Designing Future Sustainable Cryptocurrencies: Principles and Expectations

Behzad Esmaeilian[1*], Mark Jamison[2], Joseph Sarkis[3], Sara Behdad[4*][0000-0002-7080-7497]

[1]Andrew F. Brimmer College of Business and Information Sciences, Tuskegee University, Auburn, AL, 36088 USA
[2]Warrington College of Business, University of Florida, Gainesville, FL, 32606, USA
[3]Worcester Polytechnic Institute, Worcester, MA, 01609, USA
[4]Environmental Engineering Sciences, University of Florida, Gainesville, FL, 32606, USA

besmaeilian@tuskegee.edu, mark.jamison@warrington.ufl.edu, jsarkis@wpi.edu, sarabehdad@ufl.edu

Abstract. This book chapter introduces the principles of designing cryptocurrencies and outlines the key characteristics expected from future currencies. The chapter provides an overview of the foundational components of cryptocurrency networks and emphasizes scalability, security, and sustainability as pivotal characteristics for the next-generation currencies. It begins by introducing the fundamental elements involved in designing cryptocurrency networks, which include hash functions, data structure, and digital signatures. It further explains the primary processes necessary for achieving decentralization, and the procedure of mining and verifying transactions. Additionally, the chapter describes the environmental sustainability aspects of crypto networks, with a specific focus on three key areas: (1) energy consumption, (2) electronic waste generation, and (3) opportunities for sustainable practices through decentralized transactions. Finally, the chapter highlights the potential for sustainable practices and the social benefits that can be derived from future cryptocurrency technology.

Keywords: Cryptocurrency Design Principles, Sustainable Cryptocurrency, Decentralized Transactions, Blockchain, Mining, Environmental Sustainability, Digital Currencies, Social Benefits.

1 Introduction

The number of cryptocurrencies worldwide has surpassed 10,000 as of 2022 [1]. With the proliferation of cryptocurrencies and the growing significance of decentralized networks, it becomes crucial to comprehend the theoretical mechanisms underlying them and integrate sustainability principles into their design. Future crypto networks are anticipated to possess three key attributes: scalability, security, and sustainability. Currently, the open-source development community and practitioners have been at the forefront of cryptocurrency advancements, prioritizing the reduction of costs associated with electronic transaction systems [2]. Nevertheless, the design of robust

cryptocurrencies necessitates collaborative efforts involving diverse disciplines such as computer scientists, system designers, finance experts, environmental engineers, economists, and social scientists. By bringing together expertise from multiple fields, the development of capable cryptocurrencies can be realized and more innovative and sustainable solutions in the digital currency landscape can be achieved.

The contribution of disciplines beyond computer science to digital currencies has been hindered by a general lack of understanding regarding the technical aspects of cryptocurrency design and engineering. This chapter aims to bridge this knowledge gap by providing an overview of the fundamental components of cryptocurrency networks, intended to familiarize newcomers with distributed networks, as well as sustainability and scalability concerns.

Figure 1 visually represents the technical elements covered in this chapter, although it is important to note that the discussion here is not exhaustive. Rather, it focuses on a representative selection of studies and adopts a thematic review approach to previous literature, providing a comprehensive yet concise overview.

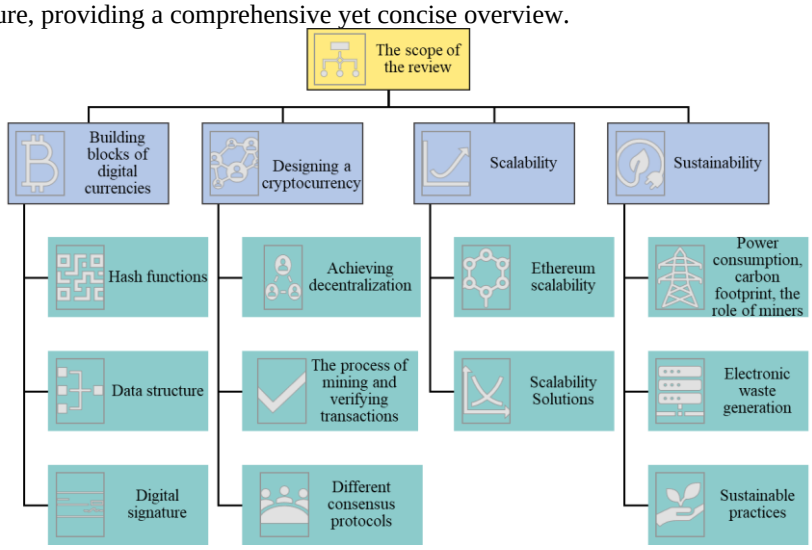

Fig. 1. The scope of the topics included in this study.

To identify and discuss the available resources, a qualitative approach inspired by Templier and Pare [3] has been employed. This approach involves six main steps: formulating objectives, collecting relevant studies, screening the results, assessing their quality and relevance, extracting pertinent information, and finally summarizing and documenting the findings. Engineering Village, ScienceDirect, Scopus, and Web of Science were the primary databases used to search for the studies.

By addressing the technical aspects of cryptocurrency design and engineering and offering insights into sustainability and scalability concerns, this chapter seeks to facilitate interdisciplinary contributions to the field and foster a broader understanding of digital currencies beyond computer science.

The remainder of this chapter is organized as follows. Section 2 introduced the technology behind cryptocurrencies. Section 3 describes the essential elements needed for

building cryptocurrency networks. Section 4 provides a comprehensive understanding of the process of mining and how to achieve decentralization in such distributed networks. Section 5 explores scalability, invulnerability, and sustainability as the three key characteristics expected from future currencies. Further, it examines the current limitations in estimating the environmental impacts of crypto networks and highlights opportunities for future sustainable practices and the social benefits they can bring.

2 The technology behind digital money

Cryptocurrencies are the newest forms of digital currencies designed to sustain trust through technology. The technology behind cryptocurrencies is known as distributed ledger technology or Blockchain. Blockchain has emerged to enable safe and secure data sharing among entities that otherwise would not trust each other. The tighter integration among mutually untrusted entities creates transformative opportunities for various applications ranging from financial services to supply chains and healthcare.

Blockchain in its abstraction form is a shared, totally ordered, tamper-resistant log of transactions. The log is created via a set of rules written in computer code that is distributed across multiple computers (called computing nodes) and executed by them. Each node holds a copy of the entire ledger. Thus the Blockchain infrastructure includes three main elements: (1) a set of rules or computer codes (known as protocol) that govern the way participants transact, (2) a decentralized network of users and computer nodes, and (3) a shared, tamper-resistant, totally ordered ledger that stores the transaction history. The tamper-resistant, distributed nature of Blockchain helps make it suitable as a replacement for traditional, centralized financial systems where an entity such as a bank serves as a trusted third party for verifying and recording transactions. In future sections, we describe the elements needed to build such a decentralized distributed ledger.

3 Essential components of digital currencies

This section provides an overview of the key components needed for a decentralized network capable of securely handling financial transactions. The three main elements include the hash function, data structure, and digital signatures (Figure 2). For clarity, we will describe the concepts using the Bitcoin network as an example and the discussions provided by Narayanan et al. [4].

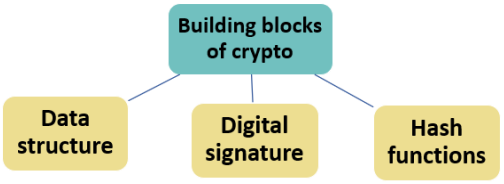

Fig. 2. The essential elements for building digital currencies

3.1 Hash functions

The data stored in Blockchain networks are encrypted using hash functions. The hash functions are necessary for ensuring that no one tampers with the data. Hash functions transform input data of varying sizes (like a text message) into a fixed size (such as 256 bits) called a hash value. Encryption converts data into a protected format from which it is nearly impossible to read the original data unless the recipient has the appropriate key.

Cryptocurrency hash functions should have the properties of collision resistance, hiding, and puzzle friendliness. Table 1 summarizes these properties, using for illustrative purposes a hash function H with input X and output H(X). The hash function H is "collision-free" if different values X and Y always give different hash results. This means each H(X) only corresponds to one X. Also, H is "hidden," which means figuring out the input from the output is extremely hard. Moreover, H is “puzzle-friendly” which makes it tough for anyone to pick an input that produces a specific output. In essence, there is no strategy much better than random guessing to solve this [4].

Hash functions are commonly used in cryptography algorithms to verify the authenticity and integrity of data and quickly retrieve and access the data. Hash functions are used in digital signatures and message authentication codes (MACs) to confirm the authenticity of messages. Different types of hash functions exist. For example, Bitcoin uses a hash function named SHA-256.

Table 1. Properties of hash functions used in crypto design (summarized from [4])

	Property	Description
1	Collision resistance	It is not possible to locate two different values, X and Y, for which $x \neq y$, but still have $H(x) = H(y)$
2	Hiding	If $y = H(x)$ represents the output of H, there exists no reasonably feasible method to determine the input x.
3	Puzzle friendliness	For any given output value y, if k is selected from a distribution with substantial min-entropy, the task of finding an x within a reasonable timeframe such that $H(k\|\|x) = y$ becomes infeasible.

3.2 Data Structure

In addition to a hash function, we need a data structure that can help identify where the data is located and stored. To design a crypto network, data structures that use pointers such as linked lists or binary search trees can be used. A linked list is a collection of data elements where each contains a piece of information that links it to the next element of the list. A binary search tree is a tree of connected nodes where, for each node, all nodes to its left contain lesser keys and all nodes to its right contain greater keys. In addition to linked lists, to find a way to retrieve the data, we need to hash the value of the data. Therefore, we need a hash pointer. Hash pointers can be used to create different types of data structures. Similar to regular pointers, they help us retrieve the data, and beyond that, they can be used to verify if the information is altered or not.

Therefore, hash pointers are necessary parts of the data structure used for building cryptos [4].

There are different types of data structures ranging from arrays and hash tables to graphs, trees, and linked lists (Figure 3).

Blockchain is a linked list, a data structure in which a series of blocks are linked together using hash pointers. Each block has data and a pointer to the previous block. This pointer is a hash pointer, so each block contains where the value of the last block as well as the hash of that value, so it helps to verify that the value of the previous block is not changed. Hash pointers give us where the information is stored and verify that the data is not changed. The hash of the previous block is stored in each block header. That is why Blockchain is known as a tamper-evident log; if any data is going to be altered in previous blocks since we stored the last block's hash, we detect the changes [4]. Remember that the hash functions are collision resistance, so if an adversary tries to alter the data in some block j, the hash in block j+1 (the hash of the entire block j) does not match up.

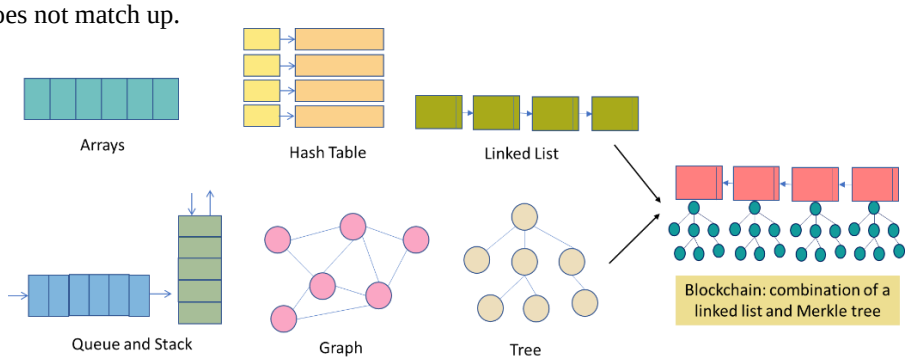

Fig. 3. Blockchain is a combination of a linked list where each block is linked to the previous block and the information within each block can be retrieved using a Merkle tree structure

3.3 Digital signatures

Besides hash functions and hash pointers, digital signatures are other building blocks of cryptocurrency. Digital signatures should have the same functionalities as handwritten signatures, where only you can create your signature. Still, anyone who sees it can verify it, and also, your signature is attached to a specific document and cannot be reattached or reused in other documents. Thus, a digital signature scheme requires three main algorithms, as listed in Table 2. The three algorithms include (1) getting a key size and generating a private key, and a public key, (2) getting a message and a private key and generating a signature, and (3) taking a public key, a message, and a signature as input, and producing a Boolean outcome – either true or false – to indicate the validity of the signature. [4].

Several practical modifications can be made to the digital signature scheme. For example, instead of signing the message itself, we can sign the hash of the message to address the concerns around message size. Moreover, we can sign the hash pointers rather than the hash of the message. This way, the whole data structure or the entire

Blockchain is signed. Bitcoin utilizes a digital signature scheme known as the Elliptic Curve Digital Signature Algorithm (ECDSA), which is a standard by the US government and employs elliptic curves.

Table 2. The algorithms needed in a digital signature scheme (summarized from [4])

Function output	function	Algorithm type
(sk,pk) := generateKeys (keysize)	Receives a specified keysize and produces a private key (sk) and a corresponding public key (pk)	randomized
sig := sign (sk,message)	Receives a message and a secret key, then generates a signature.	randomized
inValid := verify (pk, message, sig)	Takes a public key (pk), a message, and a signature as input, and produces a Boolean value of true or false.	Always deterministic

The data is encrypted using the public key cryptography method or asymmetric encryption. Two different keys, public and private keys, are needed to encrypt/lock and decrypt/unlock the data. The public key is an identity. The user uses a public key to authenticate their identity electronically or to sign or encrypt data. In Bitcoin, identities are called “addresses”. An “address” is just a hash of a public key. The public keys are just addresses that everyone can see, and other people use them to send crypto assets to each other. See [5] for more details on the asymmetric encryption method. Figure 4 shows the general analogy for describing digital signatures and the use of public and private keys.

Suppose that Alice wants to send you a message. She puts the message in a box and encrypts it using her private key. She or anyone with her private key is the only one who can lock the box. She then gives copies of her public key to anyone. Anyone who has Alice’s public key can unlock the box and decrypt the message. They can deliver the message to you using your public key. They put the message in your mailbox and lock the box using your public key. Then, you use your private key to unlock the box. To put it simply, if a message is locked with a private key (like Alice's), anyone with her public key can unlock it. But if a message is locked with a public key (like yours), only you can unlock it with your private key.

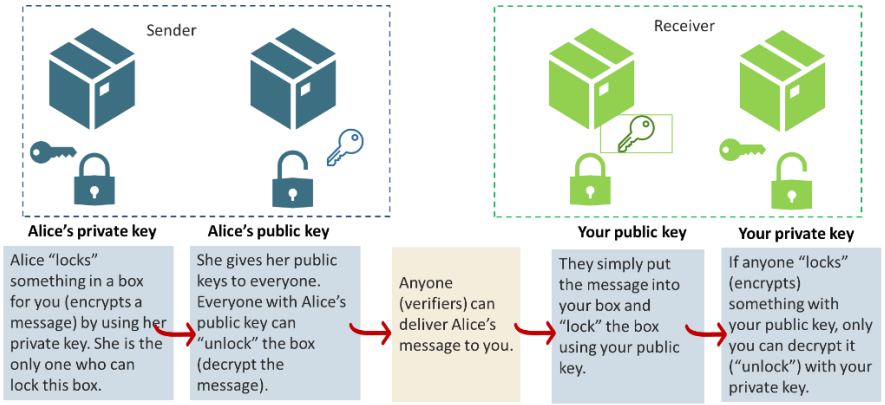

Fig. 4. A simplified overview of how public and private keys work

Now that hash functions and digital signatures are described, we put the information together and see how cryptocurrencies work.

Two properties of cryptocurrencies are that they do not rely on a central authority and they cannot be spent multiple times by the same user. Avoiding the need for a central authority improves the acceptance of the crypto by people suspicious of such authorities and can save costs. Limiting the use of a unit of the crypto to once when in the possession of a user avoids the double-spending problem, i.e., the situation where a person uses the same unit of crypto in more than one transaction, resulting in at least some of the people on the other side of the transactions being cheated. Since Blockchain uses hash pointers and users sign the history of transactions or the entire Blockchain, users can monitor the history of transactions and identify any sign of double-spending of an already-spent coin.

A network consists of two types of nodes: full nodes and Simplified Payment Verification (SPV) nodes. Full nodes verify transactions and create coins by checking the entire history of blocks. SPVs are light nodes that verify transactions without downloading the whole Blockchain by using Merkle tree properties, i.e., ensuring that every leaf on the tree is labeled. Figure 5 summarizes the basic characteristics of these nodes.

The Merkle trees (binary hash trees) are helpful structures that can be implemented using hash pointers. They are an efficient way of encrypting and storing data needed for verification purposes. The Merkle trees help users prove the integrity and validity of the data. They significantly reduce the amount of memory required as it substantially reduces the amount of data that should be maintained for verification purposes. Users can verify individual parts of a block using the Merkle tree.

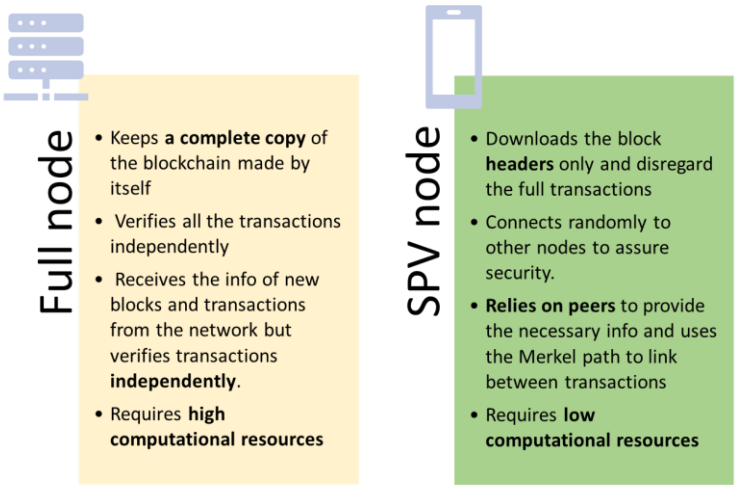

Fig. 5. The comparison of full and SPV nodes

4 Designing a cryptocurrency

A simple cryptocurrency has at least two types of transactions: creating coins and paying coins transaction, which consumes the previously created coins and creates new coins of the same value. Given the use of data structure in recording transactions, the chance of double spending is limited since all transactions are quickly recorded and can be tracked. To eliminate the need for a central authority, digital currencies are often decentralized. To achieve decentralization, we need to determine how all network users can agree upon which transactions have occurred, which transactions are valid, and create coins in a decentralized manner.

4.1 How to achieve decentralization?

In Bitcoin, decentralization is achieved through distributed consensus. Every 10 minutes, each node of the network broadcasts its outstanding transactions and suggests they be included in the next block. A valid block is indicated as the new block if the consensus is achieved among all nodes. This way, if malicious nodes suggest some invalid transactions, they will not be included in the block. Suppose there are some valid transactions by honest nodes that are not included in the block. In that case, they can wait to be included in future blocks once more nodes in the network have those transactions in the list of their outstanding transaction waiting for verification. Nodes of the network should have a consensus on which transactions were broadcasted to the network and the order in which the transactions happened.

In Bitcoin, there is no notion of global time, so the ordering of the transactions cannot be tracked using timestamps. Therefore, nodes need to have a consensus on the order

in which transactions have occurred. The consensus is not easy to make since some nodes might crash or act as malicious nodes, and further, the Bitcoin network is not fully connected since not every pair of nodes is connected to others. These points limit the type of consensus algorithms from the 'distributed consensus' literature employed in such networks.

Various algorithms have been proposed in distributed consensus, such as Byzantine General Problem, Fischer-Lynch-Paterson, and Paxos protocols. These algorithms discuss situations in which consensus is impossible. For example, in Byzantine General Problem, the consensus is impossible among loyal generals if one-third or more of the total number of generals are traitors. Most of these algorithms have analyzed distributed databases that are different from distributed networks such as Bitcoin.

In practice, Bitcoin performs better than in theory. Bitcoin is different from traditional distributed consensus protocols suggested in the literature in two ways: first, Bitcoin introduces incentives. This way, it provides natural mechanisms for nodes to act honestly. Second, Bitcoin's consensus protocol counts on randomization [4].

In Bitcoin, the consensus algorithm works without knowing the node identities. While Bitcoin does not provide complete anonymity since it can link transactions that one node makes, it offers pseudonymity where the nodes do not reveal their actual identity. Due to Bitcoin's pseudonymity, Bitcoin uses a mechanism called implicit consensus to achieve security. In each round, a random node is selected. The selected node broadcasts the next block, which consists of the node's new outstanding transactions. Other nodes in the network either accept (unspent transactions, valid signature) or reject the block. Nodes show their acceptance of a block by including its hash in the next block they create. A transaction will be included in a block once it receives numerous confirmations. While there is no magic number for the number of confirmations for a transaction, six is common.

Bitcoins offer two mechanisms to incentivize users to behave honestly: (2) block reward and (2) transaction fees. In 2015, the value of a block reward was 50 Bitcoins, and it keeps halving every 210,000 blocks or approximately every four years. It is a geometric series, meaning that there will be 21 million Bitcoins to create.

The block reward is the only mechanism for generating coins. The way it works is that the node that creates a valid block gets to create a particular transaction in that block called coin-creation transaction, through which the node can send the created coin to his address as the recipient. The block reward becomes zero in 2140. However, Bitcoin still will have another incentivization mechanism: paying transaction fees. The user who creates a transaction can assign a portion of the total value of transactions to whoever creates the block and first puts that transaction into the block. Currently, transaction fees are low. But as the block reward decreases over time, users will need to pay miners more in fees to get their transactions processed quickly.

4.2 The process of mining and verifying transactions

In previous discussions, we assume that a node is randomly selected to suggest the next valid block. However, the reality is that in the Bitcoin network, all network nodes will compete independently to propose the next block. The process is called proof-of-work

in which each node of the network will keep trying to find a number called *nonce* where the hash of that number, together with the hash of the previous hash and the current list of transactions, will be lower than a target value. This process is called solving a hash puzzle. Nodes are competing independently to find the nonce. The node that finds the nonce that satisfies this requirement will be the lucky node to propose the next block. Computationally speaking, nodes that have higher computation power are more likely to find the nonce that satisfies the following equation:

$$H(\text{nonce}, \text{previous hash}, \text{list of current transactions}) < \text{target value}$$

The processing for finding the nonce that satisfies the equation mentioned above is known as Bitcoin mining. For system security, finding this hash value should not be very easy. To adjust the difficulty level in finding the hash function, all network nodes recalculate the target value approximately every two weeks or 2016 blocks, meaning that the target level will be redefined. The average time between finding two consequent blocks is 10 minutes. The 10 minutes is an average, and in fact, the time between finding blocks follows an exponential distribution with an average of 10 minutes. The 10 minutes is not a magical number and can be set to any number (e.g., 6, 5). This time value should not be too small to help maintain system safety. There are disagreements on the best value of the Bitcoin latency, but most people agree that it should be a fixed number [4].

Knowing the average time between finding blocks helps a miner calculate how long it takes to find the next block. To find it, we just need to divide 10 minutes over the "fraction of hash power of the total network hash power" controlled by the specific miner. For example, if a miner owns 0.2 percent of the hash power in the network, he will find a block approximately every 5000 minutes. The block size and the block frequency are the parameters of protocols.

Speaking of the cost of mining, the economy of mining is a complex game theory model for several reasons. The rate of finding blocks by a miner not only depends on the miner hash power but also on the global hash power available in the network. Also, the miner reward, both block reward and transaction fee, is in Bitcoin, not fiat currencies, so the exchange rate at any given point of time influences the economy of Bitcoin mining for a specific miner.

The Bitcoin network needs to have consensus on three things: (1) the value of Bitcoin and the exchange rate of the currency, (2) the status of the system and the number of coins each user owns, and (3) the rules of the systems (e.g., soft forks and hard forks).

Figure 6 summarizes the process of finding blocks in the Bitcoin network.

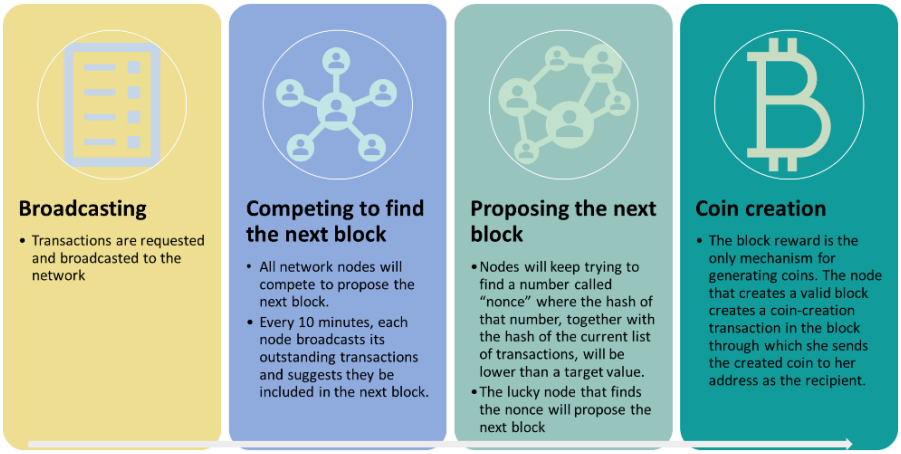

Fig. 6. The process of creating blocks in the Bitcoin network

4.3 Different consensus protocols

Since the start of cryptocurrencies, various consensus protocols have been developed to determine the miner who proposes the next block. The consensus protocols can be categorized into computational-based, capability-based, and voting-based protocols. Table 3 provides a summary of available protocols.

Table 3. Example of current consensus protocols (summarized from [6])

Type of Protocol	Description	examples
Computational-Based Consensus Protocols	A miner is selected based on the amount of computational effort she has spent.	Pure Proof of Work (PoW), Prime Number Proof of Work (Prime Number PoW), Delayed Proof of Work (DPoW)
Capability-Based Consensus Protocols	A miner is selected based on other capability-related factors such as the miner's cryptocurrency holdings, the level of trust the system places in them, their contributions to the community, or the amount of storage they possess.	Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Stake Velocity (PoSV), Proof of Burn (PoB), Proof of Space (PoSpace), Proof of History (PoH), Proof of Importance (PoI), Proof of Believability (PoBelievability), Proof of Authority (PoAuthority), Proof of Elapsed Time (PoET), Proof of Activity (PoA)
Voting-Based Consensus Protocols	A miner is chosen by using a voting system.	Practical Byzantine Fault Tolerance (PBFT), Delegated Byzantine Fault Tolerance (DBFT), Federated Byzantine Agreement (FBA), Combined Delegated Proof of Stake and Byzantine Fault Tolerance (DPoS+BFT), Raft, Federated

A miner is selected based on the computational power s/he has spent in computation-based protocols. In capability-based protocols, miners are chosen based on other factors such as the amount of cryptocurrency they own, the amount of trust the system has on the miner, and the contribution to the community. Finally, in voting-based protocols, a miner is selected using voting mechanisms.

5 The main features of future crypto networks

The current cryptocurrency networks suffer from several key features such as scalability, vulnerability (full decentralization), and sustainability (Figure 7). This section provides an overview of two of these challenges and existing solutions to address them.

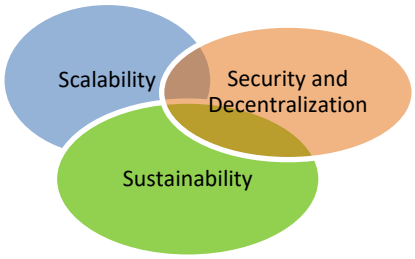

Fig. 7. Three main properties of future cryptocurrencies

5.1 Scalability

Cryptocurrency networks face various scalability issues, including problems like communication breakdowns between users, data storage, and the linear recording of transaction history [7]. The challenges with scalability stem from two primary factors: (1) the expansion of Blockchain size and transaction volume, and (2) the difficulties of consensus protocols and the maximum block size [8].

A scalable protocol is a protocol in which the waiting time for processing transactions is short, even under high transaction volume [9]. The scalability problem can be identified based on data size, transaction speed, and transaction costs. Several metrics can be used to measure the scalability of a network. Table 4 summarizes some of them.

Table 4. Key metrics for measuring scalability [10]

Scalability Metrics	**Definition**	**Bitcoin**
Maximum throughput	The maximum rate of confirming transactions by the network	3.3-7 transactions/s
Latency	Time to confirm a transaction	~10 min
Bootstrap time	Time for a new node to download and process network history	~4 days
Cost per Confirmed Transaction	Cost consumed by the entire network to confirm a transaction	$1.4 – $2.9 (with maximum throughput)

The upper bound on the transmission of information within a peer-to-peer network can be represented as $L\sqrt{N}$, where L represents the link capacity or the number of messages that each node can send or process, and N is the total number of nodes in the network [11]. Note that not all nodes are homogenous and have different capacities as some nodes have potent servers, and some are simple end devices. Bitcoin has a peer-to-peer topology making it among the first class of scalable topologies with $L\sqrt{N}$ scaling limit [12].

The node's transmission capacity is referred to as the allocated bandwidth which indicates the volume of bandwidth accessible for the node to interact with the network. A higher allocated bandwidth assists miners in swiftly sharing information, as well as receiving and transmitting blocks more speedily [13].

The structure of the network defines the vulnerability and performance of cryptocurrencies. The Bitcoin structure is complicated and is intentionally hidden to preserve users' privacy and network security against denial of service (DoS). Estimating the number of nodes and the full size of the network is difficult as nodes are covered behind firewalls. Moreover, the latency among nodes is unknown. There is often a trade-off between network scalability and the system's security goals.

The current inefficiencies in digital currency networks hinder the potential of Blockchain as a valuable technology for businesses [14]. To tackle this challenge, companies are trying to improve the scalability of their networks by enhancing the computational efficiency of mining operations. While more challenging consensus algorithms enhance the security of the Blockchain, they also restrict the technology's scalability [8]. The primary purpose of scalability is to increase the transaction speed (faster output) and transaction throughput (transactions per second), without scarifying decentralization or vulnerability.

Bitcoin is slow compared with current credit card transaction systems. At this time, while Bitcoin manages 7 transactions per second, the Visa network processes 10,000 transactions per second, and Paypal can handle 100 transactions per second. Each block's total size is 1 million bytes, and given that the average transaction size is 250 bytes, a block can accommodate 4,000 transactions in total. Since blocks are found every 10 minutes, then the network speed is 7 transactions per second. In another term, a transaction is called a confirmed transaction once it has been suppressed six blocks into the Blockchain. Since it takes 10 minutes to generate a block, it means, on average, it takes one hour for your payment transaction to be confirmed. Another limitation is that the choice of cryptographic algorithms and hash functions in Bitcoin is limited, so the Bitcoin scripting language should be extended to support new cryptographic algorithms.

How does Ethereum address scalability issues?

Ethereum tries to shorten the time to find a block, provide a fair distribution of rewards among miners, and reduce the incentive for pooled mining. Table 5 compares the time to mine a block and block size in Bitcoin and Ethereum.

Table 5. Comparison of the crypto protocol parameters

	Bitcoin	**Ethereum**
Time to find a block	~10 min	10-20 s
Block size	1 MB	Determined by execution fee, called gas

In networks with fast block time, such as Ethereum, two miners' chance to find a block simultaneously is higher than the Bitcoin. In Bitcoin, the chance of finding a block at the same time is low, where the time between blocks is approximately ten minutes, and it takes relatively 12 seconds to propagate a block to 50% of the network. Faster networks such as Ethereum generate a large number of stale blocks. Stale blocks, or orphan blocks, are propagated to the network and are verified by some miners as valid blocks but finally do not make it to the longest chain and will end up in forks. Ethereum calls those blocks uncle blocks. To promote decentralization and facilitate fair distribution of reward in the network, Ethereum uses a protocol inspired by the GHOST (Greedy Heaviest Observed Subtree) protocol, where miners of the uncle blocks receive a portion of the block reward.

The GHOST protocol tries to improve Bitcoin's scalability by modifying the selection rule of the chain. In Bitcoin, during a fork, the longest chain with the most proof-of-work becomes the main chain. In GHOST, a node selects the side chain with the most work accumulated in its sub-tree blocks [15]. Therefore, GHOST improves mining power utilization in the network. Mining power utilization shows how well a protocol uses energy in the network for actual work. It's determined by the fraction of mined blocks that stay in the main chain. In addition, GHOST improves the fairness and security of the system (Figure 8) since a higher mining power utilization makes it more costly for attackers to launch an attack; therefore, robustness against attacks increases [16].

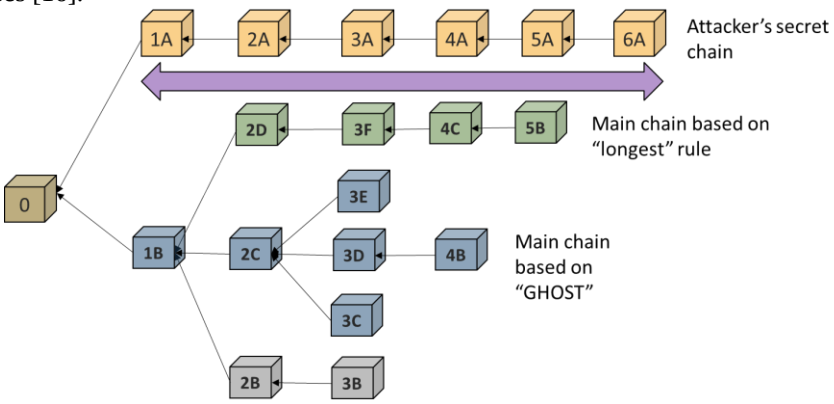

Fig. 8. The comparison of the Bitcoin largest rule protocol with the GHOST protocol (redrawn from [17])

To have updated information about the number of nodes in the network, Ethereum uses a node discovery mechanism called Kademlia. Kademlia is designed for locating and storing data in a peer-to-peer network. Ethereum uses it to help nodes keep an up-to-

date record of their connectedness and their adjacent peers, as nodes may leave or join the network and adjacent nodes may have outdated adjacency information. The node discovery mechanism in Ethereum is UDP-based, a fast and simple protocol; however, the rest of the communication in the network is TCP-based. UDP (User datagram protocol) is quicker and simpler than TCP (Transmission Control Protocol), but retransmission of lost data is only possible with TCP standards. After identifying peer connections and determining whether neighbor nodes are responsive using UDP, Ethereum uses TCP to exchange encrypted and authenticated messages [16].

Scalability solutions.

Various scaling methods have been developed in computer science literature to address scalability issues. Some researchers suggested parameter tuning, known as reparametrization of block size and intervals, as a solution for managing scalability; however, it was shown that achieving high load blockchain protocols requires a fundamental rethinking of technical approaches used in designing the network, and parameter tuning is not sufficient [10]. Another solution is using "payment channel networks" which permit users to move funds between intermediaries without needing to record every transaction on the Blockchain [18].

The scaling methods can be categorized into four main groups (1) on-chain scaling [19], (2) off-chain scaling or using Layer 2 scaling methods [20], (3) compression techniques [21], and (4) secure decentralized randomness techniques [22].

On-chain scaling methods, also known as Layer 1 techniques, improve the throughput of the based layer of the blockchain network by implementing strategies such as increasing blocksize, new address formats, smaller size signatures, database partitioning, and signature aggregation. Off-chain scaling methods, also known as Layer 2 solutions, enhance throughput without touching the main blockchain layer by creating alternative protocols and layers on top of a blockchain; they often require additional software and complexity compared to on-chain scaling approaches. Examples of off-chain methods include sidechains, colored coins, and utilizing state channels.

Sharing is an example of a Layer 1 solution for addressing scalability. The transaction throughput is increased by partitioning the database into several shards, horizontal segments, each stored on a separate server, spreading the computational and storage workload across different network users [23]. The information can still be shared among other nodes; however, nodes do not process and store all the data. The nodes should be randomly assigned and reassigned to random shards to assure security while using sharding.

Table 6 provides an overview of different solutions for addressing scalability and examples of each. It is important to note that strategies cannot be compared solely based on the transaction throughput since different methods involve additional security and trust assumptions, among other things [24].

Table 6. The summary of scalability solutions in each layer of Blockchain (summarized from [24])

	Layer	Definition	Example of solutions	Amount of scalability that can be gained
1	Hardware layer	Machines used to run Blockchain	deploy high-end hardware	Up to 5 to 10 times more throughput
2	Network layer	Communications between nodes	Solutions impacting network propagation (e.g., what data is being sent, which transmission method is used)	Up to 5 times more throughput
3	Layer 1, on-chain	On-chain design of Blockchain (e.g., block structure, consensus algorithms, the specific structure of the main chain)	minor changes (adjusting the block size or the block time interval) or major changes (sharding)	Up to 10 to 20 times more throughput
4	Layer 2 application	Moving computation off the chain	multi-sided payment channels, payment hubs, complete sidechains	Up to 10,000 to 100,000 more throughput.

No single solution can guarantee scalability. Multiple solutions can be employed to ensure scalability and reduce the overall burden on the network. Given the scalability methods mentioned above, the application of such methods is still a challenge due to the limited capability of storage and bandwidth of each node, the lack of optimal strategies for placing transactions within each shard, and the efficiency of cross-shard transactions [25].

While scalable protocols may alleviate the energy-intensive nature of verification processes, the main problem still exists since scalable algorithms often compromise security.

Discussing the security of the crypto networks is outside of the scope of this work. However, security and privacy are key requirements of any cryptocurrency. Given the financial nature of cryptocurrencies, crypto networks are an obvious target for adversaries. Various attacks have targeted different parts of the crypto ecosystem, including double-spending, transaction malleability, networking attacks, netsplit, and interfering mining processes.

A rich literature exists on the security of blockchain systems. Maleh et al. [26] analyzed 65 different cybersecurity incidents and developed a taxonomy for blockchain attacks. Based on this taxonomy, the threats and vulnerability of crypto networks can be categorized into five main groups as listed in Figure 9 [26]: (1) clients'

vulnerabilities, (2) consensus mechanisms vulnerabilities, (3) mining pool vulnerabilities, (4) network vulnerabilities, and (5) smart contract vulnerabilities.

Digital signature and hash function vulnerabilities are examples of clients' vulnerabilities. Race attacks and 51% vulnerabilities are examples of consensus mechanisms vulnerabilities. In the Race attach, two transactions are generated simultaneously for the same fund, to spend the same fund twice [27]. In the 51% attack, the malicious actor or actors control over 50% of the network computational power, where they will be able to modify the ordering of transactions or prevent confirming certain transactions [28].

Bribery attacks and the Selfish Mining attack are instances of mining vulnerabilities. In a Bribery attack, the adversary bribes miners to maximize their profits, e.g., by building on her fork [29]. In the Selfish attack, an adversary pool intentionally keeps discovered block private and does not share it with the public chain [13]. Distributed Denial of Service (DDoS) and Sybil attacks are considered examples of network vulnerabilities. In a DDoS attack, a group of adversary computers floods a targeted server with too much traffic to make it inaccessible to legitimate users [30]. In the Sybil attack, an adversary creates many fake identities to control the network [31].

Finally, Solidity vulnerabilities and Ethereum Virtual Machine (EVM) Bytecode vulnerabilities are cases of smart contract vulnerabilities. Solidity is an object-oriented language for writing smart contracts. When using solidity for developing contracts, developers often use external calls to other functions where those external calls usually do not have enough safety features. EVM is a platform that allows developers to build decentralized applications on Ethereum, which has its limitations [32].

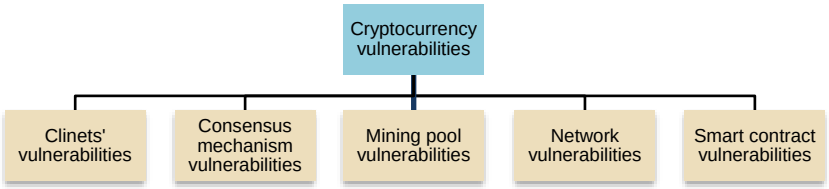

Fig. 9. Five main categories of the vulnerability of crypto networks

For example, in Bitcoin, an efficient crypto network is expected to have full pseudonymity to satisfy user privacy. Pseudonymity refers to (1) anonymity and (2) unlinkability. The client information should be unidentifiable (anonymous) as well as unlinkable. While Bitcoin provides anonymity since clients use private and public keys, it does not fully guarantee unlinkability, where the relationships between transactions can be inferred by analyzing the transactions broadcasted to the network. Researchers have shown that the linkability of cryptocurrency transactions is possible based on network analysis and transaction propagation analysis [33][34]. Therefore, one big area for improvement of future crypto networks resides in enhancing their security.

5.2 Sustainability

This section describes the sustainability of crypto networks from several perspectives: (1) the carbon footprints of the energy consumed in crypto networks, (2) the e-waste generation rate of mining hardware, and (3) sustainability practices. As can be seen, by these dimensions sustainability focuses primarily on environmental and materials sustainability—although social and economic sustainability may be more broadly related.

Power consumption, carbon footprints, and the role of miners.
The energy-intensive nature of some crypto networks is probably the most known environmental impact of the crypto networks [35–37][38]. For example, for Bitcoin, the power consumption and the consequent carbon footprint of mining Bitcoin depend on several factors ranging from the number of miners operating on the network, the type of hardware they use, their geographical region, and the source of electricity they consume—such renewable vs non-renewable energy sources.

Modeling energy consumption.
The energy required to verify transactions on blockchain networks depends on factors such as the difficulty of mining, the number of participants, the type of consensus protocol—Proof-of-Work (PoW), Proof of Stake, Proof of Authority—and even strategies set by the mining pools. As previously discussed, most consensus algorithms promoted as energy-efficient scalable algorithms do not have the security level needed for blockchain applications. So far, the most secure algorithm is PoW initially used in the Bitcoin network, which is energy-intensive and is purposely made this way to make cheating costly. The energy consumption of the mining process is measurable in terms of the network hash rates. The hash rates represent the number of calculations performed in seconds—or hashes per second.

Energy consumption is a function of the "difficulty" of mining. The difficulty refers to how difficult is to find a hash—or equivalently, a nonce—below the target value defined by the Bitcoin software (a 256-bit number). The higher the target value, the higher the chance to find a hash lower than the target value, and therefore the lower the mining difficulty and vice versa.

The Bitcoin network controls the rate of discovering Blocks or generating Bitcoins by selecting the target value T. In the Bitcoin network, the target value is noted as the difficulty level [39]:

$$Difficulty = \frac{T_{max}}{Target\ Value} \qquad D = \frac{T_{max}}{T}$$

The largest possible target value is $(2^{16} - 1)2^{208} \approx 2^{224}$ which is the original target value used in the Bitcoin network. Therefore, the difficulty compares the target value with its original value (difficulty=original target/target value). The network automatically determines the target value to ensure that the average time to create a block remains equal to 10 minutes. Therefore, as more miners join the network and start to mine, the difficulty of finding valid blocks, or an acceptable nonce, increases [40].

In the Bitcoin network, the hash function used is $H(S) = SHA256(SHA256(S))$, which ensures an even distribution between 0 and $2^{256} - 1$. This means that for any nonce value, we can calculate the probability of the hash value being less than the target value as follows [39]:

$$H(S) = Uniform\,(0, 2^{256} - 1)$$

$$\Pr(H(S) < T) = \Pr(H(Bn) < T) = \frac{T}{2^{256}} = \frac{T_{max}}{D2^{256}} = \frac{2^{224}}{D2^{256}} \approx \frac{1}{D2^{32}}$$

The number of attempts needed to acquire a block follows a geometric distribution which implies that the anticipated number of hashes required to find a block is $D2^{32}$. If a system computes hashes at a rate of R, the expected duration for finding a block is [39]:

$$E(t) = \frac{1}{p} = \frac{D2^{32}}{R}$$

The expected time can be used to find the energy needed to discover a block.

The rate at which Bitcoins can be discovered can be controlled by the Bitcoin Network's choice of the value of the target, T. The higher the target value, the lower the mining difficulty (difficulty finding a hash value less than the target value (a 256-bit number). What happens in the network is that once more miners join the network, the rate of creating blocks increases. Therefore, the average mining time decreases. However, since the ideal average mining time is about 10 minutes, the Bitcoin software increases mining difficulty by setting a lower target value. This reduces the block creation rate, and the average mining time will go back to the expected time, and this cycle repeats.

The above-discussed estimation method relies on several assumptions. For example, in practice, Bitcoin generation is faster than expected since new hash power is determined dynamically by the capabilities of the miner networks, and it can only adjust itself every 2016 block [41]. The accurate estimation of the energy requires relaxing those assumptions, including the number of miners, the speed of mining, how a system calculates hashes (the choice of hardware), and the Bitcoin economics that influence the number of miners.

The gaps in current energy estimations.

Multiple studies have assessed the energy impact of Bitcoin. Mora et al. [42] suggested that if Bitcoin gains popularity at a similar rate as other widely adopted technologies, its CO2 emissions could contribute to global warming exceeding 2°C. Krause and Tolaymat [36] estimated the energy demand to produce a US dollar through cryptocurrency mining and contrasted it with the energy used in conventional mining of minerals like aluminum, copper, and gold. They found that crypto mining consumes more energy to generate an equivalent dollar amount. Stoll et al. pointed out that data regarding the geographical locations and IP addresses of miners available through mining pools and

websites that disclose pool compositions can aid in translating energy consumption data into metrics for greenhouse gas emissions [43]. Depending on the geographical regions and the main source of electricity generation in each region the CO2 footprints can be calculated.

Although some studies aim to discuss the carbon footprint of digital ledger technologies generally, the number of studies on the energy modeling of blockchain networks is limited. While some studies have developed quantitative methods [39][44], the provided estimates vary significantly among studies since they are based on different sets of assumptions that do not fully capture the reality of the cryptocurrencies market with no consideration of miner behavior. Also, existing studies have not employed the full advantages of available empirical data. Arguments have been made that many projects over-estimate near-term Bitcoin CO2 emissions [45]. Finally, since the number of miners operating the network depends on the economy of the Bitcoin, no consideration of the crypto-economics, user adoption, and the incentives offered by the network have been incorporated into existing energy estimation. Given the discrepancies and varying perspectives, public blockchain platforms require greater investigation. Private and permissioned platforms may require significantly less energy and generate future emissions—some blockchain platforms are even selling themselves as greener alternatives. For example, the Signum currency states that it uses less than 0.002% of Bitcoin's energy to drive its Blockchain [46].

Blockchain energy consumption does not derive its main cost from the hash rate but from the collective mining process on its corresponding platform. It is essential to understand miners' roles in the digital economy to differentiate between rough estimation and valuable energy reduction innovation. In particular, it is important to understand the interaction between cryptocurrency valuation and Bitcoin adoption (by both clients and miners).

The concept of mining pools.

Miners often share their computational recourses over a network by joining some mining pools, where the award is split based on the contribution of each miner. The origin of mining pools occurs because the difficulty of mining has increased to the point that it could take centuries to create a block by one miner—so the solution is to integrate the resources of miners and reward them according to their contributed mining hash power. There are different mining pool methods to reward the miners [47], and currently, there are about 20 major mining pools; most of them—about 81% of the network hash rate—are located in China (e.g., BTCC, Antpool, BW) [48].

While pooled mining is common in the crypto market, previous energy estimations do not consider this pooling situation in energy estimation analysis. The key to overcoming this limitation is developing a framework to attribute blocks to the original miners accurately. Developing an attribution scheme for linking blocks to original miners through support from publicly available datasets helps identify more accurate hash rates used for mining each block and, consequently, a more precise estimation of the energy required for the mining process. We should note that empirically assessing the impact of merged mining on energy consumption modeling is just the first step. The ultimate purpose should be to study the effect of block sharing among mining pools and

new constructs such as multi-merged mining on resolving the energy consumption of crypto mining.

Electronics waste generation of mining hardware.
While the energy consumption of Bitcoin has generated significant discussion on the sustainability of cryptocurrency, other crypto network resource consumption with environmental sustainability implications beyond energy implications should be acknowledged. One such resource is materials associated with short-lived hardware infrastructure used for mining processes [44][49]. Hardware options ranges a spectrum from Central Processing Units (CPUs) and Graphics Processing Units (GPUs) to Field Programmable Gate Arrays (FPGAs), and more recently, Application-Specific Integrated Circuits (ASICs).

In the Bitcoin network, miners use ASICs suitable for performing hashing computations. Once hardware reaches its end-of-use lifespan, they create a considerable amount of electronic waste that requires proper collection and recovery efforts. De Vries and Stoll estimated that the lifespan of Bitcoin mining hardware is 1.29 years which results in up to 30.7 metric kilotons of e-waste equipment annually [44].

The use of special ASIC hardware contributes to e-waste generation and raises concerns about network decentralization, where specific groups of miners with access to mining hardware may control the network and influence its security. The development of ASIC-resistant algorithms is suggested as a solution for enhancing safety. Moreover, minimizing the hardware requirement should be considered a mechanism for improving the sustainability of the technology. Speaking of sustainability, we should note that these ASICS have made computing power greater to save energy per computation, but exponentially greater computation requirements make the energy savings disappear.

Some cryptocurrencies and blockchain platforms have recognized the concerns with e-waste generated by specialized equipment for consensus and mining activities. These greener alternatives state that their actions can be done by using electronic equipment's available computing and disk space. Whether or not this holds actual needs to be proven over the long run if these platforms and cryptocurrencies become more popular.

Sustainability applications of cryptocurrencies.
Improving efficiency, transparency, and traceability are often highlighted as benefits of blockchain technology, where various use cases would be possible to create more sustainable systems [50]. There is considerable potential for incorporating Blockchain into governance efficiency [51], social equity [52], industrial innovation [53], and environmental protection practices [54]. Examples of such practices include real-time monitoring of energy and resource consumption [55], tokenizing carbon credit assets [56], rewarding green actions, tracking emissions [57], addressing information asymmetry to foster resource allocations, establishing market mechanisms to manage resources properly, and financing climate change practices [58].

Proper evaluation mechanisms are needed to measure the exact sustainability consequence of any digital currency precisely. The question arises of what strategies can be employed to green the financial systems and design a low-carbon economic and

financial system. There is no consensus on the definition of green financing as it compromises various aspects. It includes financing of green investments in environmentally viable goods and services, investments in the area of prevention, reduction, and compensation of damage to the environment, and also it covers the financing of public policies that promote the implementation of damage mitigation projects or adaptation initiatives [59]. It is expected that future blockchain systems facilitate the implementation of green finance principles due to the decentralized and transparent infrastructure they create. It addresses the mistrust among stakeholders, including donors and recipients of climate change finance.

Blockchain and cryptocurrencies, through these activities, can expand the contribution to sustainability not only to those that can afford it and at the top of the economic pyramid but to all levels and locations of societies. This inclusiveness has great potential to increase equity and inclusion in financial systems [60][61] which can also be green [62]. These lead to greater potential for social sustainability, as we now discuss.

Social Sustainability.

In this section, we highlight three main directions in which cryptocurrency infrastructure influences society: (1) supporting small businesses, (2) empowering the culture of sustainable behavior, and (3) energizing new economic systems.

Supporting individuals and small businesses.

Strengthening individuals' innovation and small businesses is a potential advantage of distributed digital ledgers [63] such as NFTs. NFTs, or non-fungible tokens, are special units of data stored on blockchains that are unique and cannot be exchanged for one another. NFTs are tokens associated mainly with digital content such as images, art, songs, and social media posts [64]. NFTs have received attention recently since they facilitate the implementation of a “creator economy” or “attention economy” in which a chain of ownership can be created, and the owner of digital content can authenticate the content, dictate the value, and transfer the ownership to the future buyer with no intermediary.

NFTs allow content creators to connect to their customers directly and provide pricing tiers that give buyers flexibility in paying their desired price. The marketplace for NFTs is growing fast as the concept of “metaverse” is gaining momentum; however, we should also acknowledge that keeping track of the history of the chain of owners does not necessarily reduce market inequality. Still, projects with specific sustainability dimensions as the basic philosophy can contribute in sustainable and inclusive ways. For example, relating NFTs to the United Nation’s seventeen Sustainable Development Goals to be socially responsible can be a direction for sustainable NFT development and sale. Another aspect that can prove more socially inclusive and sustainable is to use NFT for craft manufacturers in developing nations who use sustainable materials to support their crafts [65].

Encouraging the culture of sustainable behavior.

Citizens' behavior in reducing environmental emissions and the drivers of sustainable behavior have long been studied in the literature [66–68]. Moreover, technology has

been highlighted as an enabler for promoting sustainable practices and social value creation [69,70]. For instance, the technology can help monitor consumer behavior, provide feedback to users, reward sustainable behaviors, and consequently help users adjust their behavior towards sustainability.

Blockchain capabilities in measuring, reporting, and verifying practices pave the way for regulating and standardizing habitual user behaviors and tethering society towards an appropriate culture of usage, consumption, and disposal compatible with sustainable principles. Moreover, the technology can be implemented at a larger scale in countries and regions where the international carbon markets and discussions under the Paris Agreement can be regulated [71]. There are also ways of tokenizing plastics, such as ocean plastics, to develop plastic credit within developing countries [72]. Developing general tokenized social credit systems has also been proposed and could be a way to increase effective and flexible philanthropic activities by organizations [73].

New economic systems

The crypto peer-to-peer system of exchange is formed around shared ownership and is inherently self-governing, so it has the potential to create new economic structures. For example, one challenge with the concept of the sharing economy as a socio-economic system is that while online operators and dematerialized organizations have tried to match supply and demand nodes and aggregate the resource of multiple users to provide service to others, they fail to equally distribute the value among all the participants in creating the value. A big fraction of the value often goes to the intermediaries who operate such online platforms. Scientific research is needed to explore how the distributed nature of Blockchain makes it possible to address the current imbalanced nature of traditional platforms. The crypto network aggregates the work of disparate groups of miners who can coordinate themselves and run online platforms. The transaction micro fees that users pay to the network will be paid to those who participate in operating the platforms and lessen the inequality issue [74].

The crypto market has its political consequences too. Arguments have been continued regarding whether the crypto networks should maintain pseudonymity to preserve users' privacy or should the users be identifiable to the government as the current implementation of the Know Your Customer (KYC) requirement imposes. Satoshi's intent for creating Bitcoin is not known yet, but there is a possibility that he meant Bitcoin to be an agorist currency [75]. Although Bitcoin has the potential to roll through black and gray markets, its ability to create a free market should not be overlooked. Maintaining privacy, alleviating mistrust among stakeholders, involving all people, and the infrastructure for using unutilized assets of the crowd should be used such that it paves the way for an open free market.

These social and environmental sustainability possibilities for cryptocurrency and blockchain technology require research and monitoring [76]. In each situation, social and environmental outcomes can be both negative and positive. Determining the environments, actions, practices, and decisions to determine whether negative or positive sustainability outcomes occur requires further research [77]. To complete this research knowledge and experience across disciplines, locations, regulatory, and economic systems are needed. The research can be quite substantial and necessary.

6 Conclusion

Financial systems play a critical role in guiding society toward sustainable movements. However, the business community still needs to respond to many concerns about the scalability, vulnerability, and sustainability of crypto networks. This chapter reviewed the basics of developing cryptocurrency systems and elaborates on scalability and sustainability as two main characteristics expected from future cryptocurrency networks.

With a particular focus on sustainability implications, this study provided insights into energy consumption and e-waste generation among the sustainability-related concerns of the crypto networks. It argued the need for opening a new paradigm shift for the design and development of financial systems that provide economic, environmental, and social benefits and provides opportunities for sustainable practices. Further, we have elaborated on the social sustainability of crypto technology and the need for further research on how technology should be employed to empower small businesses, establish a culture of sustainable behavior, and the emergence of new economic models and a free market.

It should be noted that much more work has been accomplished in the computer science community that has not been covered in this chapter. The primary purpose of this study was to give beginners an overview of how the cryptocurrency network functions, what opportunities for social benefits it offers, and what aspects of the technology require further investigation.

References:

[1] de Best, R., 2022, "Number of Cryptocurrencies Worldwide from 2013 to February 2022," https://www.statista.com/statistics/863917/number-crypto-coins-tokens/.

[2] Klarin, A., 2020, "The Decade-Long Cryptocurrencies and the Blockchain Rollercoaster: Mapping the Intellectual Structure and Charting Future Directions," Res. Int. Bus. Financ., **51**, p. 101067.

[3] Templier, M., and Paré, G., 2015, "A Framework for Guiding and Evaluating Literature Reviews," Commun. Assoc. Inf. Syst., **37**(1), p. 6.

[4] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S., 2016, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press.

[5] Vryonis, P., 2013, "Explaining Public-Key Cryptography to Non-Geeks," Mediu. com, August, **27**.

[6] Ismail, L., and Materwala, H., 2019, "A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions," Symmetry (Basel)., **11**(10), p. 1198.

[7] Barber, S., Boyen, X., Shi, E., and Uzun, E., 2012, "Bitter to Better—How to Make Bitcoin a Better Currency," *International Conference on Financial Cryptography and Data Security*, Springer, pp. 399–414.

[8] Conoscenti, M., Vetro, A., and De Martin, J. C., 2016, "Blockchain for the Internet of Things: A Systematic Literature Review," *2016 IEEE/ACS 13th International*

Conference of Computer Systems and Applications (AICCSA), IEEE, pp. 1–6.

[9] Sompolinsky, Y., Lewenberg, Y., and Zohar, A., 2016, "SPECTRE: A Fast and Scalable Cryptocurrency Protocol.," IACR Cryptol. ePrint Arch., **2016**(1159).

[10] Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., and Sirer, E. G., 2016, "On Scaling Decentralized Blockchains," *International Conference on Financial Cryptography and Data Security*, Springer, pp. 106–125.

[11] Gupta, P., and Kumar, P. R., 2000, "The Capacity of Wireless Networks," IEEE Trans. Inf. theory, **46**(2), pp. 388–404.

[12] Mallett, J., 2020, "SCALING AND CONSENUS IN MONETARY SYSTEMS."

[13] Eyal, I., and Sirer, E. G., 2014, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," *International Conference on Financial Cryptography and Data Security*, Springer, pp. 436–454.

[14] Blinder, M., 2018, "Making Cryptocurrency More Environmentally Sustainable."

[15] Sompolinsky, Y., and Zohar, A., 2013, "Accelerating Bitcoin's Transaction Processing," Fast money grows trees, not Chain.

[16] Gencer, A. E., Basu, S., Eyal, I., Van Renesse, R., and Sirer, E. G., 2018, "Decentralization in Bitcoin and Ethereum Networks," *International Conference on Financial Cryptography and Data Security*, Springer, pp. 439–457.

[17] Stone, D., 2018, "An Overview of Proof of Work Based Blockchain Consensus Protocols (Part 1)," https://medium.com/ [Online]. Available: https://medium.com/@drstone/an-overview-of-proof-of-work-based-blockchain-consensus-protocols-part-1-e04102885093.

[18] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., and Felten, E. W., 2015, "Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," *2015 IEEE Symposium on Security and Privacy*, IEEE, pp. 104–121.

[19] Kim, S., Kwon, Y., and Cho, S., 2018, "A Survey of Scalability Solutions on Blockchain," *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, pp. 1204–1207.

[20] Poon, J., and Dryja, T., 2016, "The Bitcoin Lightning Network: Scalable off-Chain Instant Payments."

[21] Nadiya, U., Mutijarsa, K., and Rizqi, C. Y., 2018, "Block Summarization and Compression in Bitcoin Blockchain," *2018 International Symposium on Electronics and Smart Devices (ISESD)*, IEEE, pp. 1–4.

[22] Alsalami, N., and Zhang, B., 2020, "Uncontrolled Randomness in Blockchains: Covert Bulletin Board for Illicit Activity," *2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS)*, IEEE, pp. 1–10.

[23] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., and Saxena, P., 2016, "A Secure Sharding Protocol for Open Blockchains," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 17–30.

[24] Forum, T. E. U. B. O. and F., 2019, *Scalability, Interoperability and Sustainability of Blockchain*.

[25] Zhou, Q., Huang, H., Zheng, Z., and Bian, J., 2020, "Solutions to Scalability of Blockchain: A Survey," IEEE Access, **8**, pp. 16440–16455.

[26] Maleh, Y., Shojafar, M., Alazab, M., and Romdhani, I., 2020, *Blockchain for*

Cybersecurity and Privacy: Architectures, Challenges, and Applications, CRC Press.

[27] Dasgupta, D., Shrein, J. M., and Gupta, K. D., 2019, "A Survey of Blockchain from Security Perspective," J. Bank. Financ. Technol., **3**(1), pp. 1–17.

[28] Sayeed, S., and Marco-Gisbert, H., 2019, "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack," Appl. Sci., **9**(9), p. 1788.

[29] Ebrahimpour, G., and Haghighi, M. S., 2021, "Analysis of Bitcoin Vulnerability to Bribery Attacks Launched Through Large Transactions," arXiv Prepr. arXiv2105.07501.

[30] Zargar, S. T., Joshi, J., and Tipper, D., 2013, "A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Commun. Surv. tutorials, **15**(4), pp. 2046–2069.

[31] Levine, B. N., Shields, C., and Margolin, N. B., 2006, "A Survey of Solutions to the Sybil Attack," Univ. Massachusetts Amherst, Amherst, MA, **7**, p. 224.

[32] Chen, J., Xia, X., Lo, D., Grundy, J., Luo, X., and Chen, T., 2021, "Defectchecker: Automated Smart Contract Defect Detection by Analyzing Evm Bytecode," IEEE Trans. Softw. Eng.

[33] Biryukov, A., and Tikhomirov, S., 2019, "Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis," *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, pp. 172–184.

[34] Zhang, L., Li, H., Li, Y., Yu, Y., Au, M. H., and Wang, B., 2019, "An Efficient Linkable Group Signature for Payer Tracing in Anonymous Cryptocurrencies," Futur. Gener. Comput. Syst., **101**, pp. 29–38.

[35] Li, J., Li, N., Peng, J., Cui, H., and Wu, Z., 2019, "Energy Consumption of Cryptocurrency Mining: A Study of Electricity Consumption in Mining Cryptocurrencies," Energy, **168**, pp. 160–168.

[36] Krause, M. J., and Tolaymat, T., 2018, "Quantification of Energy and Carbon Costs for Mining Cryptocurrencies," Nat. Sustain., **1**(11), p. 711.

[37] Gallersdörfer, U., Klaaßen, L., and Stoll, C., 2020, "Energy Consumption of Cryptocurrencies beyond Bitcoin," Joule, **4**(9), pp. 1843–1846.

[38] Yan, L., Mirza, N., and Umar, M., 2022, "The Cryptocurrency Uncertainties and Investment Transitions: Evidence from High and Low Carbon Energy Funds in China," Technol. Forecast. Soc. Change, **175**, p. 121326.

[39] O'Dwyer, K. J., and Malone, D., 2014, "Bitcoin Mining and Its Energy Footprint."

[40] Bitcoin.org, 2019, "Bitcoin Mining," https://bitcoin.org/en/faq#what-is-bitcoin-mining.

[41] Carter, N., 2018, "Digesting 'Quantification of Energy and Carbon Costs for Mining Cryptocurrencies,'" Medium.com [Online]. Available: https://medium.com/@nic__carter/digesting-quantification-of-energy-and-carbon-costs-for-mining-cryptocurrencies-1f019e10fad4.

[42] Mora, C., Rollins, R. L., Taladay, K., Kantar, M. B., Chock, M. K., Shimada, M., and Franklin, E. C., 2018, "Bitcoin Emissions Alone Could Push Global Warming above 2 C," Nat. Clim. Chang., **8**(11), p. 931.

[43] Stoll, C., Klaaßen, L., and Gallersdörfer, U., 2018, "The Carbon Footprint of Bitcoin."

[44] De Vries, A., and Stoll, C., 2021, "Bitcoin's Growing e-Waste Problem," Resour. Conserv. Recycl., **175**, p. 105901.

[45] Masanet, E., Shehabi, A., Lei, N., Vranken, H., Koomey, J., and Malmodin, J., 2019,

"Implausible Projections Overestimate Near-Term Bitcoin CO2 Emissions," Nat. Clim. Chang., **9**(9), pp. 653–654.

[46] PRNewswire, 2021, "Blockchain Goes Green: Signum - the World's First Truly Sustainable Blockchain Steps into the Light" [Online]. Available: https://www.prnewswire.com/news-releases/blockchain-goes-green-signum---the-worlds-first-truly-sustainable-blockchain-steps-into-the-light-301320293.html.

[47] Schrijvers, O., Bonneau, J., Boneh, D., and Roughgarden, T., 2016, "Incentive Compatibility of Bitcoin Mining Pool Reward Functions," *International Conference on Financial Cryptography and Data Security*, Springer, pp. 477–498.

[48] Tuwiner, J., 2019, "Bitcoin Mining Pools," https://www.buybitcoinworldwide.com/mining/pools/.

[49] Jana, R. K., Ghosh, I., and Wallin, M. W., 2022, "Taming Energy and Electronic Waste Generation in Bitcoin Mining: Insights from Facebook Prophet and Deep Neural Network," Technol. Forecast. Soc. Change, **178**, p. 121584.

[50] Nandi, S., Sarkis, J., Hervani, A. A., and Helms, M. M., 2021, "Redesigning Supply Chains Using Blockchain-Enabled Circular Economy and COVID-19 Experiences," Sustain. Prod. Consum., **27**, pp. 10–22.

[51] Kaal, W. A., 2021, "Blockchain Solutions for Agency Problems in Corporate Governance," *Information for Efficient Decision Making: Big Data, Blockchain and Relevance*, World Scientific, pp. 313–329.

[52] Whitaker, A., and Kräussl, R., 2020, "Fractional Equity, Blockchain, and the Future of Creative Work," Manage. Sci., **66**(10), pp. 4594–4611.

[53] Huynh, T. L. D., Hille, E., and Nasir, M. A., 2020, "Diversification in the Age of the 4th Industrial Revolution: The Role of Artificial Intelligence, Green Bonds and Cryptocurrencies," Technol. Forecast. Soc. Change, **159**, p. 120188.

[54] Esmaeilian, B., Sarkis, J., Lewis, K., and Behdad, S., 2020, "Blockchain for the Future of Sustainable Supply Chain Management in Industry 4.0," Resour. Conserv. Recycl., **163**, p. 105064.

[55] Imbault, F., Swiatek, M., De Beaufort, R., and Plana, R., 2017, "The Green Blockchain: Managing Decentralized Energy Production and Consumption," *2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, IEEE, pp. 1–5.

[56] Woo, J., Fatima, R., Kibert, C. J., Newman, R. E., Tian, Y., and Srinivasan, R. S., 2021, "Applying Blockchain Technology for Building Energy Performance Measurement, Reporting, and Verification (MRV) and the Carbon Credit Market: A Review of the Literature," Build. Environ., **205**, p. 108199.

[57] Patel, D., Britto, B., Sharma, S., Gaikwad, K., Dusing, Y., and Gupta, M., 2020, "Carbon Credits on Blockchain," *2020 International Conference on Innovative Trends in Information Technology (ICITIIT)*, IEEE, pp. 1–5.

[58] Dorfleitner, G., and Braun, D., 2019, "Fintech, Digitalization and Blockchain: Possible Applications for Green Finance," *The Rise of Green Finance in Europe*, Springer, pp. 207–237.

[59] Lindenberg, N., 2014, "Definition of Green Finance."

[60] Conlon, T., Corbet, S., and McGee, R. J., 2020, "Are Cryptocurrencies a Safe Haven for

Equity Markets? An International Perspective from the COVID-19 Pandemic," Res. Int. Bus. Financ., **54**, p. 101248.

[61] Goodell, J. W., and Goutte, S., 2021, "Diversifying Equity with Cryptocurrencies during COVID-19," Int. Rev. Financ. Anal., **76**, p. 101781.

[62] Rijanto, A., 2020, "Business Financing and Blockchain Technology Adoption in Agroindustry," J. Sci. Technol. Policy Manag.

[63] Mora, H., Morales-Morales, M. R., Pujol-López, F. A., and Mollá-Sirvent, R., 2021, "Social Cryptocurrencies as Model for Enhancing Sustainable Development," Kybernetes.

[64] Kugler, L., 2021, "Non-Fungible Tokens and the Future of Art," Commun. ACM, **64**(9), pp. 19–20.

[65] Madichie, N. O., and Hinson, R. E., 2022, "The Future of Africa's Creative Industries," *The Creative Industries and International Business Development in Africa*, Emerald Publishing Limited.

[66] Wastling, T., Charnley, F., and Moreno, M., 2018, "Design for Circular Behaviour: Considering Users in a Circular Economy," Sustainability, **10**(6), p. 1743.

[67] Amel, E. L., Manning, C. M., and Scott, B. A., 2009, "Mindfulness and Sustainable Behavior: Pondering Attention and Awareness as Means for Increasing Green Behavior," Ecopsychology, **1**(1), pp. 14–25.

[68] McKenzie-Mohr, D., 2011, *Fostering Sustainable Behavior: An Introduction to Community-Based Social Marketing*, New society publishers.

[69] Tao, R., Su, C.-W., Naqvi, B., and Rizvi, S. K. A., 2022, "Can Fintech Development Pave the Way for a Transition towards Low-Carbon Economy: A Global Perspective," Technol. Forecast. Soc. Change, **174**, p. 121278.

[70] Nguyen, L. T. Q., Hoang, T. G., Do, L. H., Ngo, X. T., Nguyen, P. H. T., Nguyen, G. D. L., and Nguyen, G. N. T., 2021, "The Role of Blockchain Technology-Based Social Crowdfunding in Advancing Social Value Creation," Technol. Forecast. Soc. Change, **170**, p. 120898.

[71] Truby, J., 2018, "Decarbonizing Bitcoin: Law and Policy Choices for Reducing the Energy Consumption of Blockchain Technologies and Digital Currencies," Energy Res. Soc. Sci., **44**, pp. 399–410.

[72] Liu, C., Zhang, X., and Medda, F., 2021, "Plastic Credit: A Consortium Blockchain-Based Plastic Recyclability System," Waste Manag., **121**, pp. 42–51.

[73] Ajwani-Ramchandani, R., and Sarkis, J., 2021, "Time to Consider Circular and Social Credits Exchanges?," Resour. Conserv. Recycl., **175**, p. 105860.

[74] De Filippi, P., 2017, "What Blockchain Means for the Sharing Economy," Harv. Bus. Rev.

[75] McElroy, W., 2016, "Bitcoin Markets: Black and Gray, White and Red," Bitcoin.com.

[76] Mustafa, F., Lodh, S., Nandy, M., and Kumar, V., 2021, "Coupling of Cryptocurrency Trading with the Sustainable Environmental Goals: Is It on the Cards?," Bus. Strateg. Environ.

[77] Bai, C. A., Cordeiro, J., and Sarkis, J., 2020, "Blockchain Technology: Business, Strategy, the Environment, and Sustainability," Bus. Strateg. Environ., **29**(1), pp. 321–322.