BLOCKBENCH: A Framework for Analyzing Private Blockchains

Anh Dinh, Ji Wang, Gang Chen, Rui Liu, Beng Chin Ooi,

Outline

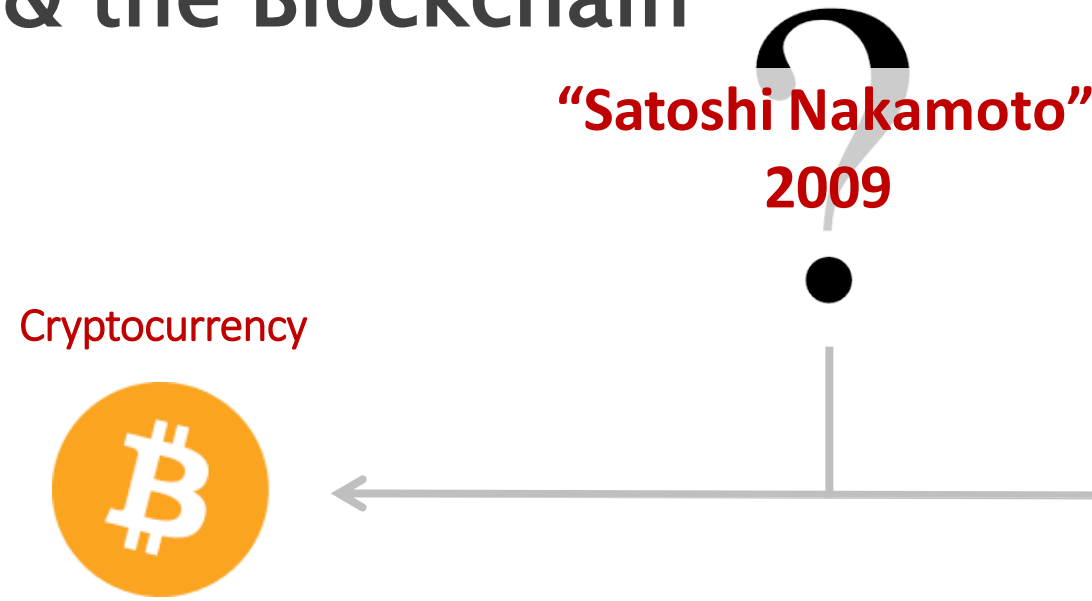
- Introduction
  - Backgrounds
  - Problem Statement
  - Related Works
- BlockBench Framework
  - System Design
  - Implementation
- Performance Benchmark
  - Macro Benchmarks
  - Micro Benchmarks
- Discussion
- Conclusion

Outline

- Introduction
  - Backgrounds
  - Problem Statement
  - Related Works
- BlockBench Framework
  - System Design
  - Implementation
- Performance Benchmark
  - Macro Benchmarks
  - Micro Benchmarks
- Discussion
- Conclusion

Backgrounds

Bitcoin & the Blockchain



Cryptocurrency

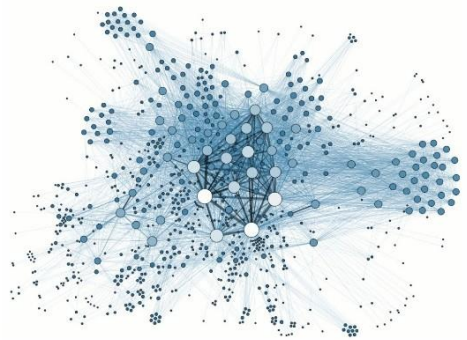
- No central bank
- Transferring coins through trustless P2P network
- ~1200 USD per Bitcoin (coinbase.com 10/03/2017)

Technology

- Blockchain
- Distributed shared ledger
- Cryptograhy (SHA-256, PKI)
- Consensus model
- Smart contracts

4 Key Concepts of Blockchain

Distributed shared ledger



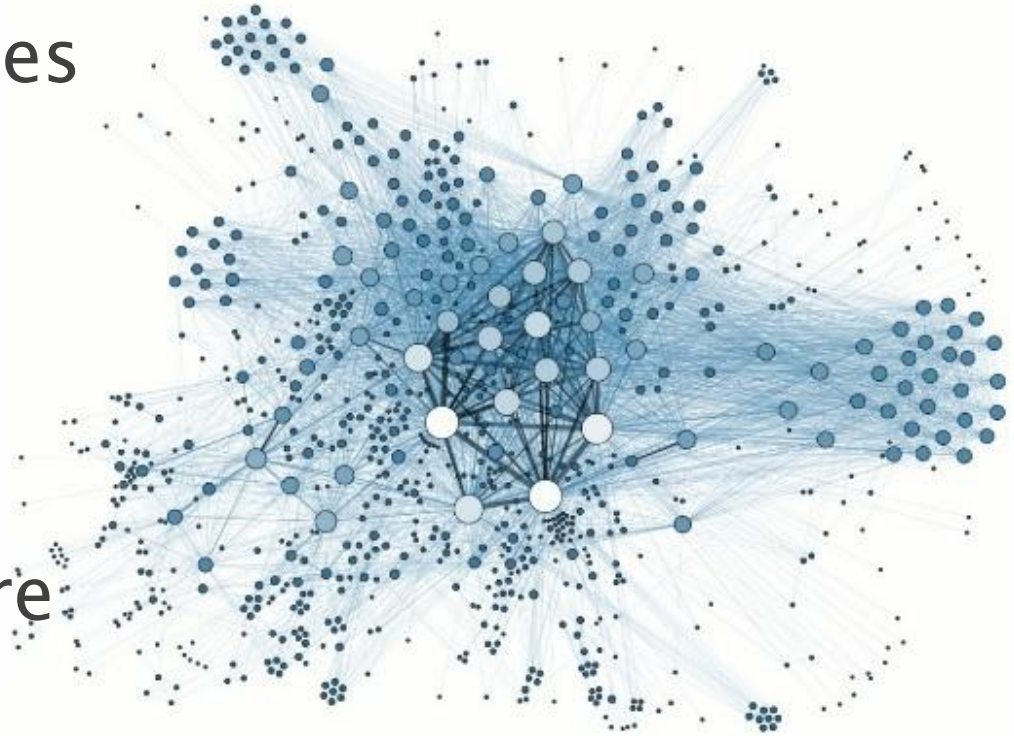
Cryptography

Consensus

Smart contracts

4 Key Concepts of Blockchain: Distributed Shared Ledger

- Group of replicated logs/databases (nodes)
- Transactions packed in blocks
- All nodes hold all transactions
- Parties identified with public key (= anonymised)
- Resilient for failure of one or more nodes



4 Key Concepts of Blockchain: 1.Distributed Shared Ledger

BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Jun 14 2015 14:01:53 GMT+0200.

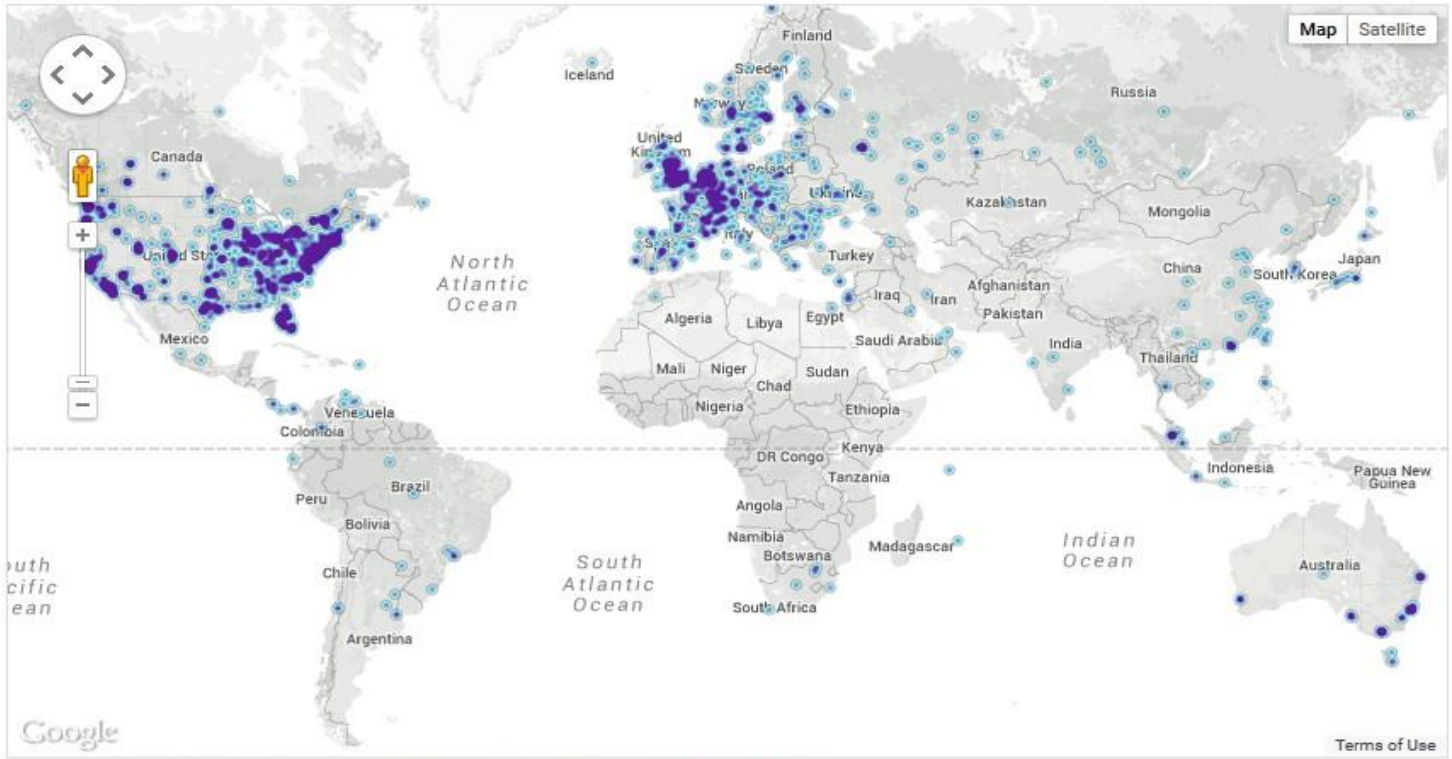
5987 nodes

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2161 (36.09%)
2	Germany	626 (10.46%)
3	France	442 (7.38%)
4	United Kingdom	375 (6.26%)
5	Netherlands	307 (5.13%)
6	Canada	302 (5.04%)
7	Russian Federation	187 (3.12%)
8	Australia	136 (2.27%)
9	Sweden	116 (1.94%)
10	China	102 (1.70%)

More (85) »



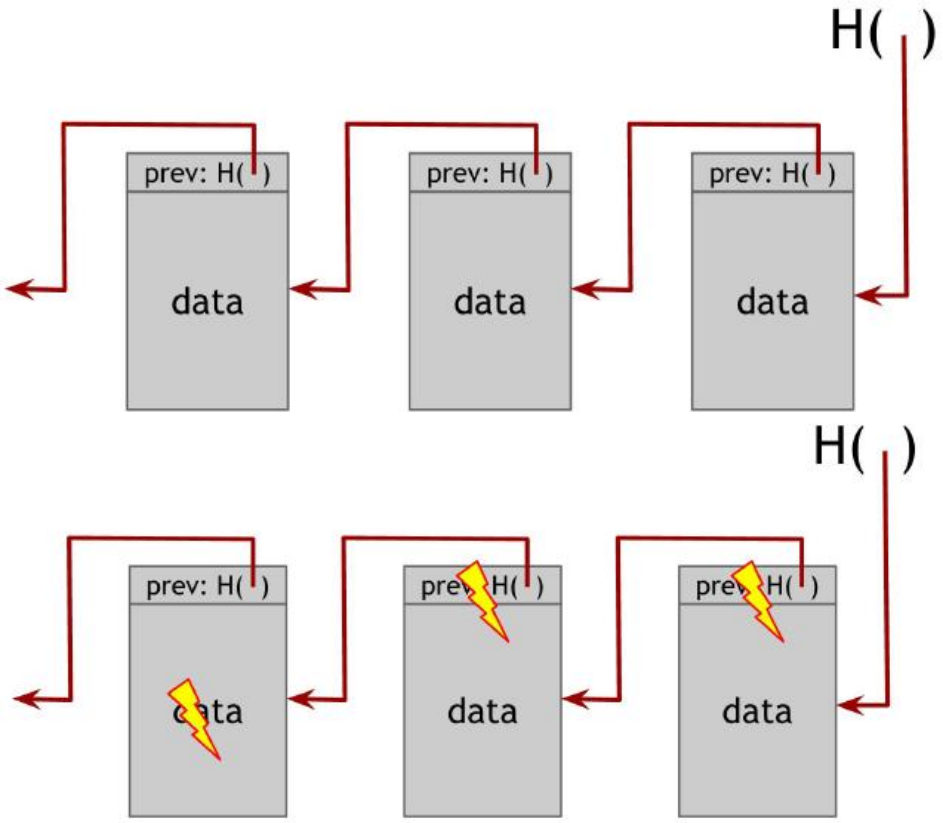
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

JOIN THE NETWORK

Be part of the Bitcoin network by running a full Bitcoin node, e.g. Bitcoin Core.

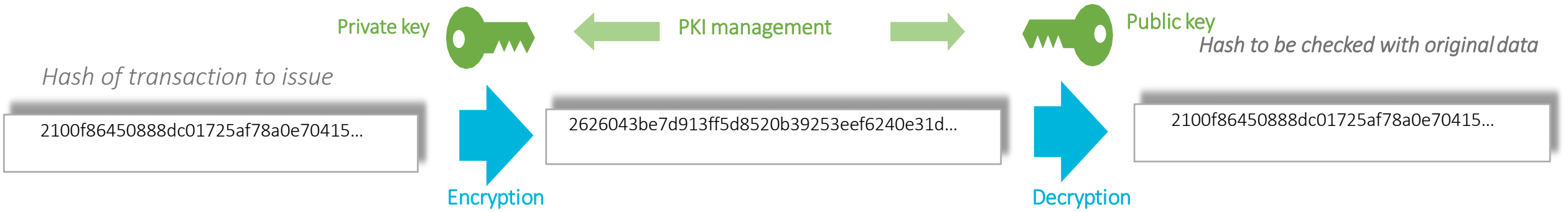
4 Key Concepts of Blockchain: 2.Cryptographic (1/2)

Tamper-proof log blocks using hash pointer



4 Key Concepts of Blockchain: 2.Cryptographic (2/2)

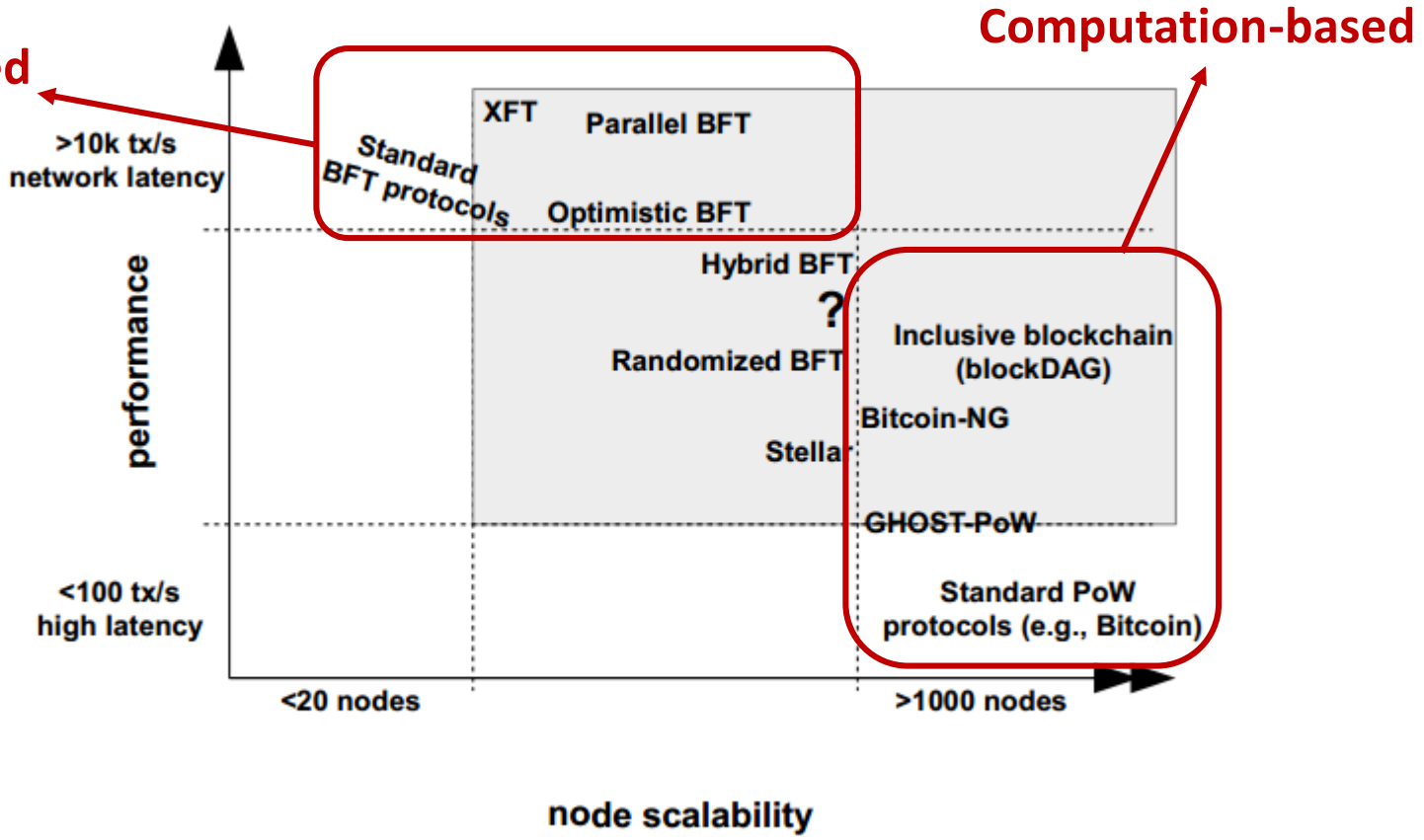
Asymmetric cryptography digital signature system



4 Key Concepts of Blockchain: 3.Consensus

Consensus

- No single point failure
- Byzantine fault tolerance

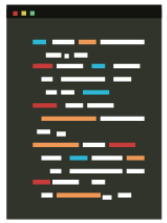


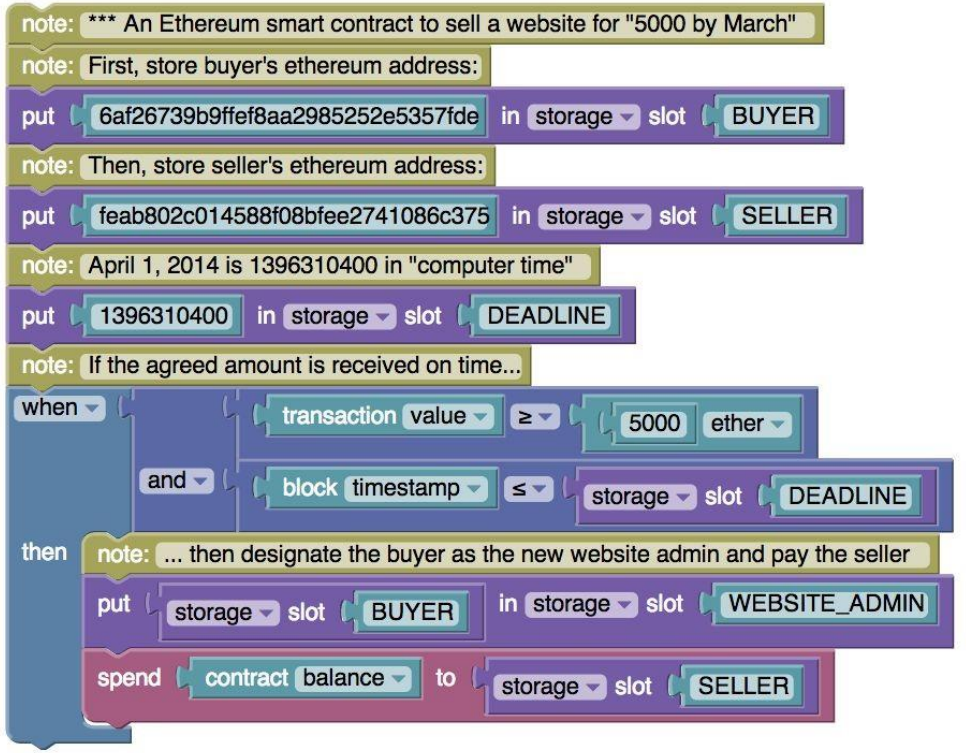
Cite: Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication."

4 Key Concepts of Blockchain: 4.Smart-Contract

Smart contracts

- Business logic that can be assigned to a transaction on the blockchain
- Acts as a 'notary' of blockchain transactions
- Holds conditions under which specific actions can/must be performed
- Facilitates escrow services
- Can't be modified without predefined permissions





Category of blockchains

Public blockchain V.S. Private blockchain

- The majority of financial services firms exploring the use of blockchain are looking at private or semi-private blockchains, rather than the fully decentralized public blockchains

Public blockchains

- No authoritative permission required in order to participate
- Participants are not vetted
- Mechanisms for maintaining the network against attacks and unwanted parties therefore add cost and complexity to the network
- Usually use computation-based consensus protocols

Private blockchains

- Participants are known and identified.
- Legal contracts can help with system mechanisms.
- Usually use voting-based consensus protocols