspen
- Σlang
Bootstrap strategy

- Treasury system – 10% of mining reward is going to treasury
- First year treasury rewards – to bootstrapping team
- EFYF (Ergo First Year Futures) token was issued on Waves platform
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://ergopлатформ.org
- Twitter: https://twitter.com/ergopлатформорг
- Email: ergopлатформ@protonmail.com