CORONA ACCOUNTABILITY BLOCKCHAIN

A PROOF OF STAKE BLOCKCHAIN PROJECT

Vaibhav Chopra

19BCE0932

mailvaibhavchopra@gmail.com

1 ABSTRACT

Blockchains are a very important interesting development in technology with all sorts of applications and approaches to develop it. Many different consensus mechanisms have been proposed over the years and all of them have their own merits.

But even after large adoption by the research and the hobbyist community, applications of blockchain are still very finance centric. Bitcoin and other cryptocurrencies are still the largest adopters of blockchains.

Many other applications and use cases of blockchain have been proposed and are being implemented daily. We are going to discuss one such non-financial application of blockchain in this report. This application also seems relevant in current circumstances of the world (as of May 2020). We are going to discuss the feasibility of a Proof of Stake (POS) based **COVID-19 Research Accountability Enforcer.**

This system hopes to introduce accountability into the COVID-19 research in these times where medical resources have been distributed all across the globe. We are all better off working together in these trying times. This project also aims to test out the feasibility of Proof of Stake (POS) which is a relatively newer consensus mechanism and aims to replace the more common Proof of Work consensus standard.

Proof of Stake seems to be a much more viable option based on long term sustainability and eco-friendliness. The various advantages of a POS-based blockchain are analysed and the limitations and shortcomings are also addressed.

Since blockchain guarantees a publicly available immutable ledger, It will be very useful for the medical sciences to collaborate and make sure that accountability is maintained among those who are working to find a cure for the Coronavirus.

2 INTRODUCTION

2.1 Coronavirus

Coronavirus disease 2019 (COVID-19) is an infectious disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). It was first identified in December 2019 in Wuhan, China, and has since spread globally, resulting in an ongoing pandemic. As of 28 May 2020, more than 5.69 million cases have been reported across 188 countries and territories, resulting in more than 355,000 deaths. More than 2.34 million people have recovered.

Common symptoms include fever, cough, fatigue, shortness of breath, and loss of smell and taste. While the majority of cases result in mild symptoms, some progress to acute respiratory distress syndrome (ARDS) likely precipitated by a cytokine storm, multi-organ failure, septic shock, and blood clots. The time from exposure to onset of symptoms is typically around five days but may range from two to fourteen days.

2.1.1 Cure Situation

According to the World Health Organization, there are no available vaccines nor specific antiviral treatments for COVID-19. On 1 May 2020, the United States gave emergency use authorization to the antiviral remdesivir for people hospitalized with severe COVID-19. Management involves the treatment of symptoms, supportive care, isolation, and experimental measures. The World Health Organization (WHO) declared the COVID-19 outbreak a public health emergency of international concern (PHEIC) on 30 January 2020 and a pandemic on 11

March 2020. Local transmission of the disease has occurred in most countries across all six WHO regions.

2.1.2 Research

No medication or vaccine is approved to treat the disease. International research on vaccines and medicines in COVID-19 is underway by government organisations, academic groups, and industry researchers. In March, the World Health Organisation initiated the "Solidarity Trial" to assess the treatment effects of four existing antiviral compounds with the most promise of efficacy. The World Health Organization suspended hydroxychloroquine from its global drug trials for COVID-19 treatments on 26 May 2020 due to safety concerns. It had previously enrolled 3,500 patients from 17 countries in the Solidarity Trial. France, Italy and Belgium also banned the use of hydroxychloroquine as a COVID-19 treatment.

There has been a great deal of COVID-19 research, involving accelerated research processes and publishing shortcuts to meet the global demand. To minimise the harm from misinformation, medical professionals and the public are advised to expect rapid changes to available information, and to be attentive to retractions and other updates.

2.2 Medical Collaboration

More than 20 different drugs have been approved or are in the process of being approved for clinical trials by different countries. There is also an environment of tension between some countries in these tough times due to the recession and economic collapse brought about by this viral outbreak. It is essential that keeping all political matters aside, doctors and the medical sectors of all the countries collaborate and fight this disease together. This project is also an attempt to ensure that. By using the permanence and reliability of distributed public

blockchains, we can ensure that there is a sync between the different strategies being adopted by medical professionals all across the globe.

3 LITERATURE SURVEY

3.1 Blockchain Mechanism

Around a decade ago Satoshi Nakamoto introduced Bitcoin. Despite the revolutionary nature of Bitcoin that made it famous around the world, there are far more potentials from the underlying technology. And that reflects in the research and literature surrounding blockchains.

This structure groups together transactions into blocks which are validated by groups of blockchain users. In traditional blockchains, e.g., Bitcoin, users compete with each other in solving difficult cryptographic/mathematical problems which are easy to verify. This process is called “mining”, and the winner gets new coins as a reward for her services. These blockchains are therefore based on the concept of Proof of Work (PoW). Practically, we consider the user to be trustworthy because she spent a considerable amount of computational effort to verify some transactions.

3.2 Proof of Stake

Consensus protocols differ based on the aspects or the attributes of the node that are being assessed. Proof-of-work (PoW) requires the node to provide the computing power to solve a mathematical problem in order to append a new block to the blockchain. The most well-known user of PoW consensus is Bitcoin where miners have to solve cryptographic hash puzzles as proof of work. In Proof-of-stake (PoS), a node has to stake something it owns, usually in the form of a cryptocurrency. If a malicious node tries to manipulate the blockchain and the other nodes detect it, the locked-up stakes get slashed or rewards are withheld. Delegated proof-of-stake (DPoS) is where the nodes of the network vote for a set of nodes to be the delegators. Other less common protocols include proof-of-correctness (Ripple) and proof-of-burn (Slimcoin).

In a PoW system, the nodes are rewarded for performing an operation that is agreed by a majority of the nodes in the system. The caveat here is that participants are not punished for performing a malicious operation. As a result, PoW systems cannot deter the participants from performing a selfish mining or participating in a 51% attack. In order to solve this problem, newer generations of blockchains (Ethereum, Tendermint, etc.) have started to use proof-of-stake as the consensus algorithm. In a PoS system, the participants are rewarded for performing a non-malicious activity just like a PoW system but they are also held accountable and are punished for any malicious operation.

3.3 Design of the Proposed System

Most blockchains require some currency or token to incentivise the nodes/validators to play fair and act honestly. This works very well in a financially oriented set up like Bitcoin or Ethereum. But we are looking for a blockchain application in the medical sector. So we have to introduce a new unit that could be used to incentivise the different players and stakeholders in the pharmaceutical industry.

3.4 The Main Idea

The major challenge in any medical research is testing. It takes years of R&D and billions of dollars just to come up with a drug for a minor disease.

A market survey by Policymed found that as of 2019, the cost to develop one new drug is $2.6 billion and the approval rate for drugs entering clinical development is less than 12%. The main challenge is to reduce or at least distribute this amount among the different parties involved in finding a cure for the Coronavirus. We need to also introduce accountability in the system so that we can pinpoint if somebody makes a mistake.

The basic idea is the following:

1. All the major drug makers will be members / validators in the accountability blockchain.
2. If any drug maker has a major development in COVID-19 research or finds a possible cure for the Coronavirus, they can propose to add that development in the blockchain.
3. To propose the addition of your research development in the blockchain, you need to ***stake*** some "Reputation Tokens" away. These Reputation Tokens are what will sustain the blockchain. If your contribution/research is valid and is reproducible in test conditions by majority of the rest of the nodes, your contribution gets added to the blockchain and your ***staked*** Reputation Tokens get refunded back to you along with some ***bonus*** Reputation Coins. There will be a net increase in the amount of Reputation Tokens that you have if your contribution is valuable.
4. But in case the proposal is not working or is invalid, other nodes won't be able to get the desired results and thus will reject the block from being added in the blockchain. And due to this, the proposer won't get a reward and you will also be penalised for your wrongful contribution.

3.5 The Challenges

We have seen how most of the blockchains currently are working on the basis of Proof of Work. But there are some problems with using Proof of Work in our application. Some of the probable reasons are listed here:

1. The different stake holders in the medical industry don't deal with ASICs and other sophisticated mining hardware. It will be difficult to bring them on board if the threshold to adoption is too high.
2. Proof of Work requires a lot of electricity to sustain in reasonably large sized blockchains
3. We have already seen with Bitcoin and other cryptocurrencies how being able to buy hashing power in the real world with real world money directly dictates your success in the PoW infrastructure. We don't want that to happen in this ecosystem. The majority

should lie with those nodes who have finding the cure for COVID-19 in their utmost priorities and not with those having the fastest mining hardware.

4. Also, reputation is the most important thing for a company in the medical industry. That is why we have Reputation Tokens at the heart of this system. The amount of Reputation Tokens you possess is directly related to how reputable your company is and how much you have contributed towards curbing COVID-19.

3.6 How Proof of Stake Fits Here

Proof of Stake is a fairly new development in the world of blockchain consensus mechanisms. Many ways to achieve it have been proposed. Many Byzantine fault tolerant and corruption resistant approaches to Proof of Stake have been proposed over the years. We would prefer a Proof of Stake approach here instead of Proof of Work because:

1. Most pharmaceutical firms won't care about accumulating hashing power.
2. There is a need to associate the success and reputation of a company or organisation in COVID research to the amount of Reputation Tokens they possess in the blockchain. That is done quite well by Proof of Stake.
3. Since there are human lives at stake, There is also a need to penalise those who don't work in line with the vision to curb COVID-19. This is possible only in Proof of Stake and not in Proof of Work. In Proof of Work, your contribution might not be accepted and you might not get a mining reward, but you are not penalised for a wrong contribution. But in Proof of Stake, when you make a mistake, intentionally or unintentionally, not only do you not get a reward, but some penalty also has to be paid from the ***staked*** amount. You don't get back the same amount that you staked in this case.

From the above arguments, it becomes quite clear that a Proof of Stake system would be more appropriate as a consensus algorithm for our purposes. Not only will it maintain the permanence and transparency like we expect from a blockchain, but also we'll be able to ensure that all stakeholders play fair and act for the betterment of the community.

4 IMPLEMENTATION

In order to illustrate the major characteristics of a proof of stake blockchain, we have made a publicly accessible REST API using NodeJS and deployed it on https://corona-blockchain.herokuapp.com/blockchain .

This model is for exhibition purposes only. To make our example clear and to compensate for the factors that rely on user-adoption and time boundedness of the algorithm, we have made some abstractions and assumptions that will make the study of the model and the rest of the report easy to understand. All these variables can be adjusted or tweaked depending on the demand of the network. We have tried to keep the characteristics as flexible as possible . Some of these characteristics are:

1) To avoid having to implement a distributed ledgering system, we have deployed the blockchain on a centralized server. Although this does cause a slight security compromise, but its good enough for our illustration. This also allows us to set up separate gossip protocols that require accounting for complex asynchronous operations.
2) We maintain a proposal buffer in our protocol where different pharmaceutical companies can present their research after becoming a node in the network. The company just needs to come up with a unique id for itself.
3) We have kept the stake lock in period to 30 minutes (this can be adjusted as per requirement) and allowed multiple proposal validations in that time. Every 30 minutes, the protocol checks for pending proposals and those proposals that have approval ratio above the threshold get added to the main blockchain. Those that don't get the required amount of validations get rejected and get penalised accordingly. The main idea behind penalising them is that in the real world, these proposals would represent those proposals that were either useless/wrong or were not contributing in any productive way according to the majority of the nodes on the network, all of which are supposed to be highly reputed medical organisations.
4) We have kept the buffer turn around to 30 minutes in order to speed up the development and code testing process. But in reality this time would be much longer (at least a week or so). This is to allow different organisations across the globe connected to the network

to have enough time to test the claims made by other nodes in their own laboratories and see if they are able to reproduce the same results or not as claimed by the proposal.

5) We have also implemented a direct consensus protocol trigger to skip this turnaround time for quick testing. In the real protocol, such a functionality will not be there.
6) In order to sustain the blockchain, we need to introduce some incentives for individual nodes, i.e. the different medical organisations that are part of the network. We have achieved this in the form of "Reputation Tokens". All the nodes start out with 50 (this can be changed) Reputation Tokens. For every accepted proposal, you get 5 additional tokens along with your staked amount. But for every non-approved proposal, you get 5 tokens deducted from your balance.

4.1 Code

All the source code used in implementing this blockchain is accessible on https://github.com/sudo-vaibhav/corona-accountability-blockchain and is publicly available under a GPL-3.0 and later license.

Refer to the above Github repo for the updated code and other useful components and to stay updated about the project.

```
const THIRTY_MINUTES = 30 * 60 * 1000
const INITIAL_BALANCE = 50 //this is the initial amount that any node starts w
ith
const STAKE_AMOUNT = 10 //this is the amount that's staked by default to make
a proposal
const REWARD_AMOUNT = 15 //you get 5 more Reputation Tokens that what you stak
ed
const PENALIZED_AMOUNT = 5 //you lose 5 Reputation Tokens if your contribution
 is not approved by the majority of nodes
const CONSENSUS_THRESHOLD = 0.5 //more than 50% of nodes have to approve your
contribution to get the reward

const port = process.env.PORT || 3000
const express = require("express")
const app = express()
const cors = require("cors")
```

```
app.use(cors())

const bodyParser = require('body-parser')
app.use(bodyParser.json())

const {
        v4: uuidv4
} = require('uuid')


class Block {
        constructor(proposerId, data) {
                this.proposer = proposerId
                this.data = data
                this.approvals = [proposerId] //obviously a proposer will appr
ove his own block
                this.blockId = uuidv4() //assigns a unique id to each proposal
 for tracking later
        }

}

class Blockchain {
        constructor() {
                this.chain = []
                this.nodes = {}
                this.proposalBuffer = []
        }

        stake(block) {
                this.nodes[block.proposer].balance -= STAKE_AMOUNT
                this.proposalBuffer.push(block)
        }

        runConsensus() {
                console.log("running consensus algorithm now!")
                this.proposalBuffer.forEach(proposal => {
                        let approvalsCount = proposal.approvals.length
```

```
                        let nodesCount = Object.keys(this.nodes).length
                        let approvalRatio = (approvalsCount / nodesCount)
                        if (approvalRatio > CONSENSUS_THRESHOLD) {
                                this.addBlock(proposal)
                                //now reward the proposer
                                console.log("proposal approved!!", proposal)
                                this.nodes[proposal.proposer].balance += REWAR
D_AMOUNT
                        } else {
                                //your block doesn't get added and you get les
s amounts of token back
                                console.log("proposal rejected!!", proposal)
                                this.nodes[proposal.proposer].balance += PENAL
IZED_AMOUNT
                        }
                })

                //now we clear the buffer as it has run its course now
                this.proposalBuffer = []
        }

        addBlock(block) {
                this.chain.push(block)
        }

        addNode(node) {
                if (this.nodes[node.id]) {
                        return false //means another node with same id already
 exists
                } else {
                        this.nodes[node.id] = node // adding a new node and al
locating it the initial balance
                        return true
                }
        }


}
```

```
class Node {
        constructor(id, blockchain) {
                this.id = id
                this.balance = INITIAL_BALANCE
                //now get this node added to blockchain network
                blockchain.addNode(this)
        }

        propose(data) {
                let block = new Block(this.id, data)
                blockchain.stake(block)
                return block.blockId // returns the uuid of proposed block
        }
}

let blockchain = new Blockchain()


app.get("/blockchain", (req, res) => {
        res.status(200).send(blockchain)
})

app.post("/proposeblock", (req, res) => {
        const {
                id,
                data
        } = req.body
        try {
                const blockId = blockchain.nodes[id].propose(data)
                res.status(200).send({
                        blockId
                })
        } catch {
                res.status(404).send("user not found")
        }

})
```

```
app.post("/addNode", (req, res) => {
        const {
                id
        } = req.body
        let node = new Node(id, blockchain)
        res.status(200).send("OK")
})

app.post("/approve", (req, res) => {
        const {
                id,
                blockId
        } = req.body
        for (let proposal of blockchain.proposalBuffer) {
                if (proposal.blockId == blockId) {
                        console.log(proposal.approvals)
                        if(!proposal.approvals.includes(id)){
                                proposal.approvals.push(id)
                        }
                        break
                }
        }
        res.status(200).send("OK")
})

app.get("/runconsensus", (req, res) => {
        blockchain.runConsensus()
        res.status(200).send(blockchain)
})

app.get("/", (req, res) => {
        res.redirect("/blockchain")
})

app.listen(port, () => {
        console.log(`listening on port ${port}`)
```

```
        setInterval(() => {
                // maintains the blockchain periodically by rewarding valuable
                // contributions and penalizing the wrong ones by deducting th
e staked amount
                blockchain.runConsensus()
        }, THIRTY_MINUTES)
})
```

5 RESULTS AND DISCUSSION

The deployed model gives a decent enough background to understand how blockchains would be of importance and use in a non-financial scenario. Here are a few screen captures of the output produced by the blockchain protocol with explanations:

Initially the blockchain starts with not entries as shown in Figure 1

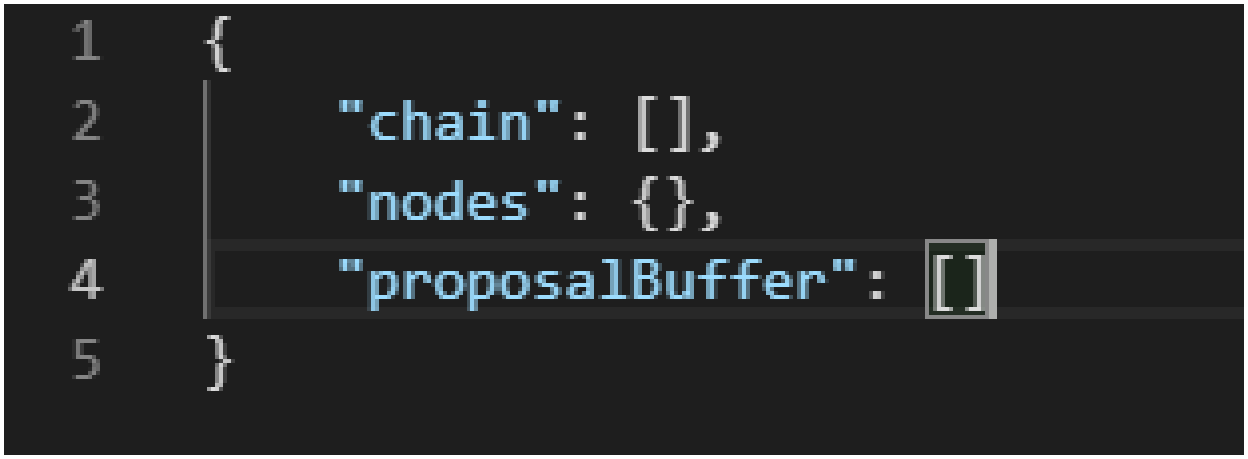


Fig 5.1 Initial View of the Blockchain

Lets add a node to the chain (this will represent an imaginary company called Alpha Pharmaceuticals)

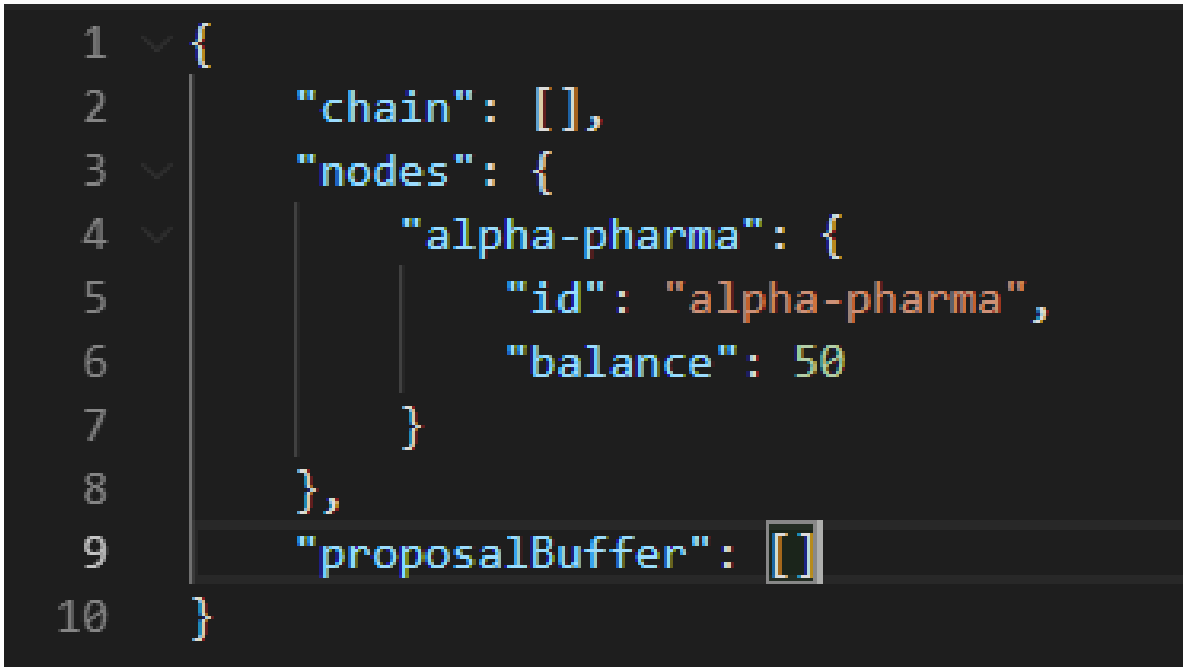
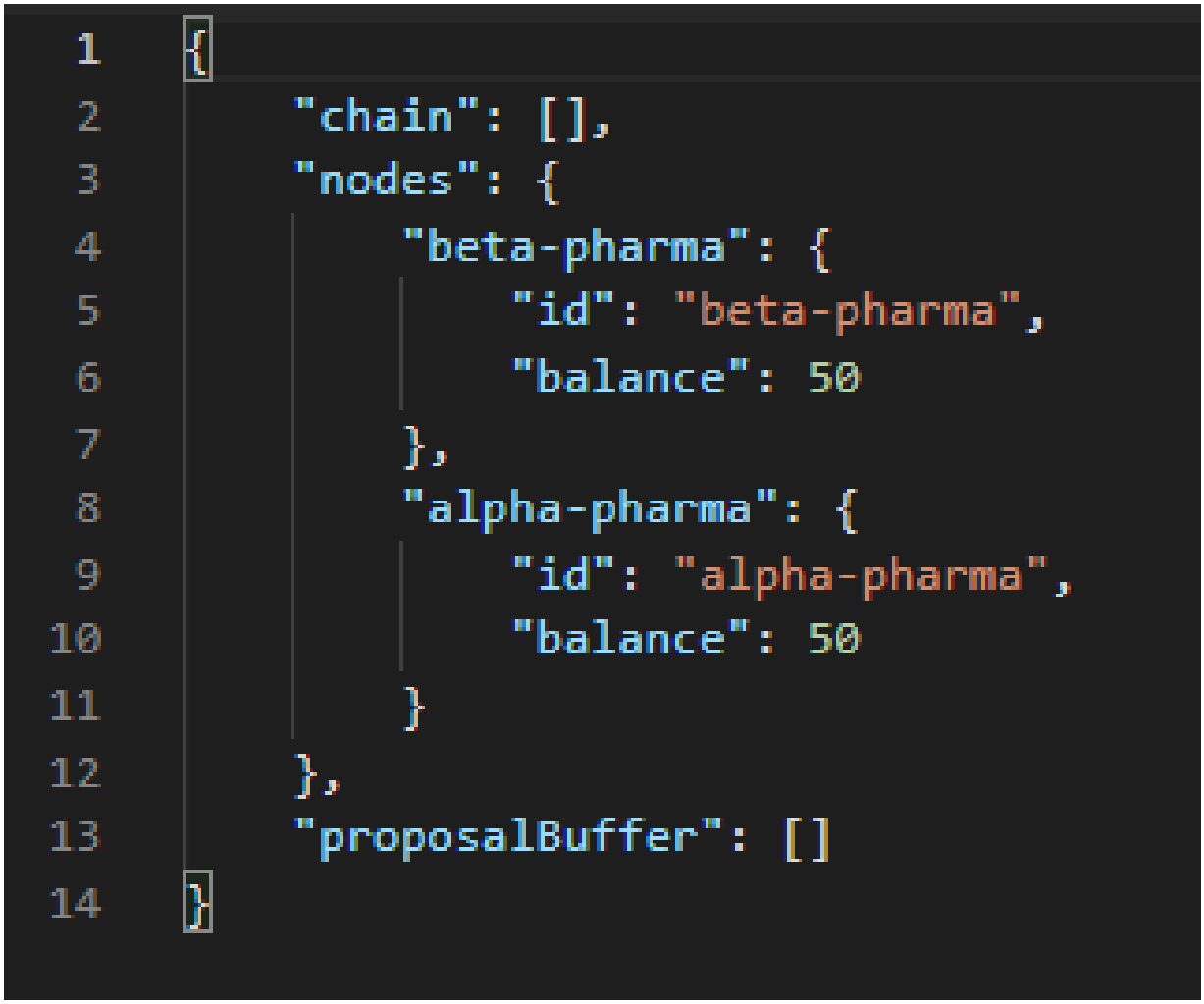


Fig 5.2 First Node Added to the Blockchain

Let’s add another one and call it Beta Pharmaceuticals.



```
{
    "chain": [],
    "nodes": {
        "beta-pharma": {
            "id": "beta-pharma",
            "balance": 50
        },
        "alpha-pharma": {
            "id": "alpha-pharma",
            "balance": 50
        }
    },
    "proposalBuffer": []
}
```

Fig 5.3 Second Node Also Added

Now let's say Alpha Pharma makes a discovery and stakes 10 Reputation Tokens to make a proposal. The balance of Alpha Pharma goes down to 40 Tokens and the proposal gets added to the buffer in return.

```
{
    "chain": [],
    "nodes": {
        "beta-pharma": {
            "id": "beta-pharma",
            "balance": 50
        },
        "alpha-pharma": {
            "id": "alpha-pharma",
            "balance": 40
        }
    },
    "proposalBuffer": [
        {
            "proposer": "alpha-pharma",
            "data": "hydroxychloroquine is not a suitable cure for older people",
            "approvals": [
                "alpha-pharma"
            ],
            "blockId": "29e2f63b-e979-4a8f-ba27-4ac49d21adef"
        }
    ]
}
```


Fig 5.4 Initial View of the Blockchain

Now if Beta Pharma approves the proposal, their id gets added in the proposal approvals in the block inside the buffer.


```
{
    "chain": [],
    "nodes": {
        "beta-pharma": {
            "id": "beta-pharma",
            "balance": 50
        },
        "alpha-pharma": {
            "id": "alpha-pharma",
            "balance": 40
        }
    },
    "proposalBuffer": [
        {
            "proposer": "alpha-pharma",
            "data": "hydroxychloroquine is not a suitable cure for older people",
            "approvals": [
                "alpha-pharma",
                "beta-pharma"
            ],
            "blockId": "29e2f63b-e979-4a8f-ba27-4ac49d21adef"
        }
    ]
}
```

Fig 5.5 Proposal Approved by Beta Pharma

After the stipulated amount of time, the consensus algorithm runs and if more that 50% of nodes approve the proposal, it will get added to the main chain and cleared from the buffer. Also notice that Alpha Pharma gets an additional 5 Tokens along with the initial 10 Token stake back to make a total of 55 Tokens which is greater than the initial amount they had.


```
{
    "chain": [
        {
            "proposer": "alpha-pharma",
            "data": "hydroxychloroquine is not a suitable cure for older people",
            "approvals": [
                "alpha-pharma",
                "beta-pharma"
            ],
            "blockId": "29e2f63b-e979-4a8f-ba27-4ac49d21adef"
        }
    ],
    "nodes": {
        "beta-pharma": {
            "id": "beta-pharma",
            "balance": 50
        },
        "alpha-pharma": {
            "id": "alpha-pharma",
            "balance": 55
        }
    },
    "proposalBuffer": []
}
```


Fig 5.6 Proposal Added to Blockchain

Now lets say Beta Pharma makes a proposal, they also have 10 Tokens deducted from their account.


```
{
    "chain": [
        {
            "proposer": "alpha-pharma",
            "data": "hydroxychloroquine is not a suitable cure for older people",
            "approvals": [
                "alpha-pharma",
                "beta-pharma"
            ],
            "blockId": "29e2f63b-e979-4a8f-ba27-4ac49d21adef"
        }
    ],
    "nodes": {
        "beta-pharma": {
            "id": "beta-pharma",
            "balance": 40
        },
        "alpha-pharma": {
            "id": "alpha-pharma",
            "balance": 55
        }
    },
    "proposalBuffer": [
        {
            "proposer": "beta-pharma",
            "data": "plasma therapy helps cure COVID-19",
            "approvals": [
                "beta-pharma"
            ],
            "blockId": "cff6485e-322e-4eea-85f8-cb1f440c18c1"
        }
    ]
}
```


Fig 5.7 New Proposal by Beta Pharma

Lets say the rest of the nodes don't like the proposal and are not able to reproduce the claim in their own laboratories in the stipulated time. So the proposer will only get 5 Tokens back instead of the staked 10. This will result in a net reduction in the amount of Reputation Tokens that Beta Pharma possesses. This system will penalize the invalid or wrong contributions in COVID-19 Research. The proposal also does not make it into the blockchain.

```
{
    "chain": [
        {
            "proposer": "alpha-pharma",
            "data": "hydroxychloroquine is not a suitable cure for older people",
            "approvals": [
                "alpha-pharma",
                "beta-pharma"
            ],
            "blockId": "29e2f63b-e979-4a8f-ba27-4ac49d21adef"
        }
    ],
    "nodes": {
        "beta-pharma": {
            "id": "beta-pharma",
            "balance": 45
        },
        "alpha-pharma": {
            "id": "alpha-pharma",
            "balance": 55
        }
    },
    "proposalBuffer": []
}
```


Fig 5.8 Bad Proposal Not Added to Blockchain

6 CONCLUSION

Maintaining a blockchain to synchronise COVID-19 research between the different medical organisations across the globe in these tough times will help speed up the process of finding the cure.

We covered how using Proof of Stake instead of Proof of Work would be a better implementation choice for our use case. As the chain grows in size and more organisations join in, the chain will keep becoming better and more secure. The different organisations don't have to worry about hashing powers or maintaining ASICs and can instead use those funds by investing them in Coronavirus research.

The most useful thing about this system is that not only it rewards you for doing good work, but it also punishes those who make mistakes. This is essential for such an important initiative where human lives are at stake.

This system is also harder to exploit as getting 50% of the Reputation Tokens will become much harder that getting 50% of hashing power as the system scales eventually. This is another advantage of having a Proof of Stake (POS) implementation.

7 REFERENCES

1) Fahad Saleh, Blockchain Without Waste: Proof-of-Stake, SSRN, May 2014
2) Evangelos Deirmentzoglou & Georgios Papakyriakopoulos & Constantinos Patsakis, A Survey on Long-Range Attacks for Proof of Stake Protocols, IEEE Access, February 2019, PP(99).
3) Naipeng Dong et al,Formal Analysis of a Proof-of-Stake Blockchain, ICECCS, December 2018.
4) Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin.org, October 2008
5) Sandeep Kumar et al., A Survey Paper on Blockchain Technology, Challenges and Opportunities, **International Journal of Computer Trends and Technology (IJCTT), Volume-67 Issue-4, 2019**
6) David Malone and K.J. O'Dwyer, Bitcoin Mining and its Energy Footprint available at https://www.researchgate.net/publication/271467748_Bitcoin_Mining_and_its_Energy_Footprint, January 2014