TwinsCoin - A provably secure PoW and PoS Cryptocurrency

Authors : Alexander Chepurnoy, Tuyet Duong, Lei Fan and Hong-Sheng Zhou
Presented by Mayank
at Tokyo Institute of Technology

Overview

- Introduction to TwinsCoin
- Introduction to 2-hop chain
- Nakamoto’s blockchain and difficulty adjustment in PoW
- TwinsCoin - Main Protocol

Introduction

- It is a provably secure PoW and PoS hybrid cryptocurrency inspired from 2-hop chain (PoS and PoW hybrid blockchain by Duong et al. - ePrint 2016).

- TwinsCoin has a fair chance of being secure even if the adversary holds majority of the computing/ mining power, by relying on majority honest stake.

- A Testnet for the system has been deployed and running right now.

- Security analysis for complex, real-world protocols is very difficult and it is better to take an already provably secure blockchain core (here, it is Duong's 2-hop blockchain) and upgrade it to suit our needs.

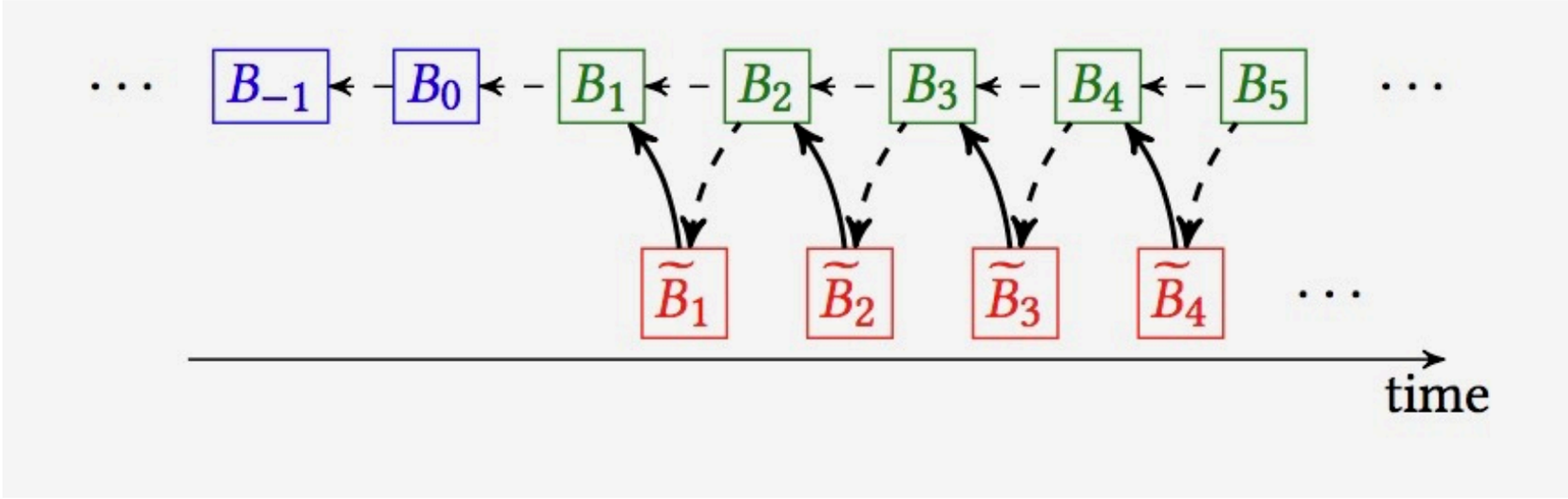
- Most of the existing PoS cryptocurrencies do not scale to large networks where people come and go at any time.

- TwinsCoin deals with the problem of people being offline when their chance to generate the next PoS block comes and hence scales very well in large networks.

Duong's 2-hop chain

- PoW -> Winning Miner -> New PoW Block -> PoS -> Winning Stakeholder -> New Block.

- Can be seen as PoS scheme that uses PoW as a biased random beacon.



Issues with Duong's chain

- It is scalable but not practical.
- Assumes static (across all the rounds total # of physical and virtual resources remain the same) protocol execution environment. This is so because there is no difficulty adjustment criterion.
- Assumes flat (each miner has the same computing power and each stakeholder has the same amount of stake) model.
- The system is assumed to be extended from an already “mature” blockchain like bitcoin blockchain.

Improvements from 2-hop chain

1. Adaptive difficulty adjustment. In 2-hop chain #PoW blocks = #PoS blocks. Here, we introduce that #PoW blocks >=#PoS blocks. #PoW blocks = #Attempting blocks + #Successful blocks.

2. Moving to not-flat setting.

3. Support for light-clients.

Nakamoto's Blockchain

- PoW : $H(h, w, x) < T$
- - where H is some hash function, h is the hash of the previous PoW block, w is the nonce, x is the record data of the block and T is the PoW target.

Difficulty adjustment in PoW

- Based on the observation made on the last m blocks, adjust the target value.

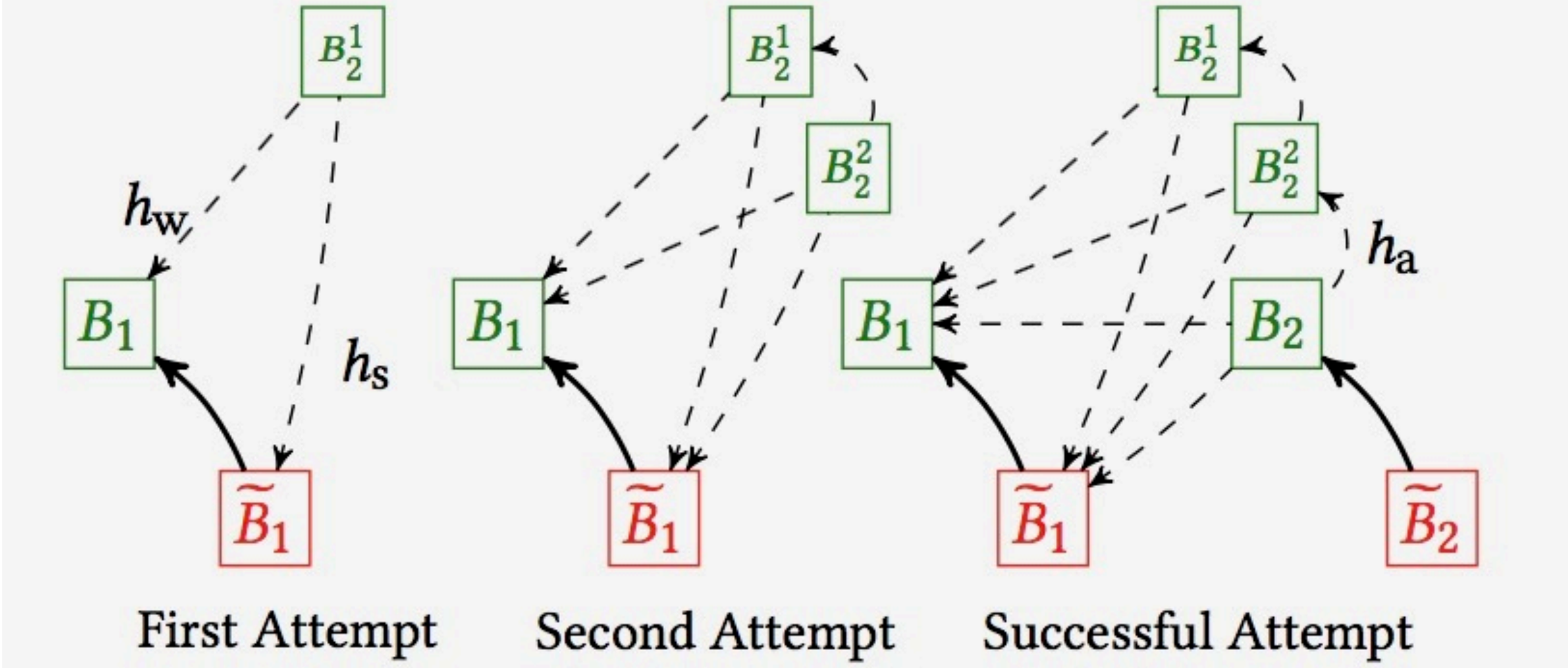
- In Bitcoin, target is adjusted every m = 2016 blocks.

- This period of m blocks is called an epoch.

- Nakamoto proposed, $T_{i+1} = (t_i/t)T_i$, where t is the expected time of an epoch.

TwinsCoin Mechanism

- 2 Players - Miners and Stakeholders.
- 2 types of PoW blocks - Attempting and Successful blocks.
- A PoW block without an accompanying PoS block is called an attempting block else a successful block.
- PoW block - $< h_w, h_s, h_a, w >$
- PoS block - $< h_w, vk, x >$



Blockchain Structure

The blocks in green are PoW blocks and the blocks in red are PoS blocks

TwinsCoin in detail

- Difficulty adjustment

1. PoS difficulty adjustment

2. PoW difficulty adjustment

- Introducing non-flat model

- Introducing light client support

TwinsCoin Difficulty Adjustment

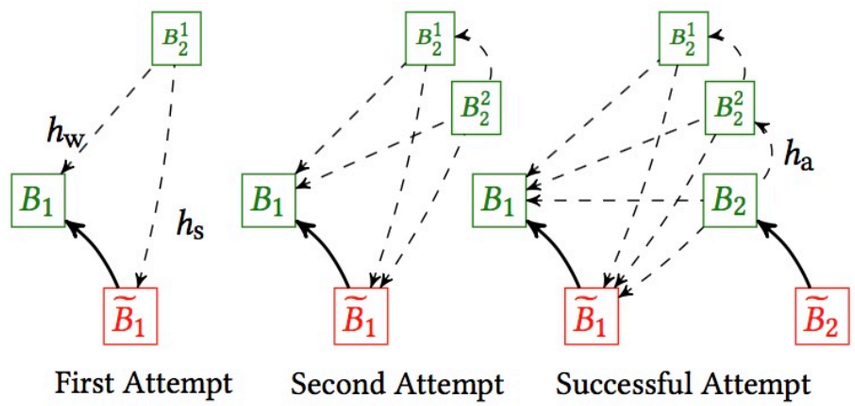
- T - PoW Target, T_i - PoW target for ith epoch, $T^{'}$ - PoS target, $T_i^{'}$ - PoS target for ith epoch.

- T determines the probability of finding a valid PoW block.

- $T^{'}$ is used to control the probability that a PoW block is successfully mapped to a stakeholder.

PoS difficulty adjustment

- $H(h_w, vk) < T^{'}$
- $T^{'}_{i+1} = (m_i R/m) T^{'}_i$



- R is the probability that a PoW block is successfully mapped to a stakeholder.

- In the image, if we consider an epoch size of m = 2 blocks, we see that m_i = 4.

PoW difficulty adjustment

- $H(h_w, h_s, h_a, w) < T$
- $T_{i+1} = (t_i/t)(m/m_i R)T_i$
- R is the probability that a PoW block is successfully mapped to a stakeholder.
- Forks are resolved by selecting the chain with the maximum # of successful blocks.

Security Arguments

- Adversary can stop to contribute in new PoW blocks for some time to increase T and then jump suddenly work out the PoW puzzle on this increased T .

- TwinsCoin is secure under this attack as it can be proved that there is a bound of $pp^{'}$ on the ratio of new epoch time t_{i+1} and t , where p = honest computing power ratio and $p^{'}$ = honest stake ratio.

Moving to non flat model

- $H(B, vk) < vT^{'}$
- where v is the stake in the account of the stakeholder with vk verification key.
- Even if the stake of the stakeholder is split across v accounts, the total probability of him generating the next block remains the same.

Adding light client support

- In PoW blockchain, validity checking for n blocks is done in $O(n)$ operations.
- In contrast, in PoS, a validity checking requires a scan through the balance sheet. Hence, for n blocks, $O(n.log(s))$ operations is required, where s is the size of the balance sheet.

- For a light client, this is a heavy validation task compared to PoW blockchains.

1. Use a 2 party dynamic dictionary so that nodes do not need to store the full dataset.

2. Also proposed a constant factor reduction by truncating the merkle tree.