The Promises and Pitfalls of Distributed Consensus Systems: From Contract Signing to Cryptocurrencies

Alexandra Dmitrienko
Institute of Information Security at ETH Zurich
alexandra.dmitrienko@inf.ethz.ch
Blockchain: The Hype or Reality?

• Bitcoin followed by a number of “altcoins”
  • Litecoin, Dogecoin, Zerocoin, Zerocash, CryptoNote, etc.

• Beyond financial transactions:
  • Instead of sending currency, send anything: contracts, smart property, digital content, anything (Ethereum)

• Many startups invest in Blockchain technology
  • $1 billion in venture capital funding until 2015
  • Predicted up to $10 billion in 2016
Why Is It So Successful?

- Is solving the problem of distributed consensus made Bitcoin work?

- Distributed consensus algorithms have been around for a long time

- What does a blockchain-based consensus promise beyond traditional Byzantine Agreement protocols?
Why Is It So Successful?

- Is it the Bitcoin incentive that makes the "blockchain" technology successful?

- Results in waste of energy
- Consumption equivalent to ca. 280,000 American households
- This is only for Bitcoin!

- If not incentivized, would Blockchain technology still work?
Blockchain’s Benefits

Trusted Third Party = Dislike
Blockchain’s Benefits

Banks = Dislike
Blockchain’s Benefits

Privacy = Like
Blockchain Problems and Challenges

- Scalability
- Throughput capacity
- Storage limits
- Integration with legacy systems
- Ever-increasing power consumption

• Can these problems be solved at all?
What about Security?

- Are the associated security and privacy problems well understood?
Security against Strong Adversaries?

Nation State Adversary (NSA)
Cryptocurrencies and Banks

- Why are banks interested in blockchain?
  - Invest, get involved, infiltrate cryptocurrencies
  - Private vs. public Blockchains

- What are the benefits of private blockchains?
- Can cryptocurrency co-exist with traditional banking?
- Can it facilitate the transactions within/between banks, e.g., cross-border payments?
Blockchains and Governments

- Voting
  - Can we do secure eVoting based on blockchains?
  - How does the future of electronic voting look like?
  - What are the eVoting advancements in real world deployment?

- First electronic voting in Estonia in 2005
  - Is Estonia a realistic model?
Summary of Questions

- What are the advantages the blockchain-based consensus vs. Byzantine agreement protocols?
- Can blockchains without incentives be as successful as Bitcoin?
- Are the related security and privacy problems well-understood?
- Will official authorities (banks, governments) accept blockchain-based solutions?
- What are the drawbacks and penalties of using blockchain-based consensus?
- Can associated challenges (e.g., scalability and throughput capacity limitations) be solved?