Investigation on Byzantine Agreement Consensus

Yu Liu, Master of Analytics, School of Software
Supervisors: Ling Chen, Wei Bian

INTRODUCTION

Blockchain serves as a public ledger that records transactions in a chain of blocks. Bitcoin has definitely raised massive concerns and interests in past few years. However, chain fork has been raising concerns regarding with its negative impacts:

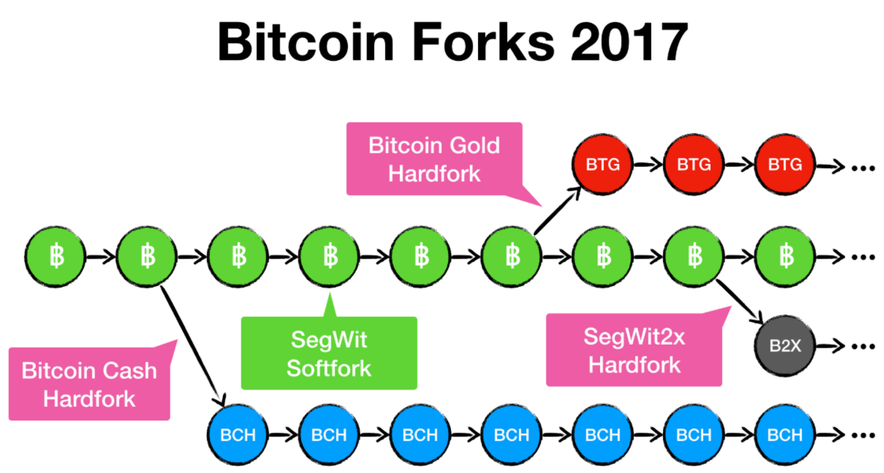
1. Security threats
2. Unpractical transaction pending time
3. Computational Waste

AIM

Investigating on Algorand Byzantine Agreement Protocol:

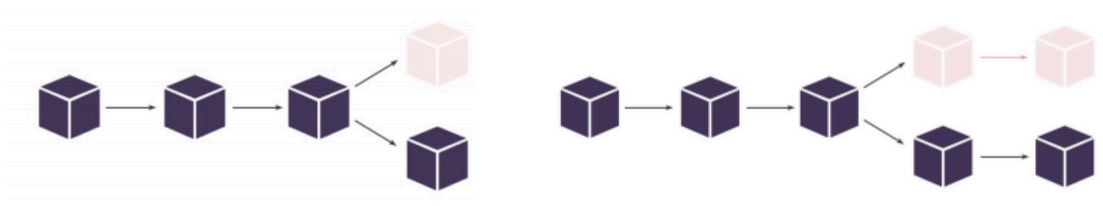
1. Fork Elimination
2. Efficiency and Scalability
3. Security

PROBLEMS OF FORKS



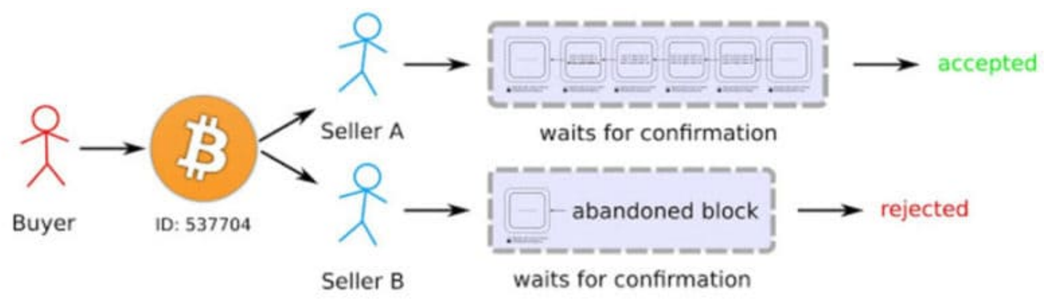
The primitive purpose was to allow developers to upgrade and maintain protocols, overwrite errors or bugs within few latest blocks.There are some other common situations when forks may take place:

1. Network poorly synchronized
2. Two miners solve the puzzle simultaneously or in a short time
3. Intentional adversary attacks



Forks could possibly cause the following problems:

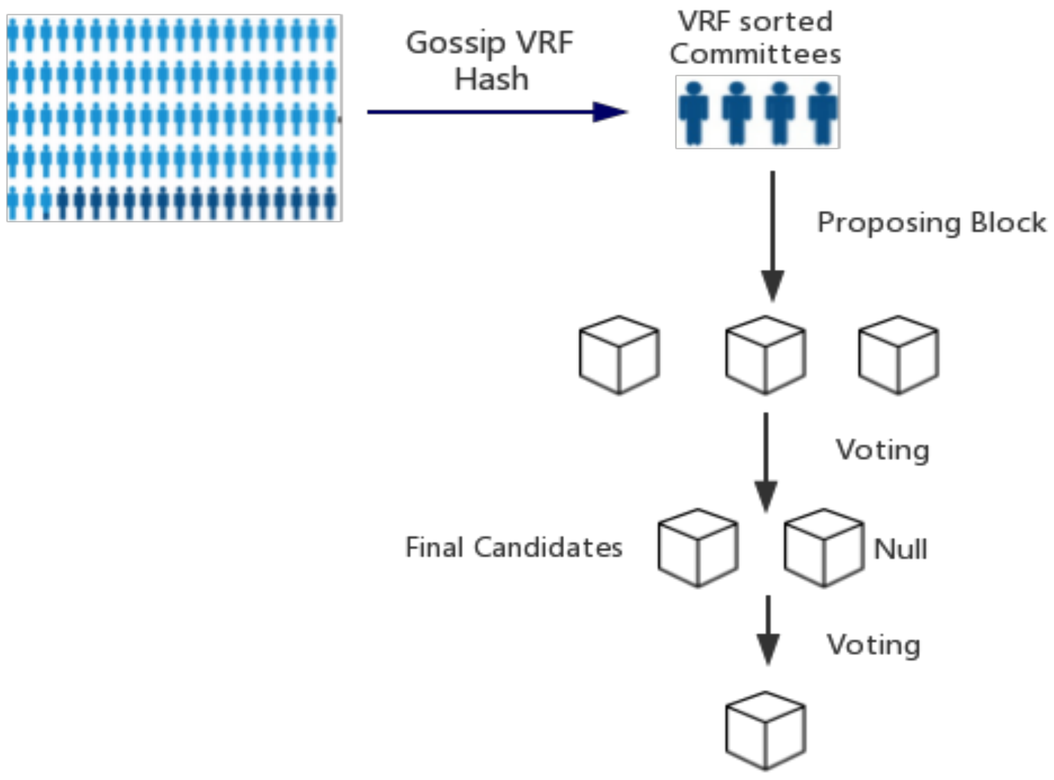
1. Temporal diverged version of ledger
2. Adversary could perform double spending attack
3. Transaction's pending time is unpractical for a day-to-day payment



BYZANTINE AGREEMENT CONSENSUS

Algorand proposed a voting based Byzantine Agreement Consensus algorithm to perform efficient and scalable blockchain system that is able to eliminate the fork. Consensus consists of the following features:

- Cryptographic Sortition
  - Verifiable Random Function
    - Hash of Private Key can be verified using Public Key
  - User perform Sortition privately and Gossip the result
  - Probability proportional to User's total tokens
- Byzantine Agreement Protocol
  - Committees vote for hash of a candidate block
  - Only candidate with at least 2/3 of votes will be valid
  - Null block will take place if votes are not enough or network timed out



Pros	Cons
Minimal Computation	No incentives
Fork elimination	Probability weighted by Tokens
Efficient and Scalable	Forward Security
Privately participating	Cost of joins

FURTURE WORK

The future work will focus on implementing adaptive Byzantine Agreement protocol, which could be simulated either under Alogrand's structure and proof-of-work based blockchain. Besides, adversary attacks will be simulated to test the security and robustness of the system.