Proceedings of the 2020 Winter Simulation Conference
K.-H. Bae, B. Feng, S. Kim, S. Lazarova-Molnar, Z. Zheng, T. Roeder, and R. Thiesing, eds.

BLOCKCHAIN: A REVIEW FROM THE PERSPECTIVE OF OPERATIONS RESEARCHERS

Hong Wan
Kejun Li

Department of Industrial and Systems Engineering
North Carolina State University
111 Lampe Drive
Raleigh, NC 27607, USA

Yining Huang

Operations Research Graduate Program
North Carolina State University
2500 Stinson Drive
Raleigh, NC 27607, USA

ABSTRACT

Blockchain is a distributed, append-only digital ledger (database). The technology has caught much attention since the emergence of cryptocurrency, and there is an increasing number of blockchain applications in a wide variety of businesses. The concept, however, is still novel to many members of the simulation and operations research community. In this tutorial, we introduce the blockchain technology and review its frontier operations-and-data-related research. There are exciting opportunities for researchers in simulation, system analysis, and data science.

1 INTRODUCTION

Blockchain is the underlying technology of bitcoin and other cryptocurrencies. It has caught public attention since 2017 when the bitcoin price has skyrocketed. As a distributed, secure record sharing system, blockchain is considered a revolution or the "future of the internet" by its believers; and a hoax by skeptics. In reality, blockchain technology does have a broad application in a wide variety of domains, but it is not a unanimous (better) solution for all systems.

Blockchain is, literally, a chain of blocks. The block here is composed of a certain amount of data, and the chain implies that the data are connected. More specifically, it is a consensus-based, peer-to-peer distributed network with "a growing list (chain) of records, called blocks, which are linked using cryptography." (Wikipedia 2020) Each block contains an index that specifies the sequence of blocks; a timestamp that records the approximate time that the block is added; the stored data, and the hashes of the current and previous blocks (Figure 1). Hash is the output of a cryptographic function that converts a meaningful message into a non-meaningful, fixed-length alphanumeric string. The input of the hash function for block k includes the block components mentioned above, the stored data of the block k, and the hash of block $k-1$. The hash value is highly sensitive to the input—a small change in input leads to a completely different hash value, which makes the function nonreversible. The hash function serves as the backbone of the blockchain security and will be discussed in more details in Section 3.

There are two essential properties of the blockchains that distinguish it from the traditional centralized network. First, the data (in block) are immutable. Specifically, if a block is changed, all blocks after it will become invalid since their previous block's hash values will be void. Second, a distributed network with consensus allows users (with authorities) to communicate directly with each other to broadcast new blocks, synchronize the network status, and download the current database. The redundancy of the data and connection channels makes the blockchain more tolerant of node failures. With these two properties, the longer the chain and more users (nodes) in the network, the harder to hack into the chain and change blocks without detection, making the blockchain more reliable (Nakamoto et al. 2008). To understand the blockchain system better, we encourage the readers to explore an interactive demonstration of a blockchain at Blockchain Demo.

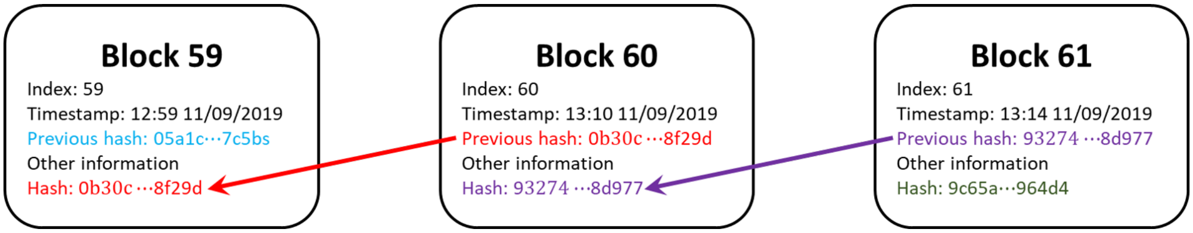

Figure 1: Blockchain demonstration.

The history of blockchain technology can be traced back to the year of 1991. Haber and Stornetta (1990) introduced a digital notary service to timestamp documents, which is regarded as the prototype of blockchain. Later, they brought their idea into effect by creating a timestamping service called Surety. They published their hash values in the New York Times once a week since 1995 to make it legitimate and unique. This service is considered to be the first blockchain in the world. Inspired by Haber and Stornetta (1990) and along with concepts of Merkle tree (Merkle 1980), consensus and fault tolerance (Castro, Liskov, et al. 1999), and proof of work (Dwork and Naor 1993), Nakamoto et al. (2008) developed the bitcoin project that is the most famous realization of the blockchain technology.

There has been numerous research on blockchain architectures, scalability, and novel consensus algorithms from the computer and electrical scientists, and discussions of blockchain applications from various areas (mostly in finance and emerging in other regions). This tutorial has no intention to cover all of the state-of-art progress in this highly-interdisciplinary area. Our goal is to introduce the new technology to the simulation and operations research communities, review the relevant research, and initiate discussions of research opportunities in blockchain design, characterization, and application. We first describe four different kinds of blockchains with varying degrees of privacy, efficiency, and scalability that fit for different scenarios in Section 2. Section 3 uses bitcoin and Ethereum to explain the basic concepts of blockchains, including mining, consensus, and smart contracts. Then in Section 4, we discuss a less famous but more widely used blockchain type, the consortium chain, and demonstrate its applications at the enterprise level. Section 5 reviews the current research of blockchain in simulation, game theory, and machine learning, all of which focuses on system design and analysis of blockchain. We conclude the paper with discussions in Section 6, including the limitations of the blockchain and research opportunities for simulation and operations research communities.

2 BLOCKCHAIN MECHANISM DESIGN

In this section, we discuss the design of the blockchain mechanism, which is mainly characterized by the following three properties:

- Who can view the data in the system? If anyone can view and download a copy of the whole ledger, we call it a public chain; otherwise, it is a private chain.
- Who can validate the data and/or add a block? If anyone can initiate and validate transactions as well as generate and broadcast blocks, then the blockchain is called permissionless chain, otherwise a permissioned chain.
- How do the network users achieve agreements or solve conflicts? This mechanism is called consensus. The two most popular categories of consensus are proof of work and proof of stake (Mingxiao et al. 2017).

The first two properties categorize different types of blockchains, which we introduced in Section 2.1. Moreover, we also discuss fundamental measurements of a blockchain system in the same section. The third property, the consensus, is decided based on the requirement of the specific application. Section 2.2 introduces two of the most popular consensus mechanisms with details.

2.1 Blockchain Types and Trade-off among Performance Measures

Note that a blockchain is public or private is independent of whether it is permissioned or not. As discussed in Chris Jaikaran's testimony to congress: "Discussing a blockchain as public or private refers to the level of freedom users have to create identities and read data on that blockchain. Discussing a blockchain as permissioned or permissionless refers to the level of access the user would have on that blockchain." (Jaikaran 2017). Table 1 classifies blockchains into four types based on these two independent properties.

Table 1: Comparison of different blockchain categories ($+$ represents desired properties, $\sim$ represents neutral, and $-$ represents shortcomings). (Parsons 2018)

Public-Permissioned	**Private-Permissioned (Consortium)**
$+$ Good scaling	$+$ Good scaling
$\sim$ Private $\rightarrow$ Public ecosystem	$\sim$ Completely isolated ecosystem
$-$ Centralized	$-$ Centralized
$+$ Independently verifiable	$-$ Not independently verifiable
$-$ Not yet implemented	$+$ Implemented by Hyperledger, etc.
Public-Permissionless	**Private-Permissionless**
$-$ Poor scaling	$-$ Poor scaling
$\sim$ Completely public ecosystem	$\sim$ Private $\rightarrow$ Public ecosystem
$+$ Distributed	$+$ Distributed
$+$ Independently verifiable	$-$ Not independently verifiable
$+$ Implemented by bitcoin, Ethereum, etc.	$-$ Not yet implemented

Most of the cryptocurrencies use public and permissionless blockchains (Section 3). Private and permissioned (consortium) chains are widely used by individual enterprise and among collaborations of businesses. Customized platforms, such as Hyperledger Fabric by IBM (Linux Foundation 2020), have been developed to facilitate enterprise blockchain implementation (Section 4). Between the two ends of the spectrum, the private and permissionless chain limits who can access data, which fits for internal sharing and auditing data. The public and permissioned chain only allows a subset of users to validate the transactions and add blocks, which can be used in asset management like real estate and intellectual properties (Martin 2018). The later two categories are still in exploring stage.

There are three major and complementary measurements of blockchains: scalability, security, and decentralization. Here scalability refers to the network's ability to handle growth, security the attack-resistance, and decentralization the degree of transparency, synchronization, and fairness among all nodes. Illustrated in Figure 2, the trade-off among these three is called the scalability trilemma, which means it is hard to maximize the other two without sacrificing the third. For example, in public and permissionless blockchains, all peers within maintain replicas of the full ledger, which enhances the system's security and reliability. However, as the degree of decentralization increases (i.e., more peers involved), it will constrain the network's throughput. Among the four categories, the public and permissionless chain has the most decentralized structure and assumes no trust among users. The private and permissioned chain, on the other hand, has the most centralized architecture and the highest level of trust among users and is widely used by individual enterprise and among collaborations of business. Table 1 summarizes the pros and cons of the four types of blockchains. The level of trust among users determines the optimal blockchain architecture and the consensus mechanism for each application.

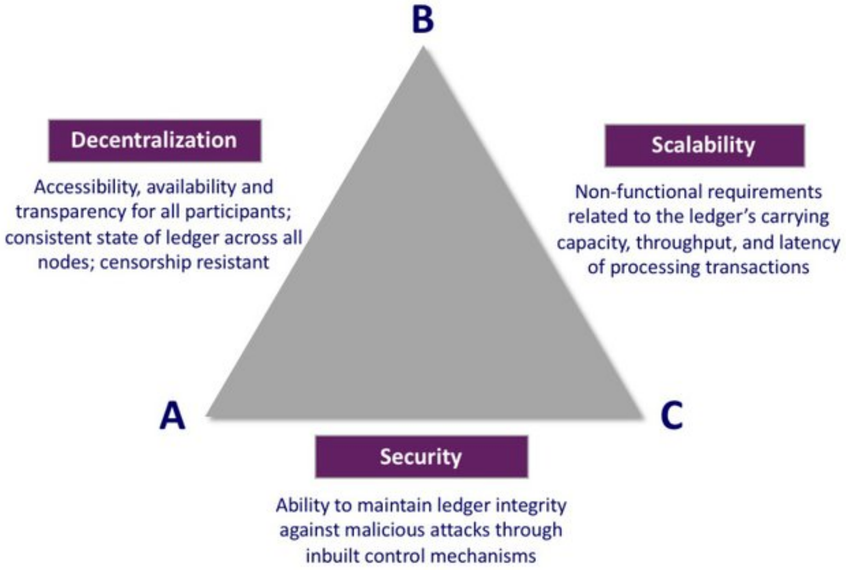

Figure 2: Blockchain scalability trilemma (ReverseAcid 2018).

2.2 Consensus Mechanism

The consensus is an algorithm to reach agreements among different nodes/participants of the distributed system to determine the ordering and confirmation of transactions. All distributed systems need to solve the Byzantine general problem (Lamport et al. 2019) to handle malicious behaviors that give false information. There have been many consensuses developed since the invention of bitcoin. Most of them are either proof-of-work-based or proof-of-stake-based.

- Proof of work (PoW) is the consensus applied by the majority of cryptocurrencies, including bitcoin. In this mechanism, the participants (i.e., miners) compete with each other to solve a complex computational puzzle that can only be done by brute-force search via a cryptographic hash function. This game is probabilistic, and the winning probability of a miner is proportional to her mining power. The winner will earn the right to add the next block and collect the transaction fees, as well as be rewarded a payoff (usually a certain amount of cryptocurrencies) by the system. Miners' workload safeguards the system with the price of energy waste. PoW is the first consensus developed for blockchain and is known for its fairness and safety. However, it is slow and expensive, and research shows that the mechanism can induce monopoly players that dominate the system.
- Proof of stake (PoS) is another widely used consensus that is complimentary to PoW. The next block is selected through a quasi-random process, whose probability depends on the stake held by a participant rather than its computation power. This mechanism is first applied by PPCoin (King and Nadal 2012). PoS is much more efficient (both time and energy wise) than PoW. However, the PoS-based system suffers from a nothing-at-stake problem, in which a node without any stake may behave maliciously since she has nothing to lose.

Besides these two most well-known consensus, there have been many other consensus algorithms proposed recently for different trust level and system requirements (Mingxiao et al. 2017; Bamakan et al. 2020).

3 BITCOIN AND ETHEREUM: MINING AND SMART CONTRACT

This section introduces bitcoin and Ethereum systems, two of the most famous public-permissionless blockchain applications (Nakamoto et al. 2008; Wood et al. 2014; Buterin 2014). These two platforms occupy more than 70% of the global mining power (Coinmarketcap 2020) and are suitable as examples to explain blockchain systems and terminologies. In Section 3.1, we elaborate on how bitcoin works and the mining process. Section 3.2 discusses Ethereum, which is a platform for digital currencies and also allows a wide variety of blockchain technology implementations through the smart contract. In fact, Ethereum users have applied smart contracts to create entire decentralized autonomous organizations (DAOs).

3.1 Bitcoin and Mining Process

The most crucial difference between bitcoin (as well as other cryptocurrencies) and the traditional currency is that the former does not have an "issuer" (government or organizations) to endorse the value of the money, validate transactions, and regulate the financial system. Therefore the cryptocurrency must have (1) a security algorithm to protect each account so that other people cannot spend your money, and (2) a self-regulation mechanism to maintain the system operation and avoid malicious behavior. For security concerns, bitcoin uses public key cryptography (or asymmetric cryptography). See Huh et al. (2017). There is no physical form of bitcoins, but records of transactions and balances for each account (node). Each account is associated with a public key and a private key, whose relationship is similar to that of an email address and password. The public key can be communicated in the network openly, and the private key allows the owner to access the fund. Mining is a unique mechanism that supports the daily operations of the bitcoin and most of the other cryptocurrencies' systems. Mining determines who can add a group of transactions, i.e., a new block to the current blockchain. When A wants to pay B one bitcoin, someone needs to validate that A's account has sufficient funds, deduct one bitcoin from A's account, and then add one bitcoin to B's account. The transaction fee is the reward that A (or B) pays for the transaction recording. To create a valid block, a participant (miner) is required to

1. find a lucky number (nonce),
2. concatenate the nonce, the previous hash, and the list of transactions as the input string,
3. and apply the SHA-256 hash function to generate the hash of this whole input,

such that the 256-bit hash output falls in a target space that is quite small in relation to the much larger output space of the hash function. In this case, the nonce will have to satisfy the following inequality:

$$\text{Hash}(\text{nonce}||\text{previous block hash}||\text{txn}||\ldots||\text{txn}) < \text{target}.$$

All miners compete to solve the above hash puzzle to achieve the PoW consensus in the bitcoin blockchain. The problem can only be solved by brute-force search. Therefore, each node's wining probability is proportional to their hashing power. Once a miner finds a required hash, she will broadcast her block to the whole network for validation. If the new block is validated by a majority of miners, the new block is formally appended to the blockchain and the block creator earns the reward (a certain amount of Bitcoin) and transaction fees. See also Narayanan et al. (2016) for details of the mining process.

The mining process is slow and energy-consuming. Each block takes about 10 minutes to generate (Nakamoto et al. 2008; Subramanian 2018), and the actual transaction validation can take much longer since each block contains only 1MB of data, and there are competitions among transactions. The higher the transaction fee offered, the quicker the transaction is likely to be handled. Moreover, based on a 2019 estimate by Vincent (2019), bitcoin mining consumes more energy than Switzerland, and the solved mathematical problem is not meaningful. However, this process is irreplaceable since the PoW is self-evident and can be agreed upon by all nodes without trust. Also, hacking a blockchain system requires significant computational powers. If these powers are used in mining, the expected rewards will be higher. Therefore it discourages cheating behaviors.

Compared with traditional currency, bitcoin is borderless, more transparent, and neutral. Moreover, the users have full control of their transactions. On the other hand, the disadvantage of bitcoin is its transaction speed, volatility, and narrow acceptance. The last one has been improved significantly in recent years.

3.2 Ethereum and Smart Contract

Ethereum is a decentralized open-source blockchain platform that features smart contracts. It provides a decentralized virtual machine that allows users to build their applications (i.e., dapps). The mined cryptocurrency is called Ether coin and is the second-largest digital currency by market cap after bitcoin. Ethereum is currently using PoW as its consensus protocol but transitioning into PoS. Validators replace miners, and they vote on which block will be added next to the chain. The more stakes (usually the cryptocurrency) a node has, the more voting power it will have. The node obtaining a larger number of coins has a more significant probability of creating a new block. The elimination of PoW mining significantly improves the efficiency of the blockchain but reduces its decentralization level.

Ethereum transactions include not only digital coins but also smart contracts. A smart contract is a piece of automatically executed code that implements certain activities when the condition fulfills. In application, the smart contract is uploaded to a node address, and other nodes can call a function of this smart contract to create a transaction. The transaction is irreversible, tracible, and transparent. Smart contracts are the building elements of DAO which are governed by a set of smart contracts without a centralized government (Shermin 2017). As discussed in Voshmgir (2019), “Blockchain and smart contracts are governance technologies that have the potential to provide higher levels of transparency while reducing bureaucracy with self-enforcing code. They can minimize existing principal-agent dilemmas of organizations and subsequent moral hazards. Tokens of distributed networks hereby provide incentives to automatically align interests in the absence of third parties.” On the flip side, the smart contract and the DAO can introduce security risks to the blockchain system (Shermin 2017), For security analysis and research of the smart contract, see Parizi et al. (2018), Watanabe et al. (2015) and Sturm et al. (2019). Smart contracts based on the blockchain technology have many potentials possibilities in various industries. For example, one main problem in the supply chain is how to determine provenance. By translating the representations of ontology to smart contracts, Kim and Laskowski (2018) found they can execute a provenance trace on the Ethereum blockchain platform. See also Lu and Xu (2017) and Galvez et al. (2018). Dolgui et al. (2020) developed and tested a new model for smart contract design in the supply chain with multiple logistics service providers and showed this problem can be presented as a multi-processor flexible flow shop scheduling. Gatteschi et al. (2018) discussed the possibility of applying blockchain and smart contracts in the insurance industry. Chang et al. (2019) designed a blockchain-based smart contract technology to facilitate international payment. For more discussions, see Section 4.

4 CONSORTIUM BLOCKCHAIN

A typical consortium blockchain involves multiple entities and stakeholders, each with customized authorizations, such as validators and users (Liu et al. 2019). A consortium chain requires an invitation to join, and each node has highly customized authorities, allowing more control of the system by regulatory agencies. As a special case of consortium blockchain, the internal blockchain is a highly customized and cryptography-protected database maintained by a specific organization. Only the organization members could take part in the consensus process. The consortium blockchain infrastructure is especially useful for data sharing and document approval during collaborations among organizations. It offers better workflow, data transparency, activity traceability and visibility, and can predict and prevent nodes’ malicious behaviors (Manupati et al. 2020). Hyperledger is one of the most well-known umbrella projects of open-source consortium blockchains and tools developed by Linux. Its most famous framework is Hyperledger Fabric (IBM) (Mao et al. 2018).

A study shows that more than 30% of fish purchased from retailers are incorrectly labeled, and that illegal fishing represents losses around $10 \sim 23$ billion dollars globally. The mislabeled and illegally sourced fish could hurt ordinary customers’ health or the reputation of grocery stores. It is essential to achieve traceability and transparency in the seafood industry. However, the complexity of seafood supply chains poses difficulties in interoperability (FishWise 2018). Sawtooth Lake blockchain-based supply chain provides an immutable record of the provenance of fish. In combination with Internet of Things (IoT) enabled sensors, Sawtooth Lake can manage the ownership and journey of fish from ocean to table. These sensors can be attached to fish from the moment they are harvested immediately and continuously record data, such as the location, temperature, and humidity of the perishable food. Moreover, the Sawtooth Lake platform could manage the chain of custody of fish, enabling ownership to be transferred and traded on the blockchain with the help of smart contracts. Figure 3 illustrates how Hyperledger Sawtooth is integrated into the seafood supply.

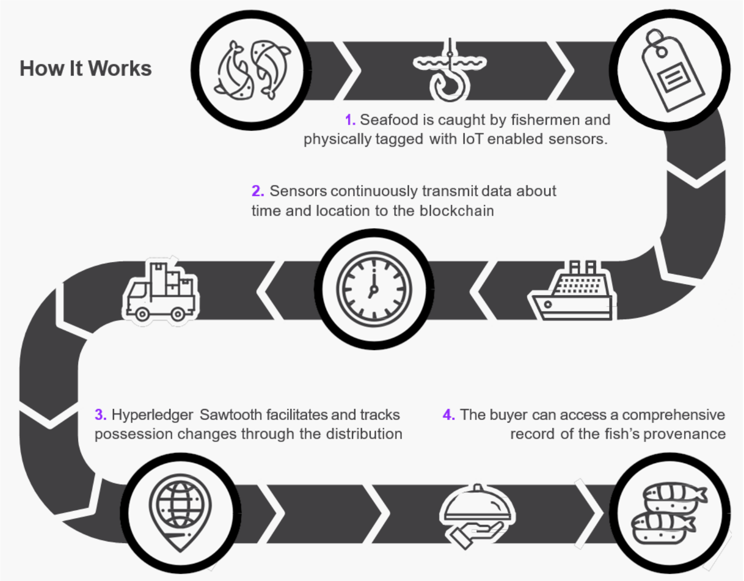

Figure 3: Flowchart of the seafood supply chain using Hyperledger Sawtooth (Blummer et al. 2018).

Additionally, Tian (2016) proposed an agri-food supply chain traceability system using radio-frequency identification (RFID) and blockchain technology. Mao et al. (2018) designed a consortium blockchain to eliminate information asymmetry in the food trade, in order to establish a sustainable and credible trading environment. Manupati et al. (2020) developed a blockchain-based approach for monitoring supply chain performance and optimising both emission levels and operational costs in a synchronised fashion, yielding the optimal outcome for the sustainable supply chain.

In pharmaceutical industry, for example, the consortium chain is used to fight counterfeit drugs by improving surveillance (Jamil et al. 2019; Tseng et al. 2018). Financial institutes use consortium chains to improve the efficiency of international trade (Chang et al. 2020). Healthcare organizations are enthusiastic in applying blockchain for healthcare data sharing and storage (Griggs et al. 2018; Zhang and Lin 2018). See also Kang et al. (2017), Li et al. (2017) and Yang et al. (2020) for applications in energy and construction areas. We expect to see more applications in the near future.

To summarize, combining with smart devices like IoT and wearable sensors, consortium chains ensure transparent, traceable, and accountable data storage and sharing among organizations and end customers. The consortium chain, with the ability of highly secured and customized data sharing, has the potential to become the neural network of the big data.

5 SYSTEM AND DATA ANALYSIS OF BLOCKCHAIN SYSTEMS

In this section, we review the recent blockchain researches from system and data points of view. Our discussion focus on three topics: simulation characterization of blockchain systems (Section 5.1), game-theory approach to understand interactions among different nodes (Section 5.2), and machine learning in and for blockchain (Section 5.3).

5.1 Simulation Study of Blockchain Systems

Recently, we see many simulation-related blockchain research appear. The current study mainly focuses on the mining behaviors of cryptocurrencies and the scalability of blockchain simulation models. Also, numerous simulators are proposed as platforms to evaluate the performance of blockchains under different conditions/attacks. We review the related literature in this session.

5.1.1 Discrete-Event Simulation

Alharby and van Moorsel (2019) proposed an event-driven model with transactions and emphasized on the block creation through PoW. Aoki et al. (2019) involved events of block generation, block propagation, and message transmission/reception. Memon et al. (2019) built a queueing model to observe the realistic behaviors of both a memory and a mining pool for any blockchain system. To investigate the large-scale blockchain networks, Wang et al. (2018) collected and defined a number of metrics to quantify the quality of blockchain. Miller and Jansen (2015) enabled the scalable execution of thousands of bitcoin nodes on a single machine in their work and included the denial-of-service attack to demonstrate the proposed simulator. Gervais et al. (2016) studied optimal adversarial strategies for double-spending and selfish mining attacks based on Markov decision processes. They constructed a bitcoin simulator to analyze the security and performance of different configurations. Göbel et al. (2016) used discrete-event simulation to study the selfish-mining attack under a network with communication delay between miners. Foytik et al. (2020) presented a blockchain simulator that utilizes a generalized representation of consensus protocols, providing insights into the performance of the consensus protocols under various networking conditions.

5.1.2 Agent-Based Simulation

Kaligotla and Macal (2018) provided a generalized framework of modeling blockchain simulation by illustrating the essential agents and functioning of the system. Cocco and Marchesi (2016) reproduced the economy of the mining process with heterogeneous agents by including the bitcoin transactions and price series. Rosa et al. (2019) developed a security attack testing platform by exploiting parallel and distributed simulation techniques with extended scalability. Intimated by the design of algorithmic trading and reinforcement learning systems, Chitra et al. (2019) proposed an agent-based simulation to model censorship properties in parallelized PoW chains. Their results illustrated how endogenous design choices affect practical protocol performance and how simulations can interact with exogenous data. Brousmichc et al. (2018) built an agent-based framework for simulating local energy market place integrating realistic consumption/production behavior and interacting with a private blockchain network. Bottone et al. (2018) developed an extendable multi-agent simulator for a block-free and fee-less distributed ledger, in which they employed NetLogo to provide a 3D visualization of the Tangle (Popov 2016).

5.1.3 Others

Goswami (2017) discussed the factors that limit the scalability of blockchains by providing a comparative analysis of several blockchain parameters with real-time data. Alsahan et al. (2020) adopted the lightweight virtualization technique for constructing a simulation model with high speed and large scalability. The impact of applying different mining difficulty levels was also studied, and the block time as well as fork occurrences were evaluated. Yasaweerasinghelage et al. (2017) used architectural modeling and simulation to measure the latency in blockchain systems under different configurations. Longo et al. (2019) developed a hybrid (discrete-event and agent-based) supply chain simulation model to recreate the supply chain operations, which was integrated by an Ethereum-like blockchain with different visibility levels through the same software connector.

5.2 Game Theory

As a powerful tool for strategic decision making, game theory plays a valuable role in the blockchain field. It optimizes the utility of each player while considering the interactions among players. Of the increasing amount of research in studying blockchain with game theory, we categorize them by types of games and discussed the research respectively.

5.2.1 Non-Cooperative Game

As the term suggests, a non-cooperative game represents the situation where players compete against each other. The ability of non-cooperative game depicting the static game and dynamic game makes it the most prevalent method in blockchain research. To avoid the pool block withholding attack, Eyal (2015) modeled it as the miner's dilemma. The non-cooperative theory was used for fork chain selection of bitcoin by Carlsten et al. (2016). Teutsch et al. (2016) illustrated that the player controlling at least 38.2% of the network's total computational power can gain more reward by deviating from the protocol in any PoW-based cryptocurrency. Liao and Katz (2017) modeled the interaction between attackers and regular miners in a whale attack, in which attackers issue an off-the blockchain whale transaction with an extremely large transaction fee in an effort to convince regular miners to fork the current chain. The condition when a miner has an incentive to mine on the fork was investigated by Kroll et al. (2013). To study the computational power allocation in the bitcoin mining competition, Dimitri (2017) characterized the mining activity as an all-pay contest. To investigate when gaps (the situation that miners would avoid mining when the available fees are insufficient) form, Tsabary and Eyal (2018) analyzed the cryptocurrency system via the gap game. Easley et al. (2019) developed a game-theoretic model to explain the factors leading to the emergence of transaction fees and the strategic behavior of miners and users. The non-cooperative theory can also be used for pool selection regarding the mining rewards allocation (Schrijvers et al. 2016). Pagnotta, Emiliano and Buraschi, Andrea (2018) showed the equilibrium price is obtained by solving a fixed-point problem.

5.2.2 Extensive-Form Game

Extensive-form games are used to describe dynamic games. The players will make decisions according to a predefined order. Aiming to verify the cloud computing at a relatively low cost, Dong et al. (2017) employed game theory with the help of smart contracts. Lewenberg et al. (2015) proposed a game theoretic model of the competition for fees between the nodes under the new structure with directed acyclic graphs. Cong, Lin William and He, Zhiguo and Li, Jiasun (2020) applied extensive game to optimize reward allocation of pool. Cong, Lin William and Li, Ye and Wang, Neng (2020) studied the topic of whether adopting blockchain market by comparing a token based equilibrium using extensive form game, to an equilibrium without token.

5.2.3 Stackelberg Game

There are two types of players in the Stackelberg game: leaders and followers. The leader moves first and then the followers will make decision based on the leader's movement. Kang et al. (2018) formulated a Stackelberg game model to jointly maximize utility of the blockchain user and profit of the miners. Feng et al. (2018) analyzed a series of results of the Stackelberg equilibrium in the market game. Xiong et al. (2018) modeled the interaction between the service provider and the miner as a Stackelberg game. Li et al. (2017) illustrated a Stackelberg game model of interaction between the users and credit bank.

5.2.4 Stochastic Game

In the stochastic game, there could be one or more players make decisions repeatedly with probabilistic transitions. Zhen et al. (2017) presented a Zero Determined strategies by modeling a two-miner mining case. The stochastic iterative game was applied here to analyze the selection between the honest and selfish mining. Aside from non-cooperative game, Kroll et al. (2013) also adopted stochastic game to decide the proper time to release the mining block. Kim (2018) focused on a new hybrid theoretical model named Blockchain Governance Game, which provides the stochastic game framework to select the block to add to the chain. Biais et al. (2018) modeled the PoW blockchain protocol as a stochastic game and analyzed the equilibrium strategies of rational, strategic miners.

5.3 Machine Learning in and for Blockchain

Machine learning refers to the science of teaching the computer system to predict based on data without explicit programming. Its efficiency relies heavily on the quantity and quality of data. Blockchain technology has attracted data scientists' attention since it allows highly customized data sharing without relying on a trusted third party. On the other hand, machine learning algorithms are powerful tools for analyzing and optimizing blockchain operations. The combination of the two technologies can be a game-changer.

Data privacy becomes a critical issue in the current digitalized society, especially for sensitive data sharing in healthcare and finance. Blockchain framework keeps the data safe through cryptography, and allows individual users, instead of a third party, to have full control of their shared data. Harris and Waggoner (2019) built a decentralized collaborative learning framework with blockchain. Chen et al. (2018) presented LearningChain, which applies a decentralized version of the stochastic gradient descent algorithm and a differential privacy mechanism to preserve user's privacy. To secure the share of updates in federated learning, Zhu et al. (2018) proposed a blockchain-based privacy-preserving framework. Liu et al. (2018) established a scheme to efficiently collect data and securely share data by incorporating Ethereum blockchain and deep reinforcement learning. We expect more blockchain-based data sharing platform to emerge in the future.

Machine learning methods prove to be efficient in categorizing bitcoin transactions and predicting its price. Yin and Vatrapu (2017) applied supervised learning and Akcora et al. (2019) proposed a topological data analysis approach to classify entities of transactions that may involve in cybercriminal activities. Jourdan et al. (2019) classified entities of transactions into common categories with a gradient boosted decision algorithm. The categorized entities of transactions are used to forecast the value of UTOXs and further predict the Bitcoin price. Akcora et al. (2018) tried to forecast Bitcoin price with the topological structure of blockchain. The concept of graphic chainlet they (Akcora et al. 2018) introduced was extended by Abay et al. (2019) to a new graphic model ChainNet. The topological features from all or multiple transactions are further evaluated and the amount of transferred Bitcoin was considered by ChainNet. McNally et al. (2018) compared performance of recurrent neural network and long-short term memory models in forecasting Bitcoin price. Lahmiri and Bekiros (2019) also implemented deep learning model to predict Bitcoin price, but applied a chaotic time series analysis first.

Furthermore, researchers are exploring the possibilities of applying machine learning technique to solve resource optimization problem. Luong et al. (2018) employed a deep learning-based auction algorithm to optimize the allocation of edge computing resources to support mobile mining activities. Nguyen et al. (2020) applied reinforcement learning to determine the optimal offloading decisions for mobile users based on blockchain transaction states. They also developed a deep reinforcement learning algorithm by using deep Q-network. To find an optimal mining strategy without knowing too much about the blockchain network, Wang et al. (2019) adopted a single-agent reinforcement learning. In addition to computing resources, capital allocation can also be solved by machine learning to construct portfolios of cryptocurrencies (Alessandretti et al. 2018; Jiang and Liang 2017).

A closer look at the studies of incorporating machine learning with blockchain technology, however, reveals some shortcomings. First, the current research mostly focus on financial sector, specifically, bitcoin mining and trading. In combining blockchain with data science, the current research is simply application of one technology to another. The benefit of using the blockchain is unclear. The papers mainly focus on using blockchain for data sharing, ignoring its property of improved safety and higher cost of cheating.

6 DISCUSSIONS

In this tutorial, we introduced the concept of blockchain, its categories, its applications, and current research in simulation area. In this section, we want to discuss the challenges of blockchain application and how we, researchers in simulation and operations research society, can contribute.

Up till this point, we have focused on the advantages of blockchain systems and their applications. However, blockchain is not a universal (better) solution for all scenarios. It has many disadvantages compared to the traditional centralized system. First, the mining processes for PoW-based cryptocurrencies are slow and energy-intense. Meanwhile, blockchain's decentralized architecture requires duplication of computations and expenditure of efforts for transaction confirmation. All of these lead to slow transaction speed (Huberman et al. 2019). Currently, the bitcoin blockchain can guarantee only 4.6 transactions per second (TPS), and Ethereum with an average of 12 TPS. For Visa, on the other hand, the value is around 24,000 TPS Strelenko (2018). The slow transaction speed is the biggest bottleneck of cryptocurrency. Similarly, the blockchain-based data sharing is slower than a traditional centralized database. Moreover, the blockchain's safety will be compromised if attackers could possess the majority (more than 50%) of hashing power in the system, which means small-size blockchains are not safe. Finally, the blockchain can only identify intent to change data, but cannot prevent initial data forging. For instance, within a perishable food supply chain integrated with blockchain, if low-quality products have forged labels initially, then the blockchain cannot screen them out.

So when should blockchain be applied? For traditional (public permissionless) blockchains, the answer is almost no cases except for cryptocurrency. For private and consortium chains, if a centralized or distributed conventional database works and you can rely on a trusted third party, you do not need blockchain. The consortium chain should be considered when there is no or only partial trust toward a third party and/or each other, or for data validation, audition, and public monitoring purposes.

While research by computer scientists have made significant progress on blockchain consensus, architecture, and scalability, characterizing the blockchain as a complex system is still in an early stage. Sophisticated mathematical and simulation models are needed to capture individual nodes' behaviors and their interactions, as well as the system's evolvement under different environments. Moreover, in current studies, nodes/agents all follow simple rules with almost no learning ability. Game theory can shed light on optimal individual decision making, incentive design, and system equilibriums (or lack of them). The current game theory study is limited and constrained. We expect that the computational game theory approach that incorporates simulation and other numerical models will be an active research area. Thirdly, blockchain cannot be apart from data. The current data-related blockchain research is at the pioneer stage and usually just a direct application of one technology to another. A highly integrated infrastructure that combines data science and blockchain technology has great potential.

REFERENCES

Abay, N. C., C. G. Akcora, Y. R. Gel, M. Kantarcioglu, U. D. Islambekov, Y. Tian, and B. Thuraisingham. 2019. "Chainnet: Learning on Blockchain Graphs With Topological Features". In *2019 IEEE International Conference on Data Mining (ICDM)*, 946–951. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Akcora, C. G., A. K. Dey, Y. R. Gel, and M. Kantarcioglu. 2018. "Forecasting Bitcoin Price With Graph Chainlets". In *Pacific-Asia Conference on Knowledge Discovery and Data Mining*, 765–776. Springer.

Akcora, C. G., Y. Li, Y. R. Gel, and M. Kantarcioglu. 2019. "BitcoinHeist: Topological Data Analysis for Ransomware Detection on the Bitcoin Blockchain". *arXiv preprint arXiv:1906.07852*.

Alessandretti, L., A. ElBahrawy, L. M. Aiello, and A. Baronchelli. 2018. "Anticipating Cryptocurrency Prices Using Machine Learning". *Complexity* 2018.

Alharby, M., and A. van Moorsel. 2019. "Blocksim: A Simulation Framework for Blockchain Systems". *ACM SIGMETRICS Performance Evaluation Review* 46(3):135–138.

Alsahan, L., N. Lasla, and M. Abdallah. 2020. "Local Bitcoin Network Simulator for Performance Evaluation Using Lightweight Virtualization". *arXiv preprint arXiv:2002.01243*.

Aoki, Y., K. Otsuki, T. Kaneko, R. Banno, and K. Shudo. 2019. "SimBlock: A Blockchain Network Simulator". In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 325–329. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Bamakan, S. M. H., A. Motavali, and A. B. Bondarti. 2020. "A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria". *Expert Systems with Applications*:113385.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta. 2018. "The Blockchain Folk Theorem". *SSRN Electronic Journal*.

Blummer, T., M. Sean, and C. Cachin. 2018. "An Introduction to Hyperledger". Technical report, Tech. rep. 2018. url: https://www. hyperledger. org/wp-content/uploads/2018.

Bottone, M., F. Raimondi, and G. Primiero. 2018. "Multi-Agent Based Simulations of Block-Free Distributed Ledgers". In *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 585–590. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Brousmichc, K.-L., A. Anoaica, O. Dib, T. Abdellatif, and G. Deleuze. 2018. "Blockchain Energy Market Place Evaluation: An Agent-Based Approach". In *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 321–327. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Buterin, Vitalik 2014. "A Next-Generation Smart Contract and Decentralized Application Platform". https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf, accessed 04th August.

Carlsten, M., H. Kalodner, S. M. Weinberg, and A. Narayanan. 2016. "On the Instability of Bitcoin Without the Block Reward". In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, 154–167. New York, NY, USA: Association for Computing Machinery.

Castro, M., B. Liskov et al. 1999. "Practical Byzantine Fault Tolerance". In *OSDI*, Volume 99, 173–186.

Chang, S. E., Y.-C. Chen, and M.-F. Lu. 2019. "Supply Chain Re-Engineering Using Blockchain Technology: A Case of Smart Contract Based Tracking Process". *Technological Forecasting and Social Change* 144:1–11.

Chang, S. E., H. L. Luo, and Y. Chen. 2020. "Blockchain-Enabled Trade Finance Innovation: A Potential Paradigm Shift on Using Letter of Credit". *Sustainability* 12(1):188.

Chen, X., J. Ji, C. Luo, W. Liao, and P. Li. 2018. "When Machine Learning Meets Blockchain: A Decentralized, Privacy-Preserving and Secure Design". In *2018 IEEE International Conference on Big Data (Big Data)*, 1178–1187. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Chitra, T., M. Quaintance, S. Haber, and W. Martino. 2019. "Agent-Based Simulations of Blockchain Protocols Illustrated via Kadena's Chainweb". In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 386–395. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Cocco, L., and M. Marchesi. 2016. "Modeling and Simulation of the Economics of Mining in the Bitcoin Market". *PloS one* 11(10).

Coinmarketcap 2020, August. "Global Charts Percentage of Total Market Capitalization". https://coinmarketcap.com/charts/, accessed 04th August.

Cong, Lin William and He, Zhiguo and Li, Jiasun 2020. "Decentralized Mining in Centralized Pools". https://academic.oup.com/rfs/advance-article-pdf/doi/10.1093/rfs/hhaa040/33178898/hhaa040.pdf, accessed 04th August 2020.

Cong, Lin William and Li, Ye and Wang, Neng 2020. "Tokenomics: Dynamic Adoption and Valuation". http://www.nber.org/papers/w27222, accessed 04th August 2020.

Dimitri, N. 2017, Sep. "Bitcoin Mining as a Contest". *Ledger* 2:31–37.

Dolgui, A., D. Ivanov, S. Potryasaev, B. Sokolov, M. Ivanova, and F. Werner. 2020. "Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain". *International Journal of Production Research* 58(7):2184–2199.

Dong, C., Y. Wang, A. Aldweesh, P. McCorry, and A. van Moorsel. 2017. "Betrayal, Distrust, and Rationality: Smart Counter-Collusion Contracts for Verifiable Cloud Computing". In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, 211–227. New York, NY, USA: Association for Computing Machinery.

Dwork, C., and M. Naor. 1993. "Pricing via Processing or Combatting Junk Mail". In *Annual International Cryptology Conference*, CRYPTO '92, 139–147. Berlin, Heidelberg: Springer Berlin Heidelberg.

Easley, D., M. O'Hara, and S. Basu. 2019. "From Mining to Markets: The Evolution of Bitcoin Transaction Fees". *Journal of Financial Economics* 134(1):91–109.

Eyal, I. 2015. "The Miner's Dilemma". In *2015 IEEE Symposium on Security and Privacy*, 89–103. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Feng, S., W. Wang, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang. 2018. "On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach". *arXiv preprint arXiv:1804.10412*.

FishWise 2018. "Advancing Traceability in the Seafood Industry: Assessing Challenges and Opportunities". https://fishwise.org/traceability/advancing-traceability-in-the-seafood-industry-assessing-challenges-and-opportunities/, accessed 04th August 2020.

Foytik, P., S. Shetty, S. P. Gochhayat, E. Herath, D. Tosh, and L. Njilla. 2020. "A Blockchain Simulator for Evaluating Consensus Algorithms in Diverse Networking Environments". In *Proceedings of the 2020 Spring Simulation Conference*, 1–12. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Galvez, J. F., J. Mejuto, and J. Simal-Gandara. 2018. "Future Challenges on the Use of Blockchain for Food Traceability Analysis". *TrAC Trends in Analytical Chemistry* 107:222–232.

Gatteschi, V., F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría. 2018. "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?". *Future Internet* 10(2):20.

Gervais, A., G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun. 2016. "On the Security and Performance of Proof of Work Blockchains". In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, 3–16. New York, NY, USA: Association for Computing Machinery.

Göbel, J., H. P. Keeler, A. E. Krzesinski, and P. G. Taylor. 2016. "Bitcoin Blockchain Dynamics: The Selfish-Mine Strategy in the Presence of Propagation Delay". *Performance Evaluation* 104:23–41.

Goswami, S. 2017. *Scalability analysis of Blockchains through Blockchain simulation*. Master of Science in Computer Science thesis, Department of Computer Science & Engineering, University of Nevada, Las Vegas, Nevada. https://digitalscholarship.unlv.edu/thesesdissertations/2976, accessed 04th August.

Griggs, K. N., O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh. 2018. "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring". *Journal of medical systems* 42(7):130.

Haber, S., and W. S. Stornetta. 1990. "How to Time-Stamp a Digital Document". In *Conference on the Theory and Application of Cryptography*, 437–455. Berlin, Heidelberg: Springer.

Harris, J. D., and B. Waggoner. 2019. "Decentralized and Collaborative AI on Blockchain". In *2019 IEEE International Conference on Blockchain (Blockchain)*, 368–375. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Huberman, G., J. Leshno, and C. C. Moallemi. 2019. "An Economic Analysis of the Bitcoin Payment System". *Columbia Business School Research Paper* (17-92).

Huh, S., S. Cho, and S. Kim. 2017. "Managing IoT Devices Using Blockchain Platform". In *2017 19th international conference on advanced communication technology (ICACT)*, 464–467. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Jaikaran, Chris 2017, Oct. https://www.banking.senate.gov/download/jaikaran-testimony-10-17-17pdf, accessed 04th August 2020.

Jamil, F., L. Hang, K. Kim, and D. Kim. 2019. "A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital". *Electronics* 8(5):505.

Jiang, Z., and J. Liang. 2017. "Cryptocurrency Portfolio Management With Deep Reinforcement Learning". In *2017 Intelligent Systems Conference (IntelliSys)*, 905–913. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Jourdan, M., S. Blandin, L. Wynter, and P. Deshpande. 2019. "A Probabilistic Model of the Bitcoin Blockchain". In *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2784–2792. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Kaligotla, C., and C. M. Macal. 2018. "A Generalized Agent Based Framework for Modeling a Blockchain System". In *Proceedings of the 2018 Winter Simulation Conference*, edited by M. Rabe, A. A. Juan, N. Mustafee, S. J. A. Skoogh, and B. Johansson, 1001–1012. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Kang, J., Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim. 2018. "Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks". *IEEE Wireless Communications Letters* 8(1):157–160.

Kang, J., R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain. 2017. "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains". *IEEE Transactions on Industrial Informatics* 13(6):3154–3164.

Kim, H. M., and M. Laskowski. 2018. "Toward an Ontology-Driven Blockchain Design for Supply-Chain Provenance". *Intelligent Systems in Accounting, Finance and Management* 25(1):18–27.

Kim, S.-K. 2018. "The Trailer of Blockchain Governance Game". *arXiv preprint arXiv:1807.05581*.

King, S., and S. Nadal. 2012. "Ppcoin: Peer-to-Peer Crypto-Currency With Proof-of-Stake". *self-published paper, August* 19:1.

Kroll, J. A., I. C. Davey, and E. W. Felten. 2013. "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries". In *Proceedings of WEIS*, Volume 2013, 11.

Lahmiri, S., and S. Bekiros. 2019. "Cryptocurrency Forecasting With Deep Learning Chaotic Neural Networks". *Chaos, Solitons & Fractals* 118:35–40.

Lamport, L., R. Shostak, and M. Pease. 2019. "The Byzantine Generals Problem". In *Concurrency: the Works of Leslie Lamport*, 203–226.

Lewenberg, Y., Y. Sompolinsky, and A. Zohar. 2015. "Inclusive Block Chain Protocols". In *International Conference on Financial Cryptography and Data Security*, 528–547. Berlin, Heidelberg: Springer Berlin Heidelberg.

Li, Z., J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang. 2017. "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things". *IEEE transactions on industrial informatics* 14(8):3690–3700.

Liao, K., and J. Katz. 2017. "Incentivizing Blockchain Forks via Whale Transactions". *Lecture Notes in Computer Science*:264–279.

Linux Foundation 2020, Jun. "Hyperledger Fabric". https://www.hyperledger.org/use/fabric, accessed 04th August.

Liu, C. H., Q. Lin, and S. Wen. 2018. "Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning". *IEEE Transactions on Industrial Informatics* 15(6):3516–3526.

Liu, Z., N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim. 2019. "A Survey on Blockchain: A Game Theoretical Perspective". *IEEE Access* 7:47615–47643.

Longo, F., L. Nicoletti, A. Padovano, G. d'Atri, and M. Forte. 2019. "Blockchain-Enabled Supply Chain: An Experimental Study". *Computers & Industrial Engineering* 136:57–69.

Lu, Q., and X. Xu. 2017. "Adaptable Blockchain-Based Systems: A Case Study for Product Traceability". *IEEE Software* 34(6):21–27.

Luong, N. C., Z. Xiong, P. Wang, and D. Niyato. 2018. "Optimal Auction for Edge Computing Resource Management in Mobile Blockchain Networks: A Deep Learning Approach". In *2018 IEEE International Conference on Communications (ICC)*, 1–6. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Manupati, V. K., T. Schoenherr, M. Ramkumar, S. M. Wagner, S. K. Pabba, and R. Inder Raj Singh. 2020. "A Blockchain-Based Approach for a Multi-Echelon Sustainable Supply Chain". *International Journal of Production Research* 58(7):2222–2241.

Mao, D., Z. Hao, F. Wang, and H. Li. 2018. "Innovative Blockchain-Based Approach for Sustainable and Credible Environment in Food Trade: A Case Study in Shandong Province, China". *Sustainability* 10(9):3149.

Martin, Rick 2018, November. "How Blockchain Will Transform the Asset Management Industry – Ignite Ltd.". https://igniteoutsourcing.com/blockchain/blockchain-asset-management/, accessed 04th August.

McNally, S., J. Roche, and S. Caton. 2018. "Predicting the Price of Bitcoin Using Machine Learning". In *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, 339–343. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Memon, R. A., J. P. Li, and J. Ahmed. 2019. "Simulation Model for Blockchain Systems Using Queuing Theory". *Electronics* 8(2):234.

Merkle, R. C. 1980. "Protocols for Public Key Cryptosystems". In *1980 IEEE Symposium on Security and Privacy*, 122–122. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Miller, A., and R. Jansen. 2015. "Shadow-Bitcoin: Scalable Simulation via Direct Execution of Multi-Threaded Applications". In *8th Workshop on Cyber Security Experimentation and Test ({CSET} 15)*. Washington, D.C.: USENIX Association.

Mingxiao, D., M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun. 2017. "A Review on Consensus Algorithm of Blockchain". In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2567–2572. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Nakamoto, Satoshi and others 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System".

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

Nguyen, D. C., P. N. Pathirana, M. Ding, and A. Seneviratne. 2020. "Privacy-Preserved Task Offloading in Mobile Blockchain With Deep Reinforcement Learning". *IEEE Transactions on Network and Service Management*.

Pagnotta, Emiliano and Buraschi, Andrea 2018, Mar. "An Equilibrium Valuation of Bitcoin and Decentralized Network Assets". https://ssrn.com/abstract=3142022, accessed 04th August 2020.

Parizi, R. M., A. Dehghantanha, K.-K. R. Choo, and A. Singh. 2018. "Empirical Vulnerability Analysis of Automated Smart Contracts Security Testing on Blockchains". *arXiv preprint arXiv:1809.02702*.

Parsons, Jackson 2018. "Blockchain Types Explained: It's More Than Public vs Private – ULedger". http://159.65.79.6/blockchain-types-explained-its-more-than-public-vs-private/, accessed 04th August.

Popov, Serguei 2016. "The Tangle". http://www.descryptions.com/Iota.pdf, accessed 04th August 2020.

ReverseAcid 2018. "The Scalability Trilemma – Steemit". https://steemit.com/blockchain/@reverseacid/the-scalability-trilemma, accessed 04th August.

Rosa, E., G. D'Angelo, and S. Ferretti. 2019. "Agent-Based Simulation of Blockchains". In *Methods and Applications for Modeling and Simulation of Complex Systems*, edited by G. Tan, 115–126. Singapore: Springer Singapore.

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

Shermin, V. 2017. "Disrupting Governance With Blockchains and Smart Contracts". *Strategic Change* 26(5):499–509.

Strelenko, Oleg 2018, October. "Blockchain and Transaction Speed: Why Does it Matter? – Medium". https://medium.com/@s_o_s/blockchain-and-transaction-speed-why-does-it-matter-80bfd100fa89, accessed 04th August.

Sturm, C., J. Scalanczi, S. Schönig, and S. Jablonski. 2019. "A Blockchain-Based and Resource-Aware Process Execution Engine". *Future Generation Computer Systems* 100:19–34.

Subramanian, Vasan 2018, February. "Why Bitcoin Payments Take 10 Minutes - UnBlockchain – Medium". https://medium.com/unblockchain/why-bitcoin-payments-take-10-minutes-c6f37f424b4f, accessed 04th August.

Teutsch, J., S. Jain, and P. Saxena. 2016. "When Cryptocurrencies Mine Their Own Business". In *International Conference on Financial Cryptography and Data Security*, 499–514. Berlin, Heidelberg: Springer Berlin Heidelberg.

Tsabary, I., and I. Eyal. 2018. "The Gap Game". In *Proceedings of the 2018 ACM SIGSAC conference on Computer and Communications Security*, CCS '18, 713–728. New York, NY, USA: Association for Computing Machinery.

Tseng, J.-H., Y.-C. Liao, B. Chong, and S.-w. Liao. 2018. "Governance on the Drug Supply Chain via Gcoin Blockchain". *International journal of environmental research and public health* 15(6):1055.

Vincent, James 2019, January. "Bitcoin Consumes More Energy Than Switzerland, According to New Estimate – the Verge". https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison, accessed 04th August.

Voshmgir, S. 2019. *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*. BlockchainHub.

Wang, B., S. Chen, L. Yao, B. Liu, X. Xu, and L. Zhu. 2018. "A Simulation Approach for Studying Behavior and Quality of Blockchain Networks". In *International Conference on Blockchain*, 18–31. Cham: Springer International Publishing.

Wang, S., L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang. 2019. "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends". *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49(11):2266–2277.

Watanabe, H., S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami. 2015. "Blockchain Contract: A Complete Consensus Using Blockchain". In *2015 IEEE 4th global conference on consumer electronics (GCCE)*, 577–578. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Wikipedia 2020, Jun. "Blockchain – Wikipedia". https://en.wikipedia.org/wiki/Blockchain, accessed 04th August.

Wood, G. et al. 2014. "Ethereum: A Secure Decentralised Generalised Transaction Ledger". *Ethereum project yellow paper* 151(2014):1–32.

Xiong, Z., S. Feng, D. Niyato, P. Wang, and Z. Han. 2018. "Optimal Pricing-Based Edge Computing Resource Management in Mobile Blockchain". In *2018 IEEE International Conference on Communications (ICC)*, 1–6. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Yang, R., R. Wakefield, S. Lyu, S. Jayasuriya, F. Han, X. Yi, X. Yang, G. Amarasinghe, and S. Chen. 2020. "Public and Private Blockchain in Construction Business Process and Information Integration". *Automation in Construction* 118:103276.

Yasaweerasinghelage, R., M. Staples, and I. Weber. 2017. "Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation". In *2017 IEEE International Conference on Software Architecture (ICSA)*, 253–256. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Yin, H. S., and R. Vatrapu. 2017. "A First Estimation of the Proportion of Cybercriminal Entities in the Bitcoin Ecosystem Using Supervised Machine Learning". In *2017 IEEE International Conference on Big Data (Big Data)*, 3690–3699. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Zhang, A., and X. Lin. 2018. "Towards Secure and Privacy-Preserving Data Sharing in E-Health Systems via Consortium Blockchain". *Journal of medical systems* 42(8):140.

Zhen, Y., M. Yue, C. Zhong-yu, T. Chang-bing, and C. Xin. 2017. "Zero-Determinant Strategy for the Algorithm Optimize of Blockchain POW Consensus". In *2017 36th Chinese Control Conference (CCC)*, 1441–1446. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Zhu, X., H. Li, and Y. Yu. 2018. "Blockchain-Based Privacy Preserving Deep Learning". In *International Conference on Information Security and Cryptology*, 370–383. Cham: Springer International Publishing".

AUTHOR BIOGRAPHIES

HONG WAN is an associate professor in the Department of Industrial and Systems Engineering at North Carolina State University. Her research focuses on the areas of experimental design and data analysis of complex simulation models and blockchain. She is the director of the ISE blockchain lab, and serves as the editor in chief of Journal of Blockchain Research and the associate editor of ACM TOMACS. Her email address is hwan4@ncsu.edu and her website is https://www.ise.ncsu.edu/people/hwan4/.

YINING HUANG is a Ph.D. student of the Operations Research Graduate Program at North Carolina State University. Her research interests are simulation and blockchain technologies. Her email address is yhuang43@ncsu.edu.

KEJUN LI is a Ph.D. student in the Department of Industrial and Systems Engineering at North Carolina State University. His research interests include applied probability, simulation, game theory, and blockchain technologies. His e-mail address is kli15@ncsu.edu.