BITS F463: Cryptography

Group 53

Anonymous Voting using Blockchain and ZKP

Group Members:

[2019A7PS0086H] - Amogh Bharadwaj
[2019AAPS0345H] - Shrikrishna Lolla

Problem Statement

Formally, our problem statement is to build a **secure, anonymous voting system** based on decentralised systems, and in particular, using the concept of blockchain technology.

Blockchain Introduction

The world has an increasing desire to move away from centralised governance, and this trend has manifested itself in networking as well. Blockchain is a concept utilising **decentralised** networks, where every node (user) in the network is equal in terms of rights, permissions etc.
In the case of Bitcoin, nodes are rewarded for performing computationally hard problems in the form of cryptocurrency (BTC). This

is called *Proof of Work* and comes under a category called **consensus algorithms**, which are algorithms to elect such nodes, which are called **miners**.
The core of any blockchain are the transactions. Transactions need to be verified before being added to a block. The block has a block header with various fields such as hash and timestamp to ensure integrity of data.

Blocks, upon verification, are pushed to what is known as a **blockchain**.

Blockchain in an Anonymous Voting Scheme

This problem can be modelled as a blockchain network, where transactions are votes made by the nodes.
Blocks consist of votes collected, along with a block header with various fields.
Nodes will have a public voter ID and a secret. The secret will be used to verify their votes using a **Zero-Knowledge Proof (ZKP)**, which will be explained in detail later in this report.
Each block and the blockchain will be verified. For example, each block's previous hash value must match the previous block's hash value.
We can use any consensus algorithm for this, but we chosen Proof of Work (PoW).

Zero Knowledge Proof Implementation

Introduction to Zero -Knowledge

Suppose you want to prove to your identity to a guard posted outside your intelligentsia building. You cannot merely speak your name outloud, for there are enemy spies lurking who may overhear that and later impersonate you. The verifier asks you a precise set of questions, which when answered will be able to prove that you are indeed who you claim to be, without leaking your identity itself. This concept / protocol is known as **Zero-Knowledge Proof**.

Zero-Knowledge Verification of A Vote

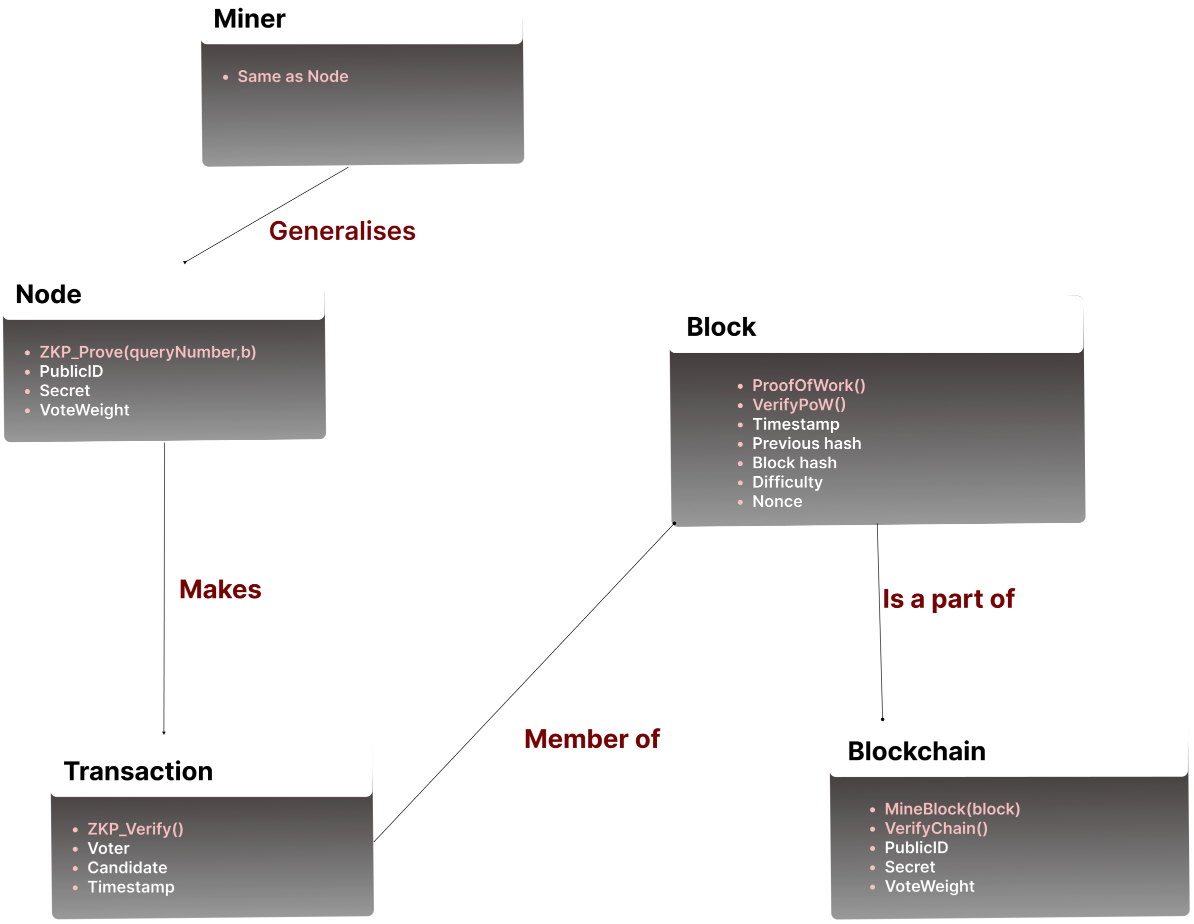
In our project, zero-knowledge protocol is used for verifying the individual transactions (votes in our case). In essence, we wish to prevent a malicious node from impersonating another in order to gain an extra vote.
Every voter in our model has their own public voter ID. Mathematically, this is of the form:

$$\begin{gathered} g^x \ mod \ P, \text{where:} \\ g \text{ is a public parameter known as a generator} \\ P \text{ is a public parameter which is prime and} \\ x \text{ is a secret value known only to the node.} \end{gathered}$$

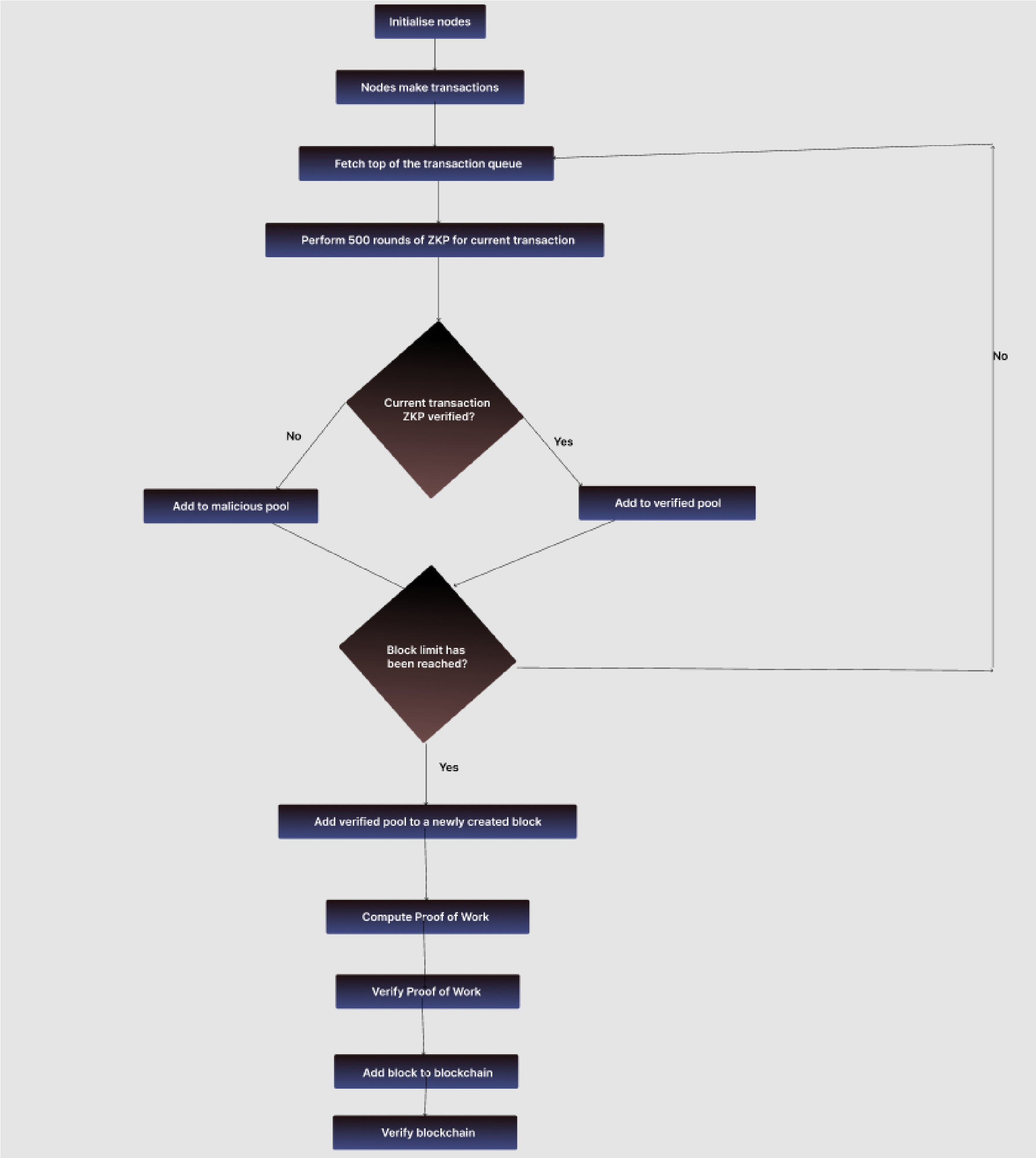
When verifying a transaction, the system will query the node for certain values (such as `h` and `s`) in order to verify the vote's authenticity. The ZKP algorithm followed is identical to the one specified in the problem document. We perform 500 rounds of ZKP verification for the probability of successful repeated guessing tends to 0.

Flowcharts and UML Diagrams

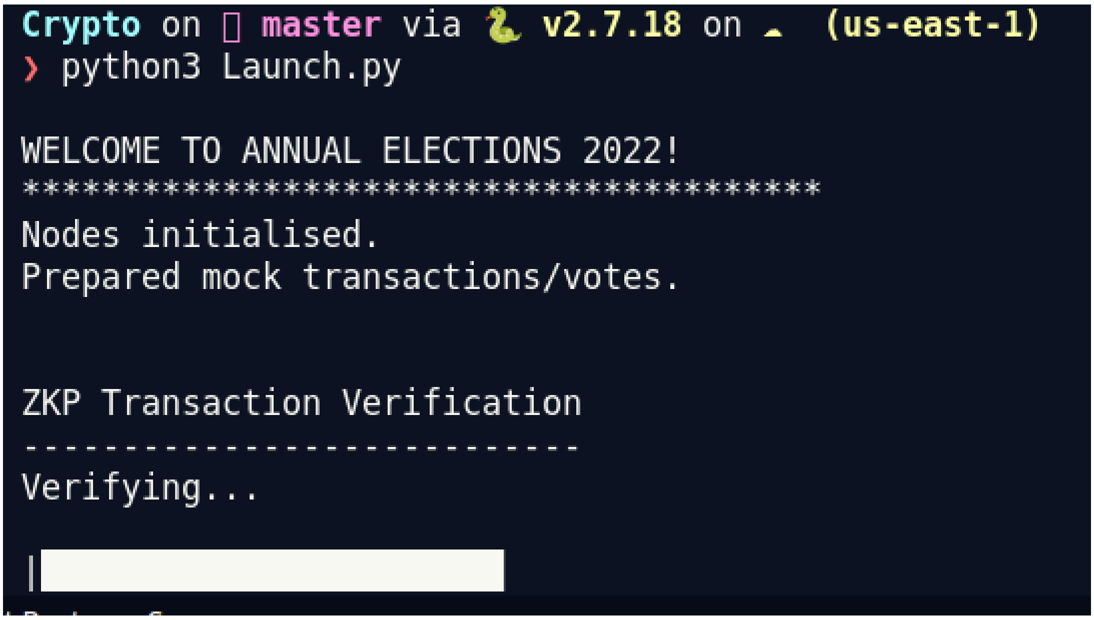
UML Class Diagram



Code Flowchart


Initialise nodes
Nodes make transactions
Fetch top of the transaction queue
Perform 500 rounds of ZKP for current transaction
Current transaction ZKP verified?
No
Yes
Add to malicious pool
Add to verified pool
Block limit has been reached?
No
Yes
Add verified pool to a newly created block
Compute Proof of Work
Verify Proof of Work
Add block to blockchain
Verify blockchain

Working Screenshots

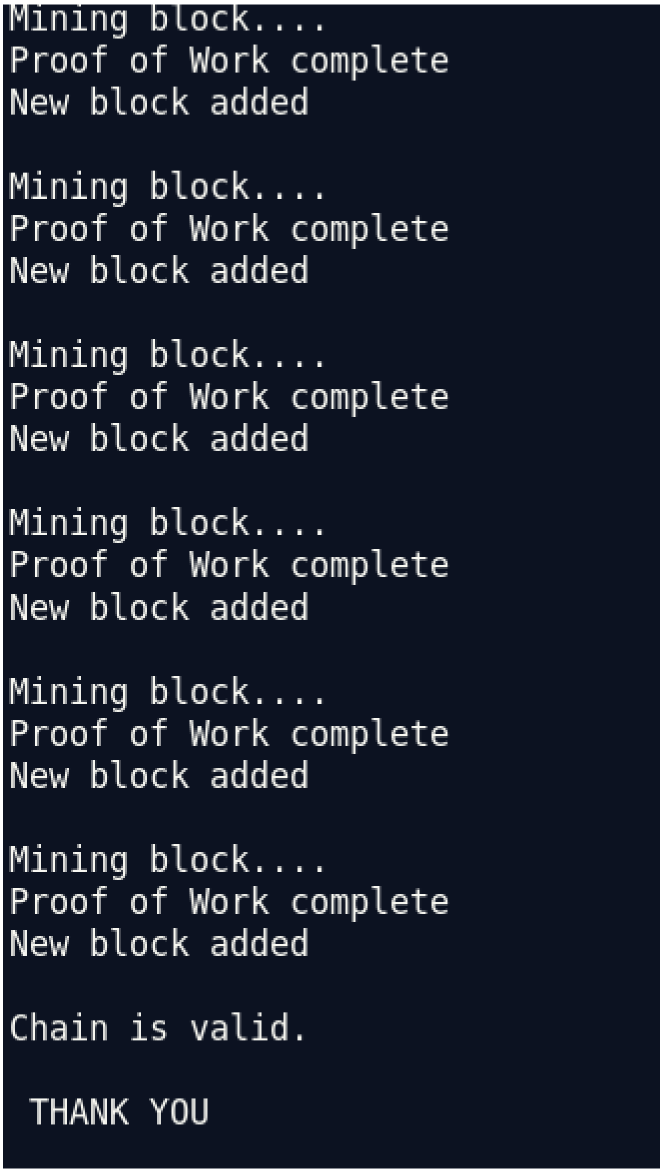


```
Crypto on  master via 🐍 v2.7.18 on ☁  (us-east-1)
❯ python3 Launch.py

WELCOME TO ANNUAL ELECTIONS 2022!
****************************************
Nodes initialised.
Prepared mock transactions/votes.


ZKP Transaction Verification
----------------------------
Verifying...

|
```



```
Mining block....
Proof of Work complete
New block added

Mining block....
Proof of Work complete
New block added

Mining block....
Proof of Work complete
New block added

Mining block....
Proof of Work complete
New block added

Mining block....
Proof of Work complete
New block added

Mining block....
Proof of Work complete
New block added

Chain is valid.

 THANK YOU
```