# 1 Introduction

As the core technology of the Bitcoin project [1], blockchain attracts various researchers from all walks of life. Most previous research preferred to construe the blockchain as a decentralized ledger, focusing on the technology components. In the past decade, there has been a surge in research activities that focus on the behaviors driven by economic principles regarding a decentralized digital ledger from different scales. Historically, the blockchain protocols were first implemented heuristically within the engineering community, and the theoretical analysis of these protocols appeared at a later time.

For this reason, there still exist a number of gaps between the engineering practices and the theoretical proofs or analyses of those protocols in terms of security, decentralization, efficiency, and other related performance indices. These theoretical gaps lead to the need of the following.

1. Reaching the consensus regarding the scope of challenges and problems faced by the protocol or mechanism design of blockchain networks, and then finding a viable paradigm of protocol modeling and design that guarantees secure operation of the target blockchain networks.
2. Investigating the interaction between a blockchain protocol and its peripheral systems or networks which overlay or underlay upon the blockchain network; furthermore, provision of the theoretical analysis with respect to different performance indices for a distributed ledger system including security, scalability, and service efficiency.
3. Providing a theoretical insight into the emerging applications of blockchain technologies in a plethora of areas, and, more importantly, supplementing a series of mathematical tools that are able quantitatively to analyze the dynamics of these blockchain-based approaches, especially from a (behavioral) economics perspective.

With the aforementioned major goals in mind, this book aims to categorize the building technologies of blockchains in a stack of protocols and mechanisms that defines the interaction among nodes in the ledger networks and service-related entities or stakeholders. Such an approach of behavior abstraction emphasizes the fundamental characteristics of agent rationality in distributed systems, and then creates a paradigm of ledger protocol design based on the mathematical tools of game theory, algorithmic mechanism design, optimization theory, and contract or portfolio theory. The proposed paradigm helps to transform the interpretation of blockchain technologies, from its

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

technical basis of computer networking and cryptography (e.g., those focusing on data communication and security) to the new perspective of a financial–social-economic network. By doing so, we are able theoretically to deal with different parties or agents involved in the blockchain networks, for example, adversaries for security modeling and rational entities for performance evaluation, with a layered but consistent framework of analysis. Such a framework of study also leads to the following main objectives of this book.

- The book provides a succinct overview of the technical components of the blockchain networks (equivalently, distributed digital ledger networks). Based on these building blocks, we dedicate seven chapters to how the mathematical tools of game theory and algorithmic mechanism design can be applied to the analysis, design, and improvement of the blockchain network protocols. In particular, from an engineering perspective of economic theory, we provide an in-depth insight into how the economic interests of different types of participants in the blockchain system shape the way of their behaviors. Consequently, by properly designing the distributed economic mechanism that regulates the interactions of the system participant, we provide a paradigm for designing the blockchain consensus protocols, which lead the blockchain network as a whole to the desired joint behaviors in the form of system equilibria.
- In addition to the economic theoretic analysis of the consensus protocols in blockchain networks, we extend our study to the more complex economic systems that are either embedded into a blockchain network, or use the blockchain network as a component subsystem. With such extended studies, we not only provide a generic and consistent framework of ecosystem analysis from the perspective of economic theory (more precisely, microeconomics theory), but also supply the readers with an extended mathematical toolbox for blockchain system analysis and design. Such an approach, in particular, emphasizes the expressiveness and power of game-theoretical analyses. We provide a series of case studies to illustrate the incorporated approaches that emphasize the importance of both theoretical analysis and engineering implementation.
- The book also provides an extensive overview of both the prevalent blockchain networks and the emerging blockchain applications in the form of a series of case studies. These case studies help the readers to understand how the blockchain network protocols evolve as the target performance indices changes at the designing stage of the protocol, and, with different economic preference, how a particular set of blockchain protocols can be adapted to meet the requirement of service provision in different scenarios.

We believe that the proposed book is useful to a variety of readers, particularly those from the computer science and computer networking fields, as well as those with an economics background. The materials from this book can be used to guide the development of more efficient, scalable, and robust blockchain protocols as well as the deployment of the blockchain applications in related domains. The target audience for this book is the researchers, engineers, and undergraduate and graduate students who

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

are looking for a source to learn the technical framework of blockchain networks, and those who need theoretical guidance in mechanism design of distributed blockchain networks and other systems alike.

## 1.1 Two Camps: Computer Science Problem and Incentive Mechanism Problem

The advent of blockchain technology benefits a wide range of areas, including finance, business, transportation, and entertainment. Blockchain is the technology that was first proposed in the Bitcoin project, followed by extensive research and application. Owing to the sophistication and diversity of the blockchain system, the interpretation of blockchain is manifested into two camps [2].

1. Blockchain is a solution to computer science problems. The first camp mainly focuses on (a) consensus analysis, (b) cryptography application, and (c) distributed system design.
2. Blockchain is a solution to incentive mechanism design problems. The second camp primarily focuses on (a) economics analysis and (b) game theory and equilibrium.

In earlier research of blockchain, the first camp had made enormous contributions to the technical components. It is worth noting that blockchain is not a single new technology but a combination of multiple technologies. The springing up and brisk developing of computer and network technologies directly promoted the blockchain evolution.

The concept of blockchain was first outlined in 1991 [3]. Stuart Haber and W. Scott Stornetta presented the fundamental notion of blockchain, a chain of hashed records, to address the time-stamping problem, the embryonic form of data structure in the blockchain, while not defining the name "blockchain." Then, in 1997, Adam Back created Hashcash [4], a Proof of Work (PoW) mechanism for email antispam and anti-DoS (denial of service) that has since formed the foundation for most cryptocurrency projects. A brief history of blockchain is shown in Fig. 1.1.

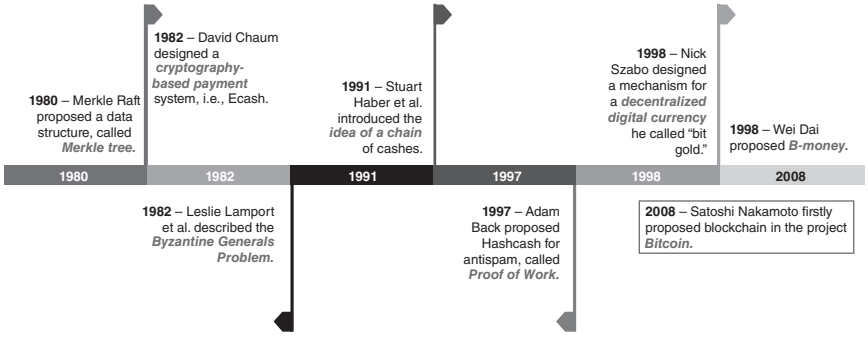


**Figure 1.1** Origins of blockchain.

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

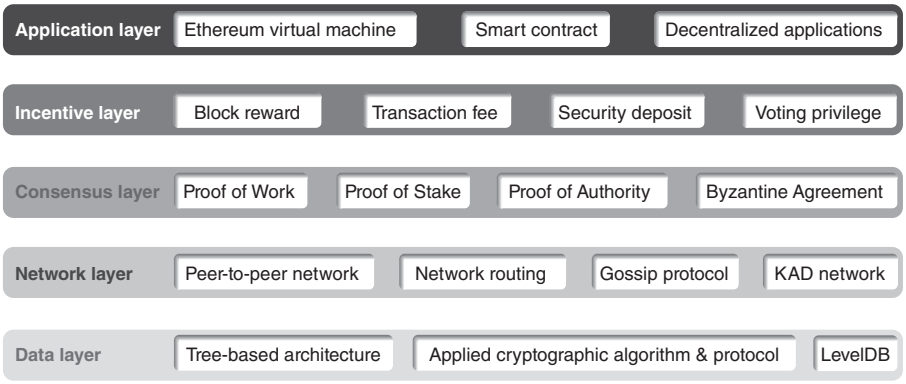


**Figure 1.2** Five layers of blockchain technology.

Until the advent of Bitcoin in January 2009, the blockchain had its first real-world application. According to bitcoin's white paper [1], "Bitcoin: A peer-to-peer electronic currency system," Satoshi Nakamoto adopted cryptography and Proof of Work (PoW) in the Bitcoin network to ensure data security and consistency and introduced incentive mechanisms to allow transactions to be completed without the involvement of a third party, ushering in a new era of decentralization.

To better understand the second camp, we first give a rough description of blockchain technical components from the first camp perspective. As a collection of technologies, blockchain is composed of a set of interdependent and interrelated components. To facilitate the description, we adopt the recognized five-layer architecture (shown in Fig. 1.2), and explain the components and layers in the following.

- **Data layer:** The data structure of most conventional blockchains is described as a linked chain of blocks in which transactions are organized in a sequential manner. In addition to Bitcoin, various PoW-based blockchain projects also use chain structure to manage the blocks. Each block of Bitcoin includes a Merkle hash tree [5], which is a tree-based data structure of transaction hashes. The root hash of tree is obtained by calculating the leaf nodes, which refer to the hashes of transaction data.

  The tree-based data structure uses the hash function to ensure the transaction data security and integrity. To verify the authenticity of transactions, a digital signature [6] is required before sending any transaction. As all kinds of cryptocurrency projects' names indicate, "crypto" means that these projects must rely on cryptography for security. Bitcoin uses an elliptical-curve cryptography to generate the public keys for users.

  All the data and information on the Bitcoin are duplicated and scattered in different nodes throughout the network. For the full nodes, they store the metadata in LevelDB [7]. Some other blockchain projects, such as Ethereum [8], also utilize LevelDB to keep all the data.
- **Network layer:** The network layer refers to the network model, network routing protocols, as well as some other communication protocols. The public blockchain

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

is built upon a peer-to-peer (P2P) network, in which each node joins by connecting to some other nodes. A P2P network consists of a group of computers or clients that communicate with each other. The term "peer" means that every node is treated equally in the network. There is no centralized party with nodes. The peer nodes serve both as providers of resources and as consumers of services. The distributed and decentralized P2P network is the foundation of blockchain.

The network layer functions are almost carried out by the P2P network. In addition to mining and transferring value, some blockchain nodes also have the same functions as P2P nodes. To participate in the network, all nodes must have the routing function [9], which helps them to share information with each other. The most often used unstructured P2P network protocol is the gossip protocol [10]. After a miner generates a block, the others will broadcast the result and block via a gossip protocol. Bitcoin changed the way it distributed gossip messages in 2015 to improve privacy. It currently employs a technique known as "diffusion" [11]. Another well-known communication protocol is called the Kademlia (KAD) protocol [12]. The KAD network refers to a P2P network that implements the KAD protocol. As a more efficient protocol, some blockchain projects adopt the KAD network as their network layer to enable the blocks and transactions transmission optimization [13].

- **Consensus layer:** The consensus layer specifies the rules for nodes to reach an agreement on blockchain's state. The popular consensus protocols include the Proof of Work (PoW) in Bitcoin and the Proof of Stake (PoS) in Ethereum. To illustrate the consensus layer, we discuss the PoW algorithm here as it is the most common algorithm for permissionless blockchains, used by Bitcoin [1]. Taking PoW as an example, the protocol determines who is eligible to create a new block, the time slot between two contiguous blocks, and stipulates all nodes to work on the longest chain. Different consensus algorithms employ various principles to determine the rules for nodes based on their actual needs. Ethereum is now experiencing the transition from PoW to PoS since PoW is energy intensive and costly [14]. Unlike PoW's elite hardware requirements, PoS only needs participants to stake some cryptocurrencies to the main chain. The creator of each block is selected randomly, similar to the miners of PoW, and is responsible for finalizing transactions and working on the longest chain [15]. Some other protocols can be referred to Proof of Authority [16] and Byzantine Agreement [17].
- **Incentive layer:** The incentives layer establishes an incentive system using the blockchain's cryptocurrency. In the initial design of Bitcoin, the incentives refer to block reward and transaction fee, incentivizing the miners to work on the longest chain and encouraging the other participants to finalize the blockchain's ledger. From the Bitcoin project it is clear that any permissionless blockchain system requires an incentive strategy to keep it running. Miners should be appropriately compensated for their effort, and incentives should push them to act honestly. As the nexus to bind the different technologies to form the blockchain, incentives are apparently less discussed by the first camp whereas they have been emphasized and characterized by the second camp. Ethereum proposed the concept of the

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

security deposit in their Casper protocol [18], which will be one of the most essential incentive components in Ethereum 2.0. According to the latest update of staking deposit requirements on the Ethereum website, everyone needs to stake some ethers to the network before joining the Ethereum [19]. Moreover, anyone who wants to become a full validator must stake 32 ethers. Another crucial incentive is the voting privilege, which is less used in PoW-based blockchain but indispensable to PoS-based blockchain. The reason is that PoS protocols rely on voting mechanisms to reach consensus [20]. Incentives are the focus of this book. We further illustrate the details in Chapters 3 and 4.

- **Application layer:** The application layer includes Ethereum Virtual Machine, smart contracts, decentralized apps (Dapps), and so on. The Ethereum Virtual Machine is a software framework that allows developers to construct Ethereum-based decentralized applications (Dapps). All Ethereum accounts' data and smart contracts codes are stored on this virtual machine [21]. Similar to the Ethereum accounts (also known as the externally owned account), smart contracts are also a type of account (contract account). The smart contract is a collection of codes with a unique address or account, which can be created by any developers and can operate automatically on Ethereum [22]. The Dapps that interface with the blockchain network make up the most important part of the application layer. These Dapps interoperate with the blockchain network via application programming interfaces (APIs). Unlike the traditional apps (centralized apps), the Dapps run on a decentralized network environment and often require the users to interact with the developer's smart contract to get the download permits. Applications can send instructions to all the underlying layers, which enables all layers to cooperate with each other to perform more advanced functions.

The first camp is much bigger than the second camp. One main reason is that many techniques of blockchain have existed for decades. The researchers in computer science have an abundance of reference literature and research experiences due to years of accumulation. Although the blockchain has remained the focus of both the industry and academia for almost a decade, most of the available literature on blockchains is still at a stage of targeting the audiences who are mainly interested in obtaining the hands-on experience of blockchain implementation. There are only a handful of books for researchers, engineers, and graduate or undergraduate students to understand theoretically the dynamics in economic incentives of blockchain networks from a comprehensive and in-depth perspective. For this reason, there is an urgent need to develop a comprehensive reference to provide a systematic treatment of the following.

1. How blockchain incentives can be modeled, designed, and analyzed.
2. What the impact of the incentives on protocols design will be.
3. How it can be further improved or incorporated into various emerging distributed applications, and with what techniques.

In Section 1.2, we introduce the second camp, which formulates a new concept called "Cryptoeconomics." This nomenclature represents the fact that cryptoeconomics

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

is an area of interdisciplinary research, which requires researchers to possess a variety of research backgrounds, including (but not limited to) cryptography and economic mechanism design, etc.

## 1.2 Cryptoeconomics Camp

Compared with the abundant research of camp one, scant attention has been paid to the incentive mechanism design for distributed systems. A sophisticated blockchain system requires multi-dimensional design, not only from the computer science perspective but also from the mechanism design perspective.

The computer science content determines the existence of a blockchain framework. Simultaneously, the incentive mechanism improves the system performance by regulating participants' behaviors and coordinating all operations through the costs and benefits. Researchers have gradually realized that computer science and economic incentives are inextricable inside a blockchain system as the technologies evolve. In order to develop blockchain technology in an all-around way, none of the parts can be studied independently.

### 1.2.1 Definitions and Explanations

Ethereum founder Vlad Zamfir first defined cryptoeconomics as "A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralized digital economy" [23]. The other versions of definition are listed as follows: "Cryptoeconomics is the application of incentive mechanism design to information security problems" [2]. Zamfir identified that cryptoeconomics has played a crucial role in distributed systems, that is, to encourage more entries and to incentivize the desired behaviors. Vitalik Buterin expounded on the concept as "Cryptoeconomics is about building systems that have certain desired properties, use cryptography to prove properties about messages that happened in the past, use economic incentives defined inside the system to encourage desired properties to hold into the future" [24]. Josh Stark proposed that "Cryptoeconomics is the practical science of using economic mechanisms to build distributed systems, where the financial incentives guarantee essential properties of that system and where the economic mechanisms are guaranteed by cryptography" [25]. He presented the most detailed explanation regarding the keywords of this definition as follows.

- Practical science: Bitcoin, PoW, Ethereum, PoS, State Channels, Plasma, Sharding, etc., are the applications of cryptoeconomics. Any incentive mechanism involved a blockchain system is designed upon the science of cryptoeconomics.
- Using economic mechanisms to build distributed systems: Cryptoeconomics has most in common with mechanism design. Mechanism design is also called "reverse game theory." An applicable economic mechanism for distributed system requires the abilities of making rules of participation, realizing microincentives, designing the scalable incentives, and being easy to execute in a leaderless environment.

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

- The important properties of that protocol are guaranteed by financial incentives: A consensus protocol functioning smoothly requires there are proper financial incentives compensating participants' costs due to working on the issued tasks. Without participants' efforts on accomplishing tasks, there will be no security guarantee in a leaderless system. Hence, the insecure system will be deemed as having no market value.
- The economic mechanisms are guaranteed by cryptography: Cryptography and cryptographic protocols are the underlying fundamentals of a blockchain network which provide secure and trusted platforms and protect all mechanisms from potential attacks. Economic incentives refer to the monetary subsidies and attributed privileges for the participants who accomplish tasks as required. Cryptography can provide protection from abuse and interruption, thus ensuring the mechanisms will operate normally.

We conclude the interpretation of cryptoeconomics concept in two ways.

- It provides the theoretical interpretation, from the perspective of untrusted economic networks, of the consensus protocols assisted by cryptographical functionalities in decentralized blockchain networks regarding the activities of the entities in the network and the dynamics of the network as a whole.
- It extends the analytical framework based on the economic networking point of view to modeling, designing, and analyzing the participant interactions in any ecosystem that is extended from or build upon blockchain networks.

Therefore, on one hand, the behavioral analysis from the economic perspective of the blockchain networks answers a series of fundamental questions regarding cryptography and distributed system security. Such an analytical approach plays a vital role in designing appropriate protocols in digital ledger networks, especially for those built upon massive P2p networks without an explicit governance infrastructure. On the other hand, from the engineering perspective, a well-functioning, scalable cryptoeconomic network is able to serve as an efficient platform for decision arbitration and allocation of the resources ranging from physical utilities (e.g., hardware) to financial assets, and, more broadly, various conceptual resources including data, trust, and social attention (e.g., votes). As a result, the convergence of computer networking, cryptography, and economic theory sheds light on better characterization of the decentralized or self-organized systems particularly relying upon the advance of the blockchain technologies, as depicted in Fig. 1.3. This, in return, requires a comprehensive study of the technical building blocks, such as consensus protocols, incentive mechanisms, cryptographic and networking functionalities, and all the related primitives from an interdisciplinary perspective.

Despite the similarities between cryptoeconomics and incentive mechanisms, the differences are certainly worth studying. Cryptoeconomics provides more of an alternative framework for analyzing decentralized projects with incentives. The second

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

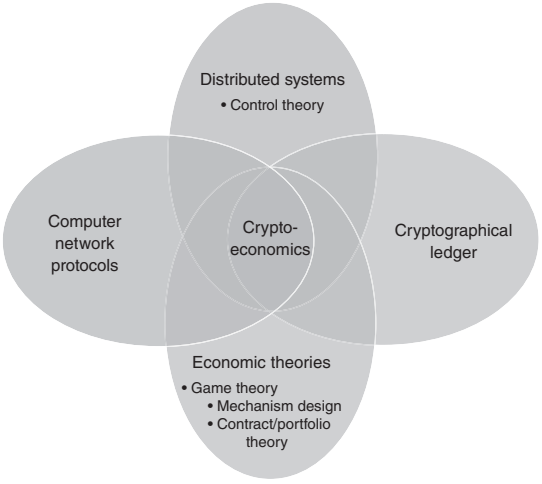


**Figure 1.3** Cryptoeconomics as an interdisciplinary analytical framework.

camp proposed a collection of primitives under the cryptoeconomics framework, providing another angle of interpretation regarding the existing cryptoeconomics applications. We will introduce the details in the following section.

### 1.2.2 Concepts, Assumptions, and Models

For better analyzing the efficiency and equilibrium of cryptoeconomic outcomes, Vitalik Buterin proposed some crucial concepts that can be referred to as the following [24].

1. **Cryptoeconomics resource:** This is the incentives that a system can distribute to the participants, and the computation power that the participants can contribute to the system. For example, tokens for block generation, or the hash power of individual computer.
2. **Cryptoeconomics security margin:** This is an amount of money $X$ such that a user can prove "either a given guarantee $G$ is satisfied, or those at fault for violating $G$ are poorer than they otherwise would have been by at least $X$." In brief, a cryptoeconomics security margin indicates the fraction of all cryptoeconomics resources that an attacker would need to take over the whole network. For example, if a blockchain network can resist a 51% attack, then we would say that the security margin is 0.5, and the guarantee $G$ is "no double-spending." It means that if an attacker wants to launch a double-spending attack, he or she must have at least one half of the total hashing power (i.e., cryptoeconomics resource).
3. **Cryptoeconomics proof:** This is a message signed by an actor that can be interpreted as "I certify that either $P$ is true. Otherwise, I have to suffer an economic

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

loss of size $X$." For example, Ethereum requires all participants to stake a certain amount of ethers before joining the network, for which the staked money serves as a "security deposit." If anyone has done something illegal, their deposit will be slashed.

There are also some reasonable assumptions that apply to cryptoeconomics [26].

1. **Rationality majority:** This refers to the case that the majority of users can be reasonably modeled as economically rational entities. This assumption is consistent with the rationality assumption in economic theory. Otherwise, we are not able to use mechanism design to obtain the economic incentives.
2. **No restriction on entry or exit:** The number of system users must be large. Anyone can enter or exit the system with no restrictions. If there must be some restrictions, the system should inform all users before the restrictions become effective.
3. **No censorship:** Any two nodes can communicate with each other.
4. **Anonymous:** The anonymous users cannot have their real identities revealed. The core natures of blockchain should not be compromised.

These assumptions are the basis for designing cryptoeconomics applications. Security models differ from the assumptions since various applications may have different security models and margins [24]. However, all the cryptoeconomics applications should follow the same assumptions mentioned.

1. **Uncoordinated choice model:** A model that assumes that all participants in a protocol do not coordinate with each other and have separate incentives, and are all smaller than size $X$.
2. **Coordinated choice model:** A model that assumes that all actors in a protocol are controlled by the same agent.
3. **Bribing attacker model:** An attack is capable of making payments to participants conditional of them taking certain actions.
   - Budget: The amount that the briber must be willing to pay in order to execute a particular strategy
   - Cost: The amount that the briber actually does pay if the strategy succeeds.
4. **Fault attribution:** This is a process by which an incentive mechanism infers which strategies were taken by the players in the network and is a nascent field of study that addresses realistic issues faced by any open or public distributed system.
   - It helps us penalize players who did not play the strategy intended by the mechanism.
   - It makes easy to have robust coalitional dominant strategy equilibrium.

These components consist of the cryptoeconomics analysis framework. So what is the outcome criterion of cryptoeconomics research? According to Ethereum Foundation's talk [27], a good outcome should meet the following requirements.

1. Easier exchange: The incentive must have good liquidity and be liquidated very quickly.

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

2. Trustless trades: The trades can be processed without a third party.
3. Liquidity for small markets: The liquidity of outcomes should not be limited or impacted by market size.

A key conclusion of the talk is that if the mechanism cannot help the system know your customers (KYC) better and always leads to the rich getting richer, then a bad outcome would always exist. Unfortunately, a considerable amount of research using game theory and economics theory cannot achieve fairness as expected.

A better mechanism should be as simple as possible, therefore reducing the dependency on parameter selection. Moreover, the mechanism must be feasible and easy to implement in a distributed and decentralized system.

As blockchain technology evolves, more and more researchers have been making strides in academic research and commercial applications, demonstrating that cryptoeconomics promises to provide sufficient stability, persistence, and robustness. The success of cryptoeconomics applications corroborates Buterin's point and enriches the related conceptual architecture.

### 1.2.3 Case Studies: Bitcoin and Schelling Coins

Bitcoin is acknowledged as the first P2P digital currency payment system due to its underlying technology, which refers to a decentralized and distributed database comprising various components. As the first application of cryptoeconomics system, we can say the following.

1. Bitcoin uses PoW consensus to resist Sybil attack.
2. Bitcoin uses block rewards and transaction fees to compensate miners for their effort, and to incentivize them to work on the longest chain.
3. Most of Bitcoin's users are honest and rational.
4. Bitcoin has no access restriction. Anyone can enter or exit the network at any time.
5. Any two Bitcoin users can communicate with each other relatively quickly.
6. Users in Bitcoin network are anonymous, and there is no way to restore users' real identities.

Therefore, as a decentralized system that is embedded with an incentive mechanism, Bitcoin is the canonical example of a cryptoeconomics application. The cryptoeconomics resource of Bitcoin refers to the hashing power which is required by PoW. Bitcoin is apparently grounded on the cryptoeconomics assumptions, as discussed in Section 1.2.2. Using the concepts and security models, Table 1.1 describes the interpretations of a Bitcoin project under the cryptoeconomics analysis framework [24].

Another canonical example of cryptoeconomics is Schelling Coin. Schelling Coins are a decentralized oracle construction. The underlying mechanism relies on a game-theoretic concept known as Schelling points, which was proposed by Thomas Schelling in his paper [28]. The way it works is as follows. Suppose two strangers are in different rooms and have not communicated beforehand. They need to pick up the same number from a set of numbers: **10000 34592 45183 40569 857**. If successful, both of them will

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

**Table 1.1** A new interpretation of Bitcoin.

| Model | Parameters | Security margin |
|---|---|---|
| Honest majority | Honest users are more than or equal to 2/3 of total users | 0.5 |
| Uncoordinated majority | The coordinated users account for less than 1/2 of total users | 0.25 |
| Coordinated majority | The coordinated users account for up to 100 percent of total users | 0 |
| Bribing attacker | Budget >(block reward + tx_fees)*number_of_blocks. | 0 |

get rewards. Otherwise, they will be punished. In theory, each number has the same probability of being selected. However, in practice, the probability of selecting **10000** is far greater than the others. The reason is that **10000** looks much more special than the others. The uniqueness results in a natural convergence point.

A similar working process happens in Schelling Coin [29].

1. During an even-numbered block, all users can submit a hash of the ETH or USD price together with their Ethereum address.
2. During the following block, users can submit the value whose hash they provided in the previous block.
3. Define the "correctly submitted values" as all values N where H(N+ADDR) was submitted in the first block and N was submitted in the second block, both messages were signed or sent by the account with address ADDR.
4. Sort the correctly submitted values.
5. Every user who submitted a correct value between the 25 percent and 75 percent gains a reward of $N$ tokens.

Similar to the case of Schelling points, everyone tries to offer a correct answer while they consider that all the others will also prefer to give the correct answers. Because the correct answer is desired the most by the system, providing a correct answer means a higher probability of obtaining the reward. Thus, we can have the following conclusions.

1. Under the uncoordinated choice model, if there is no bribing attack, it is easy to tell the same truth, but difficult to tell the same lie.
2. If there exists a bribe attack, the Schelling Coin game will be corrupted.

In addition to these two cases, some other well-known cryptoeconomics instances have been widely explored. Most of the projects focus on the efficiency issue. The main reason for this is that the scalability problem has inhibited the prospects of blockchain development. This chapter introduces two of the most representative ones.

1. **Arbitrum:** Ethereum is the worldwide second-most-valuable cryptocurrency by market value, but its exponential growth has been limited by network congestion

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

and costly fees. Arbitrum technology is one of the potential solutions to Ethereum's recent transaction cost problem, and is proposed by Offchain Labs [30]. Arbitrum intends to lower transaction costs and congestion by transferring as much processing and data storage as possible away from Ethereum's primary network (layer 1). Layer 2 scaling solutions are used to store data outside of Ethereum's blockchain. This is because it is constructed on top of layer 1 (the core Ethereum network) and so maintains Ethereum's security. Layer 2 projects such as Arbitrum are believed to be critical solutions for Ethereum's scaling problem at the present. The Ethereum network will be updated in the coming years and beyond to minimize costs and congestion. These improvements, particularly Eth 2.0, will aid Ethereum's scaling and cost reduction.

2. **Keepers:** Keepers, proposed by ChainLink, is a decentralized network that allows developers and researchers reliably to automate smart contract triggers, reducing the latency, increasing the process efficiency, and reserving the computation resources. Instead of competing with each other, nodes in Keepers are incentivized to perform all registered jobs. The advantages of joining the network include: (1) providing developers with hyperreliable, decentralized smart contract automation, (2) offering expandable computation, allowing developers to build more advanced Dapps at lower costs, and (3) achieving flexibility and programmability [31]. DeFi protocols like bZx [32] and xToken [33] have integrated Keepers to enhance functionality and improve the user experience without compromising security or transparency.

### 1.2.4 Summary: Economics, Cryptoeconomics, and Cryptography

When Vitalik first coined the concept of "Cryptoeconomics," the concept had been debated, and some microeconomists argued that it should be a subfield of economics. Furthermore, terms with similar forms are liable to be confused, such as cryptoassets and cryptocurrency. According to Vitalik Buterin's definition, cryptoeconomics bridges the cryptography and economic incentives together, focusing on the strategic interactions of different entities not only inside but also beyond the blockchain network. It follows that cryptoeconomics is not just "economics applied to digital assets like cryptocurrencies and tokens." Cryptocurrencies and cryptoassets are the new objects for economic study and analysis, and these markets have particular features and qualities. Figure 1.4 presents a brief illustration regarding the relations between cryptography, economics, and cryptoeconomics. Based on all the introductions in previous sections, we can conclude the following.

1. Cryptoeconomics is not a subfield of economics, but rather an area of applied cryptography that takes economics incentives and economics theory into account.
2. Cryptoeconomics can compete with cryptography by lowering the interactive computation.
3. Cryptoeconomics design should be distributed and decentralized, and can be applied on top of the trustless platform, where most of the economic mechanism designs are not.

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press


**Figure 1.4** Cryptography, economics, and cryptoeconomics.

Moreover, the practical implementation of cryptoeconomics differs from classical economics [23]. That is, the equilibrium and experiments are easier to achieve and conduct; this will be seen in Part III. However, the centralized software development and deployment make practice difficult, which further affects the accuracy in evaluating the cryptoeconomics implementation. We further discuss the detailed impact in Chapter 10.

This section has identified the definitions and the corresponding explanations. Finally, we can summarize that cryptoeconomics is used for incentivizing the rational participants' entries and desired behaviors in a distributed system.

## 1.3 Why Cryptoeconomics Matters

As we discussed previously, Bitcoin is the first, as well as the most significant, instance of cryptoeconomics. The integration of cryptography and mechanism design sparks a revolutionary shift from a traditional P2P network to a blockchain network.

Although cryptography is robust when assuring the security and privacy of a system, the cost of development and deployment is increasingly expensive because of unpredictable attacks and risks. According to Vlad's talk in [2], cryptoeconomics can benefit the following issues.

1. The disincentivization of Byzantine faults: Bitcoin uses the PoW consensus and incentive mechanism to solve the Byzantine General Problem.
2. The "individual rationality" of deciding whether to run a node on a blockchain protocol: How does the incentive mechanism maximize the users' utilities when running their nodes on blockchain?
3. The economic barriers to Sybil attacks: A proper economic incentive mechanism is able to resist Sybil attacks without PoW.

Building systems that have specific desired properties require the coordination of cryptography and mechanism design. To be more specific, this book explains the importance of cryptoeconomics by introducing the project of Bitcoin. As a fundamental of cryptoeconomics, the incentive mechanism is applied in every step to

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

secure the distributed system, including the **transaction confirmation**, **mining**, and **longest-chain generation.**

A Bitcoin network refers to a chain of blocks known as the shared public ledger, which records all the confirmed transactions. The data structure and chronological order of transactions, blocks, and the chain are enforced by cryptographic approaches. The incentives should be noted, motivating trustless and anonymous participants to accomplish these tasks correctly, from confirming the transactions to establishing the whole chain. A transaction recording the involved traders' account balances and terms will be broadcast to the Bitcoin network, protected by signatures, and thus immutable from being tampering by any malicious party. A general confirmation takes at least 10 minutes, completed by a participant called a miner, and through a process called mining. The validation and confirmation of transactions rely on the miner's effort. To compensate for miners' labor and get a quicker confirmation, each participant will set a customized service fee for its transaction in units of satoshi per byte. For this reason, miners will prioritize the transactions with higher fees.

Confirming and adding a transaction into a block are also known as the mining process. Only the miner winning the hash puzzle contest in PoW is entitled to append its mined block to the blockchain, relying on the miner's intensive computational resource. Note that PoW is a form of zero-knowledge proof that requires a participant to demonstrate its validity by exerting a certain amount of computation effort. This consensus protocol is the core of a blockchain system, established through cryptographic rules and for the purpose of being secure from double-spending. Similarly, a miner can exert all the energy on mining and winning PoW only because of the monetary incentive. That is the reason for the birth of BTC (the cryptocurrency issued by Bitcoin), compensating for the miners' computation cost on mining and ensuring the robustness of the Bitcoin ecosystem.

The PoW consensus cannot guarantee that only one miner wins in each round. Then the fork occurs when two winners finish mining simultaneously. The solution is called the longest-chain rule, which means only the chain of blocks that cost the greatest effort to build can be accepted as the valid version of the blockchain, preserving the consistency and neutrality of the whole network and safeguarding the efforts and benefits for a majority of miners. All recorded transactions will be deemed invalid for the blocks on forks and be shifted to unconfirmed, where the underlying efforts get no rewarded. To prevent its effort from being in vain, a rational miner will consciously comply with the rule.

By issuing tokens and offering fees, the Bitcoin network incentivizes trustless participants to operate as required. It compensates miners' work on the longest chain, coordinating all parties to defend against the Sybil attack and preserving the system's security and stability. Bitcoin uses cryptoeconomics to solve two problems: The security problem is how to resist the Sybil attack; and the incentive problem is how to motivate the unknown participants to participate correctly. Vitalik concluded the use of cryptography and incentives as follows [34].

1. Blockchain technology uses cryptography to secure the protocols and preserve the users' privacy.
   - Hashing: PoW; encoding wallet addresses; verify the integrity of data of transactions and balance of accounts on the network.
   - Elliptical curve cryptography: the Elliptic Curve Digital Signature Algorithm can ensure the transaction authenticity and integrity.
   - Erasure code: Blocks are encoded using erasure codes, so that any block of the chain can be efficiently restored from a small number of coded pieces.
   - Zero-knowledge proof, homomorphic encryption.
2. An incentive is used to motivate or drive one to do something or behave in a desired way.
   - Rewards: Increase actors' token balances if they do something good, for example, block reward and transaction fee.
   - Penalties: Reduce actors' token balances if illegal behavior occurs, for example, security deposit.
   - Privileges: Incentivize participants by giving them decision-making right, for example, voting weight.

As the foundational instance of a cryptoeconomics system, Bitcoin has clearly corroborated Josh's definition that (a) the important properties of that protocol are guaranteed by financial incentives, and (b) The economic mechanisms are guaranteed by cryptography.

Based on the explanations and analysis of cryptoeconomics, we can conclude the scenarios in which cryptoeconomics can be applied, as follows.

1. Security of lower-layer interactions: Any channel between a pair of participants, for example, state channel and payment channel.
2. Light clients: How should we design a fast and feasible incentive mechanism for a group of participants and deploy it in a decentralized system?
3. Decentralized applications: Encourage the users' participation and activity.
4. DoS resistance of off-chain protocols: Guarantee the security of on-chain assets and motivate the efforts of off-chain users.
5. Blockchain-based peer to peer markets: Incentivize the participants from the different chains to interact in a desired way.

This book intends to answer these questions based on a review of the literature, which serves as a trigger for further research.

## 1.4 Organization of the Book

The goal of this book is to provide a comprehensive overview of cryptoeconomics, introducing technical components including cryptography and mechanism design. Considering the surge in research focus on the computer science content of blockchain

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

technology, this book places emphasis on the algorithmic mechanism design and mathematical tools of game theory in or beyond a blockchain network.[1]

In particular, this book analyzes how the economic interests of heterogeneous participants shape the way of strategic behaviors and presents an in-depth insight into how rational interactions among various parties determine the decision-making of system from an engineering perspective.

Consequently, we plan to present a mechanism paradigm for assisting the blockchain consensus protocols by properly designing the economic mechanism upon a distributed system, which enables the blockchain network to function with the desired properties in the form of system equilibria.

The main objectives of this book are three-fold.

1. The first objective is to provide the readers with a generalist background and a succinct overview of the distributed ledger networks and the blockchain technology that the ledgers are constructed upon. By transforming the interpretation of the blockchain networks from a computer networking perspective to the perspective of financial–social-economic networks, we establish the formal connection between the blockchain technologies and the research domain of cryptoeconomics.
2. The second objective is to present the state-of-the-art paradigm, based on a series of economic theoretical tools such as game theory, blockchain protocol modeling, and analysis and design. This will be achieved through classification of a variety of problems in protocol analysis and design with respect to the domain to which different mathematical tools belong.
3. The third objective is to provide the audience with a comprehensive overview of the development of the blockchain network protocols and their emerging applications in a plethora of domains, including the Internet of Things (IoT), smart cities, healthcare, self-governance, etc.

By organizing the overview into a series of case studies, this book extends the aforementioned paradigm of system analysis and design from the scope of blockchain protocol design to a broader scope of modeling and analyzing the ecosystems that are either embedded into the blockchain networks or use blockchain as a subsystem. In order to achieve the above objectives, the book is composed of four parts, as described below.

- **Introduction**

  This chapter leads the contents of this book by resolving the inconsistency in the literature regarding the definition of "cryptoeconomics." It provides an intuitive description on how the concept of "cryptoeconomics" came into shape through engineering practice. By providing a succinct overview of the technical component

[1] Some text from Chapters 5–9 is reused with permission from the papers "A survey on consensus mechanisms and mining strategy management in blockchain networks, cloud/fog computing resource management and pricing for blockchain networks, contract-theoretic pricing for security deposits in sharded blockchain with Internet of Things (IoT)" and "Cloud/edge computing service management in blockchain networks: Multi-leader multi-follower game-based ADMM for pricing."

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

of blockchain networks and reviewing them from a social-economic network point of view, this chapter lays the foundation for the technical discussion of the following chapters.

- **Part I: Cryptoeconomics Basics**

  Before presenting the framework of blockchain network modeling and design, this part presents a roadmap of how a cryptographical problem or a problem of distributed system analysis can be cast into the context of social-economic network analysis. In particular, a series of issues including incentivized decentralization, incentivized security (i.e., rational cryptography), and mechanism design for distributed consensus are introduced. This part will help the readers to be well prepared with the necessary knowledge on cryptography, networking protocols, and mathematical tools in economic theory for the later discussion on protocol and system analysis and design in the rest of this book.

- **Part II: Consensus Protocol Design in Blockchain Networks**

  This part of the book provides a technical overview on the procedures, constraints, and goals of consensus protocol design in blockchain networks. In particular, an interdisciplinary point of view from both cryptographical design and distributed system design is highlighted. The inherent differences from typical distributed consensus protocols of the blockchain network protocols are reviewed. Following the quantitative description of a cryptoeconomics system, the specific goals, constraints, and challenges in protocol design from a social-economic networking perspective are discussed. This part helps the readers to learn the necessary theoretical toolbox for establishing a social-economic network-based analytical framework for blockchain networks and protocols.

- **Part III: Mechanism Design in Blockchain Networks and Beyond**

  With the scope of the study on blockchain networks and their difference from existing systems precisely identified, this part of the book focuses on the process of modeling, analyzing, and designing the blockchain networks from a social-economic network perspective. In particular, a prototypical framework for blockchain network modeling is presented, particularly by employing the mathematical toolboxes including game theory, auction theory, contract theory, and those which can be frequently found in microeconomics studies. A diversity of practical problems regarding the design, deployment, and maintenance of blockchain networks are discussed. For each problem, regarding its specific operational goals, system performance indices, resource constraints, and deployment requirement, different mathematical models are applied to either address the issues in a componential level of the blockchain network, or formulate the blockchain network from a unified macroscopic perspective.

- **Part IV: Open Questions of Cryptoeconomics**

  With the theoretical paradigm of blockchain network modeling and analysis presented in Part III, this part of the book extends the scope of the study to the

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press

various applications of the blockchain networks, and in subsequence, the impact by the social-economic network property of the blockchains on the design, deployment and maintenance of these applications. By reviewing the development of the blockchain networks and the applications built upon or interconnected with blockchains, this part also provides an insight into the prospects, challenges, and open issues in the future course of technological evolution of blockchains.

To summarize, the key features of this book are as follows.

1. A generic and unified framework of protocol analysis and design for blockchain networks, especially from the economic theory-based point of view.
2. Comprehensive treatment of the state-of-the-art analytical techniques, especially in the domain of game theory and mechanism design, for the purpose of modeling the dynamics of blockchains as well as a variety of ecosystems that are either used by, or extended from, the blockchain networks.
3. Coverage of a wide range of emerging applications of blockchains, and the related techniques for modeling, analyzing, and designing them.
4. An in-depth insight into the key research issues and open problems in the course of blockchain analysis and design to guide future research activities.

https://doi.org/10.1017/9781009026611.001 Published online by Cambridge University Press