Navigating the Consensus Landscape: A Comparative Analysis of Security and Consensus Algorithms of Ethereum in the Modern World

Ashton Thomas, Chaewon Kim, and Jingyi Sun

University of Michigan, EECS 475: Cryptography, Prof. Mahdi Cheraghchi

December 7, 2023

1 Introduction: The Evolution of Currency

Before the era of currency, humanity relied on bartering, the direct exchange of goods or services without a medium of exchange. However, as civilizations and their trading networks flourished, the need for a medium of exchange increased and led to the birth of currency.

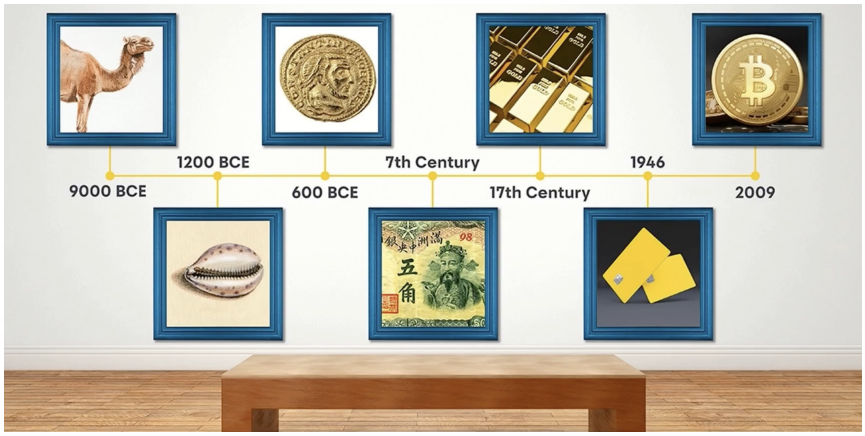

Figure 1: Currency Timeline

The earliest forms of currencies included beads, shells, and gems; materials that stood out from everyday objects for their rarity. They were also more portable compared to crops and livestock. As civilizations progressed and their population grew, the production rate of those kinds of currency could not satisfy the increasing demand for them.

Societies resolved the problem by mass producing metallic forms of currency, or as what it would be called in modern world, coins. They used rare metals like gold and silver to secure the rarity a currency should have, and stamped faces of authority figures to ensure additional importance and mark validity within the local economy.

Metallic currency was not the only currency that could be mass produced. Considering the fact that paper was invented in China during the Han dynasty, it should not be surprising that the first prototype of paper currency was invented in the Tang dynasty of China. Eventually paper currency entered circulation, but not until the Song dynasty. Over the centuries, the papermaking technology and paper currency spread to the West, first the Islamic world and then Europe.

Since paper currency is cheaper and simpler to produce, as well as lighter and more portable, its usage became more widespread than that of coins. Despite its name, paper currency is not made solely of paper anymore. Nowadays, it is more often made of several compounds such as cotton fibers, linen or plastic, which are more durable than paper.

The introduction of computer technology, often represented by the Internet, encouraged the evolution of currency and the financial system. Non-cash and nonphysical payment methods such as credit cards, web banking and mobile payment apps have become prevalent. There is also less need to visit the bank, since only a few taps on a phone can make an electronic payment.

However, computer technology never stopped evolving, and the currency and financial system has evolved alongside it to introduce an unprecedented digital financial system: cryptocurrency.

2 The Rationale for Decentralization

As briefly mentioned in the introduction, present-day bank systems might have become more convenient thanks to digital technology, but not necessarily safer and more reliable – any modern centralized financial system comes with many potential problems.

Centralized systems are often inefficient, as only a few users are selected to have control in decision making, and those control and the ownership over data and wealth are often not evenly distributed. There is no guarantee that those in control of the financial system would always make the decision that's in the best interest of the public. The main reason we have this system where a select few control these decisions is because it is difficult to derive a consensus from the public. One notable example was the PRISM program, where the United States National Security Agency gave authority to the U.S. government to access personal information of individuals. One of the greatest challenges a centralized system faces is achieving a balance between the security of the general system and freedom of an individual.

Suppose there exists a decentralized system where the masses are given equal control and the transfer of money is as efficient as possible, with optional privacy and without the possibility of fraud. With the introduction of Bitcoin this supposition became reality.

There are several benefits of decentralization. First, it allows the public to choose what's best, rather than a central figure. Also, it is more financially inclusive, since some people might not have access to traditional banking. In addition, it reduces cost, efficiency, and inflation risks – in a centralized economy, inflation is controlled by a small number of people, thus risk management is less efficient. However, as mentioned earlier, the control is equally distributed among the mass in a decentralized economy, so the risk can be managed more efficiently.

3 The Bitcoin Whitepaper and the Birth of Cryptocurrencies

In 2008, Satoshi Nakamoto published a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System", where he wrote the outline of the first blockchain cryptocurrency named Bitcoin. Bitcoin is a type of cryptocurrency that is based on Blockchain, a public database with a data structure that resembles a linked-list and utilizes a secure and decentralized ledger to enable safe decentralized transactions. Nowadays, most cryptocurrencies such as Ethereum are based on this idea of the Blockchain.

Bitcoin can be described as a chain of digital signatures that are stored on the Blockchain. Whenever an owner transfers a coin to a recipient, the transaction is recorded on a collective block. This new block is appended to the end of the Blockchain, then a hash of the previous block is stamped onto this new block in the chain. The transaction itself is signed by both the private key of the previous owner and the public key of the new owner as a way to verify the transfer of ownership.

In order to verify the validity of a transfer and avoid double spending, Nakamoto proposed an authority model that can accurately determine whether a transfer is valid without a centralized authority. In this model, all transactions are made public, and the built-in system allows every participant to vote whether a transaction should be deemed valid or invalid.

This model stores the information in the Blockchain, similar to a linked-list, in that it can be assumed that any transaction contained in a block that is linked as a previous block in the Blockchain has been executed earlier than the current block. Now since each transaction is publicly announced, then any participant who can view the Blockchain can use the timestamp information from each block to track the relative time between transactions.

An accurate estimate of the validity of each transaction can be made via Proof-of-Work (PoW), a consensus mechanism that aims to validate transactions to maintain integrity, security, and trust in the decentralized system.

To show how the transactions are communicated, Nakamoto designed a network that interconnects the Web to achieve a synchronized system by following these steps:

1. All transactions are published.
2. Every computer on the Blockchain collects transactions into a block.
3. Every computer tries to verify the block through a complicated Proof-of-Work puzzle.

4. When a computer finishes solving the puzzle, it will broadcast the block to every other computer.

5. Every computer collectively votes to accept the new block as long as all the transactions inside are valid and not spent.

6. The computers evaluate the acceptance of the new block and append it into the chain if accepted.

This effectively allows for the system to stay within consensus and lay the foundation for a system that is able to work in unison with a decentralized authority.

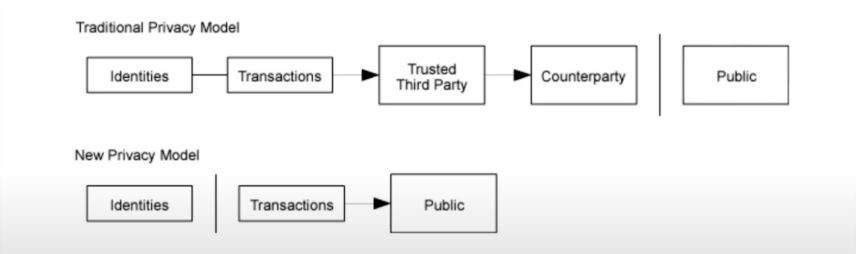

Figure 2: Bitcoin Security

However, this system seems to lack privacy. Nakamoto proposed a simple solution: making the keys anonymous and private, so the personal information would be secured. Yet it is not a flawless solution – it might significantly lower the danger of personal information leakage, but it's never zero. For example, transactions can be linked to a common wallet and raises the risk of leaking information about transactions, which should remain private only to the sender and the receiver, to the public. The simple solution to resolve this problem is to generate a new key pair for each and every transaction to avoid it being linked to any public owner. Thus transactions are ensured to be visible for verification and trust, and personal information remains protected, upholding the core principles of decentralized systems.

4 Blockchain: The Math Behind the Unbreakable Ledger

The name "Blockchain" conveys two ideas: data and states are stored in consecutive groups (called "blocks") and each block cryptographically references its parent (i.e. getting "chained" together).

Fundamentally, a blockchain is a digital ledger–an expanding list of blocks of which are linked together. Every block within the Blockchain contains the hash of the previous block, a timestamp, and a dataset, typically of a transaction. The mechanism of constructing the blocks and linking them together in the blockchain ensures that Blockchain is transparent and can be distributed to the public, but also maintains high security, as a set of data becomes nearly unchangeable once it is recorded.

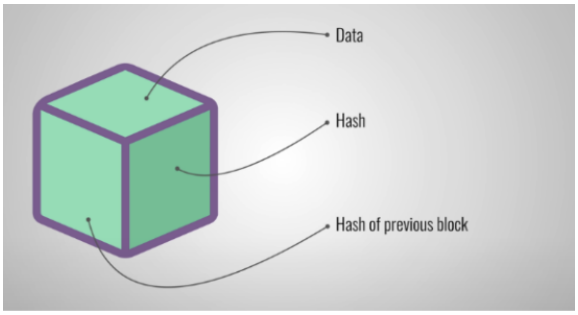

Figure 3: Block Components

The first block of the blockchain, called the Genesis Block, can contain various sets of data depending on the usage of the Blockchain. An example of this being transaction details such as the sender, recipient, the amount being transferred, and/or contractual information. When created, each block is also given a unique hash of the current block and the previous block in the chain. The hash provides a simple and quick way to search the information associated with the block. If the data of a block changes, the hash value associated with that block changes as well and signals a breach in the blockchain. The value of the Blockchain data structure lies in how each block references its predecessor, effectively linking them in chronological order. This structure forces a viable adversary to change not only the block they attacked, but also every block that follows, and its exponential cost is intended to discourage such malicious behaviors.

Initially, when the data of a block is tampered with, its hash is recalculated. Since the previous hash for the next block and so forth will be inconsistent with the current hash, the tampered block and all the blocks that follow will become invalidated. To successfully tamper, those blocks must be revalidated by rehashing and must be relinked to the previous blocks. Algorithms take this process as a foundation to construct a system called Proof-of-Work that slows down the hashing time and makes the cost exponential.

As mentioned earlier, Proof-of-Work is a consensus mechanism commonly used for cryptocurrencies. Proof-of-Work aims to add significant time, and because this takes a lot of computers and hence a lot of energy, this creates a computational resource barrier to block creation. On average it takes about 10 minutes to rehash a block. This feature is

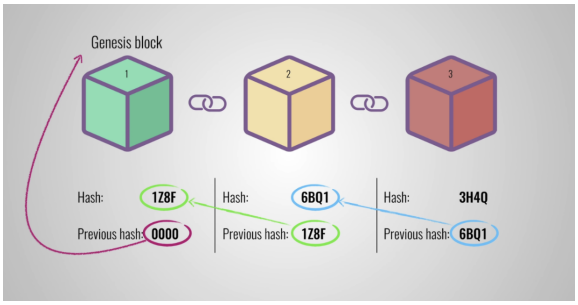

Figure 4: Block Linkage

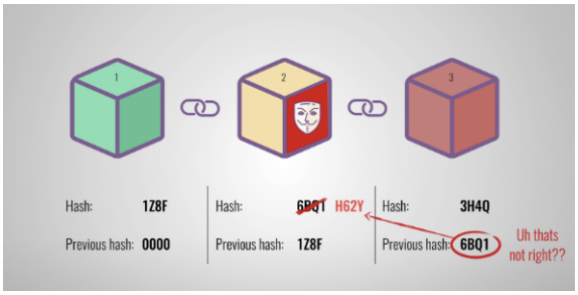

Figure 5: Blockchain Tampering

vital to deterring block tampering and maintaining integrity within many cryptocurrency structures.

The major challenge regarding security that the Proof-of-Work mechanism faces is called the Byzantine Generals' Problem. This problem begins with four generals surrounding a city. All four of the generals must attack or retreat to be in consensus, and it is considered to be successful as long as each army follows the same protocol.

Translating that analogy to the world of cryptocurrency, the challenge is to reach an accurate consensus from a group of verifiers, some of which will be malicious. If the majority of verifiers are honest, then a new block will be linked to the chain. The longest chain is considered as the most valid one, as it took most computational work to be generated.

For the adversary to tamper with the Blockchain, it needs the majority of the votes from the verifiers. However, in order to do so, the adversary must recalculate the hash of not only the tampered block, but also every block that follows it, and surpass every other honest participant to take control of the majority of the network, which takes an extensive amount of costly time and energy. Thus the system establishes high security against the attacks.

This system is not flawless as Proof-of-Work is highly energy intensive and ineffi-

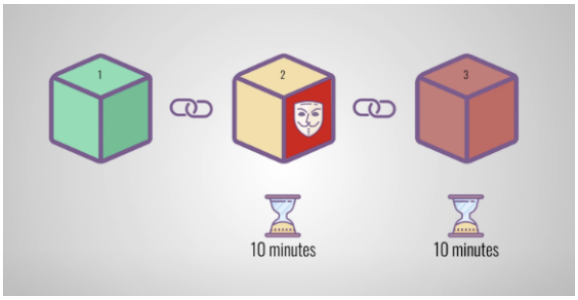

Figure 6: Hash-Delay

cient. It requires an excessive amount of computational power even for simple actions like transactions, thus making scaling more difficult. It is often stated that the Proof-of-Work concept in Bitcoin alone produces more CO2 than the entire country of Norway.

5 Ethereum's Potential for Economic Transformation: A Paradigm Shift in Value Exchange

Ethereum is a blockchain that is a basis of decentralized, permissionless, and censorship-resistant app constructions and organizations. A single, canonical computer called the Ethereum Virtual Machine (EVM) is embedded in the Ethereum universe. Every participant in the Ethereum network agrees on the state of EVM and keeps a copy of it.

Requests of arbitrary computation performance for EVM are called transaction requests. Any participant of Ethereum network can broadcast transaction requests, and while it is being broadcast, other participants verify, validate, and execute the computation. This execution triggers a state change in the EVM that is committed and propagated throughout the entire network. Cryptographic mechanisms ensure that transactions cannot be tampered after being verified as valid and added to the blockchain, as well as ensuring that the signing and execution of all transactions occurred with appropriate permissions from the participants.

The native cryptocurrency of Ethereum that allows a market for computation is named Ether (ETH). From such a market, participants acquire an economic incentive for verifying and executing transaction requests and providing computational resources to the network. In order to broadcast a transaction request, a participant must "pay the price" with some amount of ETH to the network as a bounty. Whoever eventually verifies the transaction, executes it, commits it to the blockchain, and broadcasts it to the network receives this bounty as a reward from the network.

Figure 7: Adversary Calculations

An Ethereum account, an entity with an Ether balance, can send transactions on Ethereum. The accounts can be either controlled by users or deployed as smart contracts. Ethereum has two account types: externally-owned accounts (EOA) and contract accounts. EOA is made up of a cryptographic pair of public and private keys that control account activities and can initiate transactions. On the other hand, a contract account is controlled by the logic of smart contract code and can only send transactions in response to received transactions. But both of them can receive, hold and send ETH and tokens, as well as interact with deployed smart contracts.

A Smart contract is the type of Ethereum account that runs on the Ethereum blockchain. It is a collection of codes (functions) and data (states) of Ethereum and can be the target of transactions. As its name suggests, it is not controlled by users, but deployed to the network and runs as programmed. To interact with a smart contract, user accounts can submit transactions that execute a function defined on the smart contract. The interactions with smart contracts are irreversible, and smart contracts cannot be deleted by default. Like a regular contract, smart contracts can define rules and automatically enforce them via the code.

Consensus mechanisms refer to the complete collection of ideas, protocols and incentives that authorize a distributed set of nodes to derive a general agreement on the state

of a blockchain. When a consensus is reached in the Ethereum blockchain, it means that among the nodes on the network, at least two thirds (>66.6%) agreed on the global state of the network.

Initially, the Ethereum network used a consensus mechanism that involved Proof-of-Work (PoW), which allowed the decentralized Ethereum network to derive a consensus on aspects such as account balances and order of transactions. In this mechanism, miners compete to generate, verify and add new blocks to the chain faster, motivated by the reward (part of the transaction fees and freshly minted ETH). In addition, the Ethereum chain was extremely resistant against attack or manipulation attempts, because the amount of computing power and the energy needed to claim the majority of the network mining power and attack the chain with malicious blocks was extensive, malicious behavior was discouraged.

Ethereum on PoW requires an excessive amount of energy to maintain security and decentralization of the network, leading to significant damage to the environment. Yet better energy efficiency is not the only reason Ethereum shifted to a consensus mechanism that involves Proof-of-Stake (PoS) in September 2022. In PoW, as the need for computation rises, mining pools could dominate the mining game and lead to centralization and security risks. On the other hand, PoS has randomly selected validators instead of competing miners, which makes the individual's participation in securing the network easier and promotes decentralization. However, PoS is not superior to PoW, as it is "younger" and less tested, as well as being more complex to implement thus less welcoming of newcomers.

6 Ensuring Transaction Safety in Ethereum: An Analysis of Consensus Mechanisms and Algorithms

In 1959, Edmund Eisenberg and David Gale conducted a study on subjective probability consensus, exploring how individuals sharing subjective consciousness in the same space could establish a consistent consensus under specific conditions. The initial emphasis of the consensus problem was on centralized scenarios with a restricted number of nodes considered trustworthy, which is unsuitable for decentralized cryptocurrencies since they're based on the Byzantine General's Problem which is a decentralized model.

In centralized systems, a trusted authoritative entity can deliver accurate information while preventing most of the fraudulent data throughout the network. However, decentralized systems lack such reliable sources of authority, which makes it challenging to validate the information received from other nodes.

In 2009, Satoshi Nakamoto expanded the scope of the consensus problem to the expansive and openly accessible internet environment. He proposed Proof-of-Work, a dis-

tributed and decentralized consensus mechanism that considers the possibility of malicious nodes in the environment, that is, a consensus algorithm focused on the Byzantine General's problem. It plays a significant role in categorizing consensus algorithms, of which are broadly classified as either Byzantine Fault Tolerance or non-Byzantine Fault Tolerant algorithms. Nowadays, most blockchain consensus algorithms opt for Byzantine fault tolerance, underscoring its prevalence and relevance in ensuring robust and secure decentralized networks.

In the context of a blockchain, consensus serves the critical function of ensuring unanimous agreement among all network nodes regarding the current state of the network and the legitimacy of transactions. This is indispensable for upholding the security and integrity of the blockchain. However, inherent variations persist in the computing power, storage capacities, and other machine configurations among individual nodes within a blockchain. Diverse consensus algorithms and mechanisms exhibit varying capabilities in guaranteeing equitable accounting rights for nodes. If certain nodes consistently prioritize getting accounting rights, it inevitably diminishes the motivation for other nodes to actively engage in the competition for accounting, which in turn, results in the overall inactivity of the blockchain network.

A robust consensus algorithm not only sustains the vitality of the blockchain network but also secures a reliable and continuous provision of computational power across the entire network. In contrast, an inadequately designed consensus algorithm fails to ensure that nodes within the chain contribute a substantial amount of computing power. This deficiency exposes the entire network to heightened susceptibility, making it vulnerable to disruptions, particularly during targeted attacks.

As previously discussed, the PoW mechanism employed in Bitcoin provides a robust foundation for security and effectiveness. Nevertheless, it exhibits certain shortcomings, particularly in efficiency and environmental impact. The PoW system promotes the likelihood of an entity mining a new block based on its computational resources, fostering a fair but energy-intensive process, especially in mining. The substantial computational resources, while contributing to the fairness of the system, also result in inefficiencies during the minting process. In response to environmental sustainability and scalability concerns, Ethereum shifted its consensus mechanism from PoW to PoS during the Eth 2.0 upgrade to account for these shortcomings.

Proof-of-Stake is a newer form of consensus algorithm where the selection of the next block is contingent on the stake (amount of cryptocurrency) held by the owner rather than their computational power. In the PoS algorithm, nodes within a network vie for the opportunity to validate new blocks by staking a designated amount of cryptocurrency. A selection algorithm is then employed to designate one of these candidates to validate the new block and earn the associated transaction fee. This algorithm considers various factors

such as the candidate's stake, coin age, and also simple randomization to ensure equitable treatment of all nodes in the network. Coin age, for instance, tracks the duration for which a candidate node has served as a validator; nodes with a longer history as validators enjoy enhanced chances of being selected as the new validator and therefore reap the benefits. Another influential factor is the process of random block selection where the validator is chosen based on a blend of the lowest hash value and the highest stake.

The PoS algorithm offers the advantage of sidestepping the intricate and lengthy "mining" process required by PoW, instead, we can simply use stakes to acquire accounting rights. This diminishes block and transaction processing time, resulting in substantial time and computing resource savings during consensus formation. Consequently, the efficiency of consensus attainment experiences a significant boost. Comparable to how PoW mitigates the risk of a 51% attack, PoS introduces a similar safeguard: in the event of a cyber-attack impacting the stake of the entire system, it would concurrently erode the stake of the attacker. However, a notable drawback of the PoS algorithm lies in the tendency for nodes with higher equity to garner superior accounting rights, especially in the system's initial state. This dynamic diminishes the incentive for users with lower equity to participate actively, consequently dampening the overall engagement and vibrancy of the entire blockchain network.

7 Empowering a Decentralized Future: Blockchain's Promise for a Secure, Equitable, and Transparent Digital World

Even though cryptocurrency seems to be a promising technology of the more convenient future, it does not do only good to society.

As mentioned earlier, one of the most significant drawbacks of cryptocurrency is the harm it causes to the environment. Cryptocurrencies such as Bitcoin and Ethereum are already spending as much electricity as a small country, and as the usage of cryptocurrency increases, the environmental damage would only accelerate.

Though this is not a problem that applies to only cryptocurrency, the advance of technology inevitably has inspired new types of crime, particularly the kinds that occur solely digitally. The private and anonymous nature of the internet allows the malefactor to target the victims at the opposite side of the world and avoid investigation. It is stated several times in this paper that even though cryptocurrency is thoroughly protected, the probability of the leak of personal information is never zero, as the adversary can hypothetically break the security system if given enough time and resources.

Fortunately, the evolution of technology does not only benefit the criminals. It also helps police and investigators understand the unprecedented crimes of the new era of the digital world better and resolve them. In a way, the technological advance contributes to the endless war between criminals and the police.

Just like many other technologies, the influence of cryptocurrency to the world depends on its users. Whether cryptocurrency would be used to enrich human civilization or do more irreversible harm than good to it cannot be predicted–only time will tell.

Glossary

Bitcoin Bitcoin (BTC) is a cryptocurrency, a virtual currency designed to act as money and a form of payment outside the control of any one person, group, or entity, thus removing the need for third-party involvement in financial transactions [13]. 3

blockchain Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved [16]. 4

Byzantine Fault Tolerance In a few words, Byzantine fault tolerance (BFT) is the property of a system that is able to resist the class of failures derived from the Byzantine Generals' Problem. This means that a BFT system is able to continue operating even if some of the nodes fail or act maliciously [3]. 11

Byzantine Generals' Problem The Byzantine Generals' Problem was conceived in 1982 as a logical dilemma that illustrates how a group of Byzantine generals may have communication problems when trying to agree on their next move. The dilemma assumes that each general has its own army and that each group is situated in different locations around the city they intend to attack. The generals need to agree on either attacking or retreating. It does not matter whether they attack or retreat, as long as all generals reach consensus, i.e., agree on a common decision in order to execute it in coordination [3]. 7

consensus By consensus, we mean that a general agreement has been reached. Consider a group of people going to the cinema. If there is no disagreement on a proposed choice of film, then a consensus is achieved. If there is disagreement, the group must have the means to decide which film to see. In extreme cases, the group will eventually split [6]. 3

consensus algorithm A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment [14]. 11

consensus mechanism The term consensus mechanism refers to the entire stack of protocols, incentives and ideas that allow a network of nodes to agree on the state of a

blockchain [6]. 4

decentralization In blockchain, decentralization refers to the transfer of control and decision-making from a centralized entity (individual, organization, or group thereof) to a distributed network. Decentralized networks strive to reduce the level of trust that participants must place in one another, and deter their ability to exert authority or control over one another in ways that degrade the functionality of the network [21]. 3

Ethereum Ethereum is a network of computers all over the world that follow a set of rules called the Ethereum protocol. The Ethereum network acts as the foundation for communities, applications, organizations and digital assets that anyone can build and use [10]. 4

Genesis Block The first block in a blockchain. 6

ledger In the context of cryptocurrencies, a ledger is a database or a list of every transaction that has ever taken place on the network. This decentralized ledger, known as a blockchain, is maintained by a network of computers, or nodes, who work together to verify and record transactions [15]. 4

mining Cryptomining is the process of validating a cryptocurrency transaction as a process of proof-of-work. 10

Proof-of-Stake (PoS) Proof-of-stake is a way to prove that validators have put something of value into the network that can be destroyed if they act dishonestly. In Ethereum's proof-of-stake, validators explicitly stake capital in the form of ETH into a smart contract on Ethereum. The validator is then responsible for checking that new blocks propagated over the network are valid and occasionally creating and propagating new blocks themselves. If they try to defraud the network (for example by proPoSing multiple blocks when they ought to send one or sending conflicting attestations), some or all of their staked ETH can be destroyed [**ethereumPoS**]. 10

Proof-of-Work (PoW) Nakamoto consensus, which utilizes proof-of-work, is the mechanism that once allowed the decentralized Ethereum network to come to consensus (i.e. all nodes agree) on things like account balances and the order of transactions. This prevented users from "double spending" their coins and ensured that the Ethereum chain was tremendously difficult to attack or manipulate. These security properties now come from proof-of-stake instead using the consensus mechanism known as Gasper. [9]. 4

smart contracts A "smart contract" is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain. Smart contracts are a type of Ethereum account. This means they have a balance and can be the target of transactions. However they're not controlled by a user, instead they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible. [7]. 9

References

[1] *Banknote - Wikipedia*. https://en.wikipedia.org/wiki/Banknote.

[2] Mustafa Bedawala. *Consensus Mechanisms*. https://usa.visa.com/solutions/crypto/consensus-mechanisms.html.

[3] Binance. *Byzantine Fault Tolerance Explained*. https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained. 2018.

[4] CoinTelegraph. *How Does Blockchain Solve the Byzantine Generals Problem?* https://cointelegraph.com/learn/how-does-blockchain-solve-the-byzantine-generals-problem.

[5] Decentralized Dog. *What is the Nakamoto Consensus?* https://coinmarketcap.com/academy/article/what-is-the-nakamoto-consensus. 2021.

[6] Ethereum Foundation. *Consensus Mechanisms*. https://ethereum.org/en/developers/docs/consensus-mechanisms/. 2023.

[7] Ethereum Foundation. *Introduction to Smart Contracts*. https://ethereum.org/en/developers/docs/smart-contracts/. 2023.

[8] Ethereum Foundation. *Proof-of-Stake (POS)*. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. 2023.

[9] Ethereum Foundation. *Proof-of-Work (POW)*. https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/. 2023.

[10] Ethereum Foundation. *What is Ethereum?* https://ethereum.org/en/what-is-ethereum/.

[11] Jake Frankenfield. *Cryptographic Hash Functions: Definition and Examples*. https://www.investopedia.com/news/cryptographic-hash-functions/. 2023.

[12] Jake Frankenfield. *Decentralized Applications (dApps): Definition, Uses, Pros and Cons*. https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp. 2023.

[13] Jake Frankenfield. *What is Bitcoin? How to Mine, Buy, and use It*. https://www.investopedia.com/terms/b/bitcoin.asp. 2023.

[14] GeeksforGeeks. *Consensus Algorithms in Blockchain*. https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/.

[15] GeeksforGeeks. *What is a Ledger in Cryptocurrency?* https://www.geeksforgeeks.org/what-is-ledger-in-cryptocurrency/. 2023.

[16] IBM. *Blockchain*. https://www.ibm.com/topics/blockchain.

[17] Tamas Kadar and SEON. *Global Banking Fraud Index 2023*. https://seon.io/resources/global-banking-fraud-index/. 2023.

[18] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. 2008.

[19] Katelyn Peters. *A History of Bitcoin Hard Forks*. https://www.investopedia.com/tech/history-bitcoin-hard-forks/. 2023.

[20] Gaurav Roy. *What Is Ethereum Proof-of-Stake?* https://www.ledger.com/academy/ethereum-proof-of-stake-pos-explained. 2023.

[21] Amazon Web Services. *What is Decentralization in Blockchain?* https://aws.amazon.com/blockchain/decentralization-in-blockchain/.

[22] Rakesh Sharma. *What Is Decentralized Finance (DeFi) and How Does It Work?* https://www.investopedia.com/decentralized-finance-defi-5113835. 2022.

[23] Jagjit Singh. *What is PoW Ethereum (ETHW), and how does it work?* https://cointelegraph.com/news/what-is-pow-ethereum-ethw-and-how-does-it-work. 2022.

[24] Tongji University. *A Review on Consensus Algorithm of Blockchain*. https://blockhack.osive.com/_downloads/33a65d87de38eaf5b8d817681a3e4674/7.pdf. 2017.

[25] Alan Walker. *Alan Walker - Faded*. https://www.youtube.com/watch?v=SSo_EIwHSd4. 2015.