Seat Availability System for University Study Areas

by

Ahmed Sameh Ahmed, 119200098
Abdurrahman Ahmetoğlu, 119202016
Mohamad Abo Arida, 119201024
Hamza Sallam, 120200013

Supervised by

Öğretim Görevlisi İnci Çağla Gül Şenkardeş

Submitted to the
Faculty of Engineering and Natural Sciences
in partial fulfillment of the requirements for the

Bachelor of Science

in the
Department of Computer Engineering

May, 2023

Abstract

This project dwells on using and implementing a blockchain system that runs on Quorum into the campus of universities so students can check the availability of seats in determined buildings on the campus. This problem was looked upon because students can face problems in finding seats in universities to study and it usually wastes their time. Moreover, it can help them in organizing study sessions. The system will function with integrity and will deal with possible corruption or abuse in the system. In addition, using two cryptocurrencies with different functionalities the system is more robust since the validators and the users do not deal with the same currency.

Table of Contents

Abstract ii

Table of Contents iii

List of Figures iv

1 Introduction 1

2 Related works 2

3 Methodology 3
- 3.1 Blockchain . . . 3
  - 3.1.1 What is Blockchain? . . . 3
  - 3.1.2 Types of Blockchain . . . 3
  - 3.1.3 What is a Consensus Mechanism . . . 4
- 3.2 Quorum . . . 5
  - 3.2.1 What is Quorum? . . . 5
  - 3.2.2 Consensus Mechanism . . . 5

4 Design 6
- 4.1 System . . . 6
- 4.2 Cryptocurrencies . . . 7
  - 4.2.1 Rizz . . . 7
  - 4.2.2 Baskotaya . . . 7
- 4.3 Blocks . . . 7
- 4.4 Nodes . . . 8
- 4.5 Implementation . . . 8
  - 4.5.1 Penalties . . . 8

5 Current Conclusion & Future Work 9

References 10

List of Figures

1 Classified types of Blockchains from [10] 4
2 Quorum 5
3 How the IBFT mechanism works 6
4 Block example 7
5 Flowchart of the System 9

1 Introduction

Nowadays, people are relying more on online services and transactions since it's safer and more trustworthy for people than physically paying with money, these transactions and services are done efficiently and securely due to not needing a central authority or server[1]. Blockchains come in three types: Public, permissioned, and federated. A public blockchain does not have restrictions and anyone can participate in it. A federated blockchain is a blockchain that's closely controlled by a preselected number of stakeholders. Permissioned blockchain is based upon security and only people who are granted permission from the blockchain can access specific sets of data[2]. This project will be using a form of permissioned blockchain called Quorum.

Quorum is a blockchain protocol that is intended to be used specifically in networks that are either permissioned blockchain networks or private blockchain networks, where one member owns all of the nodes[3] quorum has been widely used in different projects in various fields such as finance, business management, and even genetic engineering. The goal of this project is to create a system in which students can check the availability of a seat in any determined area around the university campus.

The usage of blockchain tech adds so much value over using web 2.0 most prominently the change of web 2.0 being a centralized network to the blockchain tech which will make that a decentralized network meaning it will give more security and privacy to everyone using the application and it distributes the data on the span of a network of nodes making it harder to reach by hackers.

The project aims to provide a fix to the limited seating places in universities that happen because of people boarding seats and not even using them which causes inconveniences for all the other students and staff that are attending the said university.

The white paper is going to be further split into the following sections. Section 2, the Related Works, previous projects that were using quorum that was used as inspiration for this project. Section 3, the Methodology, background information about blockchain, and quorum with its consensus mechanisms. Section 4, the Design and Experimental Setup, talks about the design of the project as a whole and goes into detail about how quorum is used in this project, lastly, Section 5, the Conclusion, concludes the current state of the project and discusses how it would be improved upon in the future.

2 Related works

For the related works, several different projects have already been done using Quorum in various fields which will be used as inspiration for this particular project. The following section gives general information on 4 main projects that we are using to base our proposed project upon in which it combines some aspect of each of these projects in order to build our system.

The first is ERM which is a referral and loyalty platform launched by Emaar , the firm behind the world's tallest building, Burj Khalifa. The platform rewards Emaar customers with EMR token for their loyalty and business referrals. The token could be redeemed for real estate , hotels , ecommerce , malls, etc all owned by the company . Our Seat availability platform uses the same approach, as validators get rewarded with loyalty tokens that could be redeemed on campus for various payment activities.[4]

The second is Everledger which is a London-based startup that uses blockchain technology to create secure and transparent digital records of high-value assets, such as diamonds, fine art, and wine. Everledger uses the Quorum blockchain to maintain a secure and immutable record of diamond ownership and verification. Similarly , Our service maintains secure records of student bookings and validator rewards [5].

The third is Alastria which is one of the largest permissioned, multi-sector blockchain platforms in the world .It provides robust security and privacy features. By leveraging Alastria's privacy and security features, we can ensure that information about student details and booking records is kept secure and only accessible by the validators or the staff.Alastria has also built-in support for tokenization, which might prove to be a good idea for the reward system of the validators.[6].

Lastly is Uqudo which is a digital identity company based in middle east and africa that enables customers to onboard physical id documents to their phone. The platform uses Quorum to ensure the integrity of the physical document and the corresponding digital ID. This project is a huge inspiration for our project as it can help identify the student and staff through their university application or their physical ID cards , which then can be stored in our app as a digital ID.This can help the student to enter the study hall using the app through NFC. and Their identity verification can be checked from the digital ID and the university Database.[7].

3 Methodology

3.1 Blockchain

3.1.1 What is Blockchain?

Blockchain in general is a digital shared ledger that contains certain data and all its history. The system takes all These data and all their information and saves them into a block, it then uses an algorithm to turn the block into a hexadecimal number called the *Hash*. The hash is like a signature of the previous block, it is then added and encrypted with the information of the next block created. The process continues to chain a series of blocks, thus creating a *Blockchain*. A blockchain is in its base similar to a database or a spreadsheet, yet it's different in that it's distributed. Copies of the blockchain are saved for different users (Nodes) creating a *Network*, where all the copies must match for the blockchain to be valid[8].
The first use of blockchains was to create a cryptocurrency; which is an electronic payment system that replaces trust and the need of a third-party with cryptographic proof. It was used due to its security and decentralised record of transactions.

3.1.2 Types of Blockchain

Blockchains networks are separated into two main types, depending on the accessibility it offers, permissionless and permissioned blockchains. A permissionless blockchain is non-restrictive; It allows anyone to become an authorised node by signing on certain platforms, and that by its turn allows the user to access or create data. It also gives the chance to participate in mining activities and to verify transactions. permissionless blockchains are mostly used in cryptocurrency for their decentralisation and transparency, and one of the famous examples is bitcoin.
On the other hand, a permissioned blockchain is restrictive; it is closed or under control of a certain entity. A Permissioned blockchain allows only defined participants to join. It also gives the ability to decide which information would be accessed and which not. This type of blockchains Is usually in companies or organisations, where all participants are defined and known, and not all information is accessed by everyone[9].

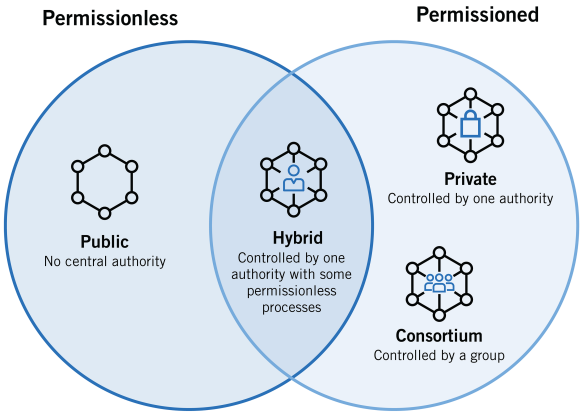

Figure 1: Classified types of Blockchains from [10]

3.1.3 What is a Consensus Mechanism

Furthermore, for a blockchain network to verify data, it needs a determined function, also known as a *consensus mechanism*. A consensus mechanism is the protocol in which is agreed by all nodes to achieve agreement and trust[11]. It determines the method in which the transactions to be verified and who will verify them. Proof of work (POW) is a widely used mechanism, it depends mainly on what are called *Miners*. Miners use high-end computer hardware to solve complicated mathematical puzzles. After solving it a block is created and then sent to other nodes to confirm it, so it can be added to the network. POW is used in bitcoin due to its safety and fair decentralisation, yet it's still relatively slow and energy demanding. Another example is Proof of stake (POS) that was developed later. POS requires users to put their stakes for them to be *Validators* to ensure the honesty of their work. Then the system selects a random validator to validate the process and create the block. POS is way faster and more scalable than POF, yet its only flaw is that it has various validators with more stakes, which limits the decentralisation[12][13]. These are only two examples of many consensus mechanisms that exist nowadays where the use of which will depend on the project itself.

3.2 Quorum

3.2.1 What is Quorum?

Quorum is a branch of the Ethereum blockchain that focuses on enterprise. Quorum was developed by J.P. Morgan to help improve the blockchain industry, and that was mainly by implementing a permission side to the Ethereum blockchain. The highlight of this network is that it ensures data privacy, and that is by using its *Private data identifier* feature. This feature allows the ability to protect some of the transaction's data by controlling who can access it. In addition, Quorum introduced privacy to the smart contracts, a smart contract is basically the program stored in the blockchain that runs when a certain condition is met, which is something that they lacked due to the replicated shared ledgers. These features allow databases in Quorum to be separated as public and private segments.
In addition to its privacy, Quorum is superior when it comes to speed, where it can carry more than 150 transactions per second, thanks to the *Quorum-Chain* consensus mechanism used[14][15][16]. This makes Quorum an ideal choice for systems that require quick and efficient transactions

Figure 2: Quorum

3.2.2 Consensus Mechanism

Quorum is unique, and most of its features are because of the *Quorum-Chain* consensus mechanism used. It is a voting-based mechanism, where only selected nodes can vote, and a majority is needed for the vote to be valid. This mechanism is way faster than proof of work and is very suitable for permissioned networks.
Proof of authority (POA) consensus is widely used in private networks, since it, in short, gives the authorised nodes their fair chance to make new blocks, and not anyone. Quorum-Chain uses mainly Istanbul Byzantine fault tolerance (IBFT) consensus, which is considered to be a modified extension of POA. IBFT was mainly made to deal with faulty nodes, and that is done by what is called a *super-majority rule* where it can tolerate up to 1/3 of faulty nodes. The authorised nodes get the right to vote, being called" *voters*. Each

time a random voter is set to be the “proposer” in which it will process the data and propose a new block, after that the proposed block is sent to all other voters to be checked. If it succeeds in getting a minimum of 66 percent of votes, it then will be valid and will be added to the blockchain. In each run the proposer is decided randomly, to avoid the possibility of it being one of the faulty nodes.IBFT also provides immediate block finality. Since there is only one chain being made the whole time, forking and uncle blocks are removed. All of that makes the effort to create and validate blocks way less, making it less energy-consuming and way faster than other consensus methods[17][18].

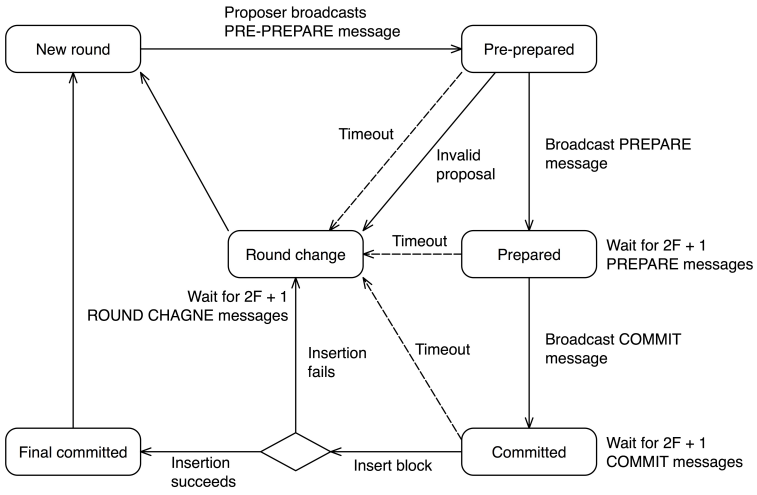

Figure 3: How the IBFT mechanism works

4 Design

4.1 System

The system consists of nodes which deal with cryptocurrency and some preset validator nodes who vote to verify the creation of blocks in order to keep the integrity and purity of the system. The system uses 2 cryptocurrencies , 3 node types all subject to a smart contract which allows the university to view all available information while setting only a few required information to public during the communication of the nodes.

4.2 Cryptocurrencies

This system functions with 2 cryptocurrencies: Rizz and Baskotaya.

4.2.1 Rizz

The currency used to book a place in the area. Users start with 5 Rizz and they spend 1 Rizz on every entry and gain 1 Rizz on every exit after a successful entry. If the User uses up all their Rizz they will be subject to administrative action if they would like to remain in the system. The starting User's balance is set to 5 in case the Users forget to document their exit or in case of any unforeseen circumstances.

4.2.2 Baskotaya

The currency used to buy products around the campus.The Validator earns Baskotaya for every block they successfully took an action towards. Baskotaya can be used all around the campus in various cafes, restaurants or shops. This motivates the staff members to engage in the system since the participation is voluntary.

4.3 Blocks

The block consists of the Timestamp, User Hash, Area Hash, Area Wallet, involved Validator Hashes, Rizz gained/spent by User and Baskotaya gained by the Validators. Figure 4 visualizes an example of the block.

Figure 4: Block example

4.4 Nodes

The nodes are split into 3 categories: User, Validator and Area.

- **User Node**: This node is the Student which deals with Rizz for exit and entry. The student's department is made public while all the other information is set to private.
- **Validator Node**: This node is the Staff who are the validators hence the voters for the system. They deal with Baskotaya and all their information is set to private.
- **Area Node**: This node is the Designated Area which deals with Rizz and all its information is set to public which consists of maximum balance and its current balance. Maximum balance is preset for every Area and current balance starts from 0. The Area cannot gain more Rizz beyond its maximum balance.

4.5 Implementation

The designated campus areas will be equipped with card and NFC scanners for entry and exit similar to those on the campus gates. The Users will scan their cards or NFC from the university app on their phones on entry to any of the areas to create a block in suspension awaiting confirmation and sends a notification to the Validators in the area. The Validators confirm or deny the block based on if the student went into the area or just falsely scanned their card/device. Since the consensus mechanism revolves around a voting system, every area will have a minimum of 3 Validators or a higher odd number. On successful confirmation of the transaction a block will be accepted into the chain and the balance for the Area node will be incremented which will simultaneously update the balance for all the other nodes involved. The Area gains Rizz spent by the Users on entry and gives Rizz to the Users on exit on successful transactions. Figure 5 visualizes the system.

4.5.1 Penalties

To maintain the integrity of the system there will be penalties applied to Students on every denied block which is subject to discussion with the authorities if claimed to be a fault from the Validator side. Furthermore, to avoid abuse of power if the Validators are found unfair in their action towards the block they will lose Baskotaya and will be subject to further punishment depending on the frequency of the faulty action.

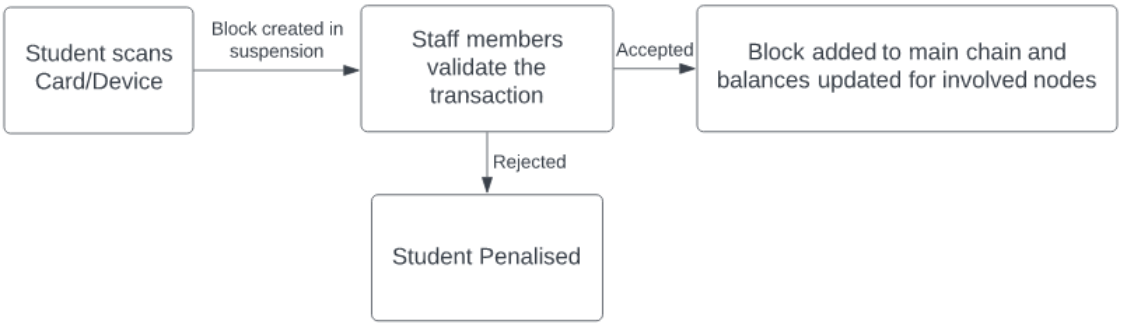

Figure 5: Flowchart of the System

5 Current Conclusion & Future Work

After researching multiple resources for information and implementations, this project is highly efficient for its expected implementation price since card scanners are already available all around the campus hence only implementation of the system is needed. The functionality could be easily integrated into BilgiCampus Mobile application along with allowing NFC for scanning instead of physical cards. Furthermore, it will aid students to socialize since the department information of the students occupying an area will be publicized which help students feel more comfortable sitting with their fellow department mates.

Moreover, this system can further be perfected and improvised upon to be useful for Large AVMs for food court so customers can save time or precheck before going to food court incase of limited seats availability. In addition, it will prove functional in libraries if further improved upon to keep track of members borrowing books or for a large living complex compound with various shops on site.

References

[1] Bitcoin Whitepaper, Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf.

[2] Oracle Website, https://www.oracle.com/middleeast/blockchain/what-is-blockchain/.

[3] Kaleido Blog, https://www.kaleido.io/blockchain-platform/quorum#:~:text=Quorum%20is%20a%20blockchain%20protocol,a%20portion%20of%20the%20network..

[4] Tokenpost blog,17 Oct 2019, https://tokenpost.com/Burj-Khalifa-owner-Emaar-taps-JPMorgans-Quorum-blockchain-for-new-rewards-and-loyalty-platform-3838.

[5] Everledger official website, https://everledger.io/.

[6] Alastria official website, https://alastria.io/en/.

[7] Uqudo official website, https://uqudo.com/features/.

[8] "Blockchain Facts: What Is It, How It Works, and How It Can Be Used ", Adam Hayes, April 23 2023, https://www.investopedia.com/terms/b/blockchain.asp.

[9] "What are the 4 different types of blockchain technology?", Christine Campbell. March 03 2023, https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology.

[10] Jdsupra blog, August 20 2022, https://www.jdsupra.com/legalnews/types-of-blockchain-public-private-or-5282575/.

[11] Cryptopedia Blog, June 28 2022, https://www.gemini.com/cryptopedia/blockchain-technology-explained.

[12] Cryptopedia Blog, March 11 2023, https://www.gemini.com/cryptopedia/blockchain-types-pow-pos-private.

[13] "8 blockchain consensus mechanisms you should know about", Naveen Joshi, April 23 2019, https://www.allerin.com/blog/8-blockchain-consensus-mechanisms-you-should-know-about.

[14] 101 Blockchains Blog, Diego Geroni, June 25 2023, https://101blockchains.com/quorum-blockchain-use-cases/.

[15] LCX Blog, July 22 2022, https://www.lcx.com/a-guide-to-quorum-blockchain/.

[16] GeekforGeeks Blog, https://www.geeksforgeeks.org/quorum-blockchain/.

[17] ConsenSys Blog, June 22 2018, https://consensys.net/blog/enterprise-blockchain/scaling-consensus-for-enterprise-explaining-the-ibft-algorithm/.

[18] Medium Blog, Ryan Golash, https://medium.com/ledgerium-io/ledgerium-blockchain-ibft-consensus-a596b3403bb1#:~:text=Ledgerium%20Blockchain%20uses%20Istanbul%20Byzantine,transactions%20in%20the%20digital%20ledger.