Security of Blockchain Consensus Protocols

Austine Onwubiko, Sarwar Sayeed, Hector Marco-Gisbert

Presented by: Austine Onwubiko

Austine.Onwubiko@uws.ac.uk

School of Computing, Engineering and Physical Sciences

University of the West of Scotland

High St, Paisley PA1 2BE, UK

About the Author

Austine Onwubiko is a Researcher at the University of the West of Scotland, UK. He holds a Masters Degree in Computer Science, Information and Network Security, and a PhD candidate at the School of Computing, Engineering and Physical Sciences of the University of the West of Scotland and as a member of the centre of Cyber Security. Austine is a co-author of the paper “Cyber KPI for Return on Security Investment”. He has been invited to some of the reputable Cyber Security conferences Such as Cyber Situation Awareness as a Prism to understanding Situations in a fast-paced Cyber World, Cyber Situation Awareness as a tool for Analysis and insight, and Cyber Situational Awareness for Predictive Insight and Deep Learning. Austine’s research interests include Cyber Security, Blockchain Consensus Protocols, And Artificial Intelligence.

Presentation Outline

- Motivation
- Introduction
- Consensus Protocol
- Problems of the Blockchain
- Security Attacks of the consensus Protocol
- Protection Techniques of the consensus Protocol
- Final Summary
- References

Motivation

- Consensus Protocol is important for the security of the Blockchain Technology.

- To verify and validate transactions in the network, the must agree that every new block that is added to the blockchain is verified and valid. The agreement establishes trust among unknown nodes in a distributed computing environment. This can be achieved by the consensus protocol, which is the core part of blockchain network.

Introduction

- Blockchain is a solution for centralization.
- It is a peer-to-peer network.
- It is a system of keeping record by everybody without the need of a central authority.
- Blockchain are made up blocks linked together as the name states.
- Blockchain are distributed digital immutable ledgers of cryptographically signed transactions.
- Blockchain also uses the consensus algorithm.

Technical Terms

Terms	Descriptions
Block	A collection of data recording of transaction and other associated details such as the correct sequence, timestamp of creation etc.
Decentralized	Data is stored on each system across the network.
Transparent	Every node on the network can see the data shared on the network.
Miner	Transaction verifiers.
Consensus	A method used to verify the transactions.
Node	The ledger in the blockchain system.

Technical Terms

Forks	The problem that arises when the nodes is used for different versions of blockchain.
Hash	One-way hash function to check the integrity of a transaction or message.
Timestamp	A date and time in the blockchain system used as an electronic time stamp for any transaction.

Some Applications of the Blockchain

- Cryptocurrency : Bitcoin, Ethereum, Bitcoin cash, Ethereum classic etc.
- Smart Contracts
- Internet of Things (IoT).

Problems of the Blockchain

- Although the decentralized aspects of blockchain are a solution to various baneful attack techniques; however, it still comprises severe weaknesses within the consensus protocol resulting in many attacks, such as 51% attack, Sybil attack, etc.

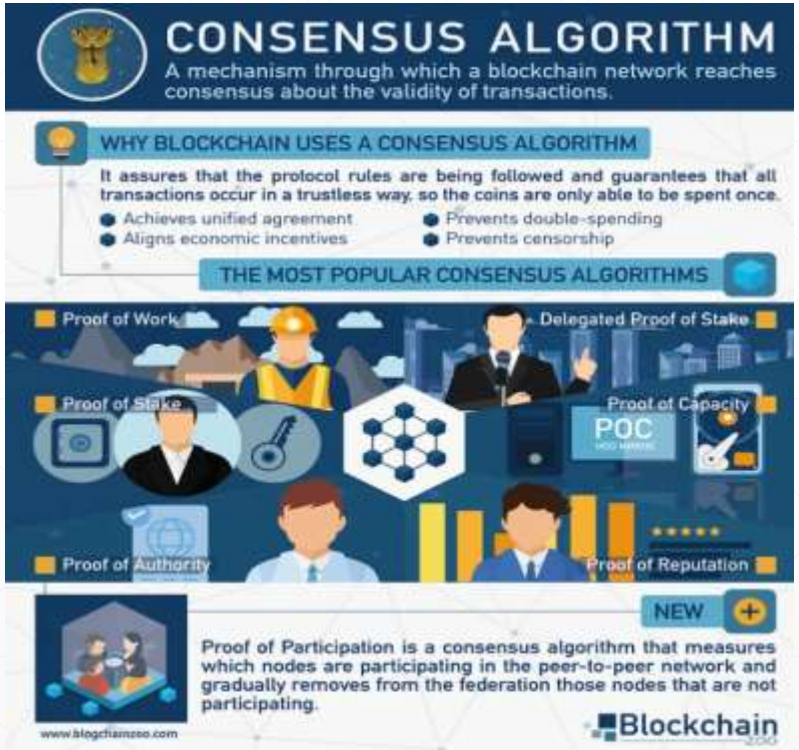
- A majority of the cryptocoins comprise only a limited number of nodes making them vulnerable to the attacks as the likelihood of a 51% attack entirely depends on the total hashing ability of an adversary.

- Although blockchain solves various security challenges that exists in the current centralised system.

- The blockchain has its issues and attackers apply different methods to execute successful attacks that may include exploiting the vulnerability in the P2P network.

Consensus Protocol

- A consensus protocol is a common agreement in the blockchain network about the present state of the distributed ledger.
- To verify and validate transactions in the network, the network must agree that every new block that is added to the blockchain is verified and is valid.
- There are various consensus protocol in the blockchain, the PoW, PoS and DPoS Are the most popular protocols adopted in the blockchain network.



CONSENSUS ALGORITHM

A mechanism through which a blockchain network reaches consensus about the validity of transactions.

WHY BLOCKCHAIN USES A CONSENSUS ALGORITHM

It assures that the protocol rules are being followed and guarantees that all transactions occur in a trustless way, so the coins are only able to be spent once.

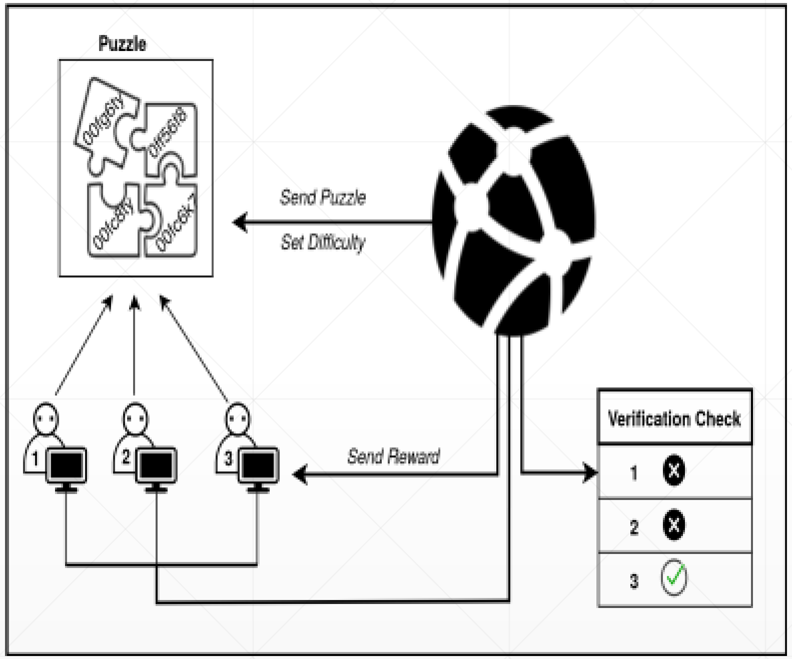
- Achieves unified agreement
- Aligns economic incentives
- Prevents double-spending
- Prevents censorship

THE MOST POPULAR CONSENSUS ALGORITHMS

Proof of Participation is a consensus algorithm that measures which nodes are participating in the peer-to-peer network and gradually removes from the federation those nodes that are not participating.

Proof of Work (PoW)

- This is a consensus mechanism, which is based on solving a mathematical equation.
- The action involves mining where each node on the network is referred to as a miner.
- The only way to verify the transaction in the blockchain network is by mining.

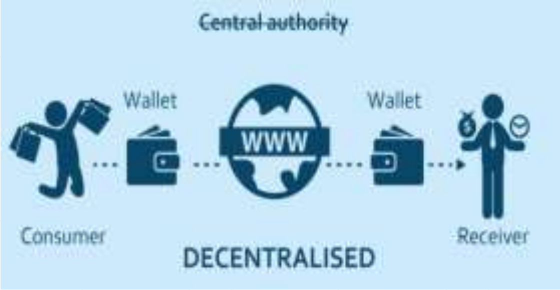


Importance of Consensus Protocol

- The consensus protocol is the main mechanisms that makes a blockchain secure.

- There no central authority or a third party involved in the Blockchain network.

- The agreement establishes a trust among unknown nodes in a distributed computing environment. This can be achieved by the consensus protocol, which is the core part of blockchain network.

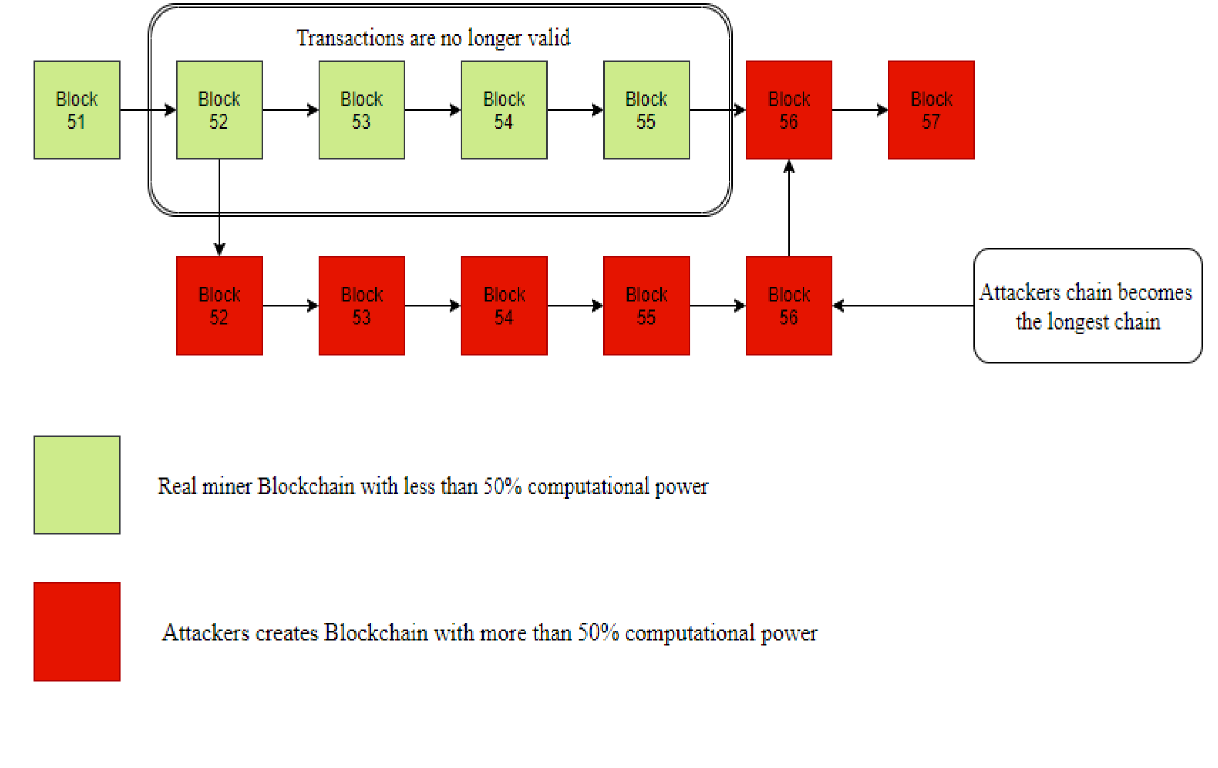


Security Attacks of the Consensus Protocol

- 51% Attack
- Selfish Mining Attack
- Balance Attack
- Long Range Attack
- Sybil Attack

51% Attack

- An Attacker with 50% mining power will be able To control half of the network.
- The will be able to double spend coins, forcing Miners to accept fake transactions and adding it To the network.
- The corrupt version of the transaction has to be longer than the current version to reverse the transaction.

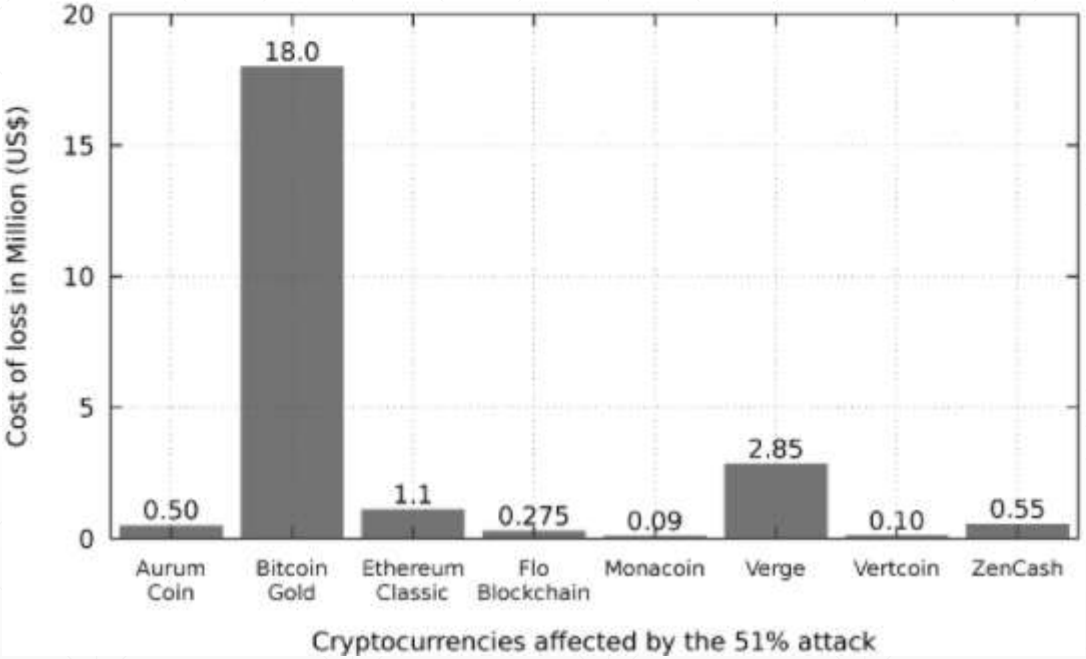


🟩 Real miner Blockchain with less than 50% computational power

🟥 Attackers creates Blockchain with more than 50% computational power

Assets lost to 51% Attack

- Blockchains that have suffered 51% attacks include Ethereum Classic (ETC), Feathercoin (FTC), Bitcoin Gold (BTG), Vertcoin (VTC) and Verge (XVG).
- 2018 was notably one of the worst years to see 51% Attack, and ultimately attacks in this year netted hackers Close to $20million in profits, according to The Next Web.



Protection Techniques of the consensus Protocol

Historical Weighted Difficulty based Proof of work

Random Mining Group Selection

- This protection mechanisms is proposed to protect against 51% Attack.

Indegree and Outdegree

- This protects against Eclipse Attack.

Self-Registration

- This protects against Sybil Attack.

Protection Techniques of the consensus Protocol

Backward-Incompatible Defense

Tie Breaking Defense

- These mechanisms protects against Selfish Mining Attack.

Dynamic and Auto Responsive Approach

- This a protection mechanism against DDoS Attack.

These approaches helps to reduces the possibility of an attack, but the attack is still happening

Final Summary

- Consensus protocols are the most significant factors of this technology as weaknesses in the protocol results in various attacks.
- The protection techniques are not robust enough to defense; hence, a strong protection approach required to mitigate the attacks.
- For our future work, we aim to perform a deep analysis of the limitations of the major consensus protocol to propose a robust security approach to mitigate the attacks.