IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 30, 2020, accepted December 16, 2020, date of publication December 25, 2020,
date of current version January 7, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3047365

Blockchain System Defensive Overview for Double-Spend and Selfish Mining Attacks: A Systematic Approach

KERVINS NICOLAS[1,4], (Student Member, IEEE), YI WANG[1], (Member, IEEE), GEORGE C. GIAKOS[1], (Fellow, IEEE), BINGYANG WEI[2], AND HONGDA SHEN[3]

[1]Department of Electrical and Computer Engineering, Manhattan College, New York, NY 10471, USA
[2]Department of Computer Science, Texas Christian University, Fort Worth, TX 76109, USA
[3]Electrical and Computer Engineering Department, The University of Alabama in Huntsville, Huntsville, AL 35899, USA
[4]IBM, Armonk, NY 10504, USA

Corresponding author: Yi Wang (yi.wang@manhattan.edu)

ABSTRACT Blockchain is a technology that ensures data security by verifying database of records established in a decentralized and distributed network. Blockchain-based approaches have been applied to secure data in the fields of the Internet of Things, software engineering, healthcare systems, financial services, and smart power grids. However, the security of the blockchain system is still a major concern. We took the initiative to present a systematic study which sheds light on what defensive strategies are used to secure the blockchain system effectively. Specifically, we focus on blockchain data security that aims to mitigate the two data consistency attacks: double-spend attack and selfish mining attack. We employed the systematic approach to analyze a total of 40 selected studies using the proposed taxonomy of defensive strategies: monitoring, alert forwarding, alert broadcasting, inform, detection, and conceptual research design. It presents a comparison framework for existing and future research on blockchain security. Finally, some recommendations are proposed for blockchain researchers and developers.

INDEX TERMS Blockchain, double-spend attack, selfish mining attack, systematic review.

I. INTRODUCTION

Blockchain has emerged as an innovative technology to address the privacy risks and security vulnerabilities in a decentralized and distributed network, which have achieved huge success in various domains, such as Internet of Things (IoT), unmanned aerial vehicles (UAVs), healthcare, power systems, and financial services [1]–[9]. Blockchain is a shared immutable database ledger that stores data across a peer-to-peer (P2P) network. In addition, it is also a decentralized or distributed public ledger [10]. The data are stored in a chain of data blocks which are timestamped and validated by miners. Miners are linked to the P2P blockchain network which allows data to be shared directly between systems and networks in the chain. Each data block contains a list of transactions and a hash to the previous block. Blockchain stores a history of all the data transactions and provides a global distributed trust. It allows secure transactions to be processed and implemented without the need for a middleman or central governing system. However, although the feature of blockchain technology may bring us faster, safer, and reliable services, the security issues of blockchain is an important topic [11]–[13]. Some measures need to be put forward to address them.

The associate editor coordinating the review of this manuscript and approving it for publication was Taehong Kim.

A. MOTIVATION

From a data security point of view, the security attacks on blockchain data can be classified into three categories: data privacy attack, data availability attack, and data consistency attack [14], [15]. Data privacy attack includes the actions that violates the transaction privacy and identity privacy [16], [17]. Data availability attack includes network traceability attacks [18], [19], denial of service [20], [21], and eclipse attacks [22], [23]. Data consistency attack includes double-spend, selfish mining and block withholding attacks that makes the blockchain data inconsistent. Double-spend attack happens when a digital coin or cryptocurrency is spent more than once [24]. This type of attack allows multiple transactions to occur without a fair exchange in the network. Selfish mining occurs when attackers secretly mine a private

branch by creating a fork to the blockchain. The goal is to invalidate the honest miner's work and obtain a revenue larger than its ration of mining power [25]. Block withholding happens when an attacker privately withholds the block to cause loss to the miner and mining pool [26]. Selfish mining attack and block withholding attack are very similar since attackers usually withhold blocks for selfish mining [27], [28]. The only difference is that block withholding does not necessarily bifurcate the chain. In this article, we refer block withholding attack as a generalized selfish mining attack that creates fork.

Double-spend and selfish mining attacks are two data consistency attacks in the Blockchain, which are closely associated with the 51% attack in the system, so that attacker controls a majority of the network computing power and prevents other miners from completing the block. Double-spend attack leads to the 51% attack in a way of potentially increasing its success rate. Although double-spend attack can gain profitability using any proportion of computing power, double-spend attack tends to be more successful if it gains 51% of network's mining hash rate [29], [30]. On the other hand, a selfish mining attack is formed by secretly mining blocks instead of broadcasting it to the network. Selfish mining attack can make 51% attack easier in a way of increasing of the fraction of stale or orphan blocks due to constant fork, which cause 51% attack or consensus failures [31].

Selfish mining attacks can engender features of a double-spend attack and vice-versa making these two attacks closely associated with each other. When the blocks are finally broadcasted, due to the blocks the attacker has already mined, a double-spend attack can boost revenue. This leads to network monopolization because this does not present an equal opportunity for all users in the network [30], [32].

B. RELATED WORK

Blockchain has been applied to many areas to improve security, such as financial services, supply chain, IoT, healthcare, power grids, and energy management, etc. For example, blockchain has been used to perform securities and derivatives transactions [33], [34], digital payment [35]–[37]. Besides, blockchain can aid in asset tracking, secure order fulfillment and transaction records, to enhance the resilience and sustainability of supply chain [38]–[40]. In addition, healthcare organizations can leverage blockchain technology to securely process sensitive medical data [41], [42]. Medrec was the first functioning prototype proposed to manage electronic medical records (EMRs) [43]. Xia *et al.* proposed MeDshare, a medical data sharing system among the cloud service provider. This system utilized blockchain to provide data access control, provenance, and auditing [44]. Besides, the convergence of blockchain and IoT provides the trustworthiness in IoT data [45]–[47]. Bahga *et al.* proposed a blockchain platform for IoT. In this platform, smart contracts associated with machines are deployed on blockchain network to ensure trustiness [48]. Wang *et al.* discussed that IoT security can be enhanced by blockchain's identity authentication and access management [49]. Fernández-Caramés *et al.* discussed the blockchain-based IoT (BIoT) architectures with respect to the deployment and the optimizations [50]. Additionally, several recent studies have utilized blockchain to secure data sharing in energy management [51]. A consortium blockchain-oriented approach was proposed to address the energy trading users' privacy in the smart power grid [52]. Ferrag *et al.* presented DeepCoin, a novel blockchain-based energy framework to exchange the excess energy among neighboring nodes to ensure privacy preservation [53].

There are several recent reviews with respect to the security of blockchain. Zhang *et al.* provided a review on the blockchain architecture, consensus algorithms, and challenges. Specifically, the challenges include scalability, privacy, and selfish mining [54]. However, it fails to discuss the defensive strategies against these challenges thoroughly. Li *et al.* surveyed several real attacks, including selfish mining attack, DAO attack, Border Gateway Protocol (BGP) attack, liveness attack, and Eclipse attack. However, they only generally discussed several countermeasures to these attacks without comparison and analysis [55]. Joshi *et al.* discussed the blockchain security and privacy issues with an application perspective, specifically in the applications of finance, healthcare, IoT, mobile applications, defense, and automobile industry [56]. Similarly, Taylor *et al.* discussed blockchain security towards different application domains [57]. The applications were classified into nine domains: IoT, public key infrastructure, data storage, virtual network management, malware, data privacy, web applications, networking, Wifi. However, both failed to analyze and discuss the security mitigation strategies with respect to the blockchain protocol itself. Hence, there is a lack of a comprehensive review focusing on the defensive strategies towards the blockchain security attacks.

C. OVERVIEW

Unlike the aforementioned reviews, this work presents the first in-depth evaluation of the blockchain's security countermeasures in terms of two data consistency attacks of blockchain: double-spend attack and selfish mining attack. This article presents details on the overall capability of blockchain and its security parameters, which sheds light on the security design characteristics, mechanisms, and potential applicability. In order to accomplish our goal, we employed a systematic review approach based on the software engineering community research involving guidelines for creating a compelling research overview [41], [58], [59]. Utilizing the systematic review, a total of 40 primary studies have been identified as fitting to our research objective (See Section 3.2). These primary studies are based on the field of interest, validation techniques, technical solutions, and research trends. In short, the main contributions of this research are as follow:

1) Employ a systematic approach to summarize and analyze the defensive strategies for both double-spend attack and selfish mining attack in the blockchain.

2) Propose a taxonomy of defensive strategies for double-spend and selfish mining attacks based on design parameters and proposed security solutions. They are monitoring, alert forwarding, alert broadcasting, inform, detection, and conceptual research design. These six strategy types were proposed based on their design parameters and security solutions.
3) Make implications of future research directions on defensive strategies for double-spend attack and selfish mining attack.

The rest of this article is formulated in five main sections. In the section titled *Background* (Section II), we gave an overview of the characteristics and capabilities of a blockchain. We also present double-spend attack, and selfish mining attack. The next section titled *Methodology* (Section III), provides details on the systematic review approach and the taxonomy of the defense strategies. Next, the section titled *Double-spend Attack Defensive Strategies* (Section IV), presents an evaluation of the double-spend attack countermeasures that include the advantages and disadvantages of each proposed strategy. Following that, is a section titled *Selfish Mining Attack Defensive Strategies* (Section V), which provides details of a selfish mining attack countermeasures and explanation of the advantages and disadvantages of the proposed strategies. In the next section titled *Implication of Future Research* (Section VI), we present a research evaluation, details on blockchain security implications, and future works. The paper is concluded in Section VII.

II. BACKGROUND

In this section, we present the background information of blockchain, and security of blockchain with respect to two integrity attacks: double-spend attack and selfish mining attack.

A. BLOCKCHAIN

Blockchain is defined as a block comprised of a successive chain, as shown in Fig. 1. Each block is linked to the previous block in the chain. The structure of each block includes four components: block size, block header, transaction counter and transaction. Block size component uses 4 bytes to store the size of the whole block. Block header component size is 80 bytes. It stores an encrypted unique hash that identifies each block. The size of transaction counter component ranges from 1 to 9 bytes. It is the number of the transactions that follows. Transaction components contains the transaction saved in the block. The size of this component depends on the transaction size [60]. Blocks are then implemented into a successive public database which is referred to as a chain. The blockchain is based on a P2P networking system that allows transactions to happen from any part of the world [61], [62]. This decentralized structure removes the need for a physical central location to be used as the mediator for all transactions. This system allows nodes in the network to be the main source of transaction confirmations. Before a transaction can be integrated into a block and hashed, new transactions are sent to the nodes in the network to validate.

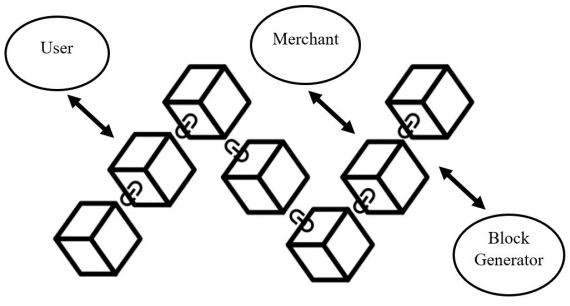

FIGURE 1. Blockchain System.

There are three primary actors in the blockchains system at the business level: user, merchant, and block generator. User is a human actor that creates transactions that stores in blockchain. Merchant is a business entity that accepts transactions in term of cryptocurrencies, e.g. bitcoin as a means of payments. Block generator is a human or system actor that validates the transactions and adds the new block in the chain [63]. The process of adding new blocks to the block is blockchain mining. The nodes that generate a new block are blockchain miners. A block, in blockchain, is comprised of data, block number, the cryptographic hash of the previous block, a hash of the current block, and timestamp all linked in a successive ''chain'' using cryptography. The blockchain transactions will be verified by a majority of the network participants through a consensus mechanism [64], [65]. Consensus mechanism includes incentivized consensus and non-incentivized consensus. Incentivized consensus mechanism is widely used in public blockchain, which rewards the participants for adding a new block in the blockchain. Non-incentivized consensus is used in private blockchain systems, where only authorized users can create and add a new block [66], [67].

B. DOUBLE-SPEND ATTACK

The objective of a double-spend attack is to spend a currency token more than once, by convincing both the merchant and the network that the currency token being spent is valid [29], [68]. If the attacker can finalize a transaction with a merchant and has successfully enabled the rest of the network to accept the transactions, then the attacker is able to gain both the product and the currency token that was spent.

Fig. 2 displays a scenario of a double-spend attack in a bitcoin blockchain. This can be done by the attacker who simply creates the two conflicting unconfirmed transactions A and B, where B has the same unspent transaction output (UTXO) with A. Before A is added to the main chain, attacker secretly mines his own chain following the current latest block. B is included in attacker's own chain to move funds to the attacker's second address. There are two branches of the blockchain, and the race will begin. After the merchant received enough confirmations for A, the product is sent to the

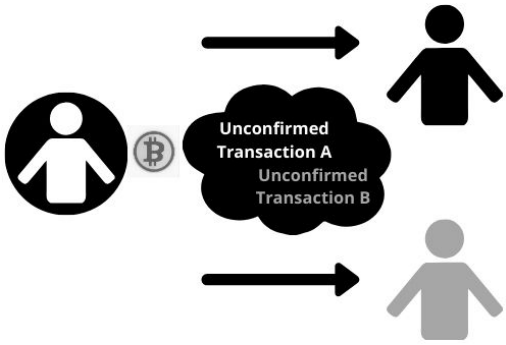

FIGURE 2. Double-spend Attack.

attacker. Then, the attacker keeps mining until his own chain is longer than the main chain and broadcast it to the network to create a fork. The longest chain rule makes the attacker's own chain valid and B is replaced by A. The attacker gets both the funds and product finally [24], [68].

C. SELFISH MINING ATTACK

A selfish mining attack relies on "block concealing" and make the network adapt to their block solutions and claim block rewards [25], [69]. In selfish mining, the selfish miner or selfish mining pool with a hash rate of α secretly withholds newly mined blocks instead of publishing or distributing them to the rest of the network [70]. This private chain will continue to mine until they have reached a greater length than the main chain. Pool managers can broadcast their blocks to deceive honest miners into thinking that the pool is safe, but honest miners that have unknowingly joined a selfish mining pool use their computing powers to generate blocks that do not produce rewards. As seen in Fig. 3, we outline this attack procedure. Once the next block is found, the miners will then publish the block to either keep the successive chain flowing and obtain a mining reward or to create a fork. A fork occurs when two or more blocks have achieved the same block height and the one which contains a longer and valid PoW will become the main chain. If the attacker publishes their blocks first, the chain will diverge into another set of protocols. The network adapts the new chain and miners in the network will begin mining on the chain.

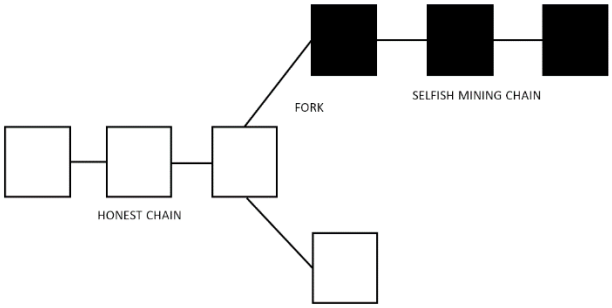

FIGURE 3. Selfish Mining Attack.

III. METHODOLOGY

A. SYSTEMATIC APPROACH

Fig. 4 shows an overview of our design procedure into formulating this study [71]. Our systematic review is broken down into five phases: planning, developing, quantitative research, qualitative research, and documenting. To increase the overall potential of this study, we created this multiphase conceptual review process to provide a high level of validity and technical understanding. In the following, we will go through the various phases of the systematic review.

1) PLANNING

In this phase, we set the research goals and project the overall extent that we would like to achieve in this study. Some of the tasks that we need to accomplish our main objective are presented in the form of research questions to provide key aspects of this study. This phase presents the research questions, protocols, and design targets.

2) RESEARCH DEVELOPMENT

In this phase, we formulate the steps to identify, analyze, and classify relevant research to be able to perform this study. We perform these activities by dividing them into two parts. A quantitative, and qualitative research method [72].

Quantitative Research is a contribution of studies with an experimental base and theoretical design models from various parts of the world at different time periods. We optimize the quantity of valid research integration by exploring outside knowledge pertaining to this study. To implement our systematic approach, we collected various studies from a great number of places such as blockchain polling websites, questionnaires involving blockchain users, graphs, short essays, and articles. This type of approach broadens our research capabilities and allows for the potential of an unbiased study. The collection of performance data, observational data, computational data, and strategic statistical test analysis are all included.

- *Studies collection:* we perform a technique in order to identify relevant works pertaining to our research goal. This search involved the integration of electronic, manual and anomaly search strategy
- *Studies selection:* we refine the candidates that pertain to our objective and create a conclusive list of works that will be reviewed to formulate a finalized version of primary studies. This also involves publication research trends of primary studies.
- *Search strategy*: we were able to gather and process the data necessary for this research by combining electronic, manual, and anomaly search strategies.

Qualitative Research evaluates and explores the research studies to identify, analyze, and classify the works. The review of this method is to address the research goal and to proceed with interpreting reports.

- *Publication trends:* we summarized the development of publications involved with blockchain countermeasures.

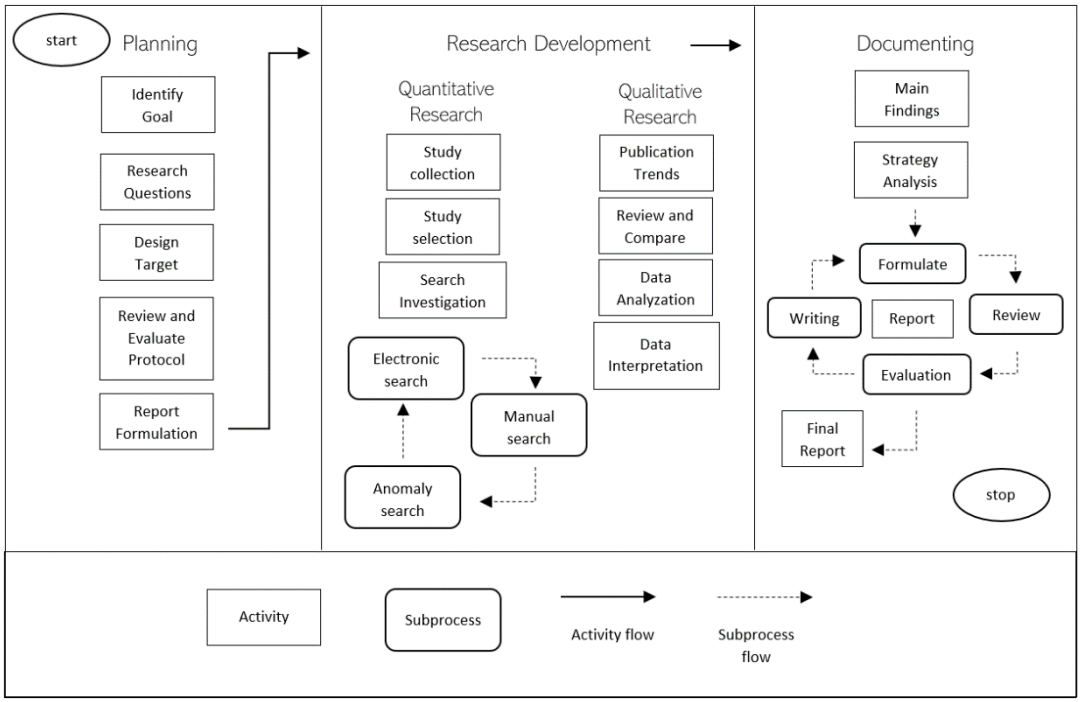

FIGURE 4. Overview of Systematic Approach.

- *Review and compare:* we conduct a special inspection of the studies and examine distinct parameters to compare proposed methods and strategies.
- *Data analysis:* we extract information provided in primary studies to analyze theories and frameworks.
- *Data interpretation:* we filter the extracted data and provide details and elaborate on the main overview presented.

3) DOCUMENTING

This phase is comprised of the results of the literature review. We were able to compose six strategy types for double-spend and selfish mining attack countermeasures to present the main findings of our research. The written summary of the proposed studies, documents, articles, and reports are all processed through the systematic design mechanism [73]. They are reviewed, critiqued, and reevaluated until a final report can be established.

B. TAXONOMY OF DEFENSE STRATEGIES

In this section, we summarize the primary studies and proposed taxonomy of defense strategies based on their design parameters and security solutions. Fig. 5, shows the distribution of the primary studies from 2007. From the data, we were able to analyze that the security of blockchain research proposals involving attacks on the network has significantly increased over the years. Since 2013 we have been able to see that there is an upward trend in blockchain security study in both experimental design frameworks and publications with respect to the double-spend attack and selfish mining attack. Dealing with various cyber-attacks on the chain has helped

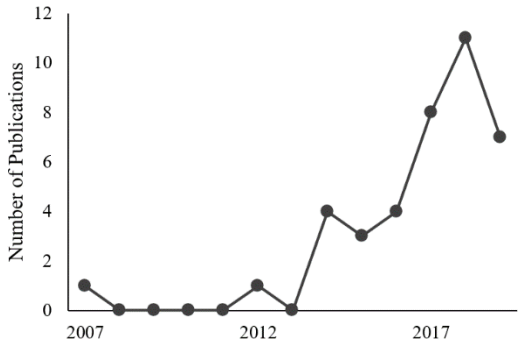

FIGURE 5. Primary studies distribution by year.

improve the types of research proposals created to enforce security measures on the system.

The six types of defense strategies are detailed as follows. They are monitoring, alert forwarding, alert broadcasting, inform, detection, and conceptual research design.

- **Monitoring:** Established to record user activity based on time, usage, and tasks in order to determine possible illicit activities. Implementations of this method involve analysis to filter attack data and evaluate distinct features. Monitoring is a strategy based on the imposition of identity on data inputted into the system. The configurations to apply this strategy is in the form of neighboring vendors or software implementation. Nodes registered to detect abnormalities based on prior configuration can be used to recognize patterns of unique attacks. Providing a software application, that can accomplish the same task with more input parameters for deep analysis is also an option.

- **Alert Forwarding:** Communication based alert system that notifies nodes of network activities. Dispatching blockchain validation notifications or peer forwarding are some of the use cases.
- **Alert Broadcasting:** Simultaneous transmissions of network activities provides public system information to recipient addresses. Broadcasting is a strategy used to decrease the amount of attack in the chain by providing private details relating to the attackers. The differences between the broadcasting methods rely on the methods used to forward the transaction details in the chain. This is based on the configuration design to provide a constant flow of data to the rest of the nodes in the system or relying on a randomized method to forward attack indications based on features presented by a specified source.
- **Inform:** Summarization of data which includes raw facts, models, figures, processes, and mathematical algorithms of blockchain to decipher blockchain deficiency and engender a defensive solution.
- **Detection:** Based on setting design parameters to indicate abnormalities and misbehavior in the system. Design parameters are indicators of the misbehaviors that directly or indirectly affect the system. The system will be modified, and the user will be get notified.
- **Conceptual research proposal:** Refers to theoretical defensive design solutions proposed to enhance blockchains capabilities based on constructed predictive models and theory-based techniques. In order to present a study that is capable of being viable in the ongoing research of countermeasures of double-spend and selfish mining attack. The conceptual research proposal is a type that identifies multiple proposed methods from a diversified group of papers to stretch the boundaries of this research. Providing control theoretical analysis, computational complexity, graph theory to examine protection-based defensive mechanisms. These methods vary from the previously discussed methods to ideas engendered by simple frameworks to reduce the attractiveness of attacking a blockchain.

As depicted in Fig. 4, we utilized our systematic review process to characterize each framework to distinguish and outline proposed implications on the blockchain network. Fig. 6, displays the distribution of the double-spend and selfish mining countermeasure strategy types. The distribution of the primary study types is as follows.

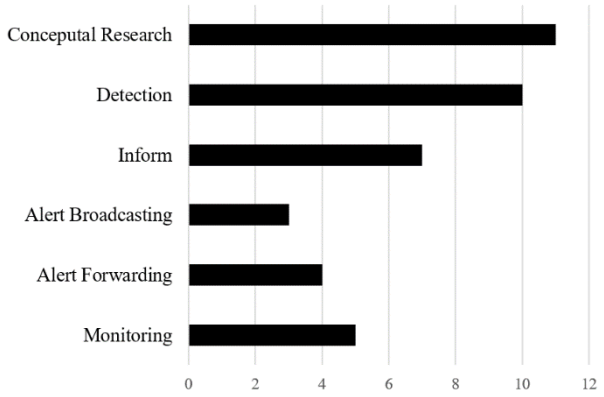

FIGURE 6. Distribution of primary study strategy type.

IV. DOUBLE-SPEND ATTACK DEFENSIVE STRATEGY

Double spending attack defense strategies are compared and summarized in Table 1.

A. ALERT BROADCASTING

Utilizing the confirmation system in blockchain, the Zero-Confirmation Transaction was proposed to describe a scenario that multiple transactions generated by double-spend attack can be broadcasted selectively in the network [74]. The mechanism is to penalize the attacker who broadcasts the double-spend transactions by disclosing his/her secrete key using a special type of outputs. Hence, the attacker risks losing all funds deposited in their address due to peers being able to derive private keys in the system. Specifically, this will be achieved by generating special transaction outputs. If the different digital signatures of the same outputs are revealed, the private key used to sign the signature will be disclosed. This exposed key will allow observers to conduct the third transaction of same spending, which discourages double-spend transactions.

This defensive strategy for this alert broadcasting type of attack utilizes the Elliptic Curve Digital Signature Algorithm (ECDSA) signature scheme and fixed-r pay-to-pubkey script (FR-P2PK). ECDSA cryptographical algorithm ensures that funds can only be spent by the owner of that coin. The FR-P2PK is a proposed Bitcoin script that requires a signature with a specified r value. r is deterministically generated from integer k and fixed parameters of the ECDSA. Where k is in the range of $[1, q-1]$, and q is a prime number corresponding to the order of generator G of the elliptic curve. Before broadcasting or even publishing the block into the chain, blocks are stored in the memory pool.

This countermeasure goes through two phases: initialization and fast payment. During a transaction in the initialization phase, a miner will be able to choose a random integer and public key (the secret key is known only to the miner). Once the transaction is confirmed and moves to the fast payment to be spent to a vendor, the vendor can validate if the transaction has been spent before by being able to redeem the private key information and checking all associate transactions attached with similar transaction detail. The main advantage of this strategy is that it affects all attackers that broadcast transactions in the network which can secure the zero-confirmation transactions. The limitation of this work is that it lacks experimentally testing on this countermeasure.

B. ALERT FORWARDING

Meni Rosenfeld analyzed the probability of a successful double-spend attack based on the amount of confirmation

TABLE 1. Double-spend attack countermeasures – benefits and limitations.

Strategy	Type	Benefits	Limitations
Zero-confirmation transactions [74]	Alert Broadcasting	Digital signature broadcasting	No experiment on testing the proposed method
Wait for confirmation [75]	Alert Forwarding	Increases confirmation	Greater computing power results in a potential disregard for confirmation
Forward double-spending [76]	Alert Forwarding	Attacker node peer monitoring technique to optimize overall security measure	Presents denial-of-service attack
Peer forwarding [77]	Alert Forwarding	Detect matching transaction	Can cause network performance issues
Formula based probability [78]	Conceptual research design	Attack probability determination	Derived by algorithm, no simulation data
Increase confirmation Selective peer status [79]	Conceptual research design	Simple countermeasures	Slow down the responsiveness of the system; limit the availability of the system
Listening period, Inserting observers, Forwarding[80]	Conceptual research design	Proposes various defensive mechanisms for a robust blockchain network	Lacks simulation results
Logarithmic waiting time [81]	Conceptual research design	Provide more security than waiting for a fixed number of confirmations	Requires a few confirmations to grow. Lacks network testing
Delayed proof of work [82]	Conceptual research design	Flexibility and security enhancement using notary node network	Short confirmation transaction can be at risk
Privacy and anonymity [83]	Conceptual research design	Provide privacy and anonymity to combat various attacks	Vulnerable to DoS attacks. No formal testing on countermeasures
E-cash protocols [84]	Detection	No need for a trusted third party, real-time detection	Presents transaction aggregation issues
Wait for many confirmation blocks [85]	Detection	Counterfeit chain detection	Takes a long time to make the reward negligibly small for the attacker
Compare global and local state hashing values [86]	Detection	Mitigate inconsistent execution of the smart contract state machine	High computational overhead
Incorporate accountability [87]	Detection	Complements privacy and reduce misbehavior	No scientific model or analysis
Enhance network policy [29]	Inform	Limit profitable double-spend attack	Can be configured and bypassed
Limit number and sizes of Whale transactions [88]	Inform	Mitigate a minority double-spend attack, called whale attack	Proof-of-concept without implementation
Gambler's ruin [89]	Inform	Simulate the race between honest miners and attackers	Provide only simulation, no implementation measures
Inserting Observers [90]	Monitoring	Lightweight countermeasure	No verification of efficiency
ENHOBS [91]	Monitoring	Deep observational analysis	No analysis of large network attacks
Limit time advantage [92]	Monitoring	More general than existing models	No formal mathematical semantics or verification

and the hash rate of the attacker, q. If the attacker's overall computing power reaches 50% or above, there will be a 0% chance of stopping a double-spend attack [75]. Rosenfeld argues that increasing the amount of confirmation exponentially decreases the probability of an attack and not the amount of time waited. Following the Poisson distribution formula stated by Satoshi in the blockchain whitepaper, Rosenfeld engineered a mathematical formula to calculate the number of blocks found by the attacker before the honest mining network finds a block [93]. With this information, the success rate of an attack on the system was able to be calculated to the nearest decimal. The system's disadvantage relies on the attacker's computing power. With a machine that is capable of parallel processing or equivalent features, this can produce a high potential disregard for confirmation.

Two forwarding methods were evaluated and compared based on some of their distinct characteristics. Grundmann *et al.* proposed forwarding double-spend attacks [76]. This can be done by forwarding all attacks to the network nodes or by randomly selecting attacks. This method exploits distinct addresses and transactions in the system in order to warn the peers in the network. One drawback of this method can be the potential for a Denial of Service (DoS) attack. Flooding the network with double-spend attack notification can possibly harm the network and reduce the overall performance of blockchain. Randomly selecting double-spend attacks allows the network to monitor and observe all incoming transactions and provides a mitigation factor to the network. Karame *et al.* proposed a similar method but with a focus on peer forwarding [77]. This is done by having the vendor employ observers in the pool that will be able to detect an attack if another transaction is sent with the same coin. If the coin is found and resides in the blockchain or memory pool, the vendor will then receive alerts from the peer observers in the network. The attempted attack is notified. Whenever a new transaction is received, this

checking procedure will enable for classification of whether the coin should be added to the memory pool or discarded. It also evaluates the accountability of attackers. In contrast with the current bitcoin protocol where node IP addresses that misbehave in the network are banned from the network for twenty-four hours, this countermeasure believes in enforcing address blacklisting. It adds misbehaving addresses to a public blacklist where nodes in the network will avoid all contact with that address.

C. CONCEPTUAL RESEARCH DESIGN

This section focuses on the theoretical proposed models to combat attacks on a blockchain system. These methods are proposed theoretically without experimental testing. Some of the possible solutions include: increase confirmation, selective peer status, inserting observers, listening period, forward double-spending, anonymity proposals, listening and insert observers.

Increasing the number of confirmations is the simplest countermeasure by waiting for a higher number of confirmations. The attack tends to be disrupted and keeping the duration of an attack becomes more difficult. It can increase the probability of detecting an attack. However, this process decreases the responsivity and slows down the transaction rate [79]. Another method discussed by Ekparinya *et al.* is selectively querying the status of the peers. Before the transaction is committed, the merchant queries the status of a transaction from many peers selectively from different locations, even further away in the network topology. Querying the status of a transaction is able to detect an attack in the network by finding the group of verification nodes and tracking the transaction data. When the number of verifications from the peers is high, the attack rate is lower. However, this method may limit the availability of the system during deployment.

Inserting observers in the network is proposed based on the capability of detecting and providing the network with attack data from malicious addresses [80]. This enables the vendor to disable incoming connections and discard double spent coins from their memory pool. In addition, Rathold *et al.* present another mechanism called the ''listening period''. This mechanism defines a listening period for each transaction. The transaction will be delivered only when no double-spend attack has been detected. Another countermeasure is peer alert notification. It would allow more miners to be mindful of misbehaving addresses and attack transactions in the system.

Sompolinsky *et al.* discussed bitcoin's security against double-spend attacks, specifically Finney Attack and Vector76 attack [81]. Finney attack is a fraudulent double-spend attack that is carried out at a moment selected by the attacker. It is a pre-mining attack that the pre-mined transaction can be spent again before the block is invalidated by the public network [94]. Vector76 attack is one confirmation attack that privately mined block can be used to perform double spending [95]. The transaction has one confirmation that can still be reversed in this attack. Mitigation techniques are introduced: 1) Large transaction recipients should commit to wait a number of confirmation logarithmic in the length of the chain that will provide the appropriate amount of time needed in order to guarantee a safe transaction; 2) Small transaction recipients must advise distinct policy checks before proceeding to a transaction.

Maintain user privacy and transaction anonymity is another countermeasure for block security vulnerabilities, including double-spend attack. The deployment of anonymity can also defend against various attacks using a collateral system. This system is a CoinJoin implementation that no external party is involved with the transaction validation [96]. To enhance the design of blockchain and cryptocurrency design protocols, some practical techniques are proposed to address, including secure timestamping, overlay protocols, and digital tokens, etc [97]. In addition, several other techniques were proposed to improve the privacy and anonymity of bitcoin [83]. For example, Dandelion provides strong anonymity by establishing a network policy that prevents deanonymization. However, it is vulnerable to Denial of Service (DoS) and Sybil attacks [68]. A Sybil attacker can create many forged identities to break the trustworthiness of the system [98], [99]. CryptoNote utilized a ring signature to provide viable anonymity benefits, but it brings higher computational complexity. MimbleWimble is a scalable and compatible design for confidential cryptocurrency transactions. However, it is not compatible with smart contracts.

Delayed proof work (dPoW) is proposed by Komodo to protect against the double-spend attack. The main feature of this mechanism is recycling the hashrate and secure other blockchains. It provides a tokenization platform and integrates a notary node network, which adds a security layer to mitigate 51% attack. In addition, its integration with notary nodes can check the security of hash and has been deployed in about 20 blockchains [82]. However, transactions with short confirmation time can be at risk [30].

Concentrating on a mathematical closed-form formula for the probability of success of a double-spend attack, Grunspan *et al.* correct Satoshi Nakomoto's analysis which simply assumes that honest miners validate block at the expected rate [78]. Since the probability success rate of double-spend attack increases with the validation time T, they conduct a rigorous analysis by considering the conditional probability assuming T. This risk analysis utilized the Regularized Incomplete Beta Function, which provides a viable understanding of the probability of certain conditions to take effect. This resulted in clearing up the capabilities and disadvantages of the current blockchain network.

D. DETECTION

Detection techniques are one of the strategies that provide countermeasures to blockchain attacks. They provide the user with the ability to be notified of misbehavior that can cause issues in the system. This notification provides more awareness of system modifications that users can adjust accordingly.

One detection method is a mitigation technique to provide a robust system to combat attacks that were developed in alignment with the e-cash protocols. This method provides a real-time detection which does not need a trusted third party [84]. The implementation includes three protocols: withdrawal, payment, and deposit. Withdrawal, when the client is buys coins. Payment, the client buys merchandise using a coin. Deposit, the merchant receives client coin transactions. This study allows for an inspection of the various stages of cryptocurrency.

Chohan understands that double-spend attacks pose accounting and accountability challenges in the blockchain infrastructure. In order to allow the network to flow without attack issues, another detection countermeasures presented in this article result in implementing a lightweight defensive strategy that enables the detection of attacks in a fast transaction [87]. Increasing the number of accountability miners have, will enable for more honest mining procedures followed to benefit the performance of the chain.

Another detection strategy is proposed by Ramezan *et al.* to detect and analyze chain activity [85]. This strategy formulates an attack on the system that observes the length of the honest chain in order to produce a counterfeit chain. This counterfeit chain model will allow more conventional attacks to formulate in the system and allow attack rewards to increase over time. Even if the network nodes decide to follow the misbehaving chain, increasing the number of confirmation blocks to a larger validation factor will allow for a viable countermeasure strategy. However, we need to wait for a long time so that the expected received reward can be negligibly small for the double-spend attacker.

Inconsistent execution of the smart contract state machine will create a fork in the entire blockchain network, which can lead to double-spend attack. A detection-based countermeasure was proposed to detect the equal results from the hash of the local state and the hash of the global state. If the result is equal, no double-spend attack can happen since this will not generate a fork. However, hashing the global state brings a high overhead issue [86]. To solve this issue, only matching and verifying the write sequences locally that changes the global state can potentially reduce the computational overhead.

E. INFORM

The inform category is based on analyzing the security of blockchain using mathematic models. Over the years, researchers and practitioners have analyzed the multitude of formulas and models that Nakomoto invoked in the blockchain to solve double-spend [100]. Ozisik *et al.* analyze Satoshi Nakomoto's blockchain security and proposed that the probability of the double-spend attack can be simulated as solving a Gambler's Rin problem [89]. It is defined as a persistent gambler raising a bet to a fixed fraction. Monte Carlo simulation is used to validate the proposed mathematical model. The results demonstrate that the probability of attacker success is increased with attacker's mining power. However, no real-world implementation is conducted for validation.

Another inform strategy is based on the countermeasure against whale attack, which is an enhancement of a double-spend attack for minority attackers [88]. This attack includes a pre-mining phase and a race phase. It works by providing an incentive to rational miners to collude. Honest miners in the network should be cautious of attackers with incentives that are out of the ordinary bounds of standard blockchain protocols. They should also be mindful of the anomalously large parameter configurations. The simulation results proved the feasibility of this attack. The strategy to mitigate this attack is limiting the size and number of whale transactions. They are the upper bounds of the cost to carry out this attack. However, this work is a proof-of-concept without real implementation.

Double-spend attack can still gain profit using any proportion of the computing power. It is proposed that the implementation of a strong network policy can provide a safety chain. Based on the network policy, restricting the value of transactions will limit the profit of double-spend attack [29]. Misbehaving miners would sometimes be linked to risky networks. This can have significant effects on the block confirmation, average block mining period, and expected mining profit.

F. MONITORING

Countermeasures based on monitoring will record user activities based on time, usage, and tasks, etc. The fundamental monitoring strategy is inserting observers. Karame *et al.* proposed this countermeasure for fast payment transactions. Fast payment transactions are regarded as exchanges that have a shorter time to process and finalized than a normal transaction. Attacks are more likely to occur in this case due to the ingenuity of attackers and the lack of understanding that unsuspecting users have of the overall capabilities of the blockchain. Inserting observers' strategy employ observers within the network that are controlled and used to detect attacks. These observers are connected to many peers in the network. In order to boost the probability of finding misbehaving addresses sending attacks to the system. The observer nodes will be able to detect duplicate coins that share the same common input but different outputs. An alert will be sent to the vendor within a few seconds. Since this method allows neighboring nodes to be able to receive forwarded attack flags, without the correct configurations, DoS attacks can propagate through the network. The flooding of target nodes with message prompts can potentially trigger a crash and cause the network to shut down. It is a lightweight countermeasure, but the efficiency of this method is not analyzed.

Enhanced observes (ENHOBS) is a hybrid monitoring countermeasure based on the combination of the listening period and the use of observers [91]. Unlike the observer model that will relay all transactions in the network and leaving the vendor to find to detect the duplicate transactions, ENHOBS is built to detect and alert the system of

double-spend attacks. This is done by having the ENHOBS analyze the inputs as well as the outputs that are generating in the network. Any transactions detected as being an attack that matches the same input data as a transaction currently in the memory pool is dropped. Once an alert has been validated, miners will run a one-time scan of the transactions in the memory bank and if there is no match, nothing happens but if there is, that transaction will be dropped due to the threat that it can cause to the miner. This alert will resonate through the system until two new blocks have been validated and incorporated into the main blockchain. Once the blocks have been appended to the system, the process will start again.

ENHOBS will be provided to peers as a subscription-based system and alerts will only be sent to them regarding any double-spend attacks propagating through the system. Non-subscribers will not incur any issues regarding resources or monetary intake. The balance for this countermeasure is to maintain the performance of the system while also providing for a low-cost solution. Even though this system is built to mitigate attacks on the system, it does not address the potential for malicious intent. No analysis of this countermeasure applied to a larger network is presented as well.

Monitoring the new time difference after the new block is produced is a countermeasure against double-spend attack. It is proposed that the attacker who has enough time advantage can increase the attack probability [92]. The time advantage model indicates that time is one of the main factors to carry out a viable attack. There are two models that consider the time advantage, generalized model, and time-based model. A generalized model adds a time parameter to the mining process. The time-based model makes use of the times that honest miner and attacker last mined a block. Compare to the hash rate-based models, the proposed two models demonstrated its advantage of limiting the double-spend attack by monitoring the time difference. In addition, they are more general in practice than other existing models.

V. SELFISH MINING ATTACK DEFENSIVE STRATEGIES

Selfish mining attack defense strategies are compared and summarized in Table 2.

A. ALERT BROADCASTING

Zhang proposed a broadcasting strategy for combatting selfish mining attacks on a blockchain [101]. Originally when a block fork occurs in the chain, the longest chain rules are in effect [102]. The miner or pool that has the longest block height and is trying to implement their block on the chain is picked. Hard forks change the rule on the size of the block and the software protocol. The GHOST rule, in contrast to the longest chain rule, incorporates the weight of a block [101]. The branch with a larger weight value will have priority in implementing its block into the chain. The weight of the block is determined by the PoW and the communication overhead.

FruitChain is a new block reward scheme that implements a broadcast channel to mitigate the selfish mining attack [103]. As it can be seen in Fig. 7, the broadcast channel is a second

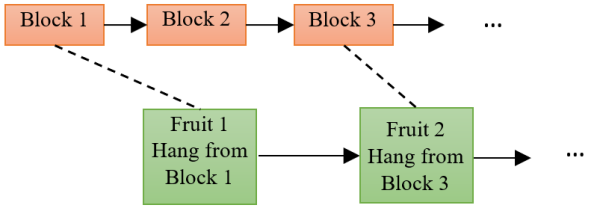

FIGURE 7. FruitChain Architecture.

mining process and is parametrized as a different mining hardness, called fruit hardness p_f. Records m are put inside "fruit" denoted as f, and they solve a proof of work with p_f. The block mining and fruit mining are linked by each other. A fruit must be "hang" from a block that is not too far from the block which has records of the fruit. The distance between the fruit and the linked block is controlled by recency parameter R. In this case, honest miner needs to simultaneously mine both a fruit and a block. When a fruit is mined, it broadcasts the fruit to other players. It prevents selfish mining attack by requiring the fruits to be recent. Therefore, attackers cannot withhold fruits for a long time. Overall, this new block reward scheme focuses on the overall security enhancement of the blockchain protocol. However, it brings a lot of modifications and computational overhead to the existing blockchain. Deploying this new scheme in real blockchain environments is difficult.

B. ALERT FORWARDING

One forwarding strategy is forwarding the secret block information to honest miners by implementing counter-attackers to infiltrate the selfish mining pools [25]. Selfish mining pools are constructed by miners since the average computation required for mining is high so that individual miners cannot afford it. Miners who chose to collude together in order to attack the network can hide inside a selfish mining pool. Information regarding the various bitcoin and IP addresses that are attacking the chain is not made public. Therefore, implementing an exploitation mechanism, unsuspecting honest miners can gain reliable information regarding misbehaving addresses and pools.

Specifically, they implement a uniform tie-breaking scheme that uniformly selects the chain to mine from several equal length competing branches [104]. However, this method has the limitation of increasing the power of poor communicating attackers. Additionally, it also increases the chance of match action from the attacker even if no block is prepared ahead of time.

C. CONCEPTUAL RESEARCH DESIGN

One conceptual research proposal is computing closed-form formulas for long term strategies for Bitcoin and Ethereum, the results show that depending on the time and relative hash rate of the attacker, profitability and resiliency is impacted significantly [105], [106]. Counter mining is a strategy that obtains the PoW task of a selfish mining attacker and

TABLE 2. Selfish mining attack countermeasures – benefits and limitations.

Strategy	Type	Benefits	Limitations
GHOST [101]	Alert Broadcasting	Header weight advantage	Mitigates but does not eliminate attack
FruitChain [103]	Alert Broadcasting	Implements a broadcast channel as an additional mining process	Deployments in a real environment are difficult
Uniform tie breaking [25]	Alert Forwarding	Expose the secrete blocks easily	Increase the power of poor communicating attackers and the chance of match actions.
Counter mining [107]	Conceptual research design	Get significant extra revenue	Adversely affecting the revenue of honest miner.
Trusted peer mining pool [26]	Conceptual research design	Mitigate withholding attack under subversive miners	Mining pool cannot be too large or too small
PoW bonus, Miner fee, Honeypot [108]	Conceptual research design	Benefits honest mining practices	No implementation or validation
Chain Locks [30]	Conceptual research design	Faster and more private	Only one currency can be protected, vulnerable to double-spend
Orphaned block broadcasting [106]	Conceptual research design	Adjust the difficulty to make the attack non-profitable	The possibility of attack is not reduced
Freshness Preferred [110]	Detection	Time-based advantage	Subject to time-jacking and slothful mining attacks, no simulation or real environment testing
ZeroBlock [69]	Detection	Timestamp-free detection	Does not solve accidental forks
Infiltration detection & punishment [111]	Detection	Consumes little resource	Limitation in a real environment without assumptions
Truth state [112]	Detection	Effectively deters selfish mining	Not effective when an adaptive attacker includes fewer or no transactions in each block
Weighted fork-resolving policy[113]	Detection	Backward-compatible, decentralized and effective	Assumptions on a synchronous model, inconsistency, no simulation or real environment testing
PPLNS (pay per last N shares) [114]	Detection	Keep lesser impact of selfish mining attacker than traditional proportional reward scheme	No test on a real private blockchain system
Increase the number of simultaneous attackers [115]	Inform	Focus on multiple simultaneous selfish mining attackers	Fails to consider the network capacity of selfish mining attackers
SquirRL[116]	Inform	Deep learning methods for vulnerability detection automatically	Do not consider multiple partially cooperative agents
Adjust uncle reward [117]	Inform	Decrease the ratio of uncle block in Ethereum	No test under simulation or in a real private blockchain system
Minimize communication delay [104]	Inform	Insights on the impact of communication delays	No considerations on delays among competing selfish mining pools, no testing results
A new payoff scheme [118]	Monitoring	Does not require any adjustment of the current public protocols	No test under simulation or in real private blockchain system
Blockchain fork heights[119]	Monitoring	Monitor blockchain fork height deviating from the standard	Several false positive and false negatives when calculating the detection accuracy

complicates the attacker's strategy [107]. A new PoW will be created using the leaked information. It enables other miners to mine on an unpublished chain of a selfish miner [89]. When the attacker mines on a block and tries to publish the findings with an unknown previous block hash, a detection parameter is met indicating selfish mining behaviors. The method disturbs the private mining chain and increases the revenue of the counter miners who employed the counter mining method. As a result, the selfish miner may lose their revenue. However, this method might be harmful to the blockchain system by adversely affecting the revenue of honest miner. More than 10% of the total range of revenues of the honest miners can be damaged.

Game theory is used to analyze the effects of selfish mining attacks on a pool [108]. It is designed to allow a portion of the pool participants to attack other pools. This game presents the miner's dilemma that the participating pool will earn less if they attack one another than the fact that they do not perform the attack. Due to the practical size of the pools made, detection of selfish mining, has been hard to determine the overall risk of an attack. Four countermeasures are proposed: 1) PoW bonus: miners who submit full blocks will gain a bonus. Providing a full PoW would indicate honest mining features. This concept would encourage miners to stay in the parameters of an honest miner. 2) Miner fee: New miners joining a pool would incur a fee based on the amount of work done on the pool. When a reputation is established, the pool would increase the miner's revenue to a regular miner rate. 3) Honeypot: Miners in the pool are sent a PoW task that will result in a full PoW. Miners who are not able to provide the necessary data are flagged as attackers. 4) Hardware/software modification: Using computing systems that are configured to have a robust defensive mechanism that blocks selfish mining attacks. However, there is a lack of implementation or simulation on these countermeasures.

ChainLocks is proposed to secure Dash, a blockchain that was forked out of the bitcoin to provide faster and more private transactions to users [30]. It is proved that it can mitigate selfish mining attack. The main feature is its fast and simple confirmation mechanism. The transactions are confirmed only after a single block confirmation. It enhances a secure transaction after one confirmation by creating a network-wide vote process utilizing a valid signature for the validation of new transactions. The limitation is that only one currency can be protected. Additionally, it is vulnerable to double-spend under one confirmation attack.

Another countermeasure is the trusted peer mining pool. Pool miners only communicate with trusted parties. Pool should be dissolved or shut down by pool managers if pools did not contain known or trustable users. This countermeasure is proposed by Courtois *et al.* under a relatively new block withholding attack using subversive strategies. This new block withholding attack generalizes the ''sabotage'' attack and subversive miners get a huge reward [109]. This study believes that the best defense against block withholding attacks is to only allow trusted parties to be able to have access to your pool. Members that are not trusted can provide a greater quantity of revenue due to block creation and computing power but can be very detrimental to the overall health of the pool. An attacker can work inside a pool as one that takes advantage of other's mining power and use that to gain while decreasing the value of an honest miner's pool. As soon as a flag is raised based on a change in standard pool earning, a pool manager must immediately act for the benefit of the pool. This countermeasure has several limitations. First, it is not easy to identify trustable people in the pool. Second, the pool cannot be too large or too small.

Grunspan *et al.* introduced the idea to mitigate selfish mining attacks in the network that involves orphaned blocks [106]. Orphaned block or stale blocks are blocks that have been rejected from being added to a chain due to another block either being quicker or having a larger share of the PoW to be accepted in the chain. Once rejected, these blocks exist in the network but not the blockchain. In this case, a large amount of hashrate of the honest miner is lost. By incorporating the number of orphan blocks in the difficulty adjustment formula, the proposed method reinforces the PoW concept of blockchain during a fork and adds a priority level, which provides an advantage to blocks containing the most PoW with orphaned block. This method makes the selfish mining attack non-profitable by adjusting the difficulty. However, the possibility of selfish mining is not reduced.

D. DETECTION

The detection method relates to proposed research studies that are based on investigating and identifying attacking data to mitigate malicious effects on the blockchain. To decrease the profitability of an attack with selfish mining features, ''Freshness Preferred'' is a type of detection strategy that focuses on unforgeable timestamps [110]. The unforgettable stamps are provided by random beacons. This method can ensure that the block is generated after the timestamp. Utilizing the timestamp, the miner can prove that the block has been mined already. The Freshness Preferred strategy provides an enhanced feature to create a safe network but has disadvantages that weaken it to other attacks. It provides an advantage for honest mining by giving rights to new block implementation to blocks that have been mined recently. One goal for a selfish miner or a selfish mining pool is to increase the probability of block implementation in the blockchain by having a good number of past blocks to be able to create a fork. This Freshness Preferred strategy is primarily focused on that factor. Specifically, blockchain peers verify a random string value K and a matching timestamp. Any new transaction trying to be implemented will, in seconds, have generated an unpredictable random K. A timestamp will also be associated with this value. When that transaction is later trying to be appended in the blockchain the proof of the creation time of that block will be published. Therefore, verifying the time of a transaction become easier to identify. Any transaction that is too old or has no or future timestamp is attacking and would raise a flag in the system. However, time-jacking and slothful mining attacks are some of the attacks that the Freshness Preferred strategy cannot avoid.

Different from the Freshness Preferred, Solat *et al.* presented a timestamp-free detection of selfish mining attacks called the ZeroBlock [69]. This mechanism can create a low possibility of a profitable selfish mining attack. The main idea of this strategy is to use an interval as the detection strategy, which is the maximum acceptable time for the new received block. If the time for receiving the block is outside of the interval, it will be recorded as a dummy block. Besides, the strategy alleviates the stress from the chain from intentional forks as the consequences of the block withholding. However, it cannot reduce the accidental forks, which comes from the Poisson nature of PoW.

One method proposed by Lee *et al.* involves a two-phase method to prevent block withholding attacks against attacking pools that have infiltrated an honest mining pool [111]. These two phases are infiltration detection and infiltration:

1) *Infiltration detection:* the strategy involves implementing an honest miner into an attacker pool. This infiltration strategy allows the honest miner to work as a sensor that will investigate the activities of the pool, the manager, and the PoW task being distributed. This sensor will be able to leak information to the honest mining pool based on the findings.
2) *Infiltration punishment:* The honest mining pool can react to an attack by adjusting the compensation of the block withholding pool, reducing the profits shared by the attacking pool.

The main feature of this method is to add sensor miners in the detective pool for selfish mining attack detection, then modify the share of block withholding attacker miners to punish them. The advantage of this method is little resource is used by the sensors since they do not need much mining power. However, the proposed method has limitations in

real environments. The drawbacks of this method are discussed in four situations: task without Coinbase transactions, anonymized infiltration miners, attack with private infiltration and misunderstanding as an attack.

The ''truth state'' is another detection method [112]. This strategy is ideally integrated for the fork instant and used to identify selfish mining attacks. Using the height of the block to indicate the position of the latest block implemented in the chain, the truth state creates an expected height of the next transactions to be mined using the expected conformation height, which is appended in the data structure of the transaction. The expected confirmation height for future transactions can be determined by the transaction size, mining fee and size of the memory pool. If the mining fee is large, then transactions are more likely to be prioritized in a block. A large memory pool size creates a transaction backlog. Combining these different factors, the estimated height is created. Transactions that are the value of the truth state will have priority over transactions that have a larger difference between the expected height and the block height. To prevent a selfish mining attack, the honest miner must have a higher truth state than the selfish miner. However, this method has drawbacks when an adaptive attacker includes fewer or no transactions in each block. In this case, the truth state of the selfish miner is higher than the honest miner. In addition, the overhead of appending expected confirmation height is not analyzed or quantified.

Another detection solution allows for backward compatibility. Since the goal of an attacker is to maximize their expected relative revenue, this countermeasure focuses on utilizing the weighted FRP (Fork-Resolving Policy) [113]. The main feature is creating a dilemma that the secret block cannot assist selfish miners in the block races. This method is effective and decentralized. The weighted FRP is as described as follows: 1) Miners mine on the longest chain if it is longer than m blocks. If it does not fit the standard then miners will choose the chain with the largest weight; 2) If multiple chains achieve the largest weight simultaneously, miner chooses at random. However, there are several limitations to this method. First, the assumption is based on a synchronous model with an upper bound of block propagation time. Second, inconsistency can occur among honest miners when fail-safe parameter is larger than 1. Third, no simulation or real-world environment testing is performed. Some factors are ignored, such as natural forks and transaction fees.

E. INFORM

The mathematical analysis of selfish mining explores the various aspects, including network configurations, communication delays, multiple pools, and reward schemes that affect the rewards in the blockchain systems [120].

The concept of adjusting uncle blocks to decrease the probability of selfish mining attack in Ethereum is quantified by Ritz and Zugenmaier [117]. There are three types of block rewards considered in profitability: static block reward, uncle block reward, and nephew block reward [121]. The uncle block is a stale block whose parent is a regular block. A future regular block is also a nephew block if it references the uncle block. The profitability of selfish mining threats on an Ethereum system is analyzed using a mathematical model, i.e., Markov process [106], the results show that the adjusting uncle block can affect the mining profitability. A later study was able to analyze the effect of uncle block using Monte Carlo simulation. The simulation results demonstrate the increased uncle block ratio can lead to lower resilience to selfish mining attack. On the contrary, decreasing the ratio of uncle block can potentially lower the possibility of selfish mining attack. However, this countermeasure was not tested in a simulation or real private blockchain environment.

A mathematical model is proposed to investigate the profit threshold for selfish mining attack in the presence of block propagation delays under a Poisson process for block creation [104]. Using this model, the profit threshold decreases to zero for selfish mining attacker. In comparison, the profit threshold is above 25% under SM1 model for all ranges of communication capability of the attacker. SM1 is the mode proposed by Eyal *et al.* [25]. In this case, selfish mining attackers can easily gain profits. Based on the results, one countermeasure is minimizing the communication delays to increase the profit threshold. This countermeasure gives us insights on the impact of the communication delays. However, this method only considers the delays from the attack to the honest network. No considerations on delays among competing selfish mining pools. In addition, no testing on the real private blockchains is provided for this solution.

Multiple selfish miners can gain profitability more than honest miner if they are strategic miners: 1) with larger than 38% of the total system hash; 2) or with larger than 26.8% of the total system hash rate if they can quickly propagate blocks to other miners [122]. The above results were proved under a simple selfish mining scenario called semi-selfish mining (SSM) where each selfish miner cannot keep a private chain with a length larger than two. A countermeasure associated with inform strategy is a recent research focusing on multiple simultaneous selfish mining attackers [115]. It is the first work to demonstrate that lower possibility attackers can earn through his mining reward if the number of simultaneous attackers increases. Different from the convention model which treats the mining process from one global entity, the proposed model mimics the individual mining process from several different concurrent entities. In addition, this model assumes that each attacker cannot switch between honest mining and selfish mining frequently to maximize the reward. Based on this assumption, the experiment was carried out for 1, 2 and 3 selfish miners. The results show that less miner reward will earn by the attacker in proportion to the number of selfish miners when the number of miners increases from 1 to 3. However, the proposed model fails to consider the network capacity of selfish mining attackers. Besides, the model was only tested on discrete event simulators, not the blockchain simulators.

A deep reinforcement learning based framework called SquirRL, is recently proposed to identify blockchain attack strategies under multiple selfish miners. Specifically, the results demonstrate that selfish mining attack can be mitigated by increasing the number of selfish mining agents. It comes from the fact the selfish mining will steadily become less profitable when the number of agents grows. As shown in Fig. 8, SquirRL framework includes a three-stage pipeline to realize a target incentive mechanism M: 1) build a simulation environment to execute the protocol that builds M; 2) choose an adversarial or attack model to specify the number and types of strategic agents; 3) select a reinforcement learning (RL) algorithm for the environment and adversarial model in previous states. Specifically, Deep Dueling Q-Networks (DDQN) is used for single-agent setting, and Proximal Policy Optimization (PPO) is used for multi-agent setting [123], [124]. This proposed framework applied the state-of-the-art deep learning algorithms to automatically detect the blockchain vulnerabilities. However, the proposed framework does not consider the scenario that multiple partially cooperative agents only share incomplete information. The other drawback is the deep RL algorithm itself is sensitive to hyperparameters, which may cause errors when proving the security of the protocol.

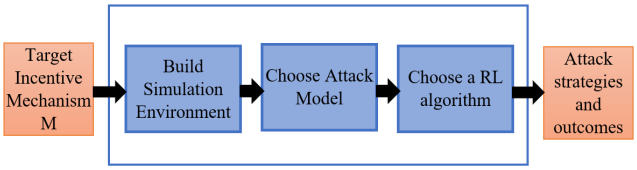

FIGURE 8. Schematic of SquirRL Learning framework [116].

The PPLNS (pay per last N shares) is a new reward scheme that can be used to mitigate the selfish mining attack. The main feature of this reward scheme is temporal share submission activities. It allows the pool reward to be distributed among miners who have submitted their shares in the intervals, not based on the rounds in the mining process [114]. This method makes the selfish mining attack more difficult since naively submitting as many shares as possible may not succeed. The attacker needs to change their attack strategy to mine a faster rate than other pool member and submitting shares in an interval. The advantage of this method is its deployment and compatibility on the cloud systems, keeping lesser impact of selfish mining attacker than traditional proportional reward scheme. This drastically reduces the impact of attackers withholding rewards from miners. However, this method has not been tested on a real-time private blockchain system so that the temporal features of the method can be fully implemented.

The decentralized nature empirical analyst of the distributive features of mining and the capability of mining pool sharing was examined. This states the case that miners can group together on this decentralized system in order to create an attack with a high success rate due to cross-pool mining [125]. Using mining pools to group together to increase the hash rate to more than 50% of the overall computing power of the system a centralized P2P network can be formulated. This affects the ingenuity and structure of blockchain by allowing an attacker to propel coin configurations in the system. To counteract blockchain must impose a significant amount of change in the system where there is a balance between transparency and privacy. This solution presents attackers with a dilemma by when publishing their chain either: block will be made an uncle block or block will be considered late and will not be accepted into an honest mining chain.

F. MONITORING

Liu proposed a new type of selfish mining named BWD (Block Withholding Delay). Compare to the traditional block withholding, instead of dropping valid blocks, BWD delays the submission of blocks to the pool manager [118]. Besides, BWD does not contribute to the pool but only shares the reward of pool members. To combat this attack, a monitoring technique is proposed to track pool members' using a new payoff scheme. This scheme implements an interval type-2 Takagi-Sugeno-Kang fuzzy inference system (IT2-TSK-FIS) which generates fuzzy delay times. This countermeasure increases the risk of revenue loss of attackers by dynamically distributing the reward to pool members. In addition, it implements a pool incentive based on the amount of time that it takes a block to be published in the system. This is a practical method that does not require any adjustment of the current public protocols and is applicable to private mining pools. However, this countermeasure is not tested under simulation or private blockchain environments.

One defense strategy is proposed recently to detect selfish mining attacks by monitoring blockchain fork heights in real time [119]. In order to get the financial reward, selfish miners secretly hold a chain and disclose it until they can get the biggest chain. The experiments are conducted in an NS3 bitcoin simulator [64]. Nodes with hash power ranging from 5% to 30% of the total hash power are selected as possible attack targets. Both selfish mining attack and stalker attack are detected. Stalker attack is a variant of selfish mining attack which aims to withhold blocks or a particular transaction. The results show that: 1) the highest height of fork under Bitcoin network without attack is equal to 1; 2) if the attacker's hash power increases, the average height of the fork grows; 3) if the mean height of the fork is higher than 2, the blockchain system is under selfish mining attack. However, there are several false negatives and false positives when calculating the detection accuracy, caused by honest forks. The future work includes using machine learning to improve the performance of this monitoring method.

VI. SUMMARIZATON OF CURRENT RESEARCH

Based on the above systematic examination of the defense strategies of double-spend attack and selfish mining attack in the current research, a summarization is presented below.

To combat double-spend attacks, methods related to increasing the number of confirmations or increasing the waiting time is the most common approaches employed in our study [74], [75], [79]–[81], [85]. The implementation of this method is easy compared to other methods. The effectiveness of this method also has been demonstrated. Inserting observers in the monitoring type strategy and alert forwarding type strategy are also considered lightweight methods for implementation [24], [80], [91]. Most of the conceptual research design strategies fail to provide experimental testing in simulation or real environments, the effectiveness needs future investigation. Some methods add a lot of computational overhead, such as comparing global and local state hash values [86], and delayed proof of work which adds a notary node network [82]. In addition, some methods concentrating on the indirect way to limit double-spend attack also needs future verification for the effectiveness. They enhance network policy or increase privacy and accountability [29], [83], [87].

To combat against selfish mining attack, several recent proposed approaches are proved with experiment to mitigate selfish mining attack effectively, including weighted FRP (Fork-Resolving Policy) [113], truth state [112] in the detection type method, blockchain fork heights [119] in the monitoring type method, and SquirRL [116] in the inform type method and chain locks [30] in the conceptual research design type method. Some methods bring a lot of computational overhead which limits the possibility of real-world deployment, such as FruitChain [103] introduced a second mining process, counter mining [111] introduced sensor miners, and new payoff scheme [118]. In addition, some other methods using parameters, such as time, to detect selfish mining, including Freshness Preferred [110], ZeroBlock [69], Minimize communication delay [104]. The drawback of these methods is that they still need more future investigation for the computation overhead in in a real private blockchain environment. Overall, it is challenging to present a comprehensive defense strategy can deal with different situations of selfish mining attacks, including: one selfish miner, multiple simultaneous selfish miners, multiple partially cooperated selfish miners, competing selfish mining pools.

VII. THE IMPLICATION OF FUTURE RESEARCH

We have identified a set of primary studies and analyzed the defense strategies to combat both double-spend attack and selfish mining attack in blockchains. Based on our systematic review and observation, we present the following directions of defense strategies for double-spend and selfish mining attacks that are worth future investigation.

A. BLOCKCHAIN PROTOCOL

To mitigate the challenges of blockchain security, several methods that require changes in the blockchain protocols have been proposed by the research and professional communities. These approaches focus on the overall security enhancement of the blockchain protocol, which can mitigate the selfish mining attack and double-spend attack. The changes on blockchain protocol include: 1) adding another chain; 2) two-layer structure. The purpose of the changes is to include a second mining process with a separate consensus mechanism to improve fairness, efficiency, flexibility, and security. Back *et al.* introduced a pegged sidechain attached to the main blockchain to add more functionalities and enhance security [126]. It is a two-way peg that the sidechain and main chain can transfer assets in both ways at a fixed rate or deterministic exchange rate [127]. Pass *et al.* introduced a new block reward scheme by adding another chain called FruitChain to store records [103]. Each fruit in this chain is linked to an earlier block in the original blockchain. However, this method does not require a two-way peg. Goshawk, is a two-layer hybrid chain consisting of keyblocks and microblocks [128]. It also includes a ticket-voting mechanism. However, none of the above research systematically analyze their effectiveness against blockchain attacks. One future research direction is to design an experiment to evaluate the two-chain or two-layer blockchain protocol under double-spend attack and selfish mining attack. In addition, a multi-blockchain system can be introduced in the future. This system allows the mainchain and several sub-chains to exchange data to improve the security in a distributed network. However, some protocol changes may be heavyweight which prevents the deployment. It is a research challenge to deploy a lightweight modification on blockchain protocol with the purpose of addressing security issues.

B. DATA-DRIVEN MODELING AND ARTIFICIAL INTELLIGENCE

Data-driven modeling framework will be one important research direction to not only accurately identify issues in the system but to also adjust its security parameters to be able to remove potential attacks in an effective way. This data-driven method leverages Artificial Intelligence (AI) capabilities, such as machine learning and deep learning, that can ultimately provide the solution to secure the blockchain system. Specifically, machine learning will be able to create statistical models that can perform pattern and inference-based tasks that can enable better detection configurations.

Detection of the selfish mining attack and double-spend attack can be conducted through data analytics using machine learning and deep learning methods. There are some discussions on Blockchain-based IoT (BIoT) applications using machine learning and deep learning for real-time data analytics [129], [130]. Huge volumes of data collected from sensors, smart devices will be stored in a private blockchain after preprocessing steps. The blockchain can ensure all the sensor data stored are with high integrity and cannot be tampered with. Fewer errors will be caused, such as duplication, missing values, noises, etc. In addition, there have been several research using blockchain to protect deep learning by collaborative fairness and privacy-preserving [131], [132]. However, there is limited research on using machine learning or deep learning to secure the blockchain systems. A framework,

called SquirRL, was recently proposed to employ deep learning to mitigate selfish mining attack [116]. This framework is based on Deep Reinforcement Learning (DRL) that can detect attacks on incentive mechanisms besides selfish mining. DRL provides a powerful solution on multi-agent games in a Markov Chain Process to simulate blockchain incentive mechanism. Consider that deep reinforcement learning is sensitive to hyperparameters, investigation on other deep learning approaches are desired. Some popular deep learning approaches have been used in cybersecurity, such as Deep Brief Networks (DBN), Convolution Neural Networks (CNN), Recurrent Neural Networks (RNN), and Generative Adversarial Networks (GAN)[133], [134]. Adopting other deep learning approaches can potentially improve the accuracy of the model by learning different attack vectors to battle against them on blockchain.

Another research direction is adversarial deep learning approaches used in the complex AI systems to secure the blockchain systems. Adversarial machine learning and deep learning have been widely deployed in cybersecurity systems [135], [136]. It generates adversarial examples which are specially crafted noises in the training data sets. They cause deep learning model to make mistakes [137]. In this adversarial environment, we can extend the existing work using deep learning by considering adversarial examples. This approach can identity sophisticated cyber-attacks in blockchain.

C. COMBINED ATTACKS

Combating combined attacks involved with selfish mining and double-spend is an open challenge. These attacks happen when attacker exploits the vulnerabilities in blockchain and carries out multiple attacks successively and cooperatively to achieve the attack goal. The attack goal of the combined attack is to increase the probability of a single attack alone. Several studies investigated the effect of a combination of selfish mining and double-spend with other attacks. Nayak *et al.* proposed stubborn mining, a generalized selfish mining to collaborate with an eclipse attack [23]. Eclipse attack separates the victim with the rest of its peers. Stubborn mining extends the traditional selfish mining by violating the longest chain rule, where attackers can keep mining on the private chain event if the public chain is ahead. This combined attack can significantly expand attacker's mining revenue, comparing to a single selfish mining attack. Bissias *et al.* analyzed the effect of a double-spend attack with a concurrent eclipse attack [138]. The results indicated that it has more advantage for double-spend attack with a combined eclipse attack when the given merchant confirmation requirement z is low. Sapirshtein *et al.* indicated the combination of selfish mining and double-spend can be more profitable than selfish mining alone [104]. This attack involves two simultaneous processes. First, the attacker continuously initiative selfish mining by hiding a conflicting transaction in its private blocks, Second, at some point, the payment is accepted by the payment receiver which causes a double-spend right after the selfish mining attack finishes. Zhang *et al.* proposed a novel attack model that combines double-spend attack and Sybil attack [68]. Double-spend attack leverages the Sybil attack to increase block propagation delay. This increased delay can slow down the growth of the main chain and increase the probability of attacker' chain exceeding the main chain. Thus, it is advantageous for double-spend attacker to achieve his goal. However, none of the research has addressed defensive strategies under the combined attacks. The combined attack brings a more sophisticated attack environment for double-spend attack and selfish mining attack. Hence, there is an ever-increasing need to provide a comprehensive defensive solution.

D. COORDINATED ATTACKS THROUGH MULTI-AGENTS

Coordinated attacks through multiple agents is another future research direction. Multiple fully cooperative agents can share information and conduct more effective attacks to the entire blockchain system. Several research studies have opted to investigate the effect on multiple selfish mining attackers [81], [116], [125]. It is proposed that increasing the competition of multiple pools can make selfish mining profitability more difficult. This study proposed a novel Markov model that yields a closed-form expression of the profitable threshold of two miners, showing the relations between the profitable time range and the mining power of an attacker. This study concluded that selfish mining profitability decreases as the number of attackers in the system increases. The profitable threshold will converge as the length of the private chain increases. However, defense strategies on the coordinated attacks, especially double-spend attacks, remain poorly understood. Hence, a potential research agenda is to modify the existing defensive strategies on one attacker setting to multiple coordinated selfish mining attacks and double-spend attacks.

VIII. CONCLUSION

Blockchain security countermeasure is a relatively new research domain that is experiencing growth in both academic and scientific interest. In this article, we presented a comprehensive review on the countermeasures of both double-spend and selfish mining attacks on a blockchain. We evaluated the pros and cons of these countermeasures based on the proposed taxonomy of defensive strategies: monitoring, alert forwarding, alert broadcasting, inform, detection, and conceptual research design. From the data obtained by the systematic review, we were able to analyze the increasing research trends and the improved research publications of various security methods. Since 2007, we have seen a drastic increase on various research regarding blockchain security in terms of selfish mining and double-spend. Dealing with these two integrity attacks on the blockchain was able to improve the safety of the blockchain in various applications. Due to the current security features of the blockchain network and the advancement of technology, attackers have found new and intuitive ways to discredit blockchain's integrity. The goal of

this research is to understand and learn the various strengths and weaknesses of the different countermeasures and to be able to enhance blockchain to make it a robust network that will benefit the blockchain community.

REFERENCES

[1] M. L. Di Silvestre, P. Gallo, J. M. Guerrero, R. Musca, E. R. Sanseverino, G. Sciumè, J. C. Vásquez, and G. Zizzo, "Blockchain for power systems: Current trends and future applications," *Renew. Sustain. Energy Rev.*, vol. 119, Mar. 2020, Art. no. 109585.

[2] L. Mendiboure, M. A. Chalouf, and F. Krief, "Survey on blockchain-based applications in Internet of Vehicles," *Comput. Electr. Eng.*, vol. 84, Jun. 2020, Art. no. 106646.

[3] C. A. Bai, J. Cordeiro, and J. Sarkis, "Blockchain technology: Business, strategy, the environment, and sustainability," *Bus. Strategy Environ.*, vol. 29, no. 1, pp. 321–322, Jan. 2020.

[4] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Veh. Commun.*, vol. 23, Jun. 2020, Art. no. 100249.

[5] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Comput. Surveys*, vol. 53, no. 2, pp. 1–27, Jul. 2020.

[6] W. Viriyasitavat, L. D. Xu, Z. Bi, and V. Pungpapong, "Blockchain and Internet of Things for modern business process in digital economy—The state of the art," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1420–1432, Dec. 2019.

[7] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surveys*, vol. 53, no. 1, pp. 1–32, May 2020.

[8] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain, "Authentication protocol for cloud databases using blockchain mechanism," *Sensors*, vol. 19, no. 20, p. 4444, Oct. 2019.

[9] B. S. Balaji, P. V. Raja, A. Nayyar, P. Sanjeevikumar, and S. Pandiyan, "Enhancement of security and handling the inconspicuousness in IoT using a simple size extensible blockchain," *Energies*, vol. 13, no. 7, p. 1795, Apr. 2020.

[10] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *Int. J. Res. Eng. Technol.*, vol. 05, no. 9, pp. 1–10, Sep. 2016.

[11] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, 2019.

[12] E. Zaghloul, T. Li, M. Mutka, and J. Ren, "Bitcoin and blockchain: Security and privacy," 2019, *arXiv:1904.11435*. [Online]. Available: http://arxiv.org/abs/1904.11435

[13] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*, vol. 7, pp. 77894–77904, 2019.

[14] L.-H. Zhu, B.-K. Zheng, M. Shen, F. Gao, H.-Y. Li, and K.-X. Shi, "Data security and privacy in bitcoin system: A survey," *J. Comput. Sci. Technol.*, vol. 35, no. 4, pp. 843–862, Jul. 2020.

[15] L. Zhu, B. Zheng, M. Shen, S. Yu, F. Gao, H. Li, K. Shi, and K. Gai, "Research on the security of blockchain data: A survey," 2018, *arXiv:1812.02009*. [Online]. Available: https://arxiv.org/abs/1812.02009

[16] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[17] B. Zheng, L. Zhu, M. Shen, X. Du, and M. Guizani, "Identifying the vulnerabilities of bitcoin anonymous mechanism based on address clustering," *Sci. China Inf. Sci.*, vol. 63, no. 3, pp. 1–15, Mar. 2020.

[18] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol with chains of variable difficulty," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2017, pp. 291–323.

[19] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin P2P network," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2014, pp. 15–29.

[20] S. Wu, Y. Chen, M. Li, X. Luo, Z. Liu, and L. Liu, "Survive and thrive: A stochastic game for DDoS attacks in bitcoin mining pools," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 874–887, Apr. 2020.

[21] M. Mirkin, Y. Ji, J. Pang, A. Klages-Mundt, I. Eyal, and A. Juels, "BDoS: Blockchain denial-of-service," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2020, pp. 601–619.

[22] B. Alangot, D. Reijsbergen, S. Venugopalan, and P. Szalachowski, "Decentralized lightweight detection of eclipse attacks on bitcoin clients," 2020, *arXiv:2007.02287*. [Online]. Available: http://arxiv.org/abs/2007.02287

[23] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS P)*, Mar. 2016, pp. 305–320.

[24] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, 2012, pp. 906–917.

[25] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2014, pp. 436–454.

[26] N. T. Courtois and L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency," 2014, *arXiv:1402.1718*. [Online]. Available: http://arxiv.org/abs/1402.1718

[27] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 195–209.

[28] X. Dong, F. Wu, A. Faree, D. Guo, Y. Shen, and J. Ma, "Selfholding: A combined attack model using selfish mining with block withholding attack," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101584.

[29] J. Jang and H.-N. Lee, "Profitable double-spending attacks," 2019, *arXiv:1903.01711*. [Online]. Available: http://arxiv.org/abs/1903.01711

[30] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, p. 1788, Apr. 2019.

[31] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the instability of bitcoin without the block reward," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 154–167.

[32] Z. Liu, G. Yang, X. Yu, and F. Li, "A security detection model for selfish mining attack," in *Proc. Int. Conf. Blockchain Trustworthy Syst.* Singapore: Springer, 2019, pp. 185–195.

[33] Y. Wang and A. Kogan, "Designing confidentiality-preserving blockchain-based transaction processing systems," *Int. J. Accounting Inf. Syst.*, vol. 30, pp. 1–18, Sep. 2018.

[34] M. H. Miraz and D. C. Donald, "Application of blockchain in booking and registration systems of securities exchanges," in *Proc. Int. Conf. Comput., Electron. Commun. Eng. (iCCECE)*, Aug. 2018, pp. 35–40.

[35] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184–192, Nov. 2018.

[36] L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on blockchain," *Future Gener. Comput. Syst.*, vol. 93, pp. 327–337, Apr. 2019.

[37] L. Xu, L. Chen, Z. Gao, L. Carranco, X. Fan, N. Shah, N. Diallo, and W. Shi, "Supporting blockchain-based cryptocurrency mobile payment with smart devices," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 26–33, Mar. 2020.

[38] H. Min, "Blockchain technology for enhancing supply chain resilience," *Bus. Horizons*, vol. 62, no. 1, pp. 35–45, Jan. 2019.

[39] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019.

[40] S. F. Wamba, J. R. K. Kamdjoug, R. E. Bawack, and J. G. Keogh, "Bitcoin, blockchain and fintech: A systematic review and case studies in the supply chain," *Prod. Planning Control*, vol. 31, nos. 2–3, pp. 115–142, Feb. 2020.

[41] M. Hölbl, M. Kompara, A. Kamišalic, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018.

[42] T. McGhin, K.-K.-R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019.

[43] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[44] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[45] D. Pavithran, K. Shaalan, J. N. Al-Karaki, and A. Gawanmeh, "Towards building a blockchain framework for IoT," *Cluster Comput.*, vol. 23, pp. 2089–2103, Feb. 2020, doi: 10.1007/s10586-020-03059-5.

[46] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[47] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain technology toward green IoT: Opportunities and challenges," *IEEE Netw.*, vol. 34, no. 4, pp. 263–269, Jul. 2020.

[48] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, p. 533, 2016.

[49] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet Things*, vol. 10, Jun. 2020, Art. no. 100081.

[50] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[51] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019.

[52] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.

[53] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2020.

[54] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[55] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020.

[56] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, 2018.

[57] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020.

[58] Y. Zacchia Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: An automatic control perspective," *J. Syst. Softw.*, vol. 149, pp. 174–216, Mar. 2019.

[59] A. Ashraf, B. Byholm, and I. Porres, "Distributed virtual machine consolidation: A systematic mapping study," *Comput. Sci. Rev.*, vol. 28, pp. 118–130, May 2018.

[60] A. Ben Ayed, "A conceptual secure blockchain based electronic voting system," *Int. J. Netw. Secur. Its Appl.*, vol. 9, no. 3, pp. 1–9, May 2017.

[61] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," 2019, *arXiv:1906.11078*. [Online]. Available: http://arxiv.org/abs/1906.11078

[62] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[63] A. Ellervee, R. Matulevicius, and N. Mayer, "A comprehensive reference model for blockchain-based distributed ledger technology," in *Proc. ER Forum/Demos*, 2017, pp. 306–319.

[64] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 3–16.

[65] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2017, pp. 357–388.

[66] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," 2020, *arXiv:2001.07091*. [Online]. Available: http://arxiv.org/abs/2001.07091

[67] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, Jan. 2018.

[68] S. Zhang and J.-H. Lee, "Double-spending with a Sybil attack in the Bitcoin decentralized network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5715–5722, Oct. 2019.

[69] S. Solat and M. Potop-Butucaru, "ZeroBlock: Timestamp-free prevention of block-withholding attack in bitcoin," 2016, *arXiv:1605.02435*. [Online]. Available: http://arxiv.org/abs/1605.02435

[70] K. A. Negy, P. Rizun, and E. G. Sirer, "Selfish mining re-examined," in *Proc. 24th Int. Conf. Financial Cryptogr. Data Secur.*, Kota Kinabalu, Malaysia, Feb. 2020, pp. 61–78. [Online]. Available: https://fc20.ifca.ai/

[71] K. Nicolas, Y. Wang, and G. C. Giakos, "Comprehensive overview of selfish mining and double spending attack countermeasures," in *Proc. IEEE 40th Sarnoff Symp.*, Sep. 2019, pp. 1–6.

[72] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Newbury Park, CA, USA: Sage, 2017.

[73] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. 12th Int. Conf. Eval. Assessment Softw. Eng. (EASE)*, Jun. 2008, pp. 1–10.

[74] C. Pérez-Solà, S. Delgado-Segura, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Double-spending prevention for bitcoin zero-confirmation transactions," *Int. J. Inf. Secur.*, vol. 18, no. 4, pp. 451–463, Aug. 2019.

[75] M. Rosenfeld, "Analysis of hashrate-based double spending," 2014, *arXiv:1402.2009*. [Online]. Available: http://arxiv.org/abs/1402.2009

[76] M. Grundmann, T. Neudecker, and H. Hartenstein, "Exploiting transaction accumulation and double spends for topology inference in bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2018, pp. 113–126.

[77] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, pp. 1–32, Jun. 2015.

[78] C. Grunspan and R. Pérez-Marco, "Double spend races," 2017, *arXiv:1702.02867*. [Online]. Available: http://arxiv.org/abs/1702.02867

[79] P. Ekparinya, V. Gramoli, and G. Jourjon, "Double-spending risk quantification in private, consortium and public ethereum blockchains," 2018, *arXiv:1805.05004*. [Online]. Available: http://arxiv.org/abs/1805.05004

[80] N. Rathod and D. Motwani, "Security threats on Blockchain and its countermeasures," *Int. Res. J. Eng. Technol*, vol. 5, no. 11, pp. 1636–1642, 2018.

[81] Y. Sompolinsky and A. Zohar, "Bitcoin's security model revisited," 2016, *arXiv:1605.09193*. [Online]. Available: http://arxiv.org/abs/1605.09193

[82] Komodo. *Security: Delayed Proof of Network (dPoW)*. Accessed: Feb. 2019. [Online]. Available: https://komodoplatform.com/security-delayed-proof-of-work-dpow/

[83] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[84] I. Osipkov, E. Y. Vasserman, N. Hopper, and Y. Kim, "Combating double-spending using cooperative P2P systems," in *Proc. 27th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2007, p. 41.

[85] G. Ramezan, C. Leung, and Z. J. Wang, "A strong adaptive, strategic double-spending attack on blockchains," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1219–1227.

[86] Z. Peng and Y. Chen, "All roads lead to Rome: Many ways to double spend your cryptocurrency," 2018, *arXiv:1811.06751*. [Online]. Available: http://arxiv.org/abs/1811.06751

[87] U. W. Chohan. (Dec. 19, 2017). *The Double Spending Problem and Cryptocurrencies*. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3090174

[88] K. Liao and J. Katz, "Incentivizing double-spend collusion in bitcoin," in *Proc. Financial Cryptogr. Bitcoin Workshop*, 2017, pp. 1–16.

[89] A. P. Ozisik and B. N. Levine, "An explanation of Nakamoto's analysis of double-spend attacks," 2017, *arXiv:1701.03977*. [Online]. Available: http://arxiv.org/abs/1701.03977

[90] G. Karame, E. Androulaki, and S. Capkun, "Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin," *IACR Cryptol. ePrint Arch.*, vol. 2012, no. 248, pp. 1–17, 2012.

[91] J. P. Podolanko, J. Ming, and M. Wright, "Countering double-spend attacks on bitcoin fast-pay transactions," in *Proc. Workshop Technol. Consum. Protection*, 2017, pp. 1–3.

[92] C. Pinzón and C. Rocha, "Double-spend attack models with time advantange for bitcoin," *Electron. Notes Theor. Comput. Sci.*, vol. 329, pp. 79–103, Dec. 2016.

[93] S. Nakamoto and A. Bitcoin. (2008). *A Peer-to-Peer Electronic Cash System*. Bitcoin. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[94] R. R. Vokerla, B. Shanmugam, S. Azam, A. Karim, F. D. Boer, M. Jonkman, and F. Faisal, "An overview of blockchain applications and attacks," in *Proc. Int. Conf. Vis. Towards Emerg. Trends Commun. Netw. (ViTECoN)*, Mar. 2019, pp. 1–6.

[95] J. Joshi and R. Mathew, "A survey on attacks of bitcoin," in *Proc. Int. Conf. Comput. Netw., Big Data IoT*. Cham, Switzerland: Springer, 2018, pp. 953–959.

[96] E. Duffield and K. Hagan, "Darkcoin: Peertopeer cryptocurrency with anonymous blockchain transactions and an improved proofofwork system," BitPaper Inf., 2014. Accessed: Jun. 2020. [Online]. Available: http://cryptochainuni.com/wp-content/uploads/Darkcoin-Whitepaper.pdf
[97] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 104–121.
[98] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A sybil-resistant scalable blockchain," *Future Gener. Comput. Syst.*, vol. 107, pp. 770–780, Jun. 2020.
[99] P. Swathi, C. Modi, and D. Patel, "Preventing Sybil attack in blockchain using distributed behavior monitoring of miners," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–6.
[100] H. Wang, K. Chen, and D. Xu, "A maturity model for blockchain adoption," *Financial Innov.*, vol. 2, no. 1, p. 12, Dec. 2016.
[101] R. Zhang and B. Preneel, "Broadcasting intermediate blocks as a defense mechanism against selfish-mine in bitcoin," *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 518, 2015.
[102] K. Nærland, C. Müller-Bloch, R. Beck, and S. Palmund, "Blockchain to rule the waves-nascent design principles for reducing risk and uncertainty in decentralized environments," in *Proc. ICIS*, 2017, pp. 1–16.
[103] R. Pass and E. Shi, "Fruitchains: A fair blockchain," in *Proc. ACM Symp. Princ. Distrib. Comput.*, 2017, pp. 315–324.
[104] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2016, pp. 515–532.
[105] C. Grunspan and R. Pérez-Marco, "Selfish mining and Dyck words in Bitcoin and Ethereum networks," 2019, *arXiv:1904.07675*. [Online]. Available: http://arxiv.org/abs/1904.07675
[106] C. Grunspan and R. Pérez-Marco, "On profitability of selfish mining," 2018, *arXiv:1805.08281*. [Online]. Available: http://arxiv.org/abs/1805.08281
[107] S. Lee and S. Kim, "Pooled mining makes selfish mining tricky," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 1230, Dec. 2018.
[108] I. Eyal, "The Miner's dilemma," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 89–103.
[109] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011, *arXiv:1112.4980*. [Online]. Available: http://arxiv.org/abs/1112.4980
[110] E. Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2014, pp. 161–162.
[111] S. Lee and S. Kim, "Countering block withholding attack efficiently," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 330–335.
[112] M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen, "Countering selfish mining in blockchains," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 360–364.
[113] R. Zhang and B. Preneel, "Publish or perish: A backward-compatible defense against selfish mining in bitcoin," in *Proc. Cryptographers' Track RSA Conf.* Cham, Switzerland: Springer, 2017, pp. 277–292.
[114] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 458–467.
[115] T. Leelavimolsilp, L. Tran-Thanh, and S. Stein, "On the preliminary investigation of selfish mining strategy with multiple selfish miners," 2018, *arXiv:1802.02218*. [Online]. Available: http://arxiv.org/abs/1802.02218
[116] C. Hou, M. Zhou, Y. Ji, P. Daian, F. Tramer, G. Fanti, and A. Juels, "SquirRL: Automating attack analysis on blockchain incentive mechanisms with deep reinforcement learning," 2019, *arXiv:1912.01798*. [Online]. Available: http://arxiv.org/abs/1912.01798
[117] F. Ritz and A. Zugenmaier, "The impact of uncle rewards on selfish mining in Ethereum," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS PW)*, Apr. 2018, pp. 50–57.
[118] L. Liu, W. Chen, L. Zhang, J. Liu, and J. Qin, "A type of block withholding delay attack and the countermeasure based on type-2 fuzzy inference," *Math. Biosci. Eng.*, vol. 17, no. 1, pp. 309–327, 2020.
[119] V. Chicarino, C. Albuquerque, E. Jesus, and A. Rocha, "On the detection of selfish mining and stalker attacks in blockchain networks," *Ann. Telecommun.*, vol. 75, pp. 143–152, 2020, doi: 10.1007/s12243-019-00746-2.
[120] C. S. Wright. (Jul. 17, 2017). *The Fallacy of Selfish Mining in Bitcoin: A Mathematical Critique*. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3004026
[121] J. Niu and C. Feng, "Selfish mining in ethereum," 2019, *arXiv:1901.04620*. [Online]. Available: http://arxiv.org/abs/1901.04620
[122] F. J. Marmolejo-Cossío, E. Brigham, B. Sela, and J. Katz, "Competing (semi-)selfish miners in bitcoin," in *Proc. 1st ACM Conf. Adv. Financial Technol.*, Oct. 2019, pp. 89–109.
[123] H. Van Hasselt, A. Guez, and D. Silver, "Deep reinforcement learning with double Q-learning," in *Proc. 13th AAAI Conf. Artif. Intell.*, 2016, pp. 1–13.
[124] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, "Proximal policy optimization algorithms," 2017, *arXiv:1707.06347*. [Online]. Available: http://arxiv.org/abs/1707.06347
[125] Q. Bai, X. Zhou, X. Wang, Y. Xu, X. Wang, and Q. Kong, "A deep dive into blockchain selfish mining," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.
[126] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. (2014). *Enabling Blockchain Innovations With Pegged Sidechains*. [Online]. Available: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains
[127] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102471.
[128] C. Wan, S. Tang, Y. Zhang, C. Pan, Z. Liu, Y. Long, Z. Liu, and Y. Yu, "Goshawk: A novel efficient, robust and flexible blockchain protocol," in *Proc. Int. Conf. Inf. Secur. Cryptol.* Cham, Switzerland: Springer, 2018, pp. 49–69.
[129] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W.-C. Hong, "Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward," *IEEE Access*, vol. 8, pp. 474–488, 2020.
[130] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.
[131] A. Goel, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha, "DeepRing: Protecting deep neural network with blockchain," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CFPRW)*, Long Beach, CA, USA, Jun. 2019, pp. 2821–2828.
[132] L. Lyu, J. Yu, K. Nandakumar, Y. Li, X. Ma, J. Jin, H. Yu, and K. S. Ng, "Towards fair and privacy-preserving federated deep models," 2019, *arXiv:1906.01167*. [Online]. Available: http://arxiv.org/abs/1906.01167
[133] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.
[134] D. Berman, A. Buczak, J. Chavis, and C. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, p. 122, Apr. 2019.
[135] V. Duddu, "A survey of adversarial machine learning in cyber warfare," *Defence Sci. J.*, vol. 68, no. 4, p. 356, Jun. 2018.
[136] X. Yuan, P. He, Q. Zhu, and X. Li, "Adversarial examples: Attacks and defenses for deep learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 9, pp. 2805–2824, Sep. 2019.
[137] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," 2019, *arXiv:1906.05799*. [Online]. Available: http://arxiv.org/abs/1906.05799
[138] G. Bissias, B. N. Levine, A. P. Ozisik, and G. Andresen, "An analysis of attacks on blockchain consensus," 2016, *arXiv:1610.07985*. [Online]. Available: http://arxiv.org/abs/1610.07985

KERVINS NICOLAS (Student Member, IEEE) received the B.S. degree in computer engineering in 2018 and the M.S. degree in computer engineering from the Manhattan College, Bronx, NY, USA, in 2019. From 2018 to 2019, he was a Research Assistant with the Manhattan College. Since 2020, he has been a Systems Engineer with IBM. His research interests include the security aspects of blockchain and the latest new development to defend against vulnerabilities on the system by developing integrated techniques used to mitigate the effects of double spending and selfish mining attacks. He was a recipient of the Association des Ingénieurs Haïtiens et Américains Award, the Triple C Award, and the IEEE UEMCON Best Paper/Presentation Award in 2017.

YI WANG (Member, IEEE) received the B.S. degree in information management and information system and the M.S. degree in computer science from the Wuhan University of Science and Technology, Wuhan, China, in 2006 and 2009, respectively, and the Ph.D. degree in computer engineering from The University of Alabama in Huntsville, Huntsville, AL, in 2015. After the Ph.D. degree, he joined the Department of Electrical and Computer Engineering, Manhattan College, Riverdale, NY, as an Assistant Professor. His main research interests include image processing, artificial intelligence, cyber security, and blockchain systems.

GEORGE C. GIAKOS (Fellow, IEEE) is currently a Professor and the Chair of the Department of Electrical and Computer Engineering, Manhattan College, NY. His Doctoral Dissertation was on the "Detection of Longitudinal EM Waves in Open Media." His research interest includes technology innovation, through the integration of physics, engineering, and augmented intelligence. He is also the Founding Director of the Laboratory for Quantum Cognitive Systems and Bioinspired Engineering. He has more than 20 U.S. and foreign patents, and 350 peer-review articles. He got extensive training in the design of innovative bioinspired electrooptical imaging sensor systems; by serving as a Contractor at NASA, U.S. Airforce Laboratories (AFRL), and the Office of Naval Research. He was a recipient of the Fulbright Award to India, granted by the U.S. Department of State, 2019–2020. He has been recognized for his leadership efforts in advancing the professional goals of IEEE by receiving the 2014 IEEE-USA Professional Achievement Award in recognition of his efforts in strengthening links between industry, government, and academia. He was also a recipient of the ONR Distinguished Faculty Fellow Award, summer 2004. His team is the first to explore polarimetric imaging using near infrared (NIR) for label-free lung cancer detection. His team pioneered the characterization of CZT semiconductors for flat panel radiography. He promoted collaborations with U.S. Air Force, the Office of Naval Research, DOD, NASA, the National Academy of Sciences, Lockheed Martin, Philips, Cleveland Clinic, and Varian Medical Systems. He serves as the Founding Chairman for IEEE TC19 Imaging Systems and IEEE International Conference on Imaging Systems and Techniques, the Founding Director for IEEE International School on Imaging and IEEE Industry-Academia Forum, and the Co-Chair for IEEE TC16 Materials and Measurements.

BINGYANG WEI received the B.S. degree in computer science from the Ocean University of China, in 2010, and the Ph.D. degree in computer science from The University of Alabama in Huntsville, in 2015. He has worked as an Assistant Professor with the Department of Computer Science, Midwestern State University, from 2015 to 2018. He then joined the Department of Computer Science, Texas Christian University, in 2018, as an Assistant Professor. His main research interests include software engineering and knowledge graphs.

HONGDA SHEN received the M.Sc. degree in electrical engineering from Western Carolina University, Cullowhee, NC, USA, in 2013, and the Ph.D. degree in electrical engineering from The University of Alabama in Huntsville, Huntsville, AL, USA, in 2016. He was a Behavioral Data Scientist at Johnson and Johnson Health and Wellness Solutions and a Senior Data Scientist at Bank of America. He has published more than 20 papers in top-tier conference proceedings and journals. His research interests include computer vision, machine learning, and their applications in finance and healthcare.