2024

IEEE

IEEE Public Safety Technology™

Blockchain Technology for Public Safety

Blockchain Technology for Public Safety: An IEEE Public Safety Technology Initiative Report

Table of Contents

List of Figures

ABSTRACT

The present document aims to discuss potential opportunities and challenges of blockchain technology for public safety application. Background on blockchain technology will be described. Some use cases for using blockchain technology in public safety environment are identified as potential opportunities. For realizing these use cases, a list of technology gaps and challenges are pending for future solutions.

WHITE PAPER

1. INTRODUCTION

Blockchain technology brings with multitude benefits including immutability, transparency, traceability, decentralized trust, and security. It is envisioned that blockchain technology has great potentials for public safety.

The present document will first briefly introduce public safety applications and blockchain technology. Layered blockchain system architecture including on-chain and off-chain operations will be discussed. There are two primary blockchain work flow models: Order-Execute and Execute-Order-Validate. Key blockchain components such as consensus protocols, smart contracts, blockchain virtualization, data storage and management in blockchain, and blockchain for resource-constrained environment will be explained,

To assess the applicability of blockchain technology for public safety, a list of potential use cases will be described and analyzed. These use cases include but not limited to: gun ownership and tracing, forensics, wireless networks, distributed AI/ML, public health, and industrial workers.

Based on the analysis of use cases of using blockchain for public safety, multiple technology gaps are identified, which are building blockchain-assisted platforms, blockchain as an infrastructure, and DAO-empowered solutions.

Finally, conclusions and recommendations on blockchain technology for public safety will be given as future directions.

2. BACKGROUND

2.1. Public Safety Applications

2.2. Blockchain Technology Introduction

2.2.1. Blockchain System Architecture

Blockchain was popularized by providing a decentralized data store for Bitcoin transactions for maintaining all historical transaction records [1]. Fundamentally, blockchain is a form of distributed ledger system that verify and store transactions [2], without relying on any central trusted authority, for instance, traditional banking systems. Within a blockchain system, all participants can reach a consensus on the states of transactional data to achieve trust.

In the last decade, both researchers in academia and practitioners in industry made efforts to investigate and explore how to build next-generation applications by integrating with blockchain technology [3] [4]. Blockchain has been leveraged in decentralized finance, supply chain, international payments, registries, Internet of Things (IoT), identity and security management, government identity and taxation management, to name a few [5] [6] [7] [8]. Further, blockchain has been applied as an infrastructure to preserve trust and security in different domains. For instance, blockchain can be used to build a public key infrastructure (PKI) enhancement solution carrying out automatic responses to misbehavior and distributing incentives to users who detect and report such misbehavior [9]. Blockchain can be integrated into cloud-based data analytics for

providing data provenance information [10]. Blockchain can also ensure self-sovereign data in a decentralized way [11].

Software components are regarded as the fundamental elements for building software architectures, and blockchain can be utilized as a software component offering decentralized data storage, computational capabilities, and communication services. *Figure 1* demonstrates a high-level representation of blockchain system architecture, consisting of four horizontal layers regarding the functionality, and two vertical layers regarding the implementation context. The horizontal layers include a presentation layer, a logic layer, a data layer, and a platform layer, while the vertical layers are on-chain and off-chain. (Note: the term "layer" in this context should not be interpreted as OSI layers!)

First, system users can interact with blockchain services (e.g., smart contracts) and all other off-chain components via the user interface and provided API. Secondly, the business logic of a blockchain system is implemented through different smart contracts and other off-chain components. Specifically, the key management component can be utilized to control and manage the public and private key pairs for on-chain business. Blockchain can be used as a public key infrastructure where every participant has at least one public and private key pair. The private key is then used to generate digital signatures for on-chain transactions. If the private key is compromised, the attacker can forge on-chain transactions and have access to the related on-chain assets and smart contracts.

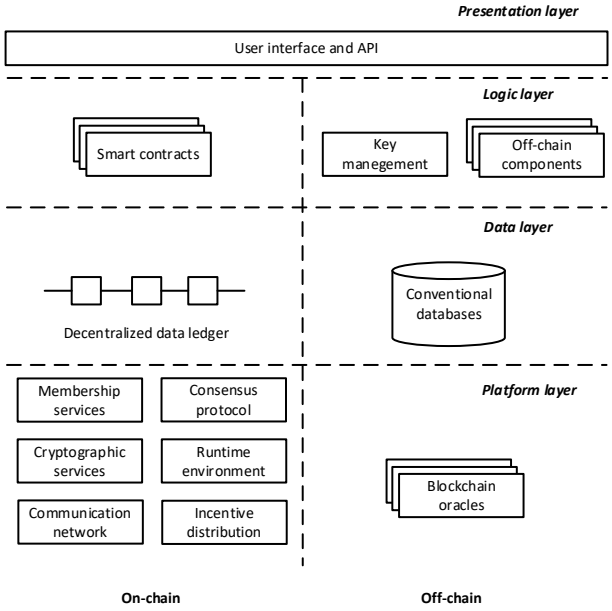

Figure 1. Blockchain System Architecture

At the data layer, off-chain conventional databases are required to store the raw data and large-size files due to the scalability and privacy requirements, while blockchain can provide a decentralized ledger to record processed data (e.g., encrypted data, hash values) for integrity verification.

Finally, at the platform layer, blockchain incorporates membership services, consensus protocol, cryptographic services, runtime environment, communication network, and event management.

Specifically, membership services are related to the deployed blockchain type. In permissioned blockchain systems, participation requires the approval of system administrator(s). Consequently, in an accountability process, the real-world identity of the responsible user can be traced. Whilst, in permissionless blockchain systems, users are identified via on-chain addresses. The deployed consensus protocol determines how new blocks are appended to the blockchain, which will be further discussed in Section 2.2.3. Cryptographic services in a blockchain system can preserve data integrity and confidentiality, while the runtime environment can support the execution of smart contract logic. The communication network connects all the nodes for block broadcast and synchronization. In a blockchain system, incentives may be distributed to reward users, for their contributions to maintain the normal operations of blockchain. In terms of off-chain architecture components in this layer, blockchain oracles are operated as the data entry, supplying information about the external world to the blockchain.

2.2.2. Blockchain Workflow

Blockchain workflow defines sequential system operations related to functions such as transaction/block generation, transaction/block verification and validation, transaction/block ordering, transaction/block execution, and transaction/block commitment. The sequence of such operations depends on the corresponding system architecture and may vary based on the detailed design. From sequential operation perspectives, there are two primary blockchain system models: Order-Execute [1] and Execute-Order-Validate [12].

Order-Execute: The Order-Execute model has been adopted in early blockchain applications especially in cryptocurrency such as Bitcoin and Ethereum, which are two typical and most popular blockchain-based digital currency. In this model, blockchain workflow follows the sequential operations: 1) A blockchain client or user creates a new transaction and sends the new transaction to the blockchain system; 2) the new transaction will be propagated within the blockchain system using underlying P2P networks; 3) All blockchain nodes (i.e., miners) will receive the new transaction, verify it, and store it to their local storage (e.g., mempool) as pending transactions; 4) Each blockchain node independently selects a certain number of pending transactions, order them, and try to include them in a new block according to a consensus protocol (e.g., PoW); 5) According to the consensus protocol, a blockchain node A wins the consensus protocol and create a new block that contains the list of ordered transactions. The new block will be linked to an existing block (e.g., the newest block on the longest chain in Bitcoin) or multiple existing blocks in the Directed Acyclic Graph (DAG)-based blockchain (e.g., PHANTOM); 6) The blockchain node A sends the new block to its neighboring blockchain nodes; 7) The new block will be propagated within the blockchain system; 8) Each blockchain node receives the new block, verifies the new blockchain according to the consensus protocol, and validates each transaction contained in the new block (e.g., to prevent double-spending); 9) Each blockchain node determines the main chain (e.g., the longest chain, or based on subtree size) and determines the order of blocks, executes the validated transactions contained in the new block, and updates the global status.

Execute-Order-Validate: Hyperledger Fabric [12] uses Execute-Order-Validate model, which has a quite different workflow: 1) A blockchain client or user creates a new transaction proposal and sends it to some endorsing peers; 2) Each endorsing peer independently receives the new transaction proposal, validates it, executes/simulates it at its local environment, generates the

execution results (i.e., write set); 3) Each endorsing peer independently generates an endorsement message containing the execution results and its signature, according to some pre-configured endorsement policies; 4) Each endorsing peer independently sends its endorsement message to the blockchain client; 5) The blockchain client receives endorsement messages from one or multiple endorsing peers; 6) If the blockchain client receives enough number of endorsement messages (e.g., as specified by endorsement policies), it generates a new transaction containing the required number of endorsement messages; 7) The blockchain client sends the new transaction to an ordering peer; 8) The new transaction will be propagated among all ordering peers; 9) Ordering peers use a consensus protocol (e.g., pBFT) to order new transactions received from different blockchain clients (e.g., first-come-first-serve) and pack them in a new block; 10) The new block is sent to and propagated within multiple committing peers; 11) Each committing peer independently validates each transaction (e.g., check that the contained execution results have not any confliction) of the new block, commits each validated transaction (e.g., record the execution results to its ledger), and accordingly updates the global status.

2.2.3. Consensus Protocols

Essentially, blockchain can be regarded as a distributed ledger technology for storing and sharing data across a set of network participants (i.e., blockchain nodes). Every blockchain node needs to maintain a local replica of all historical ledger contents. Nevertheless, a critical concern is how to preserve data consistency among all the blockchain nodes. Failure on this aspect may cause negative influences on the security and availability of on-chain data. On one hand, malicious nodes may tamper with the local records, causing conflicts between different nodes. On the other hand, users need to access on-chain data via blockchain nodes, and the inconsistency between nodes will result in different responses to users regarding the same request at the same time.

Consensus protocols can align the data states of blockchain nodes and hence address the above issues. When a node first participates in a blockchain system, it needs to download all historical ledger contents via other connected nodes for synchronization. In the daily operation of a blockchain system, data consistency between nodes is achieved by adding the same new block to the local replica. The deployed consensus protocol will select the block validator for each round, who is eligible to decide, validate, and broadcast a new block across the network.

The block validator can be selected according to different criteria, consequently, a set of consensus mechanisms is designed and implemented. For instance, Bitcoin and Dash blockchain systems both employ a Proof-of-Work consensus mechanism, where the candidates need to compete to calculate a complicated puzzle. Tezos and Polkadot blockchain systems implement a Proof-of-Stake consensus mechanism where the block validator is selected according to their staked blockchain tokens. Ethereum recently underwent a shift from Proof-of-Work to Proof-of-Stake, to improve the system's scalability and reduce energy consumption. Quorum uses Proof-of-Authority where the block validators are defined by the system administrators, since Quorum offers permissioned blockchain systems for enterprises and individuals. A consensus protocol is deployed considering multiple aspects, e.g., the usage context, system scalability, and throughput, security and accountability, etc. In recent years, there have been a lot of studies exploring the diverse consensus mechanisms [13] [14] [15].

2.2.4. Smart Contract

When Bitcoin was first released to the public, the computation capability of its underlying blockchain infrastructure was limited, which can provide merely a public ledger to store transaction information of Bitcoin's cryptocurrency [1]. Later, a programmable infrastructure named "smart contract" has been deployed to enhance blockchain technology, by enabling the execution of business logic on-chain, such as triggers and conditions [16]. Blockchain users can invoke smart contract services via transactions.

Ethereum provides a Turing-complete programming language, Solidity, for scripting smart contracts[1], which now is supported by all blockchain systems that employ the Ethereum Virtual Machine. To ease the learning curve, Solidity was designed to be similar to the existing object-oriented programming languages. A contract in Solidity can be considered as a "class" in Java. Further, Solidity offers a series of mechanisms such as interface, inheritance, exception, etc.

Based on the enhanced computation capability, existing design patterns can be applied to improve the design of smart contracts, addressing the reoccurred problems [17] [18] [19] [20] [21]. Specifically, researchers analyzed certain software attributes of smart contracts, for example, security [22], and how to apply design patterns when developing blockchain-based applications using smart contracts [23] [24].

2.2.5. Handling Heterogeneous Data with Blockchain

The deployment of the Artificial Internet of Things (AIoT) results in the generation of massive data, which belongs to different devices and is heterogeneous. The storage and exchange of such massive data from a diverse range of devices require data security to ensure smooth processing and avoid data breaches. The utilization of cryptographic algorithms may not be relevant in such scenarios due to iterative encryption and decryption overheads, and obligatory secured key exchange. Furthermore, the snapping point of the cryptographic algorithms depends upon the length of the key, which also casts the tradeoff of managing long keys. For instance, operations in AES-128 and AES-256 need 10 and 14 rounds, respectively. Blockchain is the prominent solution that helps in providing security to the data generated by AIoT devices. It utilizes the concept of verification from the group of miners to add data. To verify the data, blockchain utilizes algorithms called consensus algorithm which makes the miners reach a common agreement. This helps in mitigating the single point of failure. Further, blockchain utilizes the concept of hashes and cryptography to provide secure storage of data. Apart from this, blockchain guarantees transparency and immutability of data which mitigates the chances of corruption of stored data. However, the adoption of conventional blockchain may not suffice the need for heterogeneous data as there is a trade-off between security, decentralization, and scalability. Further, there is also a need to handle divergent data dynamically because it may diversify in terms of range, volume, entropy, and sampling rate. The utilization of conventional blockchain and the stringent consensus is not sufficient for heterogeneous data as these results in astounding consequences over processing routines, power consumption, and delay.

To resolve these issues, there is a need for solutions that select consensus mechanisms according to the needs of the data. In A-Blocks, the data is categorized based on their attributes such as

[1] https://solidity.readthedocs.io/en/develop/

range, volume as well and sampling rate, and further consensus mechanism is selected according to the stipulation of data [25]. For example, A-Blocks utilize Practical Byzantine Fault Tolerance for the data with a high sampling rate and Proof of Work for the data requiring more security.

2.2.6. Virtualization of Blockchain

Virtualization is a computing technology using which end users can create multiple instances of an entity such as hardware or software. The end users utilize resources from the decentralized pool and get a view that the resources are available at a centralized location. Virtualization is necessary for reducing the workload of the software as well as hardware and offering better uptime. Further, virtualization is also necessary for the fast deployment and allocation of resources by keeping the overall cost the same very cheap and saving energy.

To ensure public safety, there are various activities that safeguard people from accidents, disasters, crimes, and potential dangers. These activities need to be handled independently and there is a need to store the data of these activities separately. The data of these activities need to be stored securely to ensure public safety. Blockchain is a prominent solution that can handle the data of these activities securely and transparently. However, conventional blockchain does not suffice the need for these heterogeneous activities as it is not capable of performing parallel consensus and handling the data of divergent activities in a parallel fashion. Further, the utilization of separate blockchain networks for handling these activities leads to the waste of resources. Apart from this, there is a need for a solution that provides a unified view to the end users to improve their experience and the data in real time.

To ensure this, the virtualization of blockchain is necessary as it speeds up the processing by achieving parallel consensus. Virtualization of blockchain virtualizes the physical miners present in the network so that these can handle multiple blockchains in a parallel manner and the data of heterogeneous activities independently. The virtualization of physical miners allows them to perform different types of consensus mechanisms in a parallel manner for different blockchains. This helps in improving the experience of end users as different blockchains can implement divergent consensus according to the requirement of activities.

Shadows is a virtualized blockchain that utilizes smart contracts for handling different activities and providing a unified view to the end users [26]. There are three smart contracts deployed in Shadows: Antumbra, Penumbra, and Umbra which are responsible for virtualizing the physical miners and handling different activities independently. Autumbra is responsible for the creation of virtual nodes according to the requirement of divergent activities. These virtual nodes handle different blockchains in a parallel manner. Apart from this, Antumbra is also responsible for the authentication of the end users and allows only the verified users to access the data from heterogeneous blockchains. Indeed, there is a need to dynamically allocate resources to various blockchains in Shadows to ensure seamless virtualization. Penumbra is responsible for the allocation of resources to divergent blockchains dynamically. It utilizes the concept of Osmotic computing for the dynamic allocation of resources. Further, Umbra provides a unified view to the end users and allows different blockchains to interact with each other.

2.2.7. Data Storage in Blockchain

In recent years, like many other fields, there have been various advanced developments in smart public safety such as predictive analysis of machine data to prevent failure, monitoring of gas levels in industries to make the environment safer for industrial workers, and many others. With these advancements, there is a generation of massive data that needs to be stored securely. There are various solutions available such as cloud computing, file systems, centralized/decentralized databases, and many others, which are capable of storing massive data. However, along with storage, there is a need for transparency, security, and immutability to handle this data. Blockchain-enabled solutions help in achieving these features and consequently result in public safety. The primary advantages of storing data in blockchain are transparency, security, immutability, traceability, and trust.

- **Transparency:** Blockchains are transparent which means that anyone in the network can check the process by which blockchain is applied and accurately receive information which further helps in improving efficiency promptly. The transparent nature of blockchain helps in ensuring public safety because the process is visible to everyone. It is difficult for the attacker to attack the process and make changes in the underlying code. This further helps in monitoring the complete process and prevents any kind of malfunction. For example**:** In the food industry, improper monitoring of various processes such as emulsification, fermentation, mincing, and others can result in inedible food, which may affect the health of the people and harm public safety. Implementation of blockchain in food industries helps in monitoring the various processes and prevents any kind of malfunction. This helps in achieving public safety by preventing humans from eating inedible food, which may degrade their health [27].
- **Security:** As mentioned earlier, public safety means safeguarding people from various potential dangers such as accidents, hazards, crimes, and others. The security of human data from various attacks also delineates public safety. The advancement in technology not only provides comforts and conveniences to humans; however, but it also provides opportunities for criminals to commit illegal jobs such as stealing identities, fraud, violating privacy, trafficking in child pornography, and others. To prevent these cyber crimes, there is a need for a solution that stores confidential data securely. Blockchain is one of the proficient solutions, which ensures the security of the data by utilizing cryptographic algorithms and hash functions. This prevents attackers from corrupting private data and ensures public safety by protecting the individual's confidential data and identity. For example**:** In financial systems, it is difficult to manage millions of transactions and prevent attackers from forging the identity of others. The attackers may steal the identities and make huge transactions, which can result in fraud and violate the privacy of others. However, the implementation of blockchain systems prevents attackers from stealing the identity of other individuals and prevents fraud [28].
- **Immutability:** In the blockchain, one cannot alter the data added to the blockchain. This prevents the attackers from making any modifications to the data stored in the blockchain. In conventional systems such as centralized servers and databases, the attackers can make changes in the stored data, and with the advent of AIoT, there is a boost in predictive analysis based on large amounts of data. If an attacker changes the data then the results of the analysis go wrong which can harm public safety and result in accidents as well as hazards. For example**:** In vehicular networks, analysis is performed on data to predict the

traffic, anticipate the condition of the vehicle, predict faults, and others. Further, predictive analysis and decision-making are crucial in an automatic vehicle to decide various activities such as speed control, changing gears, and others. Even a diminutive error in decision-making is adverse and can result in accidents. Therefore, accurate data is crucial for which error-free data is required. To prevent the data from errors and being changed, it is necessary to make the collected data immutable. Blockchain utilizes hash technology to make the stored data immutable and prevent the same from various attackers. Indeed, immutability results in the usage of error-free data in predictive analysis and decision making which further prevents potential accidents and ensures public safety [29].

- **Traceability:** Blockchain stores timestamped data which results in the traceability of all the processes and prevents potential malfunctioning. The timestamped data gives the complete history of the processes and products and prevents the attacker from making any kind of modification to the data. The traceability feature ensures public safety as the timestamped data gives the complete history of any product or process during its lifetime and prevents the production of products, which are not suitable for humans. The production of malfunctioned products as well as processes harms the health of humans and also results in accidents and various hazards such as leakage of harmful gasses. To prevent these potential attacks, there is a need for a solution that provides complete traceability of data. As mentioned above, blockchain is one of the proficient solutions that prevent these attacks and ensure public safety. For instance**:** In the manufacturing industries, there is a need to trace the products from the seller of the raw material to the manufacturing of the end product to prevent the manufacturing of faulty products, which may harm the safety of the public. Blockchain stores the time-stamped data of each product and process which consequently helps in the complete traceability and ensures public safety by preventing various accidents, that occur due to improper tracing of data [30].
- **Trust:** Blockchain utilizes the concept of consensus algorithm which helps the different miners present in the network to reach an agreement and prevents the addition of corrupted data. Further, blockchain utilizes cryptographic functions to ensure trust and prevent corrupted data from getting added to the blockchain. This helps in ensuring public safety by maintaining the confidentiality and integrity of the private data of the public. For example**:** In the healthcare industry, it is required to maintain the integrity, confidentiality, and privacy of the patient's data. Blockchain helps in achieving the same by utilizing consensus algorithms as well as cryptographic algorithms and consequently results in public safety [31].

However, there are some challenges in integrating blockchain with AIoT to enable a Smart Public Safety System. The challenges are mainly categorized into three areas: dynamic management of data, scalable handling of AIoT devices, and secure sharing of data. The next era of blockchain-enabled public safety systems aims to ensure the privacy of the user, real-time analysis of data to prevent various hazards as well as accidents, and seamless integration of technologies.

2.2.8. Blockchain for Resource-Constrained Environments

With the advancement in technology and the development of billions of IoT devices for ensuring public safety, big data handling has become a major issue. Further, there is a need to store and

securely manage data as there are chances of colluding peers to attack the system and corrupt the data. This harms public safety as cyber-attacks lead to the leakage of private data. Further, the modification in data leads to wrong decisions which can further result in accidents and hazards.

Blockchain acts as a prominent solution that prevents attacks on the data as it is based on cryptography and hash technology. However, there is a need to achieve consensus in blockchain to store data. Achieving consensus is a computationally expensive task and resource-constrained devices are not capable of performing such jobs. To resolve these issues blockchain can be integrated with the cloud such that the former can borrow resources from the latter and perform consensus.

Further, the data generated by AIoT devices to achieve public safety is massive. There is a need to handle such massive data without harming its integrity. There are various solutions to resolve this issue. These solutions are majorly categorized into four categories:

- **Synergy with the cloud:** The data is transferred to the cloud for storage after regular intervals of time. Blockchain only stores the most frequent data and offloads the remaining data to the cloud for storage as well as analysis. Further, the blockchain layer also leases resources from cloud technology and utilizes those for achieving consensus and storing massive data.
- **Integration with Inter-Planetary File Systems (IPFS):** To handle massive data over resource-constrained devices, blockchain integrates the Inter-Planetary File Systems (IPFS). The integration of IPFS and blockchain technology helps blockchain to scale up and handle the data of millions of devices.
- **Hierarchical Blockchain:** To deploy blockchain over resource-constrained devices and enable it to handle massive data, layering of the same is the prominent solution. In layered blockchain or hierarchical blockchain, various tasks such as achieving consensus, computation, payment, and storage are performed at separate layers. This helps the blockchain to split the load over various layers and handle massive data.
- **Storing Meta Data:** The offloading of data to the cloud and integration of blockchain with IPFS vanishes the major advantage (decentralization) of blockchain as well as adds extra overhead for fetching data. To resolve these issues metadata can be stored rather than complete data in the blockchain. The utilization of various machine learning models such as LSTM (Long Short-Term Memory), ARIMA, and others to generate the actual data from the meta-data can be used to regenerate the actual data again [32].

3. Use Cases of Using Blockchain for Public Safety

3.1. Blockchain for Gun Ownership and Tracing

Gun violence is a long-standing public safety concern and a security threat, as noted in several studies [33]. This reinforces the importance of designing systems that can be used to support firearm tracing, for example in ensuring complete, accurate, and immutable documentation of firearm-related metadata and sales data. For example, a recent report released by the U.S. Government Accountability Office noted that:

> *firearms trace results have provided investigative leads and helped law enforcement agencies in partner countries to prosecute violent criminals, in some cases by linking disparate criminal acts committed with the same firearm*[2]

As we posited in a recent work, blockchain can be used to facilitate gun ownership, tracing, and investigations by providing a mechanism to manage gun registry, ownership, and transfers [34]. In the conceptual blockchain-based system (see *Figure 2*), for example, we demonstrate how smart contracts can be used to capture firearm sales and facilitate the tracking of firearms transactions. In other words, blockchain can be used to improve data integrity and trust, and consequently, it becomes easier to successfully track the path of a crime gun along its chain of custody to a potential crime suspect.

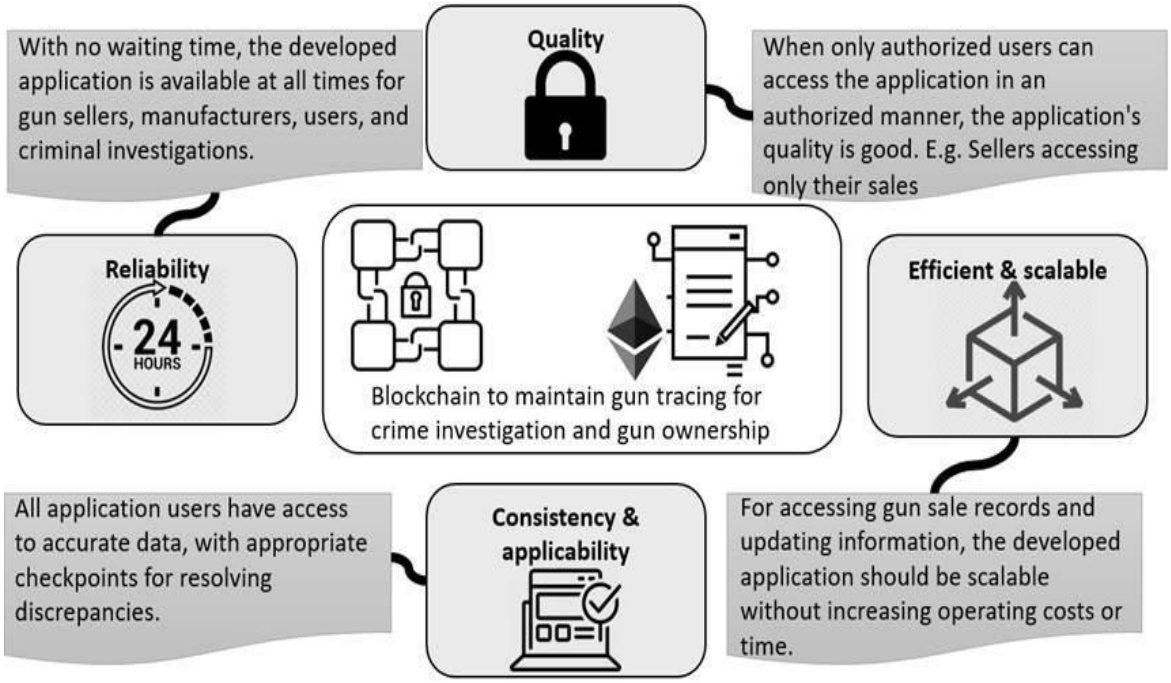

Figure 2. Conceptual Blockchain-based Firearm Ownership and Tracing System [34]

However, to achieve the desired long-term benefits (e.g., reduction in gun violence as a result of improved gun-related investigative processes and successful prosecutions of gun-related crimes), commitments and involvements of a broad range of stakeholders, such as those from national security and law enforcement agencies and the relevant industries (e.g., firearm manufacturers and firearms retailers), are crucial. For example, involving key stakeholder groups in the co-design methodology allows system designers to work closely with these stakeholders (e.g., end-users in law enforcement, policy- and decision-makers) and collaboratively identify and assess the associated near-, mid-, and long-term system needs, while also taking into consideration operational and regulatory priorities, preferences and requirements.

[2] https://www.gao.gov/assets/gao-22-104680.pdf (page 29, last accessed November 6, 2022)

3.2. Blockchain for Forensics

Predicting the future is never an easy task, but one can say with high confidence that as our society becomes increasingly smarter and more interconnected (e.g., due to our reliance on technologies), there will be more opportunities for exploitation and the cyber-physical threat landscape is likely to evolve. In other words, threats to our society and nation can come from unexpected sources and directions – a 360-degree challenge, since technologies can be used as an extension to facilitate and enhance traditional forms of warfare, as well as create new forms of warfare.

Box 1: A hypothetical example of a coordinated terrorist attack

Setting: A large state (e.g., Texas) that comprises several smart cities. In each of these smart cities, there are a large number of smart Internet-connected devices (e.g., IoT devices in the city, IoT devices worn and carried around by human citizens, and IoT devices embedded within the bodies of human citizens). These devices are typically connected to the state's critical infrastructure sectors, and these devices are tasked with collecting and sensing data before sending them to some computationally powerful devices (e.g., servers) for further analysis.

Attack scenario: A group of attackers successfully discover and/or have access to the following vulnerabilities (including zero-day vulnerabilities):

- Vulnerabilities on unmanned autonomous and aerial vehicles of a certain make and model, which can be exploited to pinpoint the vehicles as well as take over control of these vehicles.
- Vulnerabilities in the cities and/or state's communication systems that can be abused by the attackers to disrupt real-time communications among the frontline and emergency response teams and the residents, for example by jamming the communications or injecting fake audio or video messages (or messages that impact on our five senses).
- Vulnerabilities in wireless charging stations and popular consumer devices (e.g., next-generation smart lenses/glasses), or charging stations for electric vehicles, which can be exploited to result in electricity overloads, which can potentially result in human casualties.
- Vulnerabilities in devices (e.g., smart weapons) and systems (e.g., servers) that allow the attackers to obtain unauthorized access to the data, take over control of the systems (e.g., to fire indiscriminately), and inject malicious data to taint or corrupt the training of the underlying AI model so that the attack is considered normal by the AI defensive system (also referred to as adversarial machine learning in the literature).

The attackers can then attempt a coordinated attack, targeting several cities simultaneously during peak hours by taking over control of the vulnerable autonomous and aerial vehicles in the vicinity to crash into buildings and/or pedestrians, while at the same time disrupting the cities and/or state's communication systems. This will likely maximize the impact of the attacks, by creating chaos and confusion. In addition, the attackers can also cause devices to explode or malfunction, due to electricity overloads. Any AI-driven defensive systems monitoring the network/systems may not detect such attacks, due to the use of adversarial machine learning techniques.

In addition to causing mass casualties, politically- or ideological-motivated attackers can also attempt to carry out targeted assassination against key position holder(s), for example by seeking to exploit vulnerabilities in devices that can be turned into improvised explosive devices (IEDs) – see Box 2.

Box 2: A hypothetical example of targeted assassination against key position holder(s)

Setting: Some politically- or ideological-motivated attackers wish to make a political statement, and/or coerce a nation-state (or government) into aborting certain operations.

Attack scenario: The attackers successfully discover and/or have access to the following vulnerabilities (including zero-day vulnerabilities):

- Vulnerabilities in smart home devices, such as Internet-connected cooking appliances (e.g., stoves and cooktops), or smart office devices (e.g., by releasing certain materials that can cause a chemical reaction), which can be exploited to result in electricity overloads, gas leaks and/or poisonous gas release.
- Vulnerabilities in the targets' embedded or wearable devices (e.g., next-generation smart lenses/glasses, medical devices such as pacemakers, and prosthetic body parts), which will allow the attackers to take over control of the targets' actions (e.g., commit suicide).
- Vulnerabilities on unmanned autonomous and aerial vehicles of a certain make and model, which can be exploited to take over control of these vehicles as well as to pinpoint the target's location.

The attackers can then carry out a coordinated series of attacks, targeting the environment of the targets (e.g., home via smart home devices and transportation), and the actual individual (e.g., via the targets' embedded or wearable devices),.

The attackers can also seek to compromise other individuals (e.g., joint staff or attaché personnel with access to the target), for example by taking over control of these individuals' actions to carry out the assassination.

National security and/or public safety solutions are seldom absolute. When a cyber-related security incident occurs, we need to conduct an investigation to establish the root cause of the incident and how it could be prevented in the future. To examine the causes of an incident, investigators rely on the residual data from systems, affected by the incident and supporting systems. As we previously noted [35] [36], such data, which might not always be available for a variety of reasons include short data retention times, a lack of extraction capabilities, and the costs associated with conducting such investigations. Hence, moving forward we need to implement forensic-ready systems and infrastructure. Such a concept (also referred to as forensic-by-design) is analogous to secure-by-design and privacy-by-design, where requirements for forensics are integrated into relevant phases of the system development lifecycle, to develop robust forensically-ready systems (e.g., a digital forensic black-box). Due to the underpinning properties of blockchain (e.g., immutability), the latter can be used to support the design of forensically-ready systems and complement other existing digital forensic readiness strategies, such as those described in ISO/IEC 27043:2015.

In the context of a smart grid system within a smart city, *Figure 3* explains how a digital forensic black box (implemented as a secure multi-tenant storage in the figure) can be deployed. In such a setting, artifacts of forensic interest/relevance can be identified and collected using AI agents, and these artifacts can then be stored in some secure locations based on blockchain or distributed ledger since the latter can be utilized to ensure the integrity of the stored artifacts. The data stored in these digital forensic black boxes can also be used to train AI-driven cyber defensive systems to identify future threats and facilitate future cyber investigations and attributions.

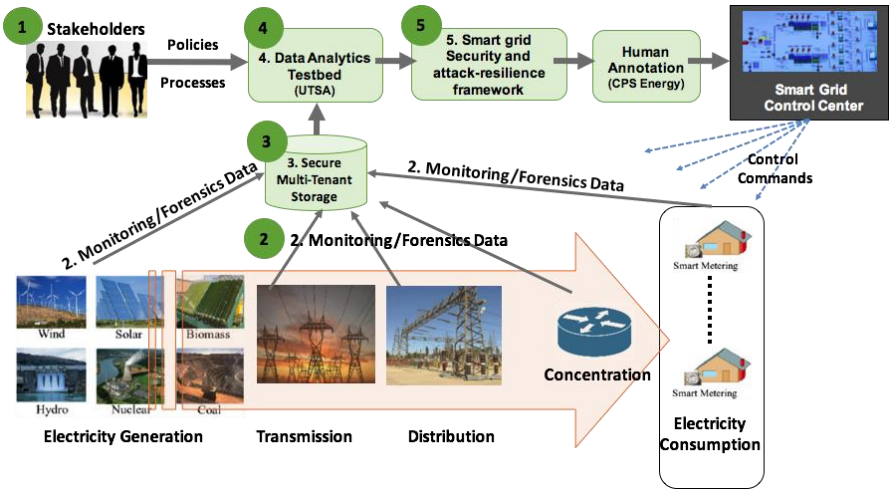

Figure 3. Conceptual Forensic-driven Security Monitoring Framework [37]

3.3. Blockchain for Wireless Networks with Public Safety Perspectives

Blockchain technology [38] [39], by combining with other emerging technologies such as software-defined networks, edge, and distributed computing for wireless networks [40] [41] [42], is regarded as a mechanism to provide robust resource allocation for ensuring public safety communications. In case of an emergency, the wireless network could be overloaded because of its heavy use where we need to ensure that wireless resources are reserved/available to the emergency response team for their timely communications and operations. Furthermore, blockchain-enabled wireless resource allocation can prevent double-spending/allocation of wireless resources for different purposes at the same time. Because of the nature of the digital ledger, any related actions could be traced back if needed for accountability or better planning for future activities. The blockchain-based wireless networks are emerging for different applications such as vehicular networks while providing verifiable secure vehicle-to-everything communications by using non-private information such as the number plate of the vehicle (like in ParkMobile App or E-ZPass systems use) for integrity and accountability [42]. Another application of blockchain-enabled wireless networks is healthcare for emergency systems related to public safety [39].

3.4. Blockchain for Distributed AI/ML for Public Safety

An Artificial Intelligence system utilizes advanced computer hardware to automatically study a large amount of various data for different purposes, including classification, clustering, decision-making, deep learning (DL) [43], supervised learning [44], unsupervised learning [45], and reinforcement learning [46]. Blockchain can assist AI systems for public safety by providing a distributed infrastructure for secure data sharing and an essential programmable platform with characteristics of immutability, auditability, traceability, etc. [47].

In recent years, researchers have been exploring integrating blockchain and AI to enhance public safety services. Two significant domains are the Internet of Things (IoT) and healthcare [48]. For instance, a permissioned blockchain network can conduct identity authentication when new IoT devices join the network, and IoT devices can upload the captured data to the blockchain, while the edge cloud server can acquire the data for antisocial and abnormal behavior detection [49]. In this manner, blockchain and AI-assisted IoT systems can realize social distancing schemes monitoring and tracking to combat COVID-19 [50], or even perform penalties [51]. AI can be used to analyze patients' medical images and symptoms for efficient and effective treatments, while blockchain can provide healthcare data sharing with reliable data management solutions [52]. In addition, blockchain aligns well with federated learning, where machine learning tasks are assigned to edge clients, and a cloud server is responsible for model aggregation. A blockchain-based federated learning system can be used to analyze COVID-19 medical images in the way that clients train local models and send the updated parameters to the cloud server, where the parameters are aggregated to form a new global model [53]. Hereby, the hash values of model parameters are recorded in the blockchain, to achieve data provenance, auditability, and accountability.

3.5. Blockchain-Enabled Public Health

In healthcare, the deployment of various AIoT devices for the collection, analysis, and utilization of patient health data results in the generation of massive data. The data is generated by various devices such as telepath tools, blood glucose monitors, wearables, health applications, and home scales. The generated data has colossal potential for predicting the health of the people and ensuring their safety. The extraction of relevant information from this massive data requires analysis and corruption in the same leads to erroneous analysis and mistaken discussions. To prevent this there is a need for a solution for sharing and storing precisely. Blockchain is a prominent solution that prevents the unauthorized alteration of data and prevents the same various attacks. It has the potential to impact healthcare in a positive direction and improve the health of the public by integrating with various sectors of public health such as remote monitoring, verification of credentials of medical staff, supply chain management, health records management, and insurance settlements.

Remote Monitoring: With the advancement of technology, the employment of remote health monitoring systems has become the biggest trend with the help of which the measurement of patient vitals becomes easier. Various sensors are deployed in the wearables which measure the vitals of the patients and share the same with the medical officers for preventive and proactive care. However, the privacy of the individual and the security of vital data are major concerns. Tampering with data and the creation of false information from the same harm public safety. In certain scenarios, where connected wearables are responsible for the generation of alarms in emerging situations, for instance, the generation of alarms in the case of heart attack are resilient

to various attacks such as distributed denial of service which has a prominent impact on public safety. Indeed, there is a need for secure data storage to ensure public health and safety. The utilization of hash functions and cryptographic methods provides secure storage of the data of the individuals and prevents tampering with the same. Attackers can't tamper with the data which is stored in the blockchain. Further, the decentralized storage of the data prevents the same from DDoS attacks.

Verification of Credentials of Medical Staff: In healthcare, it is necessary to verify the credentials of medical professionals to ensure the safety of the public. The involvement of any intruder may result in the leakage of private data of the patients as well as risk their lives. The experience of the medical officers is a crucial factor on which the lives of the patients are dependent. Therefore, there is a need for a tracking and verification system that verifies the staff of healthcare to prevent the involvement of intruders. Blockchain is a competent solution for credentialing the staff of healthcare by storing their details in an immutable fashion. The intruders are not able to corrupt the data and forge the details stored in the blockchain. The forging of data risks the lives of the patients as there are chances that medical officers practice in various healthcare without having proper training and qualifications. Further, there are chances of malpractice insurance and hospital affiliations which risks public health and safety. To prevent this, blockchain stores the data along with timestamps and utilizes a consensus mechanism to verify the licenses of hospitals as well as practitioners. Apart from this, the credentialing process results in the addition of redundant data to the verification system. This results in the addition of extra overhead in the process of verification. To prevent this, the blockchain system adds the data of staff with timestamps and prevents redundancy of the data. This also fastens the process of credentialing and prevents the possibility of malpractices in healthcare.

Supply Chain Management: The provenance of medical equipment and medicines is important for ensuring their authenticity and the safety of the public. Blockchain provides complete transparency and traceability of products by storing timestamped data. The utilization of a blockchain system for tracing the medical products in each stage prevents the counterfeiting of the prescription and prevents thousands of deaths. The integration of AIoT and blockchain systems in the supply chain management of medical products results in:

- Patient Confidence: Patients can track their medicines at each stage such as manufacturing, shipping, and others. This helps in building confidence among them and ensuring their safety.
- Compliance: Blockchain also helps in the enforcement of law between the manufacturers of medical tools and the pharmaceuticals which helps in ensuring the safety of the public.
- Optimization: The utilization of blockchain for the management supply chain helps in the prediction of demands of the products and prevents any kind of delay in the delivery of products. The prediction of demands for health equipment and goods is necessary for the medical field to prevent any kind of shortage which may risk the health of the individual during an emergency.

Health Record Management: Due to improper management of data and incomplete medical history, doctors are not able to diagnose the patients. This results in poor coordination between the medical officers and erroneous medical records of the patient which further may result in the improper diagnosis of patients and sometimes leads to death. In such a situation, blockchain proves to be a proficient solution as it provides immutable storage of the health records of the

patients along with timestamps. This also allows various medical officers to coordinate with each other without any conflict and diagnose the patients.

Insurance Settlement: Blockchain helps in settling the claims and medical bills of the patients without any disputes. It also prevents the patients from making double payments and claims for duplicate bills. Blockchain makes immutable storage and prevents any kind of fraud in the healthcare systems which further ensures public safety. Blockchain not only ensures public health; however, also protects the data from fraud and ensures public safety.

3.6. Blockchain for Safety of Industrial Workers

Modern manufacturing systems comprise an assortment of various Industrial IoT (IIoT) devices and sensors, which require data technology, information technology, and operational technology for their successful implementation. The various features of blockchain make it a promising solution to enable these technologies by enabling both manufacturing service and device-level data transmission. Specifically, the sensors' data stored in the blockchain is utilized to predict the quality of the job and store the certificate in the blockchain for the continuous monitoring of the jobs to provide better efficiency. Blockchain technology enables us to achieve the following features:

- Traceability and Transparency: Blockchain stores the data of the sensors along with the timestamp, which allows tracing the value of data at any instant in time. Also, the transactions and the data stored in the blockchain are transparent. Anyone present in the network can see the history and the details of any transaction. Using the timestamped data, it is easy to achieve a high level of transparency and traceability by ensuring data integrity. Further, the complete transparency and tracking of the critical processes involved in manufacturing industries (automotive) prevent the failure of machines. This further helps in preventing accidents and hazards and faulty machines may sometimes result in accidents.
- Security: In manufacturing processes, even a tiny change in the value of data leads to a hazard and risks the health of the industrial workers. The data in the industry should be immutable and secure. Blockchains store data by performing cryptographic operations. Blockchains use hash functions to store the data. Each block contains the previous block's hash. Even a tiny change in the value of data results in a large deflection in hash value ensuring high-level security in data.
- Distributed Nature: Distributed nature is the essential feature of blockchain. The data is present over various nodes, and these nodes initially validate data and then only store it. This helps in protecting the data of industrial workers from any kind of attack and forgery which further helps in ensuring their safety.

3.7. Blockchain for Disaster Relief and Recovery

The use of blockchain technology in emergency management including disaster relief and recovery provides immutable transparent records accessible by all types of agencies involved to facilitate more efficient and coordinated use of resources. This way the resources dedicated to an area and by whom in a disaster relief scenario can be illustrated readily, Transparent record keeping for all kinds of transactions related to data (for example donations and spending, etc.)

involved in disaster relief would minimize corruption can reduce resource diversions and corruption in these types of scenarios

There have been several projects already underway from various public safety-related and other organizations such as Federal Emergency Management Agency (FEMA)'s Public Assistance program testing blockchain to track where resources are going after a disaster; Centers for Disease Control and Prevention (CDC) has been piloting blockchain to collect and communicate data to entities who treat patients in disaster relief scenarios, including local public health agencies, hospitals, and pharmacies; United Nations Children's Emergency Fund (UNICEF) testing blockchain to track the status of international grants in a secure way that is accessible by public.

There is an enormous opportunity here to investigate and identify how more and more public safety agencies at all levels can use blockchain in recording, safekeeping, and using their data [63]. The blockchain technology can be adopted as a universal system across organizations to coordinate resources in an emergency.

3.8. Blockchain for Public Safety Testbeds

Public Safety Testbeds (PSTs) have emerged as a crucial tool for enhancing emergency response and disaster management by providing a platform to develop, test, and evaluate new technologies and applications for emergencies such as natural disasters, terrorist attacks, and public health emergencies. These testbeds provide a platform to experiment with potential solutions in a controlled environment before deploying them in real-world situations. PSTs involve a range of technologies, including sensor systems, communication technologies, data analytics, AI, and machine learning algorithms [54] [55].

Blockchain technology can help reinforce the essential features of PSTs, including data integrity, security, and interoperability. By ensuring the accuracy and security of data through an immutable and tamper-evident ledger, blockchain can bolster the essential aspects of a PST.

Data Integrity: PSTs rely on data from sensors, cameras, and other devices, as well as data from government agencies, community organizations, and residents. To ensure the accuracy, reliability, and trustworthiness of data, cryptographic techniques such as hashing and digital signatures can be applied through blockchain. Blockchain technology can create an unalterable and secure ledger of all transactions, and the consensus of the network is required to modify or delete any data, thus guaranteeing its security and immutability.

Data Security: The utilization of sensitive and confidential data in public safety testbeds renders them vulnerable to unauthorized access, thereby endangering emergency response and public safety operations. The leakage or hacking of confidential information about emergency response plans or procedures can be exploited by malicious actors to compromise the effectiveness of these operations, thereby exposing individuals' lives and property to imminent risk. Furthermore, public safety testbeds often incorporate nascent and innovative technologies, such as drones, IoT devices, and machine learning algorithms, which can potentially introduce new security vulnerabilities and risks.

Blockchain can provide security benefits to Public Safety Testbeds (PSTs) by employing 3 key approaches.

- Through encryption and the use of private keys, blockchain can restrict access to authorized users only and prevent unauthorized access to the sensitive data stored within the system. Additionally, smart contracts can be utilized to regulate access to data based on predetermined criteria such as job function or role.
- Blockchain technology guarantees data immutability, ensuring that data cannot be tampered with or deleted without the consensus of the network, thereby ensuring the security and integrity of the stored data.
- The decentralized nature of blockchain allows for multiple copies of data to be stored across the network, thus mitigating the risk of a single point of failure and making it more difficult for hackers or malicious actors to gain access to the system.

Interoperability: In the context of PSTs, which are often used in emergency response scenarios, interoperability is a critical feature that enables different agencies to work together effectively. To achieve this, blockchain technology provides a decentralized platform that ensures the verifiability and immutability of all data and communication exchanged between different parties. This can help to build trust and promote collaboration between agencies. In addition, smart contracts can be used to facilitate interoperability by automating the exchange of data between different systems. For example, a smart contract could be programmed to send data from one organization's system to another when a certain trigger condition is met, such as the detection of a potential hazard. This automated process could enable emergency responders to respond to emergencies quickly and effectively.

Blockchain technology comes with challenges, including the potential emergence of "walled gardens" or closed technology platforms that do not adhere to common security, privacy, and data exchange standards [56]. Such platforms can restrict the growth and availability of a diverse, competitive marketplace of interoperable solutions that the government and industry can leverage for cost-effective and innovative services based on blockchain technologies. Other challenges include issues around scalability, and the high computational and energy costs associated with blockchain, not to mention the public acceptance and trust in this new technology. Addressing these challenges requires ongoing research, development, and collaboration among academics, the public safety community, industry professionals, regulators, and other stakeholders.

3.9. Blockchain for Public Safety Analytics

Public safety analytics involves the application of data analysis techniques to extract meaningful insights, patterns, and trends in areas related to public safety. This field spans various applications, including crime prevention, emergency response, disaster management, and risk assessment. Blockchain technology has the potential to transform public safety analytics by enhancing data integrity, security, and transparency.

Blockchain-enabled data analytics platforms empower public safety agencies to analyse large datasets from diverse sources like crime statistics, social media feeds, and sensor networks. Leveraging blockchain's transparency and data integrity features, these platforms offer valuable insights into emerging threats, crime patterns, and community needs.

The use of data analytics tools in blockchain technology allows investigators and regulatory professionals to delve deep into the complex web of transactions within distributed ledger systems. This enables them to identify interrelationships between thousands of transfers and surface connections, unlocking profound insights from blockchain activity. As adoption increases, there is a growing urgency for analytics to harness the shared nature and enhanced transparency of blockchain, providing actionable insights that support mission goals. Ultimately, mastering analytic tools empowers professionals to gain a deeper understanding of data, contributing to more effective decision-making in the realm of public safety.

4. TECHNOLOGY GAPS

4.1. Introduction

Public safety is composed of different agencies working to uphold the safety of the public. On a high level, it could contain climate change, environmental sustainability, agriculture safety, industrial supply chain safety, carbon neutrality, nuclear safety, etc. On the community level, it includes food safety, public health safety, information safety, public road traffic safety, construction safety, etc. In its current form, public safety is controlled and managed by a hierarchical, authority-based bureaucracy.

As a fast-growing trust-enhancing technology, blockchain is researched and considered to provide overturning solutions for safety and security issues. With different levels of involvement in blockchain technology, recent research could be divided into three mainstream directions. The most intuitive way is to build platforms that directly utilize the blockchain to protect data privacy and provenance, etc. This direction is the most proven and mature one in that many demos and even commercial products are developed. It only changes the technique, but does not modify underlying system logic, i.e., adopt blockchain to traditional solutions. A further step is to use blockchain as an infrastructure and build a novel public safety platform on it, e.g., a public traffic flow system with smart contracts built on blockchain, which is autonomous to serve every citizen equally and improve transportation safety. This kind of solution does not alter traditional service and management architecture, but changes service logic and model. This direction is just at its start, with many research demos and trial products. Another form overturns the current management system, which is based on web3 with blockchain as the underlying supporting technology. Generally, this kind of solution is based on decentralized autonomous organizations (DAOs), e.g., a DAO project that aims at raising funds for protecting the rainforest in which everyone could participate with trust and financial incentives provided by Web3. It changes the entire system, from technology, process model, and management to governance. DAO-based solutions are just at the beginning, as most of the projects are still in their exploration step.

4.2. Blockchain Solutions for Public Safety

4.2.1. Building Blockchain-Assisted Platforms

The most intuitive blockchain application is to directly build platforms and frameworks on the blockchain. Originally, many of these solutions targeted improving security aspects such as utilizing blockchain to directly protect data integrity, privacy, and transparency by blockchain properties, e.g., immutability and decentralization. Some of these platforms focus on safety

issues, such as food safety and public health safety. For example, Wang et al. [57] introduced a fish provenance and quality tracking project based on blockchain, attribute-based encryption, IoT, and artificial intelligence. In this case, two blockchains cooperate. The blockchains serve as the component to provide confidential, tamper-resistant data service, and they also manage keys. In addition to blockchain, many other techniques are adopted, such as NFC tags used to identify fish and narrow-band-IoT devices to detect fish quality. This is a typical case that utilizing blockchain to improve the food safety aspect of public safety.

In addition, blockchain is also utilized in other public safety use cases, such as gun tracking [58], and parking lot security [59]. In the blockchain-assisted gun tracking proposal, blockchain is used to store the gun transaction history safely, which local authorities can track every gun transaction more easily, hence reducing the crime rate. The idea in this proposal is close to the fish tracking system [57], blockchain is used as a middleware or component to achieve security storage and provenance.

4.2.2. Blockchain as an Infrastructure

In addition to the most intuitive solution that utilizes blockchain as a component to safely store data and history, some papers proposed a more complex solution that blockchain serves as an infrastructure to support upper applications. For example, Pournaras proposed an augmented democracy paradigm [60] in which blockchain is used to achieve proof of location and witness, further supporting situation awareness and collective decision-making. The author also presented an experiment to test cycling road safety and found the risk that citizens witness highly matches the empirical evidence of cycling accidents, and suggested this blockchain-based collective decision model has a strong potential to verify the status of urban space, which could help public safety in smart cities. In ParkChain [59], the blockchain provides a trusted decentralized network and interface for overlaying DApps. The parking service is controlled by smart contracts to be autonomous, where no centralized controller exists. In their paper, a secure, decentralized trustable parking sharing platform is built, not only the public parking area, but private parking spaces could join the sharing, in which parking lot safety is also protected.

Blockchain could be more than the infrastructure of smart contracts. SSI (Self Sovereign Identity), a self-sovereign and privacy-friendly alternative to the centralized identity management system proposed by W3C (World Wide Web Consortium) that facilitates secure digitized credential issuance and verification without having a centralized authority, relies on blockchain infrastructure. Currently, individuals must register a large amount of identity across the internet, e.g., Twitter, Facebook, and Google accounts. The user cannot control their data, because all the information is fetched by the large service provider during their usage. Established on blockchain, SSI could be designed properly to protect users' sensitive data. Mukta et al. [61] proposed an SSI platform that could control selective disclosure. A user may have multiple DIDs (Decentralized IDentifier), each of which represents a different identity. For instance, Alice might hold two DIDs, one as a university student, and the other as a citizen. By this design, it helps to minimize the risk of information leakage.

4.2.3. DAO-Empowered Solutions

In addition to the platform built with blockchain functional components, Decentralized Autonomous Organizations (DAOs) extend the decentralization from blockchain technologies to the entire government. Originally from the Ethereum community, a large number of Internet-native DAOs have been built, with a great portion of them concerning long-term public safety crises, including marine protection, environmental governance, and agricultural production. Diatom DAO is a well-operated DAO that aims to incentivize the removal of plastic from the ocean. A reliable decentralized supply chain incentive by Plastic Removal Credit (PRC) is built in Diatom DAO to promote the circle of the exchange of funds, digital assets, and plastic removal credit. Ecorise is an example that raises funds for the purchase of nature reserves and achieves co-ownership and governance of the lands through fundraising, minting, voting, and converting the purchased land into NFT.

A large number of conventional organizations have committed to various long-term public safety projects, commonly managed by traditional non-profit charitable organizations. These DAOs share similar goals with them in public safety protection but different approaches. Powered by blockchain technologies, smart contracts, and distributed ledgers replace a large part of the traditional government functions in conventional organizations by writing rules and execution methods into code and recording all key activities on the blockchain. Although this has been reflected in many blockchain-powered platforms, the reduction in centralized and manual management in DAO has further elevated the idea of decentralization from blockchain technology to organizational structure and governance. Different from conventional bureaucratic government, DAOs result in the most attractive feature of decentralization.

The long-term public security projects managed by DAOs with decentralization as the core feature have some advantages over projects in conventional centralized organizations. First of all, strict hierarchical management in conventional organizations increases the threshold for ordinary people to participate in core decision-making and implementation, while flat management and decision-making allow ordinary participants to be closer to the core of the project rather than just playing the role of a funder. Second, long-term public safety projects often require large financial flows. With transparency features in distributed ledger and automation in smart contracts, corruption can be greatly reduced. Furthermore, conventional public safety projects are often operated by non-profit organizations. Reducing manual maintenance and supervision can provide more utility funds for project implementation. In addition, if the flexible economic cycle of public safety DAOs is maintained, more professionals and funds can be attracted to participate in the operation.

4.3. Future Perspectives

As introduced, a large amount of blockchain-based public safety solutions are being researched and proposed, which mainly focus on three orientations.

From the long-term perspective, the solutions that directly build blockchain-assisted platforms are more likely to be utilized by consortia, which might influence several aspects of public safety, e.g., supply chain safety, food safety, and information safety that need several large suppliers to cooperate.

The second kind of solution that uses blockchain as an infrastructure and builds platforms on it is likely to improve public safety at a higher level, e.g., transportation safety perception in the local

community, worldwide safe personal digital identity, etc. With the development of blockchain and related technology, blockchain has the trend to be considered as a fundamental facility to provide trust and be integrated into the current service model (e.g., cloud computing, decision-making) to support superior public safety applications.

The overturning DAO and web3-based projects as the third kind of solutions might potentially solve some high-level safety issues that the current authority and management system cannot address in the future. In the long term, it could gradually change current public safety service models from hierarchical, centralized, and authority-based to autonomous, decentralized, and civic-participated ones, in which everyone can directly participate and benefit.

5. CONCLUSIONS AND RECOMMENDATIONS

As explained in the present document, blockchain technology has great potentials for public safety. In fact, a number of public safety use cases such as public health, disaster relief and recovery can be benefited from the use of blockchain technology for multiple purposes such as traceability and increased trustworthiness. To fully leverage blockchain technology for public safety, some recommendations on future work include:

- Frome technology perspectives, it is recommended to investigate building blockchain-assisted platforms, blockchain as an infrastructure, and DAO-empowered system. New solutions on these three areas will promote the use of blockchain for public safety.
- It is also recommended that proof-of-Concepts and testbeds of using blockchain technology for selected public safety use cases be developed and showcased.
- New services, new data models and new interfaces in blockchain-based public safety systems need to be identified and standardized.

6. REFERENCES

[1] *Nakamoto S, Bitcoin A. A peer-to-peer electronic cash system[J]. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 2008, 4: 2.*

[2] *Tschorsch F, Scheuermann B. Bitcoin and beyond A technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2084-2123.*

[3] *Distributed Ledger Technology: beyond blockchain, Technical Report, 2016. UK Government Chief Scientific Adviser.*

[4] *Staples M, Chen S, Falamaki S, et al. Risks and opportunities for systems using blockchain and smart contracts. Data61[J]. CSIRO), Sydney, 2017.*

[5] *Li X, Jiang P, Chen T, et al. A survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2020, 107: 841-853.*

[6] *Reyna A, Martín C, Chen J, et al. On blockchain and its integration with IoT. Challenges and opportunities[J]. Future generation computer systems, 2018, 88: 173-190.*

[7] *Lu Q, Xu X. Adaptable blockchain-based systems: A case study for product traceability[J]. Ieee Software, 2017, 34(6): 21-27.*

[8] *Xu X, Lu Q, Liu Y, et al. Designing blockchain-based applications a case study for imported product traceability[J]. Future Generation Computer Systems, 2019, 92: 399-406.*

[9] *Matsumoto S, Reischuk R M. IKP: turning a PKI around with decentralized automated incentives[C]//2017 IEEE Symposium on Security and Privacy (SP). IEEE, 2017: 410-426.*

[10] *Liang X, Shetty S, Tosh D, et al. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability[C]//2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). IEEE, 20.*

[11] *Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data[C]//2015 IEEE Security and Privacy Workshops. IEEE, 2015: 180-184.*

[12] *E. Androulaki, et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," In Proceedings of the Thirteenth EuroSys Conference 2018 (EuroSys '18) (https://doi.org/10.1145/3190508.3190538).*

[13] *Bach L M, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms[C]//2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Ieee, 2018: 1545-1550.*

[14] *Wang W, Hoang D T, Hu P, et al. A survey on consensus mechanisms and mining strategy management in blockchain networks[J]. Ieee Access, 2019, 7: 22328-22370.*

[15] *Lashkari B, Musilek P. A comprehensive review of blockchain consensus mechanisms[J]. IEEE Access, 2021, 9: 43620-43652.*

[16] *Omohundro S. Cryptocurrencies, smart contracts, and artificial intelligence[J]. AI matters, 2014, 1(2): 19-21.*

[17] *Eberhardt J, Tai S. On or off the blockchain? Insights on off-chaining computation and data[C]//European Conference on Service-Oriented and Cloud Computing. Springer, Cham, 2017: 3-15.*

[18] *Mühlberger R, Bachhofner S, Castelló Ferrer E, et al. Foundational oracle patterns: Connecting blockchain to the off-chain world[C]//International Conference on Business Process Management. Springer, Cham, 2020: 35-51.*

[19] *Xu X, Pautasso C, Zhu L, et al. A pattern collection for blockchain-based applications[C]//Proceedings of the 23rd European Conference on Pattern Languages of Programs. 2018: 1-20.*

[20] *Bartoletti M, Pompianu L. An empirical analysis of smart contracts: platforms, applications, and design patterns[C]//International conference on financial cryptography and data security. Springer, Cham, 2017: 494-509.*

[21] *Wöhrer M, Zdun U. Design patterns for smart contracts in the ethereum ecosystem[C]//2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CP.*

[22] *Wohrer M, Zdun U. Smart contracts: security patterns in the ethereum ecosystem and solidity[C]//2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 2018: 2-8.*

[23] *Zhang P, White J, Schmidt D C, et al. Applying software patterns to address interoperability in blockchain-based healthcare apps[J]. arXiv preprint arXiv:1706.03700, 2017.*

[24] *Liu Y, Lu Q, Xu X, et al. Applying design patterns in smart contracts[C]//International Conference on Blockchain. Springer, Cham, 2018: 92-106.*

[25] *R. Tapwal, P. K. Deb, S. Misra and S. K. Pal, "Amaurotic-Entity-Based Consensus Selection in Blockchain-Enabled Industrial IoT," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11648-11655, 15 July 15, 2022, doi: 10.1109/JIOT.2021.3131501.*

[26] *R. Tapwal, P. K. Deb, S. Misra and S. K. Pal, "Shadows: Blockchain Virtualization for Interoperable Computations in IIoT Environments," in IEEE Transactions on Computers, 2022, doi: 10.1109/TC.2022.3184271.*

[27] *C. Stach, C. Gritti, D. Przytarski and B. Mitschang, "Trustworthy, Secure, and Privacy-aware Food Monitoring Enabled by Blockchains and the IoT," IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2020, p.*

[28] *Basumatary and S. Joshi, "Adoption Of Blockchain In Trade Finance And Its Impact On Financial Decision Making," 2022 International Conference on Decision Aid Sciences and Applications (DASA), 2022, pp. 556-559, doi: 10.1109/DASA54658.2022.9765150.*

[29] *D. Chulerttiyawong and A. Jamalipour, "A Blockchain Assisted Vehicular Pseudonym Issuance and Management System for Conditional Privacy Enhancement," in IEEE Access, vol. 9, pp. 127305-127319, 2021, doi: 10.1109/ACCESS.2021.3112013.*

[30] *J. Leng et al., "Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 1, pp. 237-252, Jan. 2021, doi: 10.1109/TSMC.2020.3040789.*

[31] *M. J. Christ, R. Nikolaus Permana Tri, W. Chandra and W. Gunawan, "Exploring Blockchain in Healthcare Industry," 2019 International Conference on ICT for Smart Society (ICISS), 2019, pp. 1-4, doi: 10.1109/ICISS48059.2019.8969791.*

[32] *R. Tapwal, P. K. Deb, S. Misra and S. K. Pal, "Traces: Inkling Blockchain for Distributed Storage in Constrained IIoT Environments," in IEEE Transactions on Industrial Informatics, 2022, doi: 10.1109/TII.2022.3208311.*

[33] *https://www.pewresearch.org/fact-tank/2022/02/03/what-the-data-says-about-gun-deaths-in-the-u-s/ and https://worldpopulationreview.com/country-rankings/gun-deaths-by-country (last accessed November 6, 2022).*

[34] *Patricia Akello, Naga Vemprala, Nicole Beebe, and Kim-Kwang Raymond Choo. Blockchain Use-Case in Ballistics and Crime Gun Tracing and Intelligence: Towards Overcoming Gun Violence. ACM Transactions on Management Information Systems [In Press].*

[35] *Nurul Hidayah Ab Rahman, William Bradley Glisson, Yanjiang Yang, and Kim-Kwang Raymond Choo. Forensic-by-Design Framework for Cyber-Physical Cloud Systems. IEEE Cloud Computing 3(1): 50-59 (2016).*

[36] *George Grispos, William Bradley Glisson, and Kim-Kwang Raymond Choo. Medical Cyber-Physical Systems Development: A Forensics-Driven Approach. In Proceedings of the IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering.*

[37] *Gonzalo De La Torre Parra, Paul Rad, and Kim-Kwang Raymond Choo. Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities. Journal of Network and Computer Applications 135: 32-46 (2019).*

[38] *Yaga, Dylan, et al. "Blockchain technology overview." arXiv preprint arXiv:1906.11078 (2019).*

[39] *Rawat, Danda, Vijay Chaudhary, and Ronald Doku. "Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems." Journal of Cybersecurity and Privacy 1.1 (2020): 4-18.*

[40] *Zhao, Ning, Hao Wu, and Yali Chen. "Coalition game-based computation resource allocation for wireless blockchain networks." IEEE Internet of Things Journal 6.5 (2019): 8507-8518.*

[41] *Rawat, Danda B. "Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization." IEEE Communications Magazine 57.10 (2019): 50-55.*

[42] *Rawat, Danda B., et al. "Blockchain enabled named data networking for secure vehicle-to-everything communications." IEEE Network 34.5 (2020): 185-189.*

[43] *Schmidhuber J. Deep learning in neural networks: An overview[J]. Neural networks, 2015, 61: 85-117.*

[44] *Caruana R, Niculescu-Mizil A. An empirical comparison of supervised learning algorithms[C]//Proceedings of the 23rd international conference on Machine learning. 2006: 161-168.*

[45] *Greene D, Cunningham P, Mayer R. Unsupervised learning and clustering[M]//Machine learning techniques for multimedia. Springer, Berlin, Heidelberg, 2008: 51-90.*

[46] *Sutton R S, Barto A G. Reinforcement learning: An introduction[M]. MIT press, 2018.*

[47] *Xu R, Nikouei S Y, Nagothu D, et al. Blendsps: A blockchain-enabled decentralized smart public safety system[J]. Smart Cities, 2020, 3(3): 928-951.*

[48] *Singh S, Sharma P K, Yoon B, et al. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city[J]. Sustainable Cities and Society, 2020, 63: 102364.*

[49] *Xiao W, Li M, Alzahrani B, et al. A blockchain-based secure crowd monitoring system using UAV swarm[J]. IEEE Network, 2021, 35(1): 108-115.*

[50] *Fernández-Caramés T M, Froiz-Míguez I, Fraga-Lamas P. An iot and blockchain based system for monitoring and tracking real-time occupancy for covid-19 public safety[J]. Engineering proceedings, 2020, 2(1): 67.*

[51] *Tanwar S, Gupta R, Patel M M, et al. Blockchain and AI-empowered social distancing scheme to combat COVID-19 situations[J]. IEEE Access, 2021, 9: 129830-129840.*

[52] *Jabarulla M Y, Lee H N. A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications[C]//Healthcare. MDPI, 2021, 9(8): 1019.*

[53] *Lo S K, Liu Y, Lu Q, et al. Towards trustworthy ai: Blockchain-based architecture design for accountability and fairness of federated learning systems[J]. IEEE Internet of Things Journal, 2022.*

[54] *Nicole Hatch, Walt Magnussen, and Jian Tao. 2023. Efforts Towards a Digital Twin-based Testbed for Public Safety. In Proceedings of Cyber-Physical Systems and Internet of Things Week 2023 (CPS-IoT Week '23). Association for Computing Machinery, New York.*

[55] *Xu Wang, Guangsheng Yu, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, Kangfeng Zheng, Xinxin Niu, Capacity of blockchain based Internet-of-Things: Testbed and analysis, Internet of Things, Volume 8, 2019, 100109, ISSN 2542-6605, https://doi.org/10.1016/j.io.*

[56] *U.S. Department of Homeland Security, Science & Technology Directorate, Blockchain Portfolio (https://www.dhs.gov/science-and-technology/blockchain-portfolio), Accessed May 24, 2023.*

[57] *Wang, X., Yu, G., Liu, R.P., Zhang, J., Wu, Q., Su, S.W., He, Y., Zhang, Z., Yu, L.,Liu, T., Zhang, W., Loneragan, P., Dutkiewicz, E., Poole, E., Paton, N.: Blockchainenabled fish provenance and quality tracking system. IEEE Internet of Things Journal 9(1.*

[58] *Lokre, S.S., Naman, V., Priya, S., Panda, S.K.: Gun tracking system using blockchain technology. In: Blockchain Technology: Applications and Challenges, pp. 285–300. Springer (2021).*

[59] *Lin, F., Xia, S., Qi, J., Tang, C., Zheng, Z., Yu, X.: A parking sharing network over blockchain with proof-of-planned-behavior consensus protocol. IEEE Transactions on Vehicular Technology 71(8), 8124–8136 (2022). https://doi.org/10.1109/TVT.2022.3173989.*

[60] *Pournaras, E.: Proof of witness presence: blockchain consensus for augmented democracy in smart cities. Journal of Parallel and Distributed Computing 145, 160–175 (2020).*

[61] *Mukta, R., Martens, J., Paik, H.y., Lu, Q., Kanhere, S.S.: Blockchainbased verifiable credential sharing with selective disclosure. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp..*

[62] *Wang, X., Yu, G., Liu, R.P., Zhang, J., Wu, Q., Su, S.W., He, Y., Zhang, Z., Yu, L.,Liu, T., Zhang, W., Loneragan, P., Dutkiewicz, E., Poole, E., Paton, N.: Blockchainenabled fish provenance and quality tracking system. IEEE Internet of Things Journal 9(1.*

[63] *Public Safety Technology Gaps and Opportunities, White Paper, IEEE Public Safety Technology Initiative, May 2021.*

7. CONTRIBUTORS

Jes Kiran

Chonggang Wang

Syed Afser

Danda B. Rawat

Dr. Qinghua Lu

Jinwei Liu

Jong-Hyouk Lee

Kapal Dev

Ko Chung Wong

Lei Zhang

Kim-Kwang Raymond Choo

Sudip Misra

Vinod P.