How to trust without any trust?

Abhinav Aggarwal

University of New Mexico
Cornell University
www.abhiag6891.com

October 2017

IBM Research

5 Kinds of Perspectives!

(1)

Users

(2)

[Bitcoin, Ethereum, LiteCoin etc..]

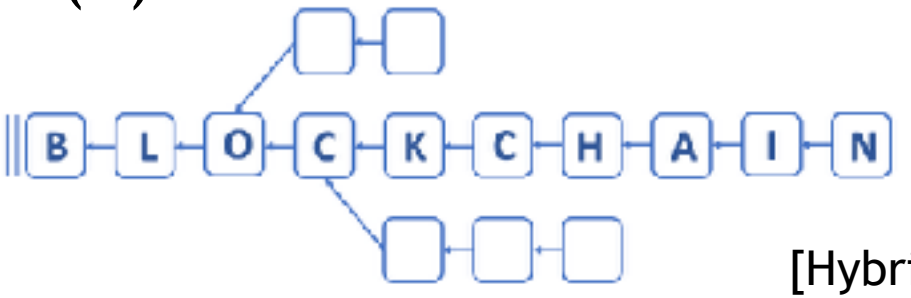
Cryptocurrency designers

(3)

[Fruitchains, Algorand, ZCash etc..]

Technology underlying digital currencies

(5)

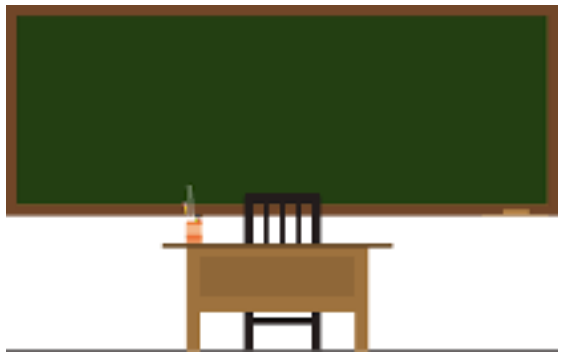


State Machine Replication

[Hybrid Consensus, Analysis of Blockchain, PBFT etc..]

(4)

[Private Data, Distributed Computation etc..]



Distributed Blackboard

Some Important Points to Keep in Mind

- Classical consensus needs someone to initiate the protocol
  - Leader
  - Committee
- Required properties
  - Security
  - Fairness - Generally depends on an incentive
  - Efficiency
- Depends on threat model
  - Static Adversary
  - Adaptive Adversary
    - Different ways of adaptive corruption: Responsiveness, Stickiness, Access controlled

The *permissionless* world!

Classical *Permissioned* world

The number of participants in the system, as well as their identities, are common knowledge, and communication among the participants take place over authenticated channels.

Permissionless-ness

Anyone can join (or leave) the protocol execution (without getting permission from a centralized or distributed authority), and authentication mechanisms are not available. Additionally, participants may join and leave the system at will.

Pass, Rafael, and Elaine Shi. "Rethinking Large-Scale Consensus." *Computer Security Foundations Symposium (CSF), 2017 IEEE 30th*. IEEE, 2017.

What are blockchains?

- *Linearized Ordered Log* abstraction
  - Also referred to as “State Machine Replication”
  - Participants maintain a growing ordered log of transactions and any participant can add transactions to the end of the log.
  - **Consistency**: at any point in the execution, all honest participants have consistent logs—that is, either their logs are identical, or one participant’s log is a prefix of the other’s.
  - **Liveness**: any honest protocol participant can propose to add a transaction; this transaction is then guaranteed to get incorporated into their logs within some fixed (small) amount of time; additionally, whenever a participant sees some transaction in their log, the same transaction will appear in every other participant’s log within some fixed (small) amount of time.

Pass, Rafael, and Elaine Shi. "Rethinking Large-Scale Consensus." *Computer Security Foundations Symposium (CSF), 2017 IEEE 30th*. IEEE, 2017.

Can inefficiencies in *classical Nakamoto consensus* be overcome?

- No authentication => Proof of work cannot be avoided!
  - Modeled as moderately hard functions
- Proof of work must be performed infinitely often in the presence of (late) spawning
- Honesty majority must always be ensured
- Upper bound on network delay must be known

Pass, Rafael, and Elaine Shi. "Rethinking Large-Scale Consensus." *Computer Security Foundations Symposium (CSF), 2017 IEEE 30th*. IEEE, 2017.

Is *Nakomoto* blockchain fair?

- Celebrated selfish mining attack.
  - A *network rushing* adversary can *steal* honest nodes' reward.
- How worse is the situation?
  - Adversary controlling just less than majority => can claim almost all the rewards
- How can fairness be defined?
  - D-coalition safe E-Nash Equilibrium (Fruitchains)

Pass, Rafael, and Elaine Shi. "Rethinking Large-Scale Consensus." *Computer Security Foundations Symposium (CSF), 2017 IEEE 30th*. IEEE, 2017.

Some Interesting Research Questions

Is it possible to establish a sybil-resistant public-key infrastructure in a peer-to-peer setting?

Existing Work :

1. James Aspnes, Collin Jackson, and Arvind Krishnamurthy. *Exposing computationally-challenged byzantine impostors*. Department of Computer Science, Yale University, New Haven, CT, Tech. Rep, 2005 - Incorrect solution
2. Marcin Andrychowicz and Stefan Dziembowski. *Pow-based distributed cryptography with no trusted setup*. In Annual Cryptology Conference, pages 379 - Excessively complicated solution with high message and bit complexity

Challenges :

1. How to prevent the adversary from creating many fake (pk,sk) pairs?
2. How to make all the nodes agree on a list of at most n (pk,sk) pairs (at most one for each node)?
3. How to deal with people joining and leaving the system dynamically?
4. Can it be done efficiently?

Overview of our Approach

- Consensus on the set of IDs
- Admission Control through PoW
- Go from almost everywhere consensus to everywhere consensus
- Avoid multiple rounds of PoW by one-time random leader election
  - Random bucketing: *The round for which I am the leader is decided based on my PoW*

Is it possible to achieve consensus in a model where nodes can become offline for arbitrary long periods of time, without assuming any shared randomness or PKI?

Existing Work :

1. Pass, Rafael, and Elaine Shi. *The sleepy model of consensus*. Cryptology ePrint Archive, Report 2016/918, 2016. http://eprint. iacr. org/2016/918, 2016.
2. Pass, Rafael, and Elaine Shi. "Rethinking Large-Scale Consensus." *Computer Security Foundations Symposium (CSF), 2017 IEEE 30th*. IEEE, 2017.

Challenges :

1. How is this model different from asynchrony? Is it strictly weaker or is it incomparable?
2. How to communicate with nodes that may become offline at an unpredictable time? What happens when they come online again?
3. If all communication is public and only diffused, is it possible to do secret sharing?
4. Is there an impossibility result lurking here w.r.t. secure coin flipping?

Overview of our Approach

- Estimate fraction of bad nodes based on how many people are online
  - Need O(log n) rounds before estimate is close to the actual value
- Secret Sharing random bits using threshold signatures
  - Only works if we assume private channels
- Perform consensus on the shares
- Reveal shares
- Can we do without private channels?

Is it possible to design a blockchain-based cryptocurrency that is fair (avoids selfish mining) to its participants and works in a truly permissionless setting?

Existing Work :

1. Pass, Rafael, Lior Seeman, and Abhi Shelat. "*Analysis of the blockchain protocol in asynchronous networks*." *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Cham, 2017.
2. Pass, Rafael, and Elaine Shi. "*Fruitchains: A fair blockchain*." Proceedings of the ACM Symposium on Principles of Distributed Computing. ACM, 2017.
3. Garay, Juan A., Aggelos Kiayias, and Nikos Leonardos. "*The Bitcoin Backbone Protocol: Analysis and Applications*." *EUROCRYPT (2)*. 2015.

Challenges :

1. How does the existing analysis for Nakamoto consensus change if nodes can leave or join arbitrarily?
2. Does the Nash equilibrium of fruitchains still hold under this dynamic setting?

Thank you for your attention ☺️

Questions?