GatorCoin: The University Cryptocurrency

Sai Sanjeev Kumar Reddy Boppidi
Dept. of CISE
University of Florida
Gainesville, Florida, USA
sboppidi@ufl.edu

Sirisha Nelapudi
Dept. of CISE
University of Florida
Gainesville, Florida, USA
sirishanelpaudi@ufl.edu

***Abstract*—This paper presents GatorCoin, a proposed cryptocurrency designed specifically for use within the University of Florida community. Through a proof-of-work consensus mechanism and blockchain technology, GatorCoin offers a decentralized and secure method for transferring value and managing finances for students, faculty, and staff. A detailed description of the currency's technical specifications is provided in the paper, which includes a description of the block mechanism, the transaction process, bootstrapping, and the communication protocol. It also discusses GatorCoin's safety, and liveness, and compares it to existing cryptocurrencies. Furthermore, the paper discusses the everyday uses of GatorCoin, offering a distribution plan and business model. Despite the challenges associated with GatorCoin, including the need to encourage adoption and manage coin distribution, the paper concludes that GatorCoin has great potential as a valuable addition to the University of Florida ecosystem.**

***Index Terms*—cryptocurrency, proof of work, consensus, mining, hashing**

I. Introduction

A cryptocurrency is a digital or virtual currency that uses cryptography to ensure its security and to verify its transactions. A cryptocurrency is decentralized, which means it does not rely on a central bank or government for its operation. They are often referred to as "decentralized digital currencies" or "digital assets." An unknown person or group of people using the pseudonym Satoshi Nakamoto created Bitcoin, the first and most famous cryptocurrency, in 2009. A network of computers around the world verifies bitcoin transactions using a decentralized ledger known as a blockchain.

Cryptocurrencies have been created in thousands since Bitcoin, each with its own unique characteristics. Ethereum, for example, allows developers to build decentralized applications using the blockchain. Dogecoin and Litecoin are considered cheaper and faster alternatives to Bitcoin. As a result of their ability to disrupt traditional financial systems and to facilitate international transactions without requiring intermediaries such as banks, cryptocurrencies have gained popularity in recent years. The trade-off is the risk of price volatility, regulatory uncertainty, and the possibility of fraud and theft.

A cryptocurrency wallet is necessary for real-world use of these cryptocurrencies. This means that cryptocurrency acts not only as a digital currency, but also as an accounting system. With GatorCoin, the consensus mechanism is based on proof-of-work. On the blockchains of cryptocurrencies, new transactions are not verified by centralized gatekeepers like they are on traditional currencies. By using a distributed network of participants, they verify incoming transactions before adding new blocks to the chain. Members of the network use proof of work (PoW) to achieve consensus by solving a hexadecimal number that has been encrypted.

Cryptocurrencies rely on consensus mechanisms to maintain security, decentralization, and trustworthiness. Consensus mechanisms check and validate transactions on a blockchain to ensure that the ledger is updated as agreed upon by all participants. Banking acts as a central authority in traditional financial systems, establishing trust by acting as an intermediary. The use of consensus mechanisms in cryptocurrency, on the other hand, is what allows the same level of trust to be achieved without the involvement of intermediaries.

It is important for cryptocurrencies to have consensus mechanisms for a number of reasons. Their first concern is ensuring the security and resilience of the blockchain against attacks. A consensus mechanism prevents bad actors from manipulating the network by requiring participants to solve complex mathematical problems. A second feature of blockchain is its decentralized nature, which is ensured through consensus mechanisms. Consensus mechanisms prevent any one entity from having too much control over the network by requiring multiple participants to agree on the state of the ledger.

In many cryptocurrencies, including Bitcoin, proof of work (PoW) is used to establish consensus. By solving complex mathematical problems, or "hashing," participants on the blockchain verify transactions. PoW works on the principle that creating a new block on the blockchain requires significant computational effort. Proof of Work refers to a computational effort that must be completed by a user in order to add a new block to the blockchain. It requires a significant amount of computational power to solve the puzzle. The process is known as mining.

An algorithm is used to mine a new block by hashing the data together with a random number known as a "nonce." In mining, a hash is used to create a unique fingerprint of the data and nonce, and the goal is to find a hash that meets a set of criteria, typically a certain number of leading zeros. To ensure that new blocks are consistently added to the blockchain, the network periodically adjusts the difficulty of the mining process. Upon solving the puzzle, miners broadcast their solution once they have found a hash that meets the

criteria. The solution is verified by other nodes on the network and the new block is added to the blockchain if it is valid. As an incentive for solving the puzzle, the miner receives a certain amount of cryptocurrency.

In our paper we are introducing GatorCoin, a cryptocurrency created specifically for the University of Florida. GatorCoin is a digital currency that can be used for various transactions within the university community, including paying for tuition fees, textbooks, and other university services. We want to introduce students as miners in our case of the network. GatorCoin can be mined by any university student. Instead of solving cryptographic hash functions traditionally, we want to gamify the mining process. GatorCoins are earned through logical puzzle solving in our gaming system. To mine GatorCoins, all students of the university would be entertained regardless of their educational qualifications. Control and decision-making are distributed through a distributed network instead of a centralized entity. Money is transferred from one bank account to another using third-party applications, such as Zelle, Paypal or ApplePay. Cryptocurrency has the advantage of eliminating third-party applications for money transfers, which is a major advantage. Students can also transfer GatorCoins among themselves. Using a crypto wallet, students can transfer coins from one to another using a peer-to-peer mechanism. All transactions are recorded in the ledger. Additionally, GatorCoins prevent misuse of the same. Using Gatorcoin is fast, secure, and easy. Transaction fees are low and transparency is high.

II. Literature Survey

Nakamoto[1] introduced the first cryptocurrency: Bitcoin to the world. This paper gives an understanding of the basic principles on which cryptocurrencies depend. They gave an idea of the transaction mechanism, the proof-of-work consensus for cryptocurrency, the process of mining, the usage of disk space, how the payments are verified and many other mechanisms used in a cryptocurrency. Bohme et.al.[2] gave a further ¨ explanation of the design principles, the transaction mechanism, the incentives of mining for the bitcoin miners, and decentralization. The paper also provides us with information on currency exchange, crypto wallets, and mining pools. The paper clearly indicates the journey of how bitcoin was used, is being used, and can be used in the future. Androulaki[3] evaluates the privacy of a bitcoin user. This paper discusses concepts of shadow addresses and addresses unlinkability. Nicolas[4] shows how the mining of a bitcoin can lead to a game-like situation between miners and elaborates on different cases in the mining of the bitcoin. Nicolas has also written a paper on the economics behind the transactions of bitcoin[5]. Here he throws light on different transaction fee scenarios based on size, and fixed. Porat et. al.[6] have explained in detail the proof-of-work consensus mechanism and its applications. Buterin[7] introduces Ethereum, a cryptocurrency, and explains its significance compared to Bitcoin. Chu et.al. [8] used GARCH models to fit them with 7 different cryptocurrencies and evaluated the fits. They concluded in their analysis that the IGARCH and GJRGARCH models fit the cryptocurrencies better than any other GARCH models in terms of volatility. Suratkar et. al.[9] provided an overview of Cryptocurrency wallets which includes the different types of wallets and their features. Kaushal et. al.[10] clearly explains the different security risks involved in crypto wallets. This helps us to pay attention to these issues when we create a wallet for GatorCoins. Albayati et. al.[11] give us an overview of the UI part of the cryptocurrency wallets in their paper. Scholten et. al.[12] explained the mining of cryptocurrencies in the form of games. He named and explained the mechanisms of several popular crypto-games. Shuaib et.al.[13] provide an approach for optimal GPU utilization for mining using Overclocking and Undervolting. Iyer and Pawar [14] mined cryptocurrencies on different CPUs and GPUs and, analysed the financial side of it. This paper throws light on the concepts like hash rates, pool mining, etc. Sonia et.al.[15] discuss the challenges faced by cryptocurrency. They highlight the inconclusiveness of a legal framework for cryptocurrencies, the market risks, and the liquidity of the cryptocurrency.

A. Related Work

Nakamoto's introduction of Bitcoin[1] to the world was a major milestone in the development of cryptocurrency. The accompanying paper lays out the fundamental principles that underpin all cryptocurrencies, including the transaction mechanism, the proof-of-work consensus algorithm that makes cryptocurrency possible, the process of mining, the use of disk space, and the verification of payments. These mechanisms have played a crucial role in the widespread adoption and growth of cryptocurrency as a revolutionary technology.

1) Overview of Proof of Work and its benefits: In universitiy's own cryptocurrecy Proof of Work (PoW) consensus algorithm is implemented in blockchain network. The basic principle used in Proof of Work (PoW)[1] consensus is to validate transactions and create new blocks in the chain. In a PoW system, miners utilize computational power to solve intricate mathematical problems, which enables them to add new blocks to the blockchain. The first miner who successfully solves the puzzle is rewarded with newly created cryptocurrency, and the block is added to the blockchain. The Proof of Work (PoW) algorithm is intended to make it difficult for any person to modify previous blocks or produce fraudulent transactions within the blockchain. This is achieved by demanding a significant amount of computational power to solve the complex mathematical problem associated with PoW. The security of PoW rests on the assumption that an attacker would require more than half of the network's computational power to alter the blockchain successfully, which is commonly referred to as a 51 percent of attack.To perform computationally intensive operations in a PoW system, miners use specialized hardware such as ASICs (application-specific integrated circuits)[16] and GPUs (graphics processing units). It involves running cryptographic algorithms repeatedly until a solution that meets a predefined difficulty threshold is found. Cryptographic algorithms like SHA-256 are used in these

operations. The process of repeatedly running these computations is referred to as mining, and it requires a significant amount of computational power to be successful. By setting a difficulty threshold, the blockchain is designed to add blocks at a steady pace, and the computation power necessary to solve the puzzles increases as network hash rates increase.Whenever a miner solves the puzzle and finds a solution that meets the threshold of difficulty, he or she broadcasts their solution to the network as soon as they have solved the puzzle. Once the solution has been verified, the other nodes in the network will be able to verify that the solution is correct and the new block will be added to the blockchain as soon as the solution has been verified.

In order to reach the next block in the chain, the first miner who is able to solve the puzzle and add the block to it is rewarded with newly minted bitcoins, as well as any transaction fees they have to pay for the transactions included in the block in order to reach the next block in the chain.In general, the PoW consensus algorithm requires a significant amount of processing power and energy in order for it to function smoothly, as it requires a significant amount of computational power. This consensus mechanism has often been criticized for its shortcomings, as it is a poor solution to decentralization and security in blockchain networks, because it is unreliable and insecure.

2) Criticisms of Proof of Work: The Proof of Work (PoW) consensus algorithm has faced criticism for several reasons.Despite these drawbacks, PoW remains a popular consensus algorithm for blockchain networks, particularly fo. cryptocurrencies that prioritize security and decentralization.Some points and a detailed explanation of the criticisms of the Proof of Work (PoW) consensus algorithm:

1) High energy consumption: There is a lot of computing power required for PoW algorithms, which means that they require a lot of electricity to run. Because of this, mining has a high energy requirement, which has raised environmental concerns due to its high energy consumption.
2) Centralization of mining power: Taking part in a PoW network is a challenging task because PoW depends on specialized hardware and a significant amount of computational power, which makes participation in a PoW network challenging for smaller-scale miners. Due to this, there have been a number of large mining pools that have gained all the power and are able to manipulate the network to their advantage. As a result, more and more large mining pools are now able to collude and compromise the network's security.
3) Vulnerability to 51% attacks : The PoW method of mining is vulnerable to an attack called a 51% attack. During a 51% attack, an attacker can take control of more than half of the network's hash rates so that they can manipulate the blockchain's contents to their advantage. It is true that the possibility of such an attack remains low, however, it remains a risk, especially for small networks with fewer miners, in which case it remains a possibility.
4) Slow and resource-intensive: PoW is a resource-intensive and slow algorithm, meaning that it has a limited capacity to process transactions at a given time. As a result, transaction confirmation times and fees are long, since PoW is limited in the number of transactions that can be processed at a given time. Consequently, these limitations have made it less suitable for applications where speed and scalability are vital factors, such as those in healthcare.

Although Proof of Work (PoW) has been effective in securing many blockchain networks, its high energy consumption, centralization of mining power, vulnerability to 51% attacks, and slow and resource-intensive nature have attracted criticisms. To address these concerns, alternative consensus algorithms, such as Proof of Stake (PoS), have been developed. Nonetheless, PoW continues to be a popular consensus algorithm in the blockchain community.

3) Comparison of Proof of Work to other consensus mechanisms: In order to replace Proof of Work (PoW), there have been several consensus mechanisms developed, each of which has its own advantages and disadvantages to offer as an alternative to PoW. Here are a few comparisons between the consensus mechanisms of the PoW and those of other consensus mechanisms:

- Proof of Stake (PoS): PoS is a newer consensus algorithm that is becoming increasingly popular. While PoW relies on miners to solve complex mathematical puzzles by competing against each other, PoS relies on validators which are chosen based on the amount of cryptocurrency they hold and are willing to "stake" or lock up as security to protect the network. A random selection of validators is then made to create new blocks and verify transactions in the block. As a result, minimal energy is consumed and centralization of the mining power is avoided by using this approach. Although PoS certainly has some advantages over PoW, there are still some downsides, like the possibility of attacks involving 51%, that it faces.
- Delegated Proof of Stake (DPoS): The DPoS protocol is a variation of the PoS protocol wherein the blockchain's token holders elect validators for the network. By voting for delegates, token holders have the opportunity to ensure that transactions are verified and new blocks are added to the blockchain as they are verified. In contrast to PoW, DPoS is capable of processing transactions quickly, is not prone to 51% attacks, and is less susceptible to manipulation than PoW. However DPoS has been criticised for being too centralized and more susceptible to manipulation than PoW.
- Proof of Authority (PoA): Essentially, PoA is an algorithm which relies on a small number of trusted nodes to verify the validity of transactions and add new blocks to the blockchain in order to achieve consensus. The validations are chosen based on the reputation or trustworthiness of the individual or organization within the

network. As a fast and energy-efficient protocol, PoA is resistant to 51% attacks, as well as fast and energy-efficient. However, it sacrifices decentralization and is only suited for private or consortium-based blockchains.
- Byzantine Fault Tolerance (BFT):An important aspect of BFT is that it is used as a consensus algorithm that requires a certain number of nodes to agree on a transaction in order for it to be valid. Despite the fact that BFT is fast, efficient, and secure, it is not suitable for large-scale decentralized networks and is typically used by private blockchains that are on a smaller scale.

While PoW still is widely used, the majority of opponents and limitations of PoW are being addressed through a variety of alternative consensus mechanisms that are being developed and implemented to address some of the criticisms and limitations of PoW. There are many different consensus mechanisms available to Blockchain networks, each of which has its own advantages and disadvantages. The selection of one consensus mechanism over another depends on the specific requirements and objectives of each network.

III. Overview

Cryptocurrencies such as Bitcoin and Algos have gained popularity due to their efficiency and the security they provide in transactions. Similarly, GatorCoin aims to provide a secure and reliable platform for transactions. To achieve this, it is crucial to ensure that no single node or user can manipulate the records without affecting the reliability and security of the blockchain. Therefore, GatorCoin needs to use a distributed ledger to hold the log of user node transactions, preventing fraudulent accusations from malicious actors.

To prevent a centralized authority, a consensus mechanism is necessary. The Proof-of-Work (PoW) consensus method is an effective way to achieve this. In PoW, the first node to solve the cryptographic puzzle would lead to the mining of GatorCoin. The cryptographic puzzle is arbitrary in the initializing process of the blockchain, and PoW ensures that a group of nodes can agree on the block initialization. This method is transparent and fair, ensuring that no single node can manipulate the information.

Deploying GatorCoins requires triggering the mining process. Cryptographic hash puzzles are solved by miners who first initialize blocks in the transaction log. A block of data contains the following information:

- In the transaction log, the block number indicates the order of the particular block
- Node-specific data block containing information about the user
- Previous hash information corresponds cryptographically to the previous block of data through pseudo-random generation
- A value called Nonce can be manipulated, which would affect the hash value, which in turn would affect the odds of solving the puzzle.
- Using blocks, previous hashes, data information, and nonce value as inputs, a hashing algorithm generates a pseudo-random number called a hash value.

Hashing is a crucial aspect of cryptography. In hashing, raw information is scrambled to the point where it cannot be reproduced back to its original form. This function passes plaintext through a function that performs mathematical operations on it. A deterministic output exists for any input. In simpler terms, the plaintext is equivalent to the hash value obtained from a hashing algorithm. GatorCoin uses the SHA-256 algorithm for hashing, which ensures that the hash value is always 256 bits, irrespective of the size of the plaintext. Nonces are also used to prevent replay attacks on private communications. GatorCoin can achieve its goals of providing a secure and reliable platform for transactions by using a distributed ledger, PoW consensus method, and SHA-256 hashing algorithm. These measures ensure that no single node or user can manipulate the records, and transactions are transparent and fair to all users.

IV. Design

The GatorCoin project will be built on the Ethereum blockchain and Proof of Work (PoW) consensus mechanism. The university community is welcome to use GatorCoin, which is designed to be a fast, efficient, and accessible digital currency. This platform will be built on Ethereum's blockchain, a flexible and robust platform for building decentralized applications (dApps). On the Ethereum blockchain, GatorCoin uses the ERC-20 standard for creating tokens, which is widely used. A token based on the ERC-20 standard is fungible, which means it can be exchanged for another token sharing the same characteristics.

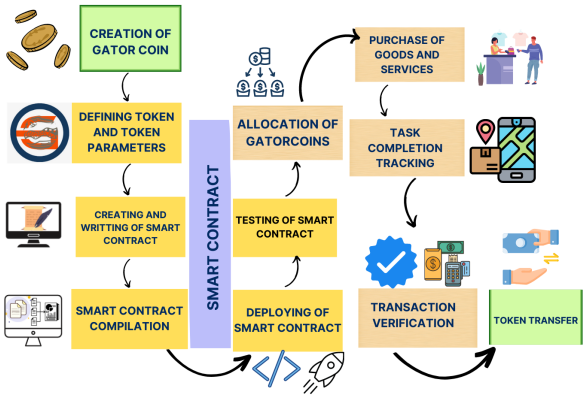

Fig. 1. A flowchart depicting the design of GatorCoin implentation

A. Consensus Mechanism

Many cryptocurrencies, including Bitcoin and Ethereum, use Proof of Work (PoW) for consensus. PoW systems reward the first participant to solve complex mathematical problems

with newly minted coins. Participants in PoW systems compete to solve complex mathematical problems.

The GatorCoin network will be operated by miners, who will process transactions and add new blocks to the blockchain. As a result, they must expend computational power in solving a difficult-to-solve secret puzzle called the "hash puzzle," which can be verified with ease. As part of the hash puzzle, you need to find a nonce, a random number, which, when combined with the transaction data and a reference to the previous block on the blockchain, produces a hash value that meets a certain criteria. The network difficulty determines this criterion, which is periodically adjusted to maintain the same rate of block production.

Until they find a nonce that meets the difficulty criteria, miners must generate millions of possible nonces until they find one that produces a hash value that meets the difficulty criteria. Computing intensively and requiring high levels of energy, mining calls for specialized hardware called ASICs (Application-Specific Integrated Circuits), which are designed specifically for the purpose. The miner broadcasts their solution to the network once they have found a nonce that meets the difficulty criteria, and other nodes on the network verify the solution by checking the hash value. In the case that the solution is valid, a predetermined amount of GatorCoins is awarded to the miner.

GatorCoin benefits from the PoW mechanism in a number of ways. Firstly, it safeguards the network, since tampering with the blockchain would require a significant amount of computational power, so an attacker would not be able to harm the system. The second benefit of the system is that it provides a fair distribution of coins, as anyone with sufficient computing resources can participate in the mining process and receive a reward. Finally, the difficulty adjustment ensures that the rate of block production remains constant regardless of changes in the number of miners on the network, which helps stabilize the network.

B. Blockchain Technology

Ethereum is an open-source blockchain platform that supports smart contracts and has gained widespread popularity. GatorCoin will be built using Ethereum. With smart contracts, terms of the agreement between buyers and sellers will be directly written into lines of code, making them self-executing. As an ERC-20 token, GatorCoin will be created on the Ethereum blockchain in accordance with the standard of creating custom tokens. With this, GatorCoin can easily be integrated with other Ethereum-based platforms and services, such as decentralized exchanges and wallets.

Furthermore, GatorCoin will benefit from high levels of security and reliability due to the Ethereum blockchain's support for custom tokens. An attacker would have a very difficult time manipulating the transaction history or taking control of the blockchain due to its distributed nature. In addition, developers around the world will constantly refine and improve the Ethereum blockchain since it is open-source and community-driven.

C. Smart Contracts

The GatorCoin platform will be powered by smart contracts, allowing numerous processes related to managing and utilizing the cryptocurrency to be automated. As a reward for validating transactions, GatorCoin tokens will be distributed using smart contracts, along with automated payment execution based on the fulfillment of specific conditions.

Our proposal is to utilize Solidity programming language specifically designed for creating smart contracts on the Ethereum blockchain in order to achieve these goals. Similar to JavaScript, Solidity provides developers with powerful programming tools that can be used to create intricate programs that can run on Ethereum Virtual Machines (EVMs).

A variety of applications and services can be built on the GatorCoin network using smart contracts powered by Solidity, including decentralized exchanges, voting systems, and supply chain management tools. Smart contracts are self-executing and self-verifying, which reduces the need for intermediaries, thereby reducing costs, while also increasing transparency and accountability. In order to facilitate secure, transparent transactions on the GatorCoin network and minimize intermediaries' costs, we propose to use smart contracts to construct a robust, decentralized ecosystem based on smart contracts.

D. Governance Structure

As part of GatorCoin's governance structure, we propose it should be decentralized and community-driven, with all participants in the network involved in decision-making. An organization called a decentralized autonomous organization (DAO) will manage GatorCoin, which will be run by smart contracts and operate without the need for a central authority. In addition to setting transaction fees, determining block rewards for miners, and implementing upgrades and improvements to the GatorCoin network, the GatorCoin DAO will be responsible for making decisions related to its development and management. The GatorCoin network will be equipped with a decentralized voting system that allows members of the community to propose changes and vote on them.

In a decentralized governance structure, all decisions are openly and democratically decided upon by all members of the community, thus promoting transparency and accountability. Having a trust-building process in place can help build confidence in the GatorCoin network, which is essential to its widespread adoption. During the initial stages of development, GatorCoin will be governed by an executive board. In addition to representatives from the university community, the board includes experts in blockchain technology and cryptocurrency. GatorCoin's development team is responsible for designing and implementing the technical aspects, such as blockchain technology, smart contracts, and user interfaces.

V. Block Proposal

GatorCoin uses a Proof of Work consensus mechanism to add new blocks to the blockchain, which is a complex and fascinating process. A comprehensive overview of the GatorCoin

blockchain will be provided in this section, covering each step in detail.

A. Transaction Verification

In order to add a block to the blockchain, transaction verification is the first step. To transfer funds between users on the GatorCoin network, users initiate transactions. Every time a user initiates a transaction, it is broadcast to all nodes in the network. Each node in the network verifies the transaction to make sure that it is valid and that the sender has sufficient funds to complete the transaction. During the validation process, GatorCoins are checked to make sure the recipient's address is valid, the transaction adheres to GatorCoin protocol, and the user has enough GatorCoins to complete the transaction. The nodes reject invalid transactions, and they are not added to the blockchain if they are deemed invalid.

GatorCoin transactions contain the public key of the sender, the public key of the recipient, and the amount being transferred. The blockchain ledger must be checked against each transaction to ensure the network's integrity. Suppose Alice wants to send Bob 10 GatorCoins, and the nodes on the network have to validate her transaction. It is checked by the nodes whether Alice has enough GatorCoins to send to Bob based on her GatorCoin balance. The transaction is deemed valid if her balance is sufficient, and it is included in the new block.

GatorCoin is a network that uses a distributed ledger, which means that each node maintains a copy of the entire blockchain ledger. This method guarantees transparency and verifiability of transactions, as well as a decentralized control system.

B. Pooling

Upon verification, a transaction is added to a pool of unconfirmed transactions awaiting inclusion in a block. It is managed by nodes within the network, which monitor the pool and add transactions to it as they arrive. In the pool, unconfirmed transactions are temporarily stored until they are added to the blockchain.

C. Block creation

A miner creates a new block containing the unconfirmed transactions after a sufficient number are added to the pool. A miner is a node on the network that is responsible for adding new blocks to the blockchain. In order to create a new block header, the miner must choose which transactions to include in the block, and create a new hash value of the previous block, along with a random nonce value. There are several steps involved in creating a block, including:

- Miners select which transactions to include in a new block based on the transaction fee and the priority of each transaction.
- Miners create block headers that include previous blocks' hashes, Merkle tree root hashes, timestamps, and nonces.
- New blocks are added with a special transaction called a coinbase transaction by the miner. Miners are rewarded with GatorCoin for adding blocks to the blockchain with this transaction.
- Miners create block headers that include previous blocks' hashes, Merkle tree root hashes, timestamps, and nonces.
- New blocks are added with a special transaction called a coinbase transaction by the miner.
- A block size limit is set by the miner to prevent block sizes from exceeding it. The maximum block size limit for GatorCoin is 1 MB.

D. Solving the Cryptographic Puzzle

Once a block has been created, the miner attempts to solve a cryptographic puzzle that is specific to the GatorCoin blockchain. The puzzle is designed to be difficult to solve and requires significant computational power. The puzzle is a cryptographic hash function that takes a block of data as input and outputs a fixed-length string of characters. Security Hash Algorithm 256-bit (SHA-256) is the PoW algorithm used in GatorCoin's blockchain. Using this algorithm, miners must find a hash value for the block header that is below a certain target value. To ensure a reasonable rate of new blocks being added to the blockchain, the target value is set by the network and adjusted periodically. GatorCoin adjusts its difficulty level approximately every two weeks, or every 2016 blocks.

The process of solving the cryptographic puzzle involves trial and error. The miner must test different nonce values until they find one that produces a hash value that meets the given criteria. The miner with the fastest and most powerful computer is more likely to find the correct nonce value first and solve the puzzle. Besides the transactions, the miner adds a special transaction called a coinbase transaction to the block. A GatorCoin is given as a reward to the miner for adding the block to the blockchain as part of the coinbase transaction. As a result of this reward, miners are motivated to keep adding new blocks to the blockchain, ensuring the network's security.

E. Adding the Block

The new block is added to the blockchain once a miner solves the cryptographic puzzle. The other nodes on the network must verify that the new block is valid once it has been added to the blockchain. In order to verify the PoW algorithm solution, the block must contain valid transactions and the PoW algorithm solution must be correct. By checking the hash of each new block, which includes the block header and transactions, each node independently verifies the block. It broadcasts the block to the rest of the network if the hash is valid. A node rejects a new block that has an invalid hash and does not add it to the blockchain if the hash is invalid.

F. Broadcasting

Once a new block has been verified, it is broadcast to the other nodes in the network. Every node on the blockchain gets a copy of the new block via the broadcast process, which allows them to update their ledgers of the blockchain. Decentralization and security of the GatorCoin blockchain are maintained through the broadcast process. With GatorCoin, all

nodes on the network receive new blocks, ensuring that there is no single point of failure and that the blockchain is not susceptible to attack.

VI. GatorCoin

This section discusses how GatorCoin addresses higher-level issues arising from the primitives we have described so far.

A. Block Format

As we discussed earlier, blocks contain the block number, nonce, data, previous hash, and current block hash. Adding your block to the blockchain requires solving a cryptographic puzzle since we use Proof of Work consensus. In the cryptographic puzzle, the objective is to have a hash value lower than the target hash. Targets are generally expressed in terms of leading zeros. Blocks are hashed using SHA-256 algorithms based on block numbers, data, previous blocks' hashes, and nonces. It is only possible for the user to change the nonce value in order to solve the puzzle. In order to achieve the target hash, users cannot use shortcuts with SHA-256. Neither the user nor the computer can predict which nonce value will result in a hash below the target. Increasing or decreasing the nonce value does not guarantee obtaining the golden hash, even if the hash value is very close to the target hash. As shown in Figure 1, the hash obtained by incrementing or decrementing very few units may be much larger than the previous one. This effect is called the avalanche effect. Therefore, there is no shortcut to obtaining the golden hash. As for the rest of the contents of the block, they remain the same. A user tries changing the nonce until they reach a hash value below the target hash in order to solve the puzzle. The user who is fastest to achieve the hash value below the target hash will have their block added to the blockchain once they have achieved it. For adding a block to the blockchain, the user receives a certain amount of cryptocurrency. Every block goes through the same process.

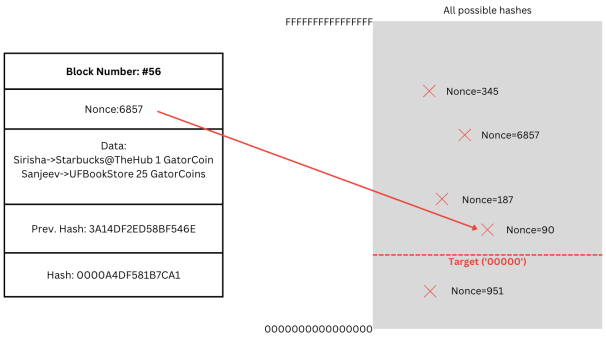

Fig. 2. Example demonstrating Avalanche effect in changing values of nonce.

B. Safety and Liveness

Cryptocurrency networks' security and reliability are largely determined by their safety and liveliness. Keeping the network safe means preventing double-spending and ensuring the integrity of transactions, while keeping the network live means processing transactions and adding new blocks on a timely basis. A combination of PoW consensus, network architecture, and incentives is used to ensure GatorCoin's safety and liveness.

1) Safety: With GatorCoin's PoW consensus mechanism, transactions are guaranteed to be authentic and prevent double-spending. PoW ensures that each new block added to the blockchain contains valid transactions by requiring nodes to solve complex mathematical problems. Furthermore, GatorCoin's network architecture minimizes the risk of a 51% attack, which could compromise the blockchain's integrity. Distributed nodes control the network, so no single node has control over it.

2) Liveness: In order for the GatorCoin network to remain live, consensus is implemented using the PoW algorithm, which ensures that blocks are generated consistently and predictably. At regular intervals, new blocks are added to the blockchain, with each block taking approximately 10 minutes to mine. Furthermore, GatorCoin's incentive system ensures that nodes are financially motivated to maintain the network and process transactions. Nodes are motivated to participate in the network by receiving rewards for mining new blocks.

C. Bootstrapping the network

In the process of bootstrapping, a new blockchain network is created and the first block is added. The first block of GatorCoin is created by bootstrapping a new blockchain network designed specifically for the University of Florida. There are several steps involved in bootstrapping GatorCoin:

1) Setting up the network: Bootstrapping GatorCoin begins with setting up a network of nodes that will participate in the blockchain. Members of the University of Florida community, such as students, faculty, and administrators, can run these nodes.
2) Creating the genesis block: In order to start creating the GatorCoin blockchain, we need to create the genesis block. A blockchain begins with the genesis block, which does not contain any transactions.
3) Distributing the genesis block: The genesis block needs to be distributed to all nodes on the network once it has been created. There are a number of ways of doing this, such as sending an email or sharing a file.
4) Starting the network: In order to create a peer-to-peer network, the nodes on the network need to start running GatorCoin software after the genesis block has been distributed.
5) Mining the first block: The first block in the GatorCoin blockchain is mined by nodes as soon as the network is up and running. Adding transactions to the first block involves solving the PoW algorithm.
6) Adding the first block: The first block can be added to the blockchain once the first block has been mined successfully. The GatorCoin blockchain has officially been launched.

A blockchain network's bootstrapping is an important first step in establishing trust and consensus between its participants. A bootstrapped GatorCoin blockchain enables students, faculty, and administrators at the University of Florida to make transactions as well as use GatorCoin to pay for university services.

D. Bootstrapping New Nodes

The bootstrapping process for new GatorCoin nodes involves following a specific process, which synchronizes them with the existing blockchain. A new node can be bootstrapped into the GatorCoin network by following these steps:

1) Install GatorCoin software: Installation of GatorCoin software is the first step to joining the GatorCoin network as a new node. With this software, all the components necessary for participating in the blockchain network are included.
2) Connect to the network: The new node must be connected to the GatorCoin network once the software has been installed. A new node can access the current state of the blockchain by connecting to existing nodes on the network.
3) Download the blockchain:To synchronize with the existing network, the new node must download the entire blockchain after connecting to the network. The speed of the internet connection as well as the size of the blockchain can affect the time required.
4) Verify the blockchain: To ensure that the blockchain matches the existing blockchain, the new node must verify its integrity once the blockchain has been downloaded. Checking the validity of each block and its transactions is part of this process.
5) Start participating in the network :GatorCoin nodes can begin participating in the network after the blockchain has been verified. It involves verifying transactions, mining new blocks, and broadcasting new blocks to other nodes.

E. Communication

A key aspect of GatorCoin's network architecture is its communication protocol, which facilitates communication between nodes and ensures that the blockchain is current and consistent throughout. GatorCoin uses a peer-to-peer (P2P) protocol for transmitting data between nodes, similar to the Bitcoin network's protocol. In GatorCoin's network, nodes communicate directly with each other in a distributed P2P topology. With no centralized point of control, this allows for a decentralized network. To establish connections with other nodes on the network, nodes exchange information about the network, such as IP addresses and port numbers, during a process called "node discovery." Nodes broadcast information about newly created blocks and transactions when they receive them from their connected nodes. Nodes in the network propagate this information until it has been received by all of them. The blockchain is therefore consistent across all nodes, and transactions and blocks can be validated. GatorCoin's PoW consensus mechanism relies heavily on its communication protocol. New blocks are verified by nodes using the communication protocol and included in the blockchain if they meet the criteria. During this step, the proof-of-work algorithm and transaction validity of the block are checked. To ensure nodes are able to recover from errors or network disruptions, the communication protocol also includes error handling mechanisms. In the event that a node cannot receive a block or transaction during the normal propagation process, they can request the missing blocks or transactions from their connected nodes.

F. Functionalities and Business Model

University of Florida students, faculty, and staff can use GatorCoin daily since it is a cryptocurrency designed specifically for the university community. Payments for tuition fees can be made with GatorCoin instead of bank transfers or credit card payments. As a result, students can pay for their education in a convenient and secure manner. Parking, housing, and dining services can be paid for with GatorCoin. It eliminates the need for cash or credit cards for payment and provides a convenient method of payment for students and faculty. Using GatorCoin, students, faculty, and staff can conduct peer-to-peer transactions. By eliminating intermediaries such as banks and payment processors, this allows you to transfer value quickly and securely. GatorCoins are rewarded when students

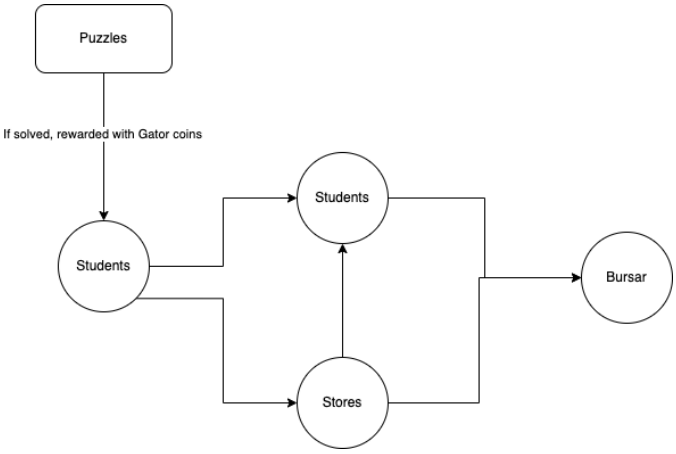

Fig. 3. A rough flow of transactions of GatorCoin

solve puzzles in the gaming system. In addition to being able to use the GatorCoin mined at any store, students can also transfer it to fellow students. Clubs and organizations within the university may also donate Gatorcoins instead of gifts. Students can receive GatorCoins instead of meal passes from stores such as Dining Services, as we discussed previously. On campus, GatorCoins can be used to purchase UF merchandise, food, and other items. These coins can be encashed at the Bursar by the stores. By considering the profit the university will make from using these coins, we can lay the foundation for a business model where there is a small transaction fee for every purchase. Energy consumption for mining can be

funded by this profit. Additionally, mining these coins makes it easier for the university to manage its idle GPU computing power.

ICO (Initial Coin Offering) will be used to issue GatorCoins. To raise funds for their projects, startups and organizations use an ICO. A cryptocurrency ICO involves investors purchasing cryptocurrency tokens in exchange for cryptocurrencies, such as Bitcoin and Ethereum. There will be clear terms and conditions for participation in the GatorCoin ICO, which will be transparent and accessible to all potential investors. GatorCoin will be launched with the funding from the ICO, along with creating liquidity for the cryptocurrency.

There will be a total supply of 1 million tokens of GatorCoin. Following is the distribution of tokens:

- 30% of tokens will be distributed during the ICO
- 40% of tokens will be reserved for the University of Florida community
- 20% of tokens will be reserved for the development team and advisors
- 10% of tokens will be reserved for marketing and promotions

As part of the University of Florida community, tokens will be used to reward students for their achievements, fund research and innovation, and support various university initiatives and projects.

In order to facilitate secure and efficient transactions for businesses and individuals, GatorCoin follows a business model centered on facilitating secure and efficient transactions. GatorCoin could act as a payment processor, offering cheaper and faster transactions than credit cards or wire transfers. GatorCoin's business model is as follows:

- GatorCoin Payment Processor: Business owners can accept GatorCoin as a payment method by using GatorCoin's payment processing service. Businesses can integrate GatorCoin into their existing payment systems, and customers can use GatorCoin to pay for products and services. For each transaction processed, GatorCoin could charge a small fee, generating revenue.
- GatorCoin Wallet: With its digital wallet, GatorCoin provides users with an easy and secure way to manage, store, and spend their GatorCoins. An online wallet could feature two-factor authentication, multi-signature transactions, and integration with popular online marketplaces. Each transaction conducted through the wallet could generate revenue for the university.
- GatorCoin Merchants: Customers who pay with GatorCoin will receive discounts or rewards from merchants who accept GatorCoin. By adopting GatorCoin as a form of payment, more businesses and individuals could benefit from its use and value.

VII. Discussion

A. Proposed cryptocurrency vs Existing cryptocurrencies

As of now, GatorCoin is using the Proof of Work (PoW) consensus mechanism, which is the same consensus mechanism that is used by Bitcoin and Litecoin, which are both cryptocurrencies that are presently being developed. A comparison between GatorCoin and some of the existing cryptocurrencies that also use the PoW consensus mechanism would be an important step towards understanding the potential advantages and disadvantages of this coin.

Bitcoin, the most popular PoW-based cryptocurrency, has a limited supply of 21 million coins. The block reward halves every four years, and it currently stands at 6.25 BTC per block. Bitcoin has a market cap of over $1 trillion and is traded on various cryptocurrency exchanges despite the high network difficulty of around 26 trillion.

Ethereum is a significant PoW-based cryptocurrency that is transitioning to a PoS consensus mechanism. It has a faster block frequency of around 15 seconds and a more flexible and programmable blockchain. Ethereum currently has a block reward of 2 ETH per block and a network difficulty of around 9 trillion. It has a market cap of over $400 billion and is traded on various cryptocurrency exchanges.

Litecoin is a faster and more efficient version of Bitcoin, created in 2011. It uses a similar PoW algorithm with some modifications, has a shorter block time of 2.5 minutes, and a total supply of 84 million coins, four times more than Bitcoin. Litecoin has a block reward of 12.5 LTC per block and a network difficulty of approximately 10 billion. It has a market cap of around $10 billion and is traded on several cryptocurrency exchanges

Compared to other cryptocurrencies, GatorCoin has potential advantages such as a specific use case within the University of Florida community, lower total supply, and an opportunity to build a strong community and new use cases specific to the university.

B. Limitations

It is essential to acknowledge that this study has certain limitations, as with any research project. The primary limitation is that our investigation focused mainly on the technical aspects of GatorCoin, and we did not delve into the social, economic, or political factors that could potentially influence its adoption and usage within the University of Florida community. To gain a more comprehensive understanding of GatorCoin's feasibility, further research could investigate these factors in greater depth. This may involve examining the viewpoints and attitudes of students, faculty, and university administrators regarding cryptocurrencies, and how these attitudes could shape the adoption of GatorCoin.

Another limitation of our study is that we did not perform an exhaustive analysis of various cryptocurrencies that utilize Proof of Work. Although we compared GatorCoin with some of the popular cryptocurrencies, there are numerous others that may also be suitable for comparison. Future research may address this issue by conducting a more thorough examination of various cryptocurrencies and investigating how they compare with GatorCoin concerning factors such as block time, difficulty level, and market capitalization.

As a final note, although discussing some of the potential benefits and challenges associated with the introduction of a new cryptocurrency, the broader implications of cryptocurrencies and their impact on society as a whole are yet to be discussed. During future research, it is possible to examine the role that cryptocurrencies are likely to play in the future, including their potential impact on financial systems, government regulation, and the privacy of individuals.

C. Future Research

One area that could be explored in terms of suggestions for future research is the possibility of GatorCoin being able to be used for other purposes apart from paying for tuition and university services, which would be an interesting area to explore in the near future. This could be used, for instance, to encourage students to participate in research studies or to facilitate the exchange of information between educators and students, for example, to encourage students to participate in research studies.

Moreover, future research could explore the possibility of integrating GatorCoin with other blockchain-based systems, such as those that are involved with credentialing and student records, in order to explore the potential of cryptocurrency.GatorCoin is one of the cryptocurrencies that uses Proof of Work to verify its transactions, and as such the environment is another area that could be researched. It is true that a Proof of Work protocol is well-established as a method of consensus, but it is also associated with high levels of energy consumption, which is potentially harmful to the environment. The topic of future research could include ways to reduce the environmental impact of cryptocurrencies, such as by using renewable energy sources or developing more energy-efficient consensus mechanisms that could be developed in the future to reduce the environmental impact of cryptocurrencies.

VIII. Conclusion

In Conclusion, GatorCoin would be able to benefit the community at University of Florida in a variety of ways. Using blockchain technology, GatorCoin offers students, faculty, and staff a secure and decentralized method of transferring value, managing finances, and investing. Proof-of-work consensus ensures network integrity and reliability, as well as motivating miners to participate in mining processes and secure the network. In addition to being a versatile and convenient payment method for members of the University community, GatorCoin could be used for a variety of everyday transactions, such as tuition payments, purchases, and charitable donations.

There are several technical and practical challenges associated with the implementation of GatorCoin, such as ensuring network security, promoting adoption, and managing coin distribution, but the currency's potential benefits make it a promising research and development topic in the future. For students, faculty, and staff at the University of Florida, GatorCoin may prove to be a reliable and efficient financial management tool with further study and refinement.

References

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[2] Böhme R, Chirstin N, Edelman B (2015) Bitcoin: economics, technology, and governance. J Econ Perspect 29(2):213–238. https://doi.org/10.1257/jep.29.2.213

[3] Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S. (2013). Evaluating User Privacy in Bitcoin. In: Sadeghi, AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg.

[4] Houy, Nicolas, The Bitcoin Mining Game (March 11, 2014). Available at SSRN: http://dx.doi.org/10.2139/ssrn.2407834

[5] Houy, Nicolas, The Economics of Bitcoin Transaction Fees (February 24, 2014). GATE WP 1407, Available at SSRN: http://dx.doi.org/10.2139/ssrn.2400519

[6] Porat, Amit et al. "Blockchain Consensus : An analysis of Proof-of-Work and its applications." (2017).

[7] A next-generation smart contract and decentralized application platform". V Buterin. 2014. weusecoins.com white paper.

[8] Chu J, Chan S, Nadarajah S, Osterrieder J (2017) GARCH modelling of cryptocurrencies. J Risk Financ Manag 10:17.

[9] S. Suratkar, M. Shirole and S. Bhirud, "Cryptocurrency Wallet: A Review," 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 2020, pp. 1-7, doi: 10.1109/ICCCSP49186.2020.9315193.

[10] P. K. Kaushal, A. Bagga and R. Sobti, "Evolution of bitcoin and security risk in bitcoin wallets," 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, India, 2017, pp. 172-177, doi: 10.1109/COMPTELIX.2017.8003959.

[11] Albayati, H., Kim, S. K., Rho, J. J. (2021). A study on the use of cryptocurrency wallets from a user experience perspective. Human Behavior and Emerging Technologies, 3(5), 720– 738. https://doi.org/10.1002/hbe2.313

[12] Scholten, Oliver Hughes, Nathan Deterding, Sebastian Drachen, Anders Walker, James Zendle, David. (2019). Ethereum Crypto-Games : Mechanics, Prevalence and Gambling Similarities. 10.1145/3311350.3347178.

[13] Shuaib, Mohammed Badotra, Sumit Irfan Khalid, Muhammad Algarni, Abeer Ullah, Syed Sajid Bourouis, Sami Iqbal, Jawaid Bharany, Salil Gundaboina, Lokesh. (2022). A Novel Optimization for GPU Mining Using Overclocking and Undervolting. Sustainability. 14. 8708. 10.3390/su14148708.

[14] S. G. Iyer and A. Dipakumar Pawar, "GPU and CPU Accelerated Mining of Cryptocurrencies and their Financial Analysis," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, 2018, pp. 599-604, doi: 10.1109/I-SMAC.2018.8653733.

[15] Arsi, Sonia Khelifa, Soumaya Ghabri, Yosra Mzoughi, Hela. (2021). Cryptocurrencies: Key Risks and Challenges.

[16] CARLA TARDI. (2022) Application-Specific Integrated Circuit (ASIC) Miner. https://www.investopedia.com/terms/a/asic.asp