Distributed Trust and Blockchains	Date: *November 7th, 2019*
Instructor: *Sujit Prakash Gujar*	Scribes: Sai Jashwanth Reddy

Lecture 20: Secure High-rate Transaction, GHOST protocol and Proof of Stake

1 Secure High-rate Transaction Processing.

1.1 Bitcoin

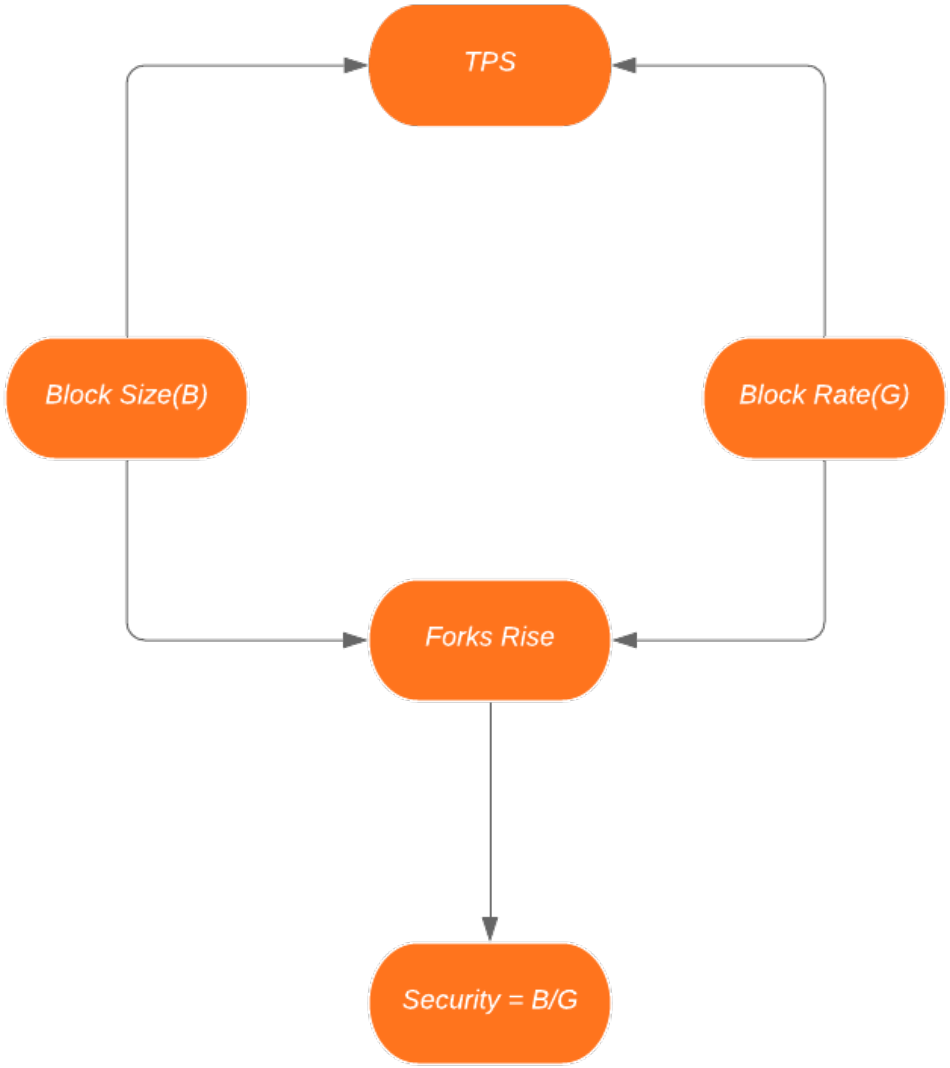
- Largely used decentralized crypto-currency
- Number of active users range from 3 million - 5 million
- 1 BTC = 610100 INR (as of November, 2019)

1.2 Bitcoin Obstacles

- **Adoption**
  - The mass adoption of Bitcoin is in its early stages and is not being performed widely, yet. The use of Bitcoin is not well-established reputationa-lly and is hard to perform for a regular person to become interested in it. There were numerous attempts to quantify the adoption rate of Bitcoin, but they were extremely complicated due to Bitcoin's privacy and lack of information about individual accounts.
- **Regulation**
  - The legal status of bitcoin varies substantially from state to state and is still undefined or changing in many of them.Whereas the majority of countries do not make the usage of bitcoin itself illegal, its status as money varies, with differing regulatory implications.While some states have explicitly allowed its use and trade, others have banned or restricted it.
- **Volatility**
  - Volatility in Bitcoin does not yet have a generally accepted index since crypto-currency as an asset class is still in its nascent stages, but we do know that Bitcoin is capable of volatility in the form of 10x changes in price versus the U.S. dollar, in a relatively short period of time.
- **Scalability**
  - Higher Transaction Rates
    - Bitcoin : 7 TPS
    - PayPal : 100 TPS
    - Visa : 2000 TPS
  - For Higher Transaction Rates, we can
    - Increase the Block size (currently 1 MB)
    - Decrease the average time between blocks getting mined
  - Processing individual transactions
  - It's effect on Security

1.3 Bitcoin Consensus

- **Fork**
  - As bitcoin is a network of nodes, we can have conflicts on which chain to accept.This results in branching or forking.There are two kinds of fork.Hard and Soft forks.
  - Resolve this conflict by saying accept the longest chain, because it has the most proof of work.
- **Effect on Security**



2 GHOST Protocol

2.1 Goal

- Greedy Heaviest Observed Sub - Tree

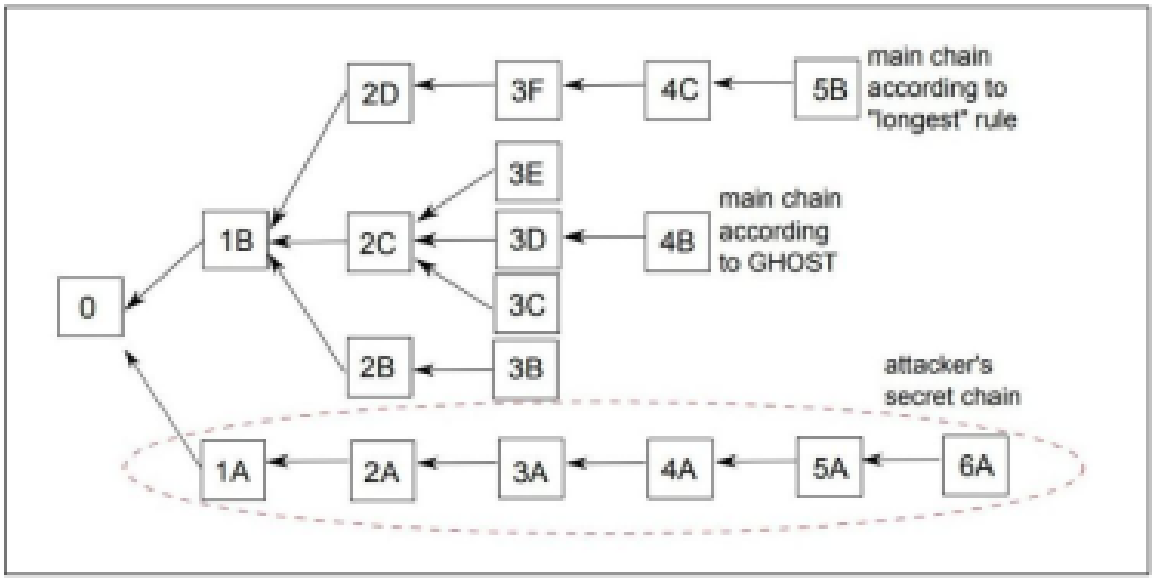
- Attackers can manipulate/create a long chain of their own, which is a major problem.
- The key idea is to propose a new policy to select the right chain.

2.2 Algorithm

Input = Block Tree(T)

- B $\leftarrow$ Genesis Block
- *if* Children $_T$(B) = ϕ then *return*(B) *and exit*
- C $\leftarrow$ Children $_T$(B)
- *else update* B $\leftarrow$ *argmax* $_C$ size(subtree $_T$(C))
- goto rule 2

2.3 Representation by Example



Source : GHOST Research Paper

2.4 Properties

- **Convergence of History**
  - **Proposition:** Every Block is either fully adopted or fully rejected.
  - **Proof :**
  - Let D be delay diameter of network.
  - Assume at time t ¿ time(B) block B is neither adopted nor abandoned.
  - Denote ϵ the event in which next block creation in system occurs between times t + D, t + 2D, and then no other block is produce until time t + 3D.
  - After time t, B is either adopted or abandoned.
  - Between time t and t+D all nodes learn of all existing blocks (as no new ones are manufactured), and therefore each pair of leaves (of the block tree) that have nodes actively trying to extend them must have equal weight subtrees rooted at some common ancestor.

- A single block is then created which breaks these ties, and another D time units allow it to propagate to all nodes, which causes them to switch to a single shared history. Notice that Pr(ϵ) is uniformly (in t) lower bounded by a positive number, as it doesn't depend on t
- Hence the expected waiting time for the first ϵ event is finite

- **Resilience to 50% attacks**
  - **Proposition:** The probability that B will be off the main chain, goes to zero as the time after its adoption goes to infinity i.e, security threshold for 50% is 1 rather than(B/G)
  - **Proof:**
  - Let t be the time in which the B is created.t+T be the time at which B is off the main chain. Then the probability that by time t + T, B was either already abandoned or already adopted, is P which goes to 1 as T goes to infinity. It follows from Markov's inequality E[B] $\leq \infty$.