Challenges in Blockchain Research

Alexander Chepurnoy

IOHK Research

2017

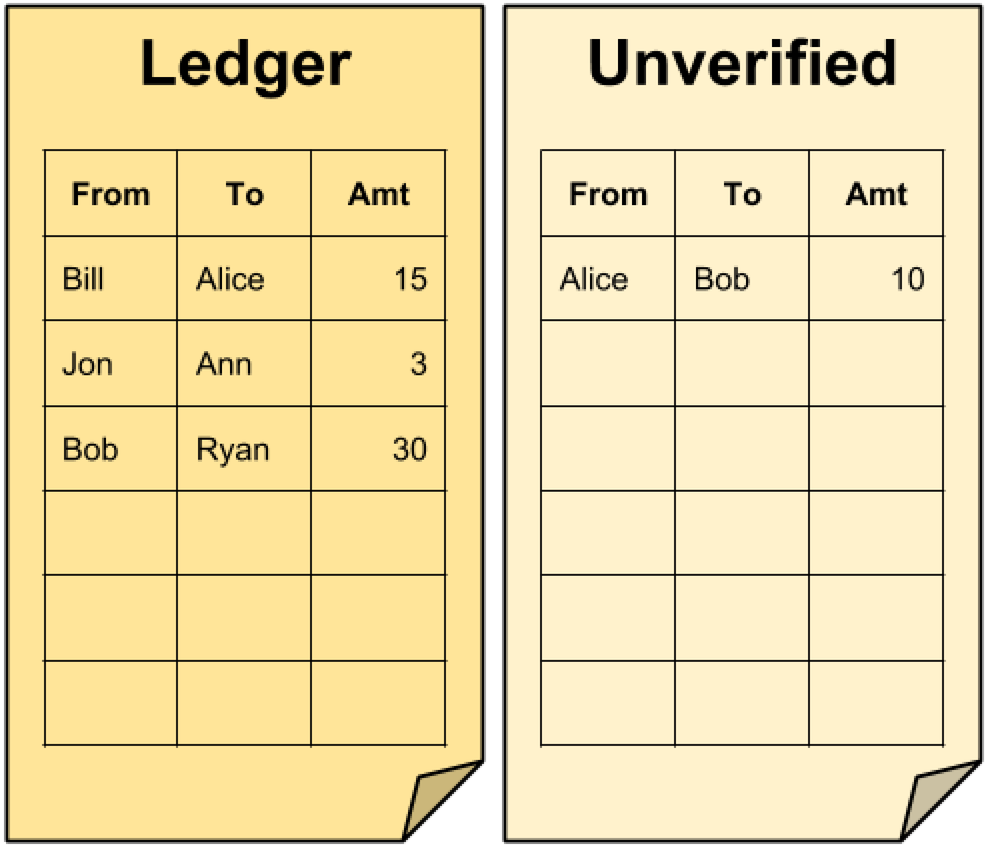
CTCRYPT

Part 0. Introduction

Bitcoin: History

- Whitepaper in late 2008
- No rigorous analysis
- Works in practice somehow
- “Forum research” 2009-now
- Academic research 2013-now

Bitcoin: Common Ledger



Ledger

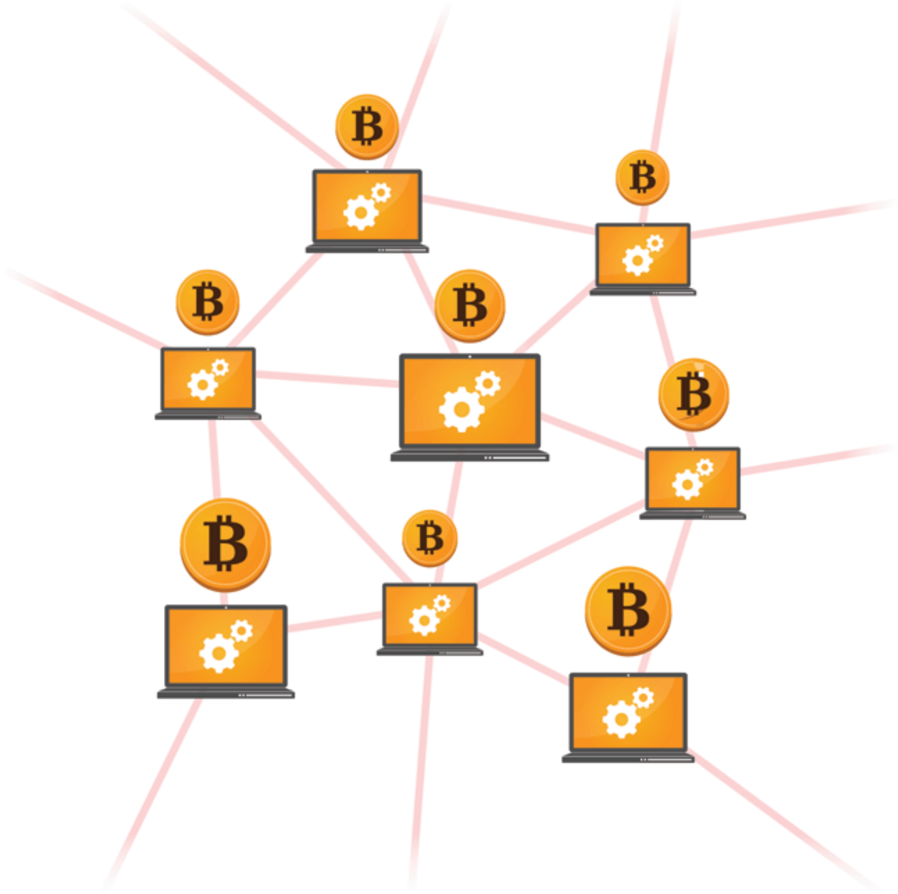
From	To	Amt
Bill	Alice	15
Jon	Ann	3
Bob	Ryan	30

Unverified

From	To	Amt
Alice	Bob	10

with no central bank!

Bitcoin: Network



Open P2P network of commodity machines

Bitcoin: Proof-of-Work

Block B = $\langle h_{i-1}, x_i, w_i \rangle$

$\mathrm{hash}(h_{i-1}, x_i, w_i) < T$

$x = \langle tx_1, tx_2, \ldots, tx_n \rangle$

$w \leftarrow \{0,1\}^k$

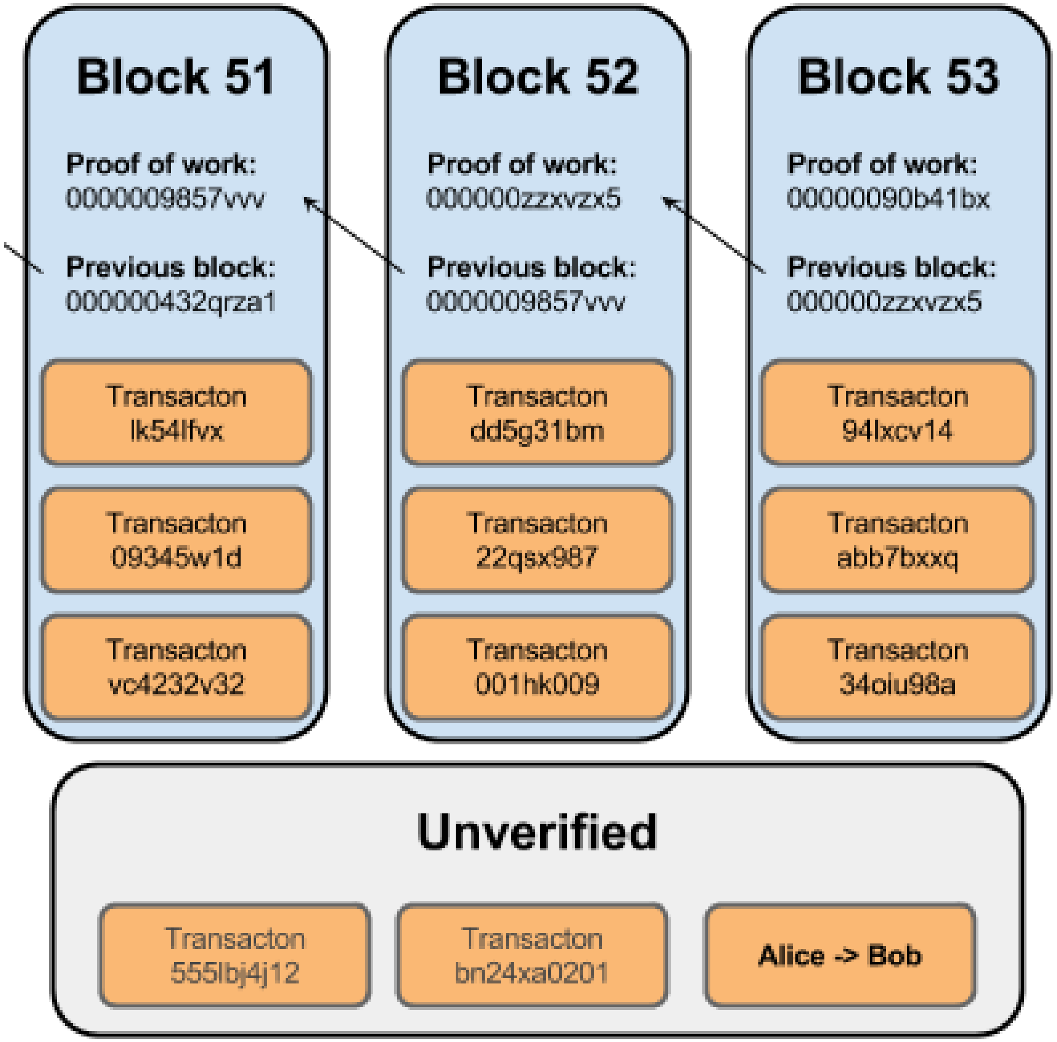
$h_{i-1} = \mathrm{hash}(h_{i-2}, x_{i-1}, w_{i-1})$

$h_0 = 0$

Probability of success per one query $p = T * 2^{-k}$

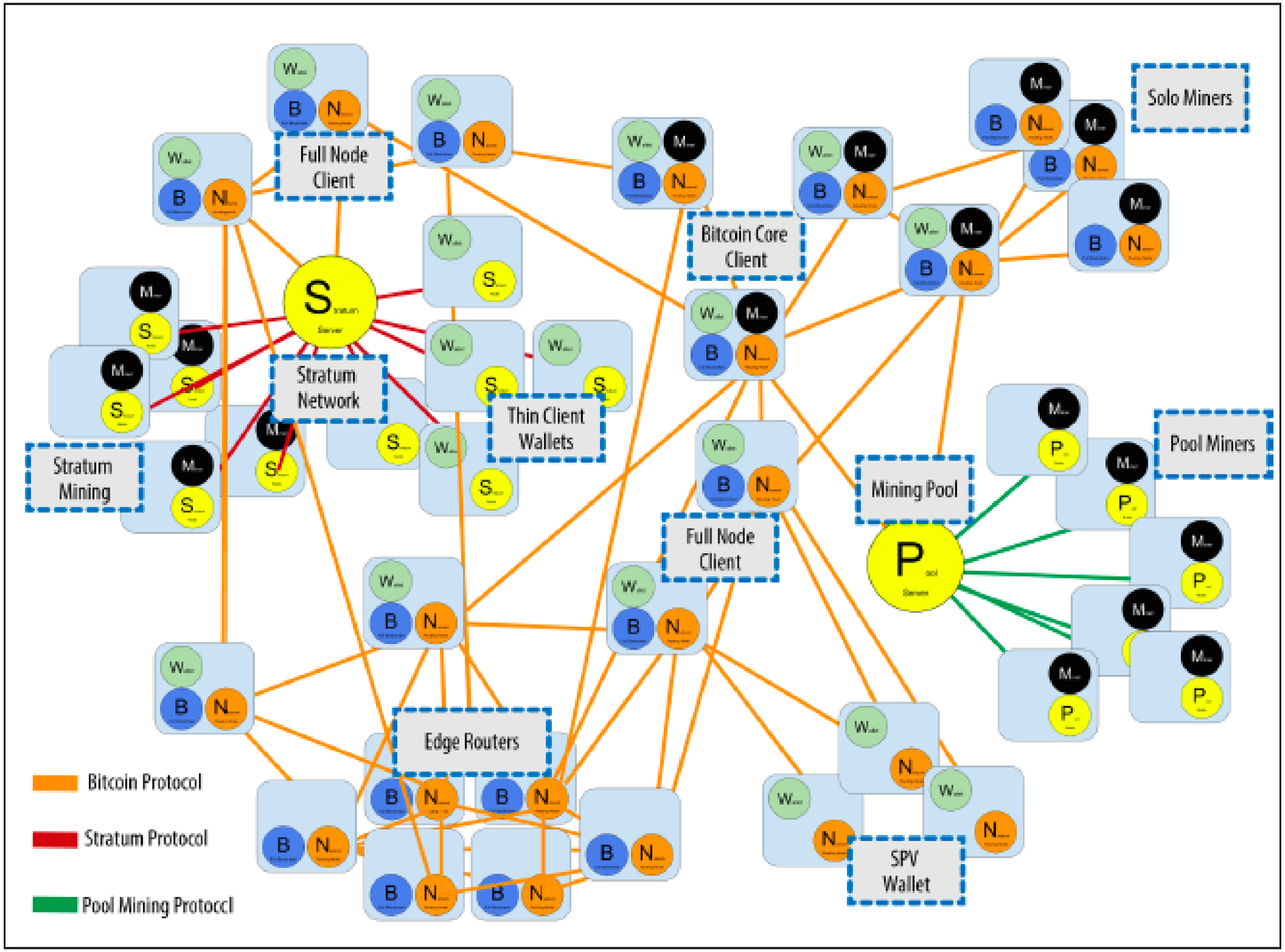
“One CPU – 1 vote”

Bitcoin: Blockchain



Fully replicated!

Real Bitcoin: Network



Real Bitcoin: Hash Fn is Not Ideal

“AsicBoost: A Speedup for Bitcoin Mining”

http://www.math.rwth-aachen.de/~Timo.Hanke/AsicBoostWhitepaperrev5.pdf

Patented!

Real Bitcoin: Mining Centralization

~~“One CPU One Vote”~~ - Failed

What Do We Know?

“No one knows how Proof-of-Work really works”

A. Kiayias, in a private conversation

Blockchain Research

- Research in Academia: careful, sound, but often not practical

- Informal (“forum”) research: reckless, usually flawed, practical, fast progress

Part I. Academic Works

Blockchain Papers

- enhancements proposals and protocols on top of a blockchain

- **find a model interesting from practical point of view, and get an interesting result**

- empirical studies and concrete security issues

Need a (PoW) Blockchain?

- “Do you need a Blockchain?”, Wüst et al. http://eprint.iacr.org/2017/375.pdf
- “The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication”, M. Vukolic http://vukolic.com/iNetSec_2015.pdf

Challenge: we need more studies!

A Proof-of-Work Blockchain

- “The Bitcoin Backbone Protocol: Analysis and Applications”, Garay et. al
  https://eprint.iacr.org/2014/765.pdf
  (the GKL model)

- “Analysis of the Blockchain Protocol in Asynchronous Networks.”, Pass et al.
  http://eprint.iacr.org/2016/454.pdf

Challenges

- We need more models: modular, closer to reality, perfectly sound
- GKL itself is being improving (last version is from March, 2017)
- “Multi-mode Cryptocurrency Systems” **C** et al. to be appeared on IACR eprint server soon

Proof-of-Work Based Hybrids

- “Bitcoin-NG: A Scalable Blockchain Protocol”, Eyal et. al https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf

- “Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing”, Kogias et al. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_kokoris-kogias.pdf

- “Secure High-Rate Transaction Processing in Bitcoin” Sompolinsky et al. (GHOST paper) http://www.cs.huji.ac.il/~avivz/pubs/15/btc_ghost_full.pdf

Challenges

- External validation is needed, a good example (regarding GHOST) “On Trees, Chains and Fast Transactions in the Blockchain” by Kiayias et al.

- Comparison of different proposals

Challenges

“A fundamental open problem in the area of blockchain protocols is whether the Bitcoin protocol is the optimal solution (in terms of efficiency, security) for building a secure transaction ledger”

From “On Trees, Chains and Fast Transactions…”

Proof-of-X (X is a Physical Resource)

- “Proofs of Space”, Dziembowski et. al http://eprint.iacr.org/2013/796.pdf
- “Permacoin: Repurposing Bitcoin Work for Data Preservation”, Miller et al. http://cs.umd.edu/~amiller/permacoin.pdf

Challenges

- More useful PoW-like schemes
- Do existing schemes any better or important in practice? (Permacoin is probably not)

Proof-of-Stake

- “Ouroboros: A provably secure proof-of-stake blockchain protocol”, Kiayias et. al https://eprint.iacr.org/2016/889
- “Snow White: Provably Secure Proofs of Stake”, Daian et al. http://eprint.iacr.org/2016/919

Challenges

- Attack vectors are still not well known
- “Provably secure” protocols are not efficient
- Security of efficient protocols is unknown

Rational Behavior?

“Bitcoin provides a rich playground in which to explore the effects of rational behavior”

Jonathan Katz

Rational Behavior?

- “Blockchain Mining Games” Kiayias et al. http://www.research.ed.ac.uk/portal/files/29075910/BlockchainMiningGames.pdf
- “Demystifying Incentives in the Consensus Computer” Luu et. Al http://www.comp.nus.edu.sg/~prateeks/papers/VeriEther.pdf
- “On the Instability of Bitcoin Without the Block Reward” Carlsten et al. http://www.cs.princeton.edu/~smattw/CKWN-CCS16.pdf

Challenges

- Literally nothing is known about how enhancement proposals do work in rational setting

- Not much known about Bitcoin of today even

- Why so few examples of non-default behavior observed?

- Will this continue to hold if Bitcoin becomes more mainstream?

Scalability and Efficiency

- “Improving Authenticated Dynamic Dictionaries, with Applications to Cryptocurrencies” Reyzin et al. https://eprint.iacr.org/2016/994

- “Proofs of Proofs of Work with Sublinear Complexity” Kiayias et al. http://fc16.ifca.ai/bitcoin/papers/KLS16.pdf

Challenges

- Just a very little work done, a very open field for research.

Empirical Studies / Security Issues

- “Eclipse Attacks on Bitcoin’s Peer-to-Peer Network” Heilman et al.

  https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf

- “Bitcoin Transaction Malleability and MtGox”

  https://arxiv.org/pdf/1403.6676.pdf

- “New kids on the block: an analysis of modern blockchains”

  https://arxiv.org/pdf/1606.06530.pdf

Challenges

- Bitcoin P2P layer still investigated poorly
- Outside Bitcoin, no much studies
- A very open field for research (e.g. Ethereum network studying, Ethereum Virtual Machine opcodes pricing)

Enhancement Proposals

- A lot of papers on anonymity, smart contract languages, escrow/gaming protocols, SMC on top of blockchain.

- “Zerocash: Decentralized anonymous payments from bitcoin” Ben-Sasson et al.

  http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6956581

Part 2. Informal Research

“UTXO commitments”

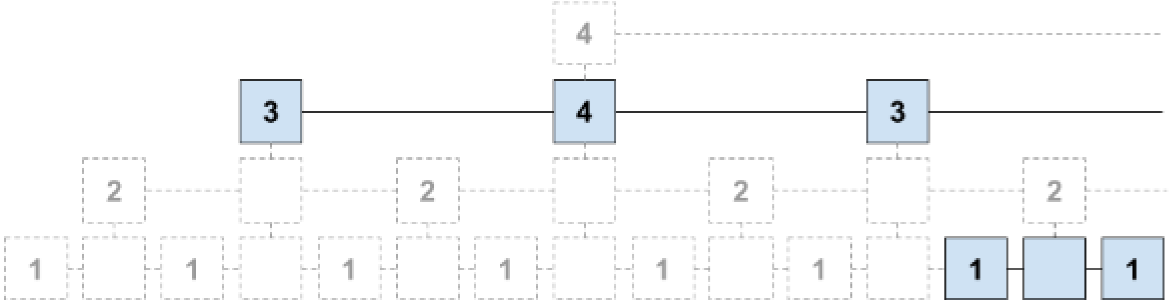
- Initial forum post: https://bitcointalk.org/index.php?topic=101734.msg1117428

- “A theory for lightweight cryptocurrency ledgers” by “Bill White”

- The ideas have been developed in “Improving Authenticated Dynamic Dictionaries, with Applications to Cryptocurrencies” (Reyzin et al.)

“High-Value Hash Highway”

- Initial forum post: https://bitcointalk.org/index.php?topic=98986.0



- The idea has been developed in “Proofs of Proofs of Work with Sublinear Complexity” (Kiayias et al.)

Informal Research

- A lot of proposals
- Most are hardly understandable
- Most of them are flawed
- Many implemented
- Some of them are valuable

Monero

- Ad-Hoc Anonymization Scheme

- “An Empirical Analysis of Linkability in the Monero Blockchain” www.monerolink.com/monerolink.pdf

Security Research

- “A Bitcoin transaction that takes 5 hours to verify”

  https://bitslog.wordpress.com/2017/01/08/a-bitcoin-transaction-that-takes-5-hours-to-verify/

- “Ethereum Network Attacker’s IP Address Is Traceable”

  https://www.bokconsulting.com.au/blog/ethereum-network-attackers-ip-address-is-traceable/

Part 3. Conclusion

- The industry is open to both academia and informal research and rushing

- Convergence between academia, enthusiasts and the industry is much needed

- A lot of research to be done

Questions?