WAVES

BLOCKCHAIN FOR THE PEOPLE

OPEN BLOCKCHAIN AND PRODUCTION READY SYSTEMS

THE CHALLENGES

ARE OPEN BLOCKCHAINS READY FOR REAL WORLD APPLICATIONS?

NO! Total market cap of open blockchains is 100 billion though...

- No strict immutability guarantees

Bitcoin backbone protocol https://eprint.iacr.org/2014/765.pdf Kiayias et al.

Transaction finality? Mining pools?

- Scalability issues. Blockchain is a fully-replicated database, all participants need to store the same data = > throughput limitations, blockchain bloat, state storage issues.

- Business logic on blockchain, smart contracts are inefficient due to scalability issues.

SECURITY OF PROOF OF STAKE CONSENSUS

Proof-of-stake algorithm uses system state to select the next miner => it’s not random, you can predict miners sequence.

Efficient randomization is needed.

https://eprint.iacr.org/2016/889.pdf

Provably secure schemes scale very badly.

SMART CONTRACTS

Current smart contracts schemes scale very poorly. Besides, Turing completeness leads to unexpected economical models.

Non turing complete zero-knowledge sigma state protocols - provably finite execution time, no new entities are introduced.

THROUGHPUT SCALABILITY

Bitcoin: 1-2 tx per second…

… You need thousands.

On-chain: Sharding, Bitcoin NG

Off-chain: Lightning networks, cryptographically secured payment channels, with eventual on-chain settlement.

MISCELLANEOUS

- Lite wallets. You need to verify transactions without storing the full database.

More efficient authenticated data structures are needed.

- Anonymization, zero knowledge based protocols.
- Eclipse attacks, efficient network protocols.
- Side chains, cross-blockchain protocols.

Quite diverse research areas, deep science that can be implemented in practice.

And total market cap is 100 billion!

JOIN US!

http://blockchaininstitute.io/
sasha@wavesplatform.com