future internet

MDPI

Article

Enable Fair Proof-of-Work (PoW) Consensus for Blockchains in IoT by Miner Twins (MinT)

Qian Qu [1], Ronghua Xu [1], Yu Chen [1,*], Erik Blasch [2] and Alexander Aved [2]

[1] Department of Electrical and Computer Engineering, Binghamton University, Binghamton, NY 13902, USA; qqu2@binghamton.edu (Q.Q.); rxu22@binghamton.edu (R.X.)
[2] The U.S. Air Force Research Laboratory, Rome, NY 13441, USA; erik.blasch.1@us.af.mil (E.B.); alexander.aved@us.af.mil (A.A.)
* Correspondence: ychen@binghamton.edu

Abstract: Blockchain technology has been recognized as a promising solution to enhance the security and privacy of Internet of Things (IoT) and Edge Computing scenarios. Taking advantage of the Proof-of-Work (PoW) consensus protocol, which solves a computation intensive hashing puzzle, Blockchain ensures the security of the system by establishing a digital ledger. However, the computation intensive PoW favors members possessing more computing power. In the IoT paradigm, fairness in the highly heterogeneous network edge environments must consider devices with various constraints on computation power. Inspired by the advanced features of Digital Twins (DT), an emerging concept that mirrors the lifespan and operational characteristics of physical objects, we propose a novel Miner Twins (MinT) architecture to enable a fair PoW consensus mechanism for blockchains in IoT environments. MinT adopts an edge-fog-cloud hierarchy. All physical miners of the blockchain are deployed as microservices on distributed edge devices, while fog/cloud servers maintain digital twins that periodically update miners' running status. By timely monitoring of a miner's footprint that is mirrored by twins, a lightweight Singular Spectrum Analysis (SSA)-based detection achieves the identification of individual misbehaved miners that violate fair mining. Moreover, we also design a novel Proof-of-Behavior (PoB) consensus algorithm to detect dishonest miners that collude to control a fair mining network. A preliminary study is conducted on a proof-of-concept prototype implementation, and experimental evaluation shows the feasibility and effectiveness of the proposed MinT scheme under a distributed byzantine network environment.

Keywords: digital twin; blockchain; Proof-of-Work; microservices; Singular Spectrum Analysis (SSA); byzantine fault tolerance

Citation: Qu, Q.; Xu, R.; Chen, Y.; Blasch, E.; Aved, A. Enable Fair Proof-of-Work (PoW) Consensus for Blockchains in IoT by Miner Twins (MinT). *Future Internet* **2021**, *13*, 291. https://doi.org/10.3390/fi13110291

Academic Editor: Christoph Stach

Received: 30 October 2021
Accepted: 16 November 2021
Published: 19 November 2021

1. Introduction

Advancement in Internet of Things (IoT), Edge Computing, Big Data (BD), and Artificial Intelligence (AI)/Machine Learning (ML) technologies makes the concept of Smart Cities realistic. However, widely adopting IoT-based applications and services in smart cities also brings new security and privacy concerns. Thanks to multiple attractive features including decentralization, auditability and traceability, blockchain has been widely recognized as a great potential to revolutionize the fundamentals of information and communication technology (ICT) [1]. Applying blockchain to smart cities is promising to bring efficiency, scalability and security properties to IoT-based applications, such as smart surveillance [2], privacy preservation [3], decentralized data marketplaces [4], time banking of community [5], identity authentication [6] and access control [7,8].

Digital Twins (DT) is being developed to optimize manufacturing and aviation processes [9]. By monitoring, simulating and mirroring the status of a physical object (PO), DT can build an intelligent and evolving system model based on the logic object (LO). Leveraging data fusion and AI/ML algorithms, DT can be used to predict the behavior of the PO given some specific situations or environments. Similar to DT, the Dynamic Data

Driven Applications Systems (DDDAS) concept developed in the late 1990s seeks to use modeling to support predictive expectations based on the coordination with models and data [10]. Thus, DDDAS can determine optimized solutions or even failure preventive actions on POs to enable an intelligent and resilient system.

Research has been conducted to apply blockchain to enable many attractive features in DTs, including transparency, decentralization, data immutability and Peer-to-Peer (P2P) communication [11]. However, directly integrating existing blockchain technologies into the highly heterogeneous IoT environments presents critical challenges in terms of scalability, performance, security and fairness [12]. Some permissioned blockchains use a Practical Byzantine Fault Tolerance (PBFT) [13] protocol, which demonstrates high throughput and low latency but only allows for a very limited network scalability in terms of the number of validators. Most permissionless blockchain networks utilize a hashing-intensive Proof-of-Work (PoW) consensus protocol to achieve security and scalability guarantees. Due to the various computation capability of miners, mining centralization in a PoW blockchain not only leads to inequity of rewarding among participants but also brings about security issues, such as majority (51%) attacks [14].

Inspired by the essential features of DTs, mirroring and monitoring, this paper proposes a novel edge-fog-cloud Miner Twins (MinT) architecture to enable a fair PoW consensus mechanism for blockchains in IoT environments. In the MinT architecture, the fog/cloud sever establishes and maintains digital twins for the miners of the blockchain, which are deployed as microservices in edge devices that participate in the blockchain network. Container technology is adopted to encapsulate PoW algorithm as microservices, and each containerized miner is dedicated to mining tasks using pre-configured computation power. As each miner has the same constrained computation resources, it becomes affordable to optimize resource limited IoT devices.

In summary, this paper makes the following contributions:

(1) A secure-by-design MinT architecture is introduced to allow for fair-mining-as-a-service (FMaaS) in heterogeneous IoT environments;
(2) We propose a novel miner twin-enabled fair-mining mechanism, which can monitor the computing resources usage at miners and can regularly apply anomaly detection to deter misbehaved nodes from unfairly overwhelming honest peers using extra computing power;
(3) A lightweight SSA Singular Spectrum Analysis (SSA)-based detection is designed to identify individual misbehaved miners that violate fair mining policies, while a Proof-of-Behavior consensus algorithm is designed to detect multiple Byzantine miners that collude to compromise a fair mining network; and
(4) A proof-of-concept prototype is implemented and tested on a small-scale private PoW mining network, and experimental results verified that the MinT is feasible and effective to ensure a fair mining system.

The remainder of this paper is organized as follows: Section 2 reviews the background on blockchain and PoW consensus and then briefly discusses the state-of-the-art research on DT. Section 3 introduces the rationale and architecture of MinT. The miner twin-enabled fair-mining mechanism including SSA and PoB-based detection algorithms is explained in Section 4.1. Section 5 presents the prototype implementation with numerical results. Section 6 concludes the paper with future work.

2. Related Work

This section introduces blockchain and PoW consensus background knowledge. Following that, we describe digital twin technology and how DT can be used to guarantee the fair mining scheme in blockchain.

2.1. Blockchain and Nakamoto Consensus Protocol

As a form of distributed ledger technology (DLT), *Blockchain* was initially implemented as an enabling technology of Bitcoin [15], which aimed to provide a cryptocurrency to

record and verify commercial transactions among trustless entities in a decentralized manner. With the decentralized P2P network architecture and cryptographic mechanisms, participants in a blockchain system maintain the immutability and auditability of data and transactions recorded on the distributed ledger instead of relying on a centralized third party trust authority.

As one of the most fundamental problems in a distributed/decentralized computing environment, *consensus* in a blockchain network can be defined as a fault-tolerant state-machine replication problem, which aims to maintain the globally distributed ledger state across the P2P network. Bitcoin adopts the Nakamoto consensus based on a Proof-of-Work (PoW) scheme to achieve pseudonymity, scalability and probabilistic finality in an asynchronous and open-access network environment. The goal of Nakamoto consensus is to ensure all participants agree on a common network transaction log as a serialized blockchain [12].

PoW is essentially an incentive-based consensus algorithm, which requires all participants to compete for rewards through a cryptographic block discovery racing game. To be a winner in PoW block generation, every miner has to solve a computing-intensive hash puzzle problem. In brief, a valid PoW solution requires exhaustively querying a cryptographic hash function for a partial preimage generated from a candidate block [16]. Finally, the hash code of a candidate block must satisfy a predefined difficulty condition parameter h, such as having a fixed length of bits as zeros.

Given current *block_data*, which consists of a block header and ordered transactions by time stamps, a miner continually calculates a hash value *nonce* until it satisfies the PoW puzzle problem. The PoW puzzle problem can be formally defined as follows:

$$hash\_block = \mathcal{H}(block\_data|nonce) \leqslant D(h), \tag{1}$$

where for some fixed length of bits L and difficulty condition, $D(h) = 2^{L-h}$. $\mathcal{H}(\cdot)$ is a predefined collision-resistant cryptographic hash function that outputs a hash string $L \in \{0,1\}^{\lambda}$, and λ is the length of a hash string.

The PoW process defined by Equation (1) is essentially a verifiable process of a weighted random coin-tossing [12]. Thus, the probability of generating a valid block is in proportion to miners' computation resources. Higher computation power leads to higher hash string rate in PoW, which means more rewards and benefits. Such a mining centralization may discourage participants who have limited computation resources, such as IoT devices; but it also lead to majority (51%) attacks if an adversary controls more than 50% of the computation resources of the whole network.

To reduce energy consumption in PoW consensus, Peercoin [17] proposed Proof-of-Stake (PoS), which requires a miner to use its coin stake to solve the puzzle solution. Unlike PoW protocols that relies on a brute-force hash calculation, PoS miners use a process of "virtual mining" manner that only consumes limited computational resources. However, PoS still has a mining centralization issue because an attacker can amplify its power by simply accumulating the credit stake. As the first practical Byzantine Fault Tolerant (BFT) consensus, Practical BFT (PBFT) [13] guarantees both liveness and safety in synchronous network environments given the assumption that at most of $\lfloor \frac{n-1}{3} \rfloor$ out of total of n participants in consensus protocol are Byzantine faults. As PBFT requires that all nodes communicate synchronously to achieve consensus purposes, it has poor scalability due to high latency and communication overhead as more nodes join the consensus network.

2.2. Digital Twins

The concept of DT was proposed in 2002 and archived in a NASA white paper in 2014 [18]. Essentially, a DT is a digital representation of the components and dynamics of a physical system [19]. Based on the functionalities, DTs can be roughly categorized into three kinds: monitoring DTs, simulational DTs and operational DTs [20]. As suggested by the names, monitoring twins allow system operators to monitor the status of a physical system; simulation twins can predict the future status of the physical system in different

scenarios using various simulation tools and ML algorithms; and operational twins is a *complex sensing and control system* that enabled human operators to interact with a cyber-physical system and to perform different actions in addition to monitoring, analysis and prediction [21], which is similar to human–machine teaming [22].

Earlier studies on DT mainly focused on the area of manufacturing covering different key factors for smart manufacturing including simulation, optimization and the use of AI. For instance, an event-driven simulation for manufacturing and assembly tasks based on Digital Twin and human–robot collaboration was presented [23]. A DT-based framework was proposed to achieve high precision and multidisciplinary coupling during the assembly process, which mainly focused on High precision products (HPPs) workshops [24]. HPP also establishes a predict and optimization model as well as a case study to verify the effectiveness and feasibility. A case study presented an ice cream machine as an application example of DT in food industry [25], which focused on the visualization and interaction based on virtual reality (VR) and augmented reality (AR) technologies. Secure data transmission was also highlighted in the framework by employing a secure gate between machine and cloud.

Recently, efforts are reported in variant aspects of smart cities including Smart Driving, Smart Grid and Smart Healthcare. For instance, the optimization issue in the electric propulsion drive systems (EPDS) of self-driving electric vehicles were discussed [26]. In the proposed DT-based framework, the connection between a logical twin in the control software with the propulsion motor drive system enables EPDS performance estimation. However, there were no experimental results presented after giving the concepts of the platform. A behaviors-based algorithm was proposed to help the drivers avoid potential risk [27]. Combining the ML techniques and DT relies on the connectivity of the system and faces challenges in optimization and accuracy [28]. A case study has been reported that tackles the management of wind farm using DT and cloud technologies combined with big data analysis to build remote control station [29].

Recently, some healthcare applications redefined DT by including living objects [30]. A DT-based healthcare framework was proposed for monitoring and predicting the health condition of an individual using wearable devices [31]. A DT-based remote surgery prototype was introduced consisting of VR, 4G and AI to create a digital twin of a patient and to realize real-time surgery over mobile network [32]. Due to the fast development of telecommunication technologies, 5G and beyond networks are very complicated as they are expected to support more emerging applications with more diverse requirements [33]. The community is considering DT as an efficient, cost-effective approach to accelerate the design, test and implementation of 5G/6G networks [34].

Due to the foreseeable importance and popularity of DT in IoT, 5G/6G and edge computing, blockchain is adopted to enhance the security, trust and reliability of DTs [11,35]. The work reported in this paper, however, is the first in this area that leverages DT to tackle the unfair mining problem in the PoW consensus protocol. Using digital twins, MinT monitors the computing resource utility of the miners and quickly detects abusers using Singular Spectrum Analysis (SSA) [36], one of the fastest change point detection algorithms [37]. Our MinT also uses a Proof-of-Behavior (PoB) consensus algorithm to guarantee byzantine tolerant anomaly detection.

3. MinT: Rationale and Architecture

Aiming at a secure-by-design fair PoW mining network in heterogeneous IoT environments, our MinT scheme leverages DT technology to continuously monitor the usage of containerized miners and discourages misbehaving nodes from unfairly overwhelming the peers by using extra computing power. Figure 1 illustrates the high-level system architecture of MinT, which adopts a hierarchical cloud-fog-edge computing paradigm. Such a hierarchical framework not only provides system scalability for large-scale fair mining tasks based on geographically distributed IoT devices but also supports flexible management and coordinated central and decentralized local decisions given heterogeneous networks

and application domains. Moreover, MinT relies on a permissioned network that provides basic security guarantees, such as the public key infrastructure (PKI) and digital signature, data integrity [2], identity authentication [6] and access control [38], etc. In essential, MinT is a partial decentralized PoW mining network. Furthermore, DTs in MinT are mainly used to monitor their associated miners and to support misbehavior detection, and they do not directly participate in the PoW mining task or impose interference on the consensus protocol. Therefore, our Mint is promising in enabling a fair mining network without sacrificing distribution and decentralization. The rationale behind the MinT is described as follows:

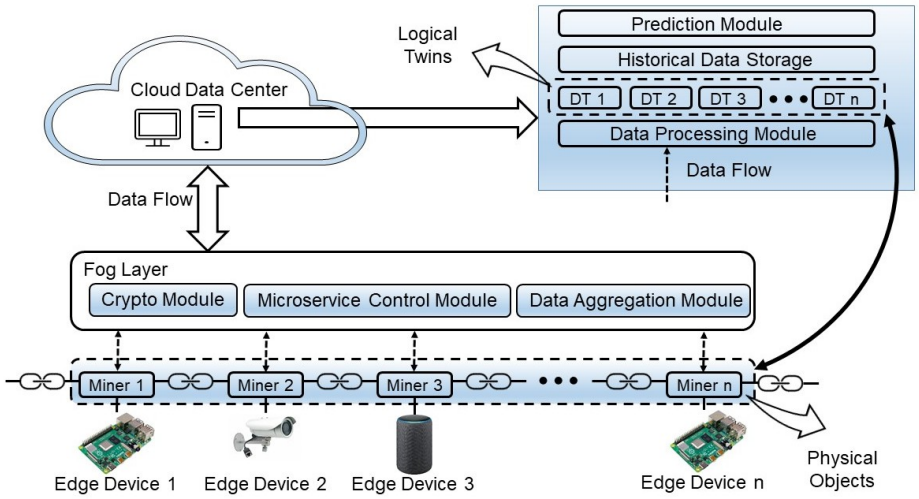

Figure 1. Illustration of MinT system architecture.

1. Containerized PoW Miner: The edge layer in MinT consists of various types of IoT devices, such as smart cameras in a surveillance system or smart meters connected to a power grid. To follow an ideal "one cup-one vote" Nakamoto consensus protocol, the Pow algorithm is encapsulated into containers as physical miners that are deployed on edge devices to participate in the blockchain network, and all containers are assigned the same computation resource for PoW mining process. Each miner has the same probability of generating blocks and being rewarded accordingly due to the uniform computation distribution of the network. Thus, these containerized PoW miners construct a fair mining blockchain network disregarding devices' capability.

2. Microservice-oriented Service: MinT utilizes an intermediate fog layer to provide middle-ware services for devices at edge and cloud level. To address heterogeneity of IoT systems, a lightweight Microservice-oriented architecture (MoA) is adopted as a fundamental service infrastructure to support functionality, such as data aggregation and microservice management, and security mechanisms, such as encryption/decryption; to identity verification; to access control, etc. Each microservice unit exposes a set of RESTful web-service APIs for interaction. The fine-granularity and loose-coupling features of the MoA framework allow for fast development and easy deployment among heterogeneous platforms using non-standard development.

3. DT-enabled Fair Mining Intelligence: As dishonest containerized miners could use extra computing power than they are permitted, MinT relies on DT technology and intelligent services on a fog/cloud server to maintain a fair mining network at the edge layer. By aggregating data flows from distributed physical miners, mirroring miners (logic objects) that are associated with their physical counterparts are created and managed by the fog or cloud server. These miner twins monitor the usage of containerized miners running on devices. By analyzing the real-time status of miner twins and historical statistics, abusers can be detected and preventive actions can be triggered to deter identified misbehaving miners such that the MinT ensures a fair mining blockchain network.

4. Miner Twin-Enabled Fair-Mining Mechanism

This section provides a comprehensive overview of the MinT-based fair mining mechanism such that readers can understand the key components and workflow. Then, we describe the miner twin process including key parameter selection. Following that, we offer details on lightweight SSA-based anomaly detection and the byzantine tolerant PoB consensus algorithm.

4.1. MinT Workflow for Fair Mining

Figure 2 illustrates the workflow of the fair-mining mechanism in the MinT system. The upstream data flow starts from the containerized miners and aggregates the fog servers installed with different modules. The fog server first normalize the data from all physical miners, which reports to it under its jurisdiction. The fog server can either construct logical miners that mirror these new physical miners or update the status of existing logical miners. The fog server further encrypts its local logical twining miners and forwards them to the cloud.

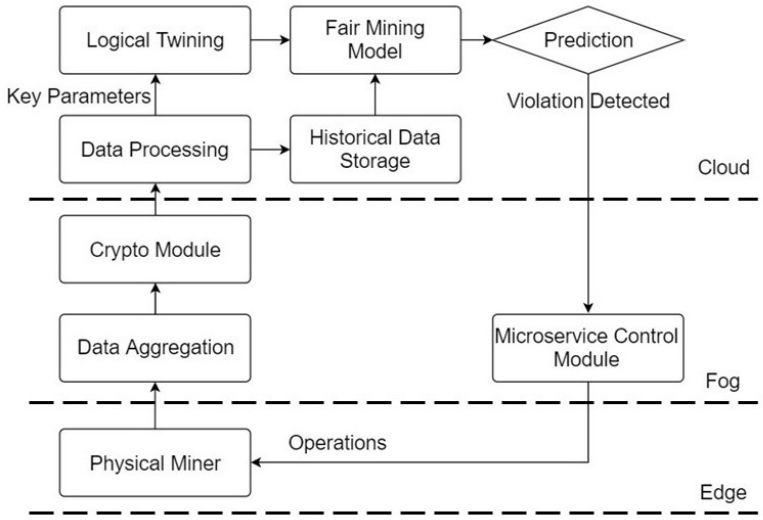

Figure 2. Miner twin-based fair-mining flowchart.

Upon receiving the encrypted data from multiple fog servers, the cloud server aggregates the information into a logical miners pool to represent a system level twinning PoW network. Using the live feed from the logical twin and the historical data, MinT uses an intelligent model for fair mining strategy. Given a fair mining algorithm, the upstream data flow starts from the predication. The predicted status is compared with the actual footprint, using anomaly detection algorithm MinT; identifies dishonest miners who violate the fair PoW consensus; and sends orders to the Microservice Control Module on a fog layer accordingly, which takes further actions on the "outlaws".

4.2. Miner Twin Process

The notations used in this paper are listed in Table 1. To mirror the physical miner, several parameters are extracted for the logical miner, including central CPU usage (C), global GPU usage (G), memory usage (M) and I/O bandwidth (B). Since PoW depends on computation intensive algorithms, the CPU usage and GPU usage are chosen as the key parameters according to the selection of calculation module, while memory, I/O bandwidth and other metrics are considered as contributing parameters. To avoid falling behind other miners, the physical miner normally uses all of the allocated CPU/GPU resources.

As the system resource allocated to each miner is restricted but identical, the data can be normalized in the form of percentages, for example $c = \frac{C}{C_{set}} \times 100\%$, where C_{set} is the preset CPU limit and c is the normalized value. Given an assumption that a con-

tainerized miner can only use its CPU to perform the PoW algorithm, then for a miner k, the parameter vector of its Physical Object (physical miner) with timestamp i would be $PO_{ki} = (c_{ki}, g_{ki}, m_{ki}, b_{ki})$, and the Key Parameter is c_{ki}. The vector for the Logical Object (logic miner) can be represented as $LO_{ki} = (c_{ki}, g_{ki}, m_{ki}, b_{ki})$, and the Key Parameter is c_{ki}.

Table 1. Relevant basic notations.

Symbol	Descriptions	Symbol	Descriptions
PO_{ki}	parameter vector of miner	LO_{ki}	parameter vector of twin
c_{ki}	cpu usage	g_{ki}	gpu usage
m_{ki}	memory usage	b_{ki}	I/O bandwidth
$\mathbb{X}$	target time series	X	trajectory matrix
N	target series length	L	SSA window length
$\vec{X}_i$	lagged vectors	K	numbers of lagged vectors
λ_L	eigenvalues	U	left singular matrix
V	right singular matrix	I	subset indices
X_I	reconstructed matrix	$\mathbb{X}_{\mathbb{I}}$	reconstructed time series
X_test	test matrix	$\vec{X}_j$	vectors of test matrix
p	starting point of test matrix	q	ending point of test matrix
Q	window length of test matrix	$D_{n,I,p,q}$	sum of the squared distances
S_n	normalized sum	W_n	CUSUM of squared distances
$\mu_{n,I}$	estimator	κ	constant of W_n
h	threshold for W_n	t_α	quantile of the standard normal distribution
$\mathcal{N}$	mining network	n_i	miners
m_i	dishonest miners	f	fraction of dishonest
B_i	behavior vector	G	global view of B_i
B^*	benchmark of B_i	$s(i)$	consensus score
s^*	ground truth of $s(i)$	d	POB window length

4.3. Fast Anomaly Detection for Fair Mining

Fast and accurate identification of the misbehaved miners is an essential step to ensuring fair mining, where MinT adopts the Singular Spectrum Analysis (SSA) algorithm to achieve this goal. SSA is recognized as one of the quickest sequential change-point detection approaches for processing time series problems [39]. By decomposing and reconstructing the interested time series, SSA extracts certain components of the origin series such as periodic pattern, noises, trends, etc. SSA is widely used in solving problems such as smoothing, extraction of seasonality components, as well as study the structure in some minor time series and change-point detection [36].

Unlike traditional methods, SSA is non-parametric and does not require prior knowledge of the parametric model of the considered time series data. Although SSA uses some statistical concepts, it does not need any statistical assumptions about the target series. Moreover, SSA algorithm can be used for processing time series with relatively small size, which make this method more suitable for edge-fog scenarios [40]. The SSA algorithm can be divided into four steps as (see Moskvina et al. at 2003) [41]:

1. Embedding: The target of SSA is a one-dimensional time series $\mathbb{X} = [x_1, \ldots, x_N]$, where N is the series length. By choosing proper window length L, one can transfer the times series into multi-dimensional series of vectors $\vec{X}_i$. Combine these vectors results in the trajectory matrix $X = [\vec{X}_1, \vec{X}_2, \ldots, \vec{X}_K]$, where $K = N - L + 1$. The multi-dimensional vectors $\vec{X}_i = (x_i, \ldots, x_{L+i-1})', i = 1, \ldots, K$, are also called lagged vectors.

2. Singular Value Decomposition (SVD) [42]: After singular value decomposing the trajectory matrix X, the eigenvalues are denoted by $\lambda_1, \ldots, \lambda_L$ in decreasing order

of magnitude and the corresponding eigenvectors $U_1, \ldots, U_L$ where the matrix $U = [U_1, U_2 \ldots, U_L]$ and $\|\mathbf{U_i}\| = 1$ is orthogonal. Then, the eigentriples are $(\sqrt{\lambda_i}, U_i, V_i)$, by denoting $V_i = X'U_i/\sqrt{\lambda_i}$. Supposing that the rank of X is d, then the trajectory matrix is $X = X_1 + \ldots + X_d$.

3. Grouping and Reconstructing: The next step is to group the matrices X_i into certain groups and to calculate the sum within these groups. Therefore, we denote a subset indices $I = i_1, i_2, \ldots, i_l$, where $l < L$. Therefore, the corresponding matrix is $X_I = X_{i_1} + \ldots + X_{i_l}$.

4. Diagonal Averaging: Using diagonal averaging, we can transfer X_I into time series $\mathbb{X}_I$.

$$\mathbb{X}_I(i) = \begin{cases} \frac{1}{i}\sum_{j=1}^{i} x_{j,i-j+1} & \text{for} \quad 1 \le i < L \\ \frac{1}{L}\sum_{j=1}^{L} x_{j,i-j+1} & \text{for} \quad L \le i \le K \\ \frac{1}{N-i+1}\sum_{j=i-K+1}^{N-K+1} x_{j,i-j+1} & \text{for} \quad K \le i \le N. \end{cases} \tag{2}$$

By selecting certain subset indices $I = i_1, i_2, \ldots, i_l$, one can reconstruct the time series. By observing the distance between the l-dimensional matrix and the test time series matrix, we can detect the anomaly by identifying a significant increase in the distance. The SSA-based Change-Point detection utilized in the paper can be described in following stages [41]:

Stage 1: Construct Base Matrix First, construct the base matrix (or target matrix) according to the four steps of the SSA algorithm. Given the target time series $\mathbb{X} = [x_{n+1}, \ldots, x_{n+N}]$, embed it into the trajectory matrix $X = [\vec{X_1}, \vec{X_2}, \ldots, \vec{X_K}]$, where $K = N - L + 1$. Then, the columns of the trajectory matrix are the vectors:

$$\vec{X_i} = (x_{n+i}, \ldots, x_{n+L+i-1})', i = 1, \ldots, K. \tag{3}$$

Then, conduct the SVD and get L eigenvectors which can be grouped into certain subset $I = i_1, i_2, \ldots, i_l, l < L$.

Stage 2: Construct Test Matrix Similarly, we select integers p, q and Q where $Q = q - p > 0$. Then, we construct the test matrix of size $L \times Q$:

$$X_{test} = [\vec{X_{p+1}}, \vec{X_{p+2}}, \ldots, \vec{X_{p+Q}}], \tag{4}$$

and the columns of the matrix are the vectors:

$$\vec{X_j} = (x_{n+j}, \ldots, x_{n+L+j-1})', j = p+1, \ldots, p+Q, \tag{5}$$

Stage 3: Compute the Detection Statistics In this stage, we first compute $D_{n,I,p,q}$, the sum of the squared Euclidean distances between the l-dimensional subspace from the base matrix and the vectors $\vec{X_j}(j = p+1, \ldots, p+Q)$from the test matrix.

$$D_{n,I,p,q} = \sum_{j=p+1}^{q} ((\vec{X_j})^T \vec{X_j} - (\vec{X_j})^T U U^T \vec{X_j}). \tag{6}$$

Then, we give the normalized sum of squared distances

$$S_n = \frac{1}{\mu_{n,I}} \tilde{D}_{n,I,p,q}, \tag{7}$$

where $\tilde{D}_{n,I,p,q} = \frac{1}{LQ} D_{n,I,p,q}$ and $\mu_{n,I} = \tilde{D}_{m,I,0,K}$ is the estimator and we make the hypothesis that no change of time series structure occurs at the time intervals where m is the largest value of $m \le n$.

We also compute the Cumulative Sum (CUSUM) W_n of the normalized sum of squared distances as the final score for the anomaly detection.

$$W_1 = S_1, W_{n+1} = max\{0, W_n + S_{n+1} - S_n - \kappa/\sqrt{LQ}\}, n \ge 1, \tag{8}$$

where κ is a constant, and in this paper, we set $\kappa = 1/(3\sqrt{LQ})$ [43].

Stage 4: Set threshold and make decisions To detect the change of the time series, we could check the values of $D_{n,I,p,q}$, S_n and W_n. Basicallys the large value of the three detection statistics indicates the change or the anomaly. In this paper, we choose the W_n-based detection algorithm as it gives greater sensitivity compared with the former two detection statistics [41]. The algorithm announces a structural change if we observe $W_n > h$ for some n where h is the threshold given by

$$h = \frac{2t_\alpha}{LQ}\sqrt{\frac{1}{3}Q(3LQ - Q^2 + 1)}, \tag{9}$$

and t_α is the $1-\alpha$-quantile of the standard normal distribution [41].

4.4. Proof-of-Behavior Consensus Algorithm for Fair Mining Enforcement

The abovementioned SSA-based detection can identify a single misbehaved miner based on its own footprint; however, it cannot handle byzantine scenarios that multiple compromised miners by an adversary collude to violate fair mining policies. By observing a miner's running operations, the calculated cumulative sum (CUSUM)-type W can indicate a miner's behavior. Inspired by deepfake detection in video surveillance systems [44,45], our MinT relies on a novel *Proof-of-Behavior* consensus algorithm that leverages CUSUM-type W calculated in SSA algorithm to detect multiple dishonest miners in distributed byzantine tolerant scenarios.

We consider a mining network $\mathcal{N}$ including n_i miners, where $i \in \{1, k\}$ and $k = |\mathcal{N}|$. All dishonest miners are denoted by $m_i \in \mathcal{M}$ and their fraction is $f = |\mathcal{M}|/|\mathcal{N}|$. We use observed CUSUM-type W_i of miner n_i to demote a behavior vector $B_i = \{b_1, b_2, \ldots, b_d\}$, where $b_k = w_k \in W_i$ and d is the SSA detection time window. Finally, each twin can maintain a global view of collected behavior vectors, which is a matrix $G = \{B_1, B_2, \ldots, B_k\}$. The PoB firstly generates a behavior score $s(i)$ for each miner n_i, which is a sum of relative Euclidean distances between other miners' behavior vector. Then, a $B_i \in G$ with minimal behavior score is selected as a benchmark B^*.

The PoB consensus algorithm aims to chooses a behavior vector B, which deviates at least from the distribution of G. However, an adversary can compromise multiple miners that generate large vectors to force "honest" miners to choose a byzantine behavior vector as the ground truth one. Thus, our PoB algorithm adopts a *Krum* aggregation rule to guarantee byzantine tolerance. We assume that honest miners within network $\mathcal{N}$ store G including $n \geq 2f + 3$ vectors in which at most f vectors are generated by byzantine nodes in $\mathcal{M}$. For B_j belongs to the $n - f - 2$ closest vectors to B_i, where $i \neq j$, we denote $i \to j$. Therefore, we could define the consensus score:

$$s(i) = \sum_{i \to j} ||B_i - B_j||^2. \tag{10}$$

Then, each node can compute behavior scores $s(1), \ldots, s(k)$ that are associated with miners $n_1, \ldots, n_k$ separately. By calculating the minimum behavior score

$$s^* = \min_{i \in \{1,\ldots,k\}} (s(i)), \tag{11}$$

all honest miners choose a behavior vector B_i that satisfies $s(i) = s^*$ as the ground truth B^*. Given assumption that an adversary controls no more than f miners, all honest miners can reach an agreement on the unique B^*.

5. Experimental Study

In this section, a proof-of-concept prototype implementation and experimental configuration are described. Following that, we evaluate effectiveness of the proposed MinT

solution based on numerical results. Finally, we discuss performance and security properties provided by MinT.

5.1. Experimental Setup

A proof-of-concept test platform is created, in which 16 Raspberry Pis (RPi) are adopted as the edge devices. Each RPi is empowered with quad-core Cortex-A72 CPU @1.5GHz and an installed RAM with 4GB memory running Raspbian OS based on Debian. The single-board computer (SBC) is capable of carrying containerized PoW module to participate the blockchain network. A desktop functions as a fog server, which has Intel Core i7-7700K CPU and a RAM of 16 GB memory. All of the RPis are connected to a fog server via local area network (LAN).

As the GPU is not available on the RPi, we select a CPU-based PoW algorithm for container construction. For fast deployment, Docker [46] is adopted as the microservice container that is affordable to RPis and transmits the data from the physical miner to a fog server through RESTfull APIs. Each of the miner containers is configured with and restricted to one CPU core, 500 MB memory and 10 percent of system I/O bandwidth. The collected data are stored in forms of vector as described in Section 4.2.

As the PoW algorithm is executed on CPU, samples of the key parameter C are collected and the historical data vector c_{hi} is used to obtain the statistic profile, where $h = 1, \ldots, 16$ and $i = 0, 1, \ldots$. For SSA based change-point detection, as the standard SSA recommendation in the book [47], we define $N = 24$ according to the size of the data sets, $L = 12$ to the half size of N, $p = 12$, $q = 24$ and $d = 1s$. We deliberately set $p \geq K$ so that the base and test matrices would not coincide. After visual inspection of the components of the decomposition of the whole time series, we choose certain l to represent ignoring the noise components. To guarantee the accuracy and reliability, we repeat each experiment scenario for at least five times and over two hours each time to avoid contingency.

5.2. Experimental Results

All 16 miners, by default, run at 100% of the assigned system resources under the jurisdiction of the fog server. Four different test scenarios are considered in our experimental study. To verify SSA-based detection on a single misbehaved miner, we first conduct test cases that only one dishonest miner uses double-assigned computation power on mining given a different parameter combination. Then, we consider a more stealthy single miner violation, which incrementally increases the computing power from 20% up to 50%. To validate effectiveness of PoB-based detection, we simulate a byzantine network, in which two miners act as byzantine nodes while 14 miners are honest members. Finally, we evaluate the false-positive rates at the network level with different threshold settings.

5.2.1. SSA-Based Detection on Static Single Miner Violation

In this scenario, one dishonest miner uses twice as much CPU power as the assigned amount at $t = 200$ s. Figure 3a presents the network level observation at the fog server. The blue line is the average CPU usage for all 16 miners in this blockchain network, and the red line is the w_n value calculated using SSA algorithm as the score. The green line is the threshold $h = 0.607$, which is computed with $t_\alpha = 1.2815$. As shown by Figure 3a, the fluctuation in the average CPU utility incurs a low peak in the distance score. However, applying the SSA algorithm on each miner twin individually avoids the false negative. Figure 3b shows that a significant peak is observed at $t = 200$ s.

We also studied the impacts of different selections of the SSA parameters varying l and $q - p$ combination. Figure 3c shows the consequence of increasing the value of l from 4 to 8 but with the same matrix size. The larger l leads to a more noise part with the signal; therefore, it would be more difficult to find a change in the signal time series. If the l is too small, which would cause underfitting, we might miss some part of the signal. Due to limited space, the figure is not included here.

Meanwhile, the matrix size $q - p$ also has significant impact on the detection distance score. Figure 3d shows that, by increasing the value of $q - p$ to 24 while $l = 4$, the distance (red) line is smoother than in Figure 3b.

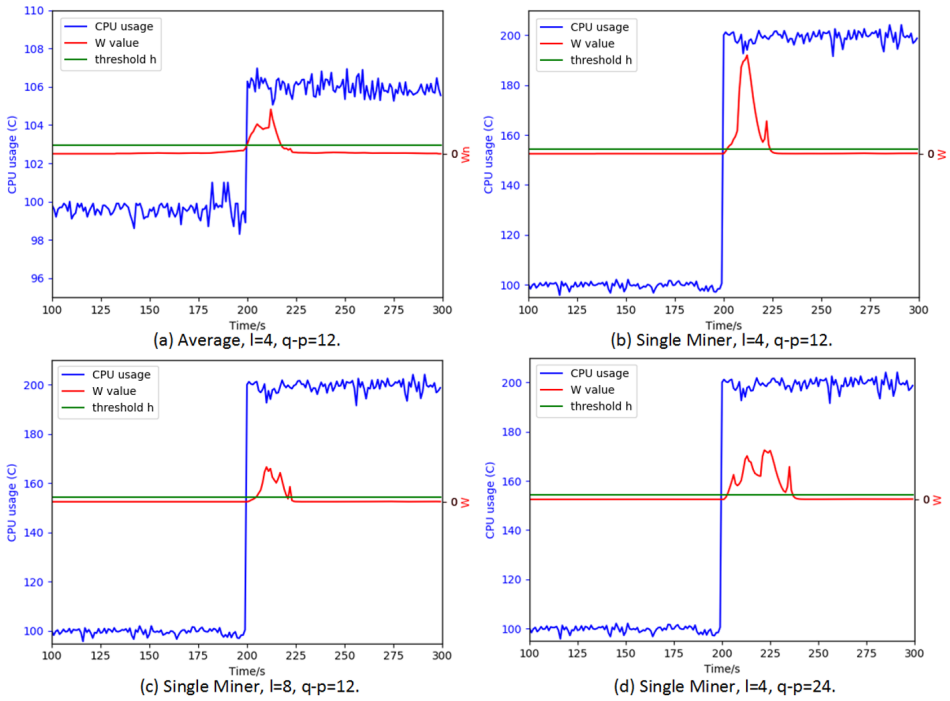

Figure 3. SSA detection on single miner violation with different parameter combinations. (**a**) Network level observation at the fog server; (**b**) Observation on a single miner; (**c**) Impacts of increasing l from 4 to 8 with the same matrix size; (**d**) Impacts of increasing the matrix size to 24 while maintain $l = 4$.

5.2.2. SSA Detection on Adaptive Single Miner Violation

The second scenario considers more stealthy behavior of a violator, which increases the computing power slowly, from 20% to 50%, taking multiple steps at time point $t = 125$ s, $t = 175$ s, $t = 225$ s and $t = 275$ s. Figure 4a shows the detection results in which a miner increases 20% CPU usage at each time point. Figures 4b–d show similar results of cases when the CPU usage increases by 30%, 40% and 50% respectively. Obviously, the SSA-based anomaly detection is able to detect the changes in the structure of the time series data and to identify the corresponding violation on mining power. However, the critical issue is how to select a threshold to ensure a high detection accuracy and to minimize the false-positive/negative rates.

5.2.3. PoB-Based Fair Mining Detection Effectiveness

We take an observation of 20 min on the 16 miners running at 100% of the assigned system resource. Two of the miners act as the byzantine (dishonest) workers, which would gain extra 10% at the 9th and 10th min. As shown in Figure 5a, the behavior vector B from dishonest workers varies from honest ones when the byzantine workers gain more computing power. During the two minutes where violation occurs, the resulting consensus scores associated with the byzantine nodes are much larger, as shown in Figure 5b.

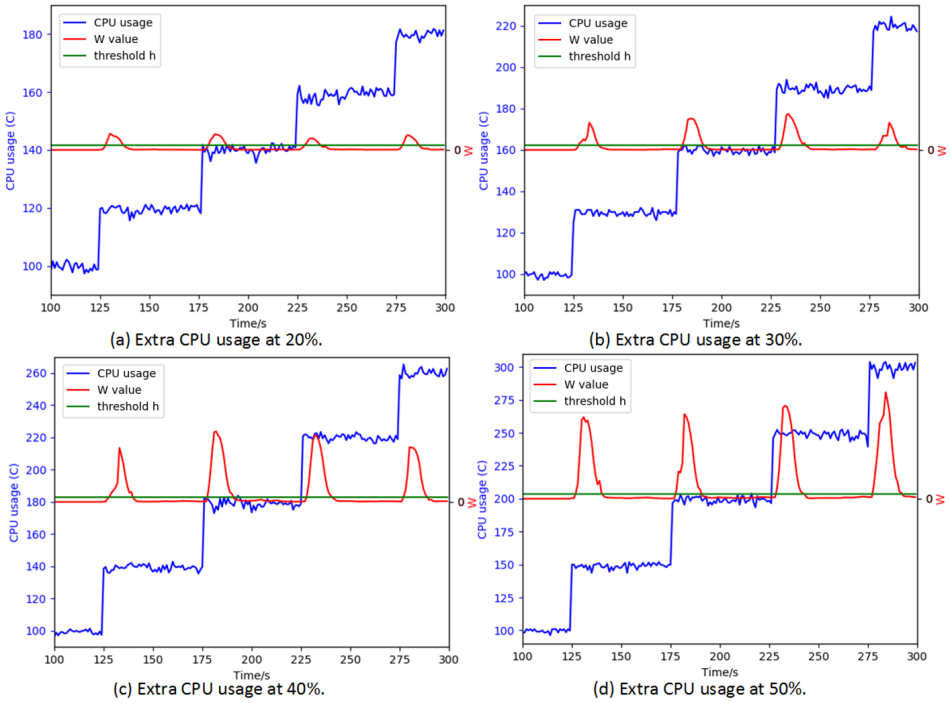

Figure 4. SSA detection on single miner violation with additive CPU usage. (**a**) One single miner increases 20% CPU usage at each time point; (**b**) One single miner increases 30% CPU usage at each time point; (**c**) One single miner increases 40% CPU usage at each time point; (**d**) One single miner increases 50% CPU usage at each time point.

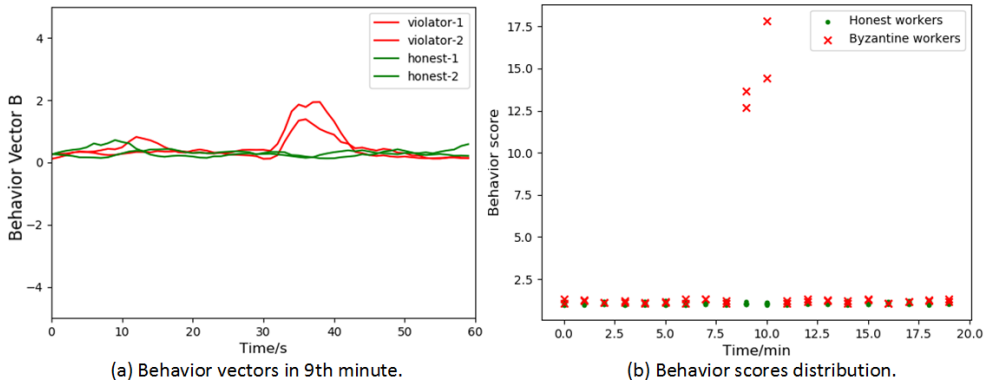

Figure 5. Behavior score distribution with sequential time spots. (**a**) The behavior vector from dishonest workers (red) varies from honest ones (green) when the byzantine workers gain more computing power; (**b**) Comparison between consensus scores associated with the byzantine nodes (red) and the honest nodes (green).

5.2.4. Fair Mining Violation Detection Performance Analysis

The fourth scenario is designed to mainly test the false positive rate from the network level observation at the fog server with different threshold settings. Figure 6 shows the false alarm rates when two of the sixteen miners gain extra system resources from 10% to 80%. The false alarm rate is calculated by comparing the averaged the W value with the threshold h. When we decrease h from 0.6 to 0.03, the false alarm rate increases rapidly at the beginning and then slowly approaches one. With the increasing percentage of the computing power the dishonest miner gains, the false alarm rate grows.

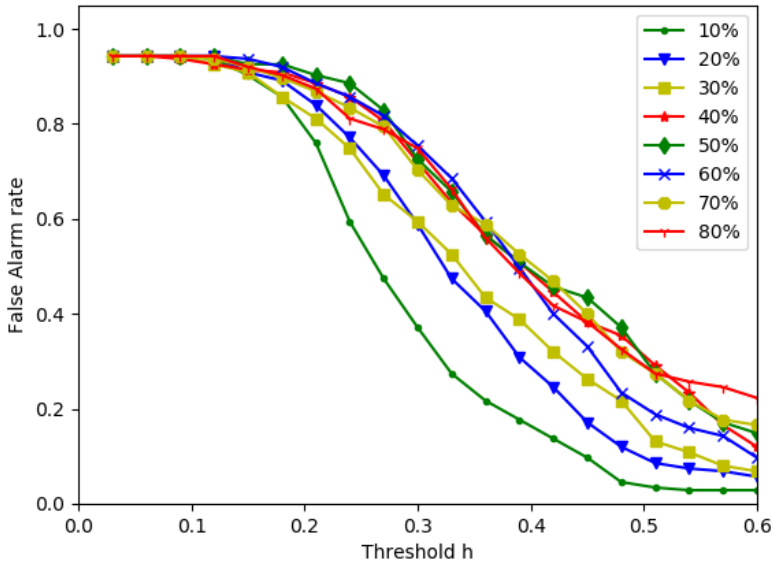

Figure 6. False alarm rate with different threshold h.

5.3. Discussions

The experimental results presented in this section are merely a preliminary study on top of a proof-of-concept platform. Our MinT relies on a permissioned network to provide basic security primitives, such as identity registration, authentication and access control, etc. Given the assumption that the adversary cannot control microservice control the module to send false parameters, we verify that SSA-based detection can identify a single dishonest miner that uses either static or adaptive mining violation strategies. Regarding byzantine scenarios that multiple dishonest miners collude to disturb fair mining mechanism, the PoB consensus algorithm adopts Krum rule in behavior score calculation, which only chooses $n - f - 2$ closet behavior vectors and precludes those $f - 1$ malicious vectors that are far away from the center of distribution. Given the assumption that an adversary cannot control more than f nodes of a mining network $\mathcal{N}$ that satisfies $n \geq 2f + 3$, all honest participants can still make agreements and output the unique benchmark behavior vector B^*.

Our MinT architecture envisions large-scale IoT networks based on a hierarchy of edge-fog-cloud paradigm. However, there are open questions that need to be addressed before bringing the proposed framework into real-world applications. We leave them for our future work.

- Although experimental results verify feasibility of SSA-based fair-mining violation detection, there still need investigation on SSA performance and accuracy given the impact of parameters, such as optimal/sub-optimal threshold selection and detection latency as scaling up miners.
- The PoB consensus is promising to guarantee byzantine fault tolerance in mining violation detection; however, the threat model based on attack scenarios in SSA detection needs more investigation, such as communication security between miner and twin and container's robustness given failed or compromised conditions. Therefore, the security mechanisms for communication between PO and LO, and container management are among the tasks of top priority.
- It is inevitable that extra overheads are incurred by security enforcement and data synchronization in fair-mining mechanism. Therefore, a comprehensive performance evaluation of the twinning process is necessary, such as computation and communication cost, network latency and storage requirement, etc.
- Furthermore, we also need to tackle scalability and heterogeneity issues such as as applying MinT into large-scale IoT networks. A hierarchical federated network frame-

work is promising to handle the trilemma in blockchain solutions that decentralization, security and scalability cannot perfectly co-exist [4].

6. Conclusions and Future Work

In this paper, we proposed MinT, an edge-fog-cloud architecture to enable a fair PoW consensus mechanism by leveraging miner twins. Experimentally, the paper validated the feasibility of the concept of using DT to monitor the miners' behaviors and to deter selfish nodes who violate the fair-mining rule. The reported preliminary results verify the effectiveness of using quick change point detection and the PoB consensus algorithm to catch fair mining violators; however, more intelligent solutions are needed to support dynamicity and optimization in fair mining network. Moreover, the above mentioned open questions need to be addressed in IoT-based mining networks. Our future work includes the following.

- We will conduct a comprehensive evaluation on SSA method in anomaly detection, especially for detection accuracy and performance, and the impact of parameter selection. Moreover, AI/ML-based algorithms will be investigated to improve anomaly detection accuracy and to support efficient dynamic resources management in the fair mining network.
- To apply MinT in a large-scale application scenario such as a smart surveillance system [48], we will implement a fully function prototype based on edge-fog-cloud architecture, in which physical containerized miners are on edge devices while digital twins are in the fog or cloud. Then, we will make a comprehensive performance analysis and assessment of security features.
- Furthermore, MinT relies on microservices that encapsulate a fair PoW mining algorithm into independent containers running on host machines. Thus, the security and privacy of containers and data reliability are among the top concerns. We will investigate the security of the container running environment, and data audition and integrity in microservice-to-microservice communication.

Author Contributions: Conceptualization, Q.Q., R.X. and Y.C.; methodology, Q.Q. and R.X.; software, Q.Q. and R.X.; validation, Q.Q., R.X. and Y.C.; formal analysis, Q.Q. and R.X.; investigation, Y.C.; resources, Y.C., E.B. and A.A.; data creation, Q.Q.; writing—original draft preparation, Q.Q. and R.X.; writing—review and editing, Y.C., E.B. and A.A.; visualization, Q.Q. and R.X.; supervision, Y.C. and E.B.; project administration, Y.C. and A.A.; funding acquisition, Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work is partially supported by the U.S. National Science Foundation (NSF) via grants CNS-2141468.

Data Availability Statement: Not Applicable, the study does not report any data.

Acknowledgments: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Air Force.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
AR	Augmented Reality
BFT	Byzantine Fault Tolerant
CUSUM	Cumulative Sum
DDDAS	Dynamic Data-Driven Applications Systems
DLT	Distributed Ledger Technology

DT	Digital Twins
FMaaS	Fair Mining as a Service
EPDS	Electric Propulsion Drive Systems
ICT	Information and Communication Technology
IoT	Internet of Things
LAN	Local Area Network
LO	Logical Object
MinT	Miner Twins
ML	Machine Learning
MoA	Microservice-Oriented Architecture
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
PO	Physical Object
PoB	Proof-of-Behavior
PoS	Proof-of-Stake
PoW	Proof-of-Work
SBC	Single Board Computer
SSA	Singular Spectrum Analysis
VR	Virtual Reality

References

1. Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
2. Nikouei, S.Y.; Xu, R.; Nagothu, D.; Chen, Y.; Aved, A.; Blasch, E. Real-time index authentication for event-oriented surveillance video query using blockchain. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), City, MO, USA, 16–19 September 2018; pp. 1–8.
3. Fitwi, A.; Chen, Y. Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain. *arXiv* **2021**, arXiv:2104.05617.
4. Xu, R.; Chen, Y. Fed-DDM: A Federated Ledgers based Framework for Hierarchical Decentralized Data Marketplaces. *arXiv* **2021**, arXiv:2104.05583.
5. Xu, R.; Zhai, Z.; Chen, Y.; Lum, J.K. BIT: A blockchain integrated time banking system for community exchange economy. In Proceedings of the 2020 IEEE International Smart Cities Conference (ISC2), Piscataway, NJ, USA, 28 September–1 October 2020; pp. 1–8.
6. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness. *Opt. Eng.* **2019**, *58*, 041609. [CrossRef]
7. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A blockchain-enabled decentralized capability-based access control for iots. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1027–1034.
8. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. *Computers* **2018**, *7*, 39. [CrossRef]
9. Barricelli, B.R.; Casiraghi, E.; Fogli, D. A survey on digital twin: Definitions, characteristics, applications, and design implications. *IEEE Access* **2019**, *7*, 167653–167671. [CrossRef]
10. Blasch, E.; Ravela, S.; Aved, A. *Handbook of Dynamic Data Driven Applications Systems*; Springer. 2018. Available online: https://link.springer.com/book/10.1007/978-3-319-95504-9#about (accessed on 15 November 2021).
11. Yaqoob, I.; Salah, K.; Uddin, M.; Jayaraman, R.; Omar, M.; Imran, M. Blockchain for digital twins: Recent advances and future research challenges. *IEEE Netw.* **2020**, *34*, 290–298. [CrossRef]
12. Xu, R.; Chen, Y.; Blasch, E. Microchain: A Light Hierarchical Consensus Protocol for IoT System. In *Blockchain Applications in IoT: Principles and Practices*; 2021. Available online: https://link.springer.com/chapter/10.1007/978-3-030-65691-1_9 (accessed on 15 November 2021).
13. Castro, M.; Liskov, B. Practical Byzantine fault tolerance. *OSDI* **1999**, *99*, 173–186.
14. Alsabah, H.; Capponi, A. Pitfalls of Bitcoin's Proof-of-Work: R&D Arms Race and Mining Centralization. SSRN 3273982. 2020. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273982 (accessed on 15 November 2021). .
15. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; Technical Report; Manubot. 2019. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 15 November 2021).
16. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
17. King, S.; Nadal, S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *Self-Publ. Pap. August* **2012**, *19*. Available online: https://decred.org/research/king2012.pdf (accessed on 15 November 2021).

18. Grieves, M. Digital twin: Manufacturing excellence through virtual factory replication. *White Pap.* **2014**, *1*, 1–7.
19. Erkoyuncu, J.A.; Butala, P.; Roy, R. Digital twins: Understanding the added value of integrated models for through-life engineering services. *Procedia Manuf.* **2018**, *16*, 139–146.
20. Van Schalkwyk, P. The Ultimate Guide to Digital Twins. 2019. Available online: https://xmpro.com/digital-twins-the-ultimate-guide// (accessed on 15 November 2021).
21. Khan, L.U.; Saad, W.; Niyato, D.; Han, Z.; Hong, C.S. Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions. *arXiv* **2021**, arXiv:2102.12169.
22. Blasch, E.; Lambert, D.A. *High-Level Information Fusion Management and Systems Design*; Artech House. 2012. Available online: http://www.cs.utah.edu/~tch/notes/BRECCIA/refs/BOOK12_High-Level%20Information%20Fusion%20Management%20and%20Systems%20Design_BLASCH.pdf (accessed on 15 November 2021).
23. Bilberg, A.; Malik, A.A. Digital twin driven human–robot collaborative assembly. *CIRP Ann.* **2019**, *68*, 499–502. [CrossRef]
24. Sun, X.; Bao, J.; Li, J.; Zhang, Y.; Liu, S.; Zhou, B. A digital twin-driven approach for the assembly-commissioning of high precision products. *Robot. Comput.-Integr. Manuf.* **2020**, *61*, 101839. [CrossRef]
25. Karadeniz, A.M.; Arif, İ.; Kanak, A.; Ergün, S. Digital twin of egastronomic things: A case study for ice cream machines. In Proceedings of the 2019 IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan, 26–29 May 2019; pp. 1–4.
26. Rassõlkin, A.; Vaimann, T.; Kallaste, A.; Kuts, V. Digital twin for propulsion drive of autonomous electric vehicle. In Proceedings of the 2019 IEEE 60th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON), Riga, Latvia, 7–9 October 2019; pp. 1–4.
27. Chen, X.; Kang, E.; Shiraishi, S.; Preciado, V.M.; Jiang, Z. Digital behavioral twins for safe connected cars. In Proceedings of the 21th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems, Copenhagen, Denmark, 14–19 October 2018; pp. 144–153.
28. Kapteyn, M.G.; Knezevic, D.J.; Willcox, K. Toward predictive digital twins via component-based reduced-order models and interpretable machine learning. In Proceedings of the AIAA Scitech 2020 Forum, Orlando, FL, USA, 6–10 January 2020; p. 0418. Available online: https://arc.aiaa.org/doi/10.2514/6.2020-0418 (accessed on 15 November 2021).
29. Pargmann, H.; Euhausen, D.; Faber, R. Intelligent big data processing for wind farm monitoring and analysis based on cloud-technologies and digital twins: A quantitative approach. In Proceedings of the 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China, 20–22 April 2018; pp. 233–237.
30. El Saddik, A. Digital twins: The convergence of multimedia technologies. *IEEE Multimed.* **2018**, *25*, 87–92. [CrossRef]
31. Liu, Y.; Zhang, L.; Yang, Y.; Zhou, L.; Ren, L.; Wang, F.; Liu, R.; Pang, Z.; Deen, M.J. A novel cloud-based framework for the elderly healthcare services using digital twin. *IEEE Access* **2019**, *7*, 49088–49101. [CrossRef]
32. Laaki, H.; Miche, Y.; Tammi, K. Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery. *IEEE Access* **2019**, *7*, 20325–20336. [CrossRef]
33. Saad, W.; Bennis, M.; Chen, M. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Netw.* **2019**, *34*, 134–142. [CrossRef]
34. Nguyen, H.X.; Trestian, R.; To, D.; Tatipamula, M. Digital twin for 5G and beyond. *IEEE Commun. Mag.* **2021**, *59*, 10–15. [CrossRef]
35. Suhail, S.; Hussain, R.; Jurdak, R.; Oracevic, A.; Salah, K.; Hong, C.S. Blockchain-based Digital Twins: Research Trends, Issues, and Future Challenges. *arXiv* **2021**, arXiv:2103.11585.
36. Hassani, H. *Singular Spectrum Analysis: Methodology and Comparison*; 2007. Available online: https://mpra.ub.uni-muenchen.de/4991/ (accessed on 15 November 2021).
37. Dong, Q.; Yang, Z.; Chen, Y.; Li, X.; Zeng, K. Anomaly detection in cognitive radio networks exploiting singular spectrum analysis. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*; Springer: New York, NY, USA 2017; pp. 247–259.
38. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. A federated capability-based access control mechanism for internet of things (iots). In *Sensors and Systems for Space Applications XI*; International Society for Optics and Photonics: Bellingham, WA, USA, 2018; Volume 10641, p. 106410U.
39. Polunchenko, A.S.; Sokolov, G.; Du, W. Quickest change-point detection: A bird's eye view. *arXiv* **2013**, arXiv:1310.3285.
40. Yang, Z.; Chen, N.; Chen, Y.; Zhou, N. A novel PMU fog based early anomaly detection for an efficient wide area PMU network. In Proceedings of the 2018 IEEE 2nd International Conference on Fog and Edge Computing (ICFEC), Washington, DC, USA, 1–3 May 2018; pp. 1–10.
41. Moskvina, V.; Zhigljavsky, A. An algorithm based on singular spectrum analysis for change-point detection. *Commun. Stat.-Simul. Comput.* **2003**, *32*, 319–352. [CrossRef]
42. Hoecker, A.; Kartvelishvili, V. SVD approach to data unfolding. *Nucl. Instruments Methods Phys. Res. Sect. A Accel. Spectrometers Detect. Assoc. Equip.* **1996**, *372*, 469–481. [CrossRef]
43. Moskvina, V.; Zhigljavsky, A. Application of the Singular Spectrum Analysis for Change-Point Detection in Time Series. Ph.D. Thesis, Cardiff University, Cardiff, UK, 2001.

44. Nagothu, D.; Xu, R.; Chen, Y.; Blasch, E.; Aved, A. DeFake: Decentralized ENF-Consensus Based DeepFake Detection in Video Conferencing. In Proceedings of the IEEE 23rd International Workshop on Multimedia Signal Processing, Tampere, Finland, 6–8 October 2021.
45. Xu, R.; Nagothu, D.; Chen, Y. EconLedger: A Proof-of-ENF Consensus Based Lightweight Distributed Ledger for IoVT Networks. *Future Internet* **2021**, *13*, 248. [CrossRef]
46. Merkel, D. Docker: Lightweight linux containers for consistent development and deployment. *Linux J.* **2014**, *2014*, 2.
47. Golyandina, N.; Nekrutkin, V.; Zhigljavsky, A.A. *Analysis of Time Series Structure: SSA and Related Techniques*; CRC Press: Boca Raton, FL, USA, 2001.
48. Xu, R.; Nikouei, S.Y.; Nagothu, D.; Fitwi, A.; Chen, Y. BlendSPS: A BLockchain-ENabled Decentralized Smart Public Safety System. *Smart Cities* **2020**, *3*, 928–951. [CrossRef]