Blockchain Use-Case in Ballistics and Crime Gun Tracing and Intelligence: Towards Overcoming Gun Violence

Patricia Akello

University of Montana, patricia.akello@mso.umt.edu

Naga Vemprala

University of Portland, Naga.Vemprala@gmail.com

Nicole Beebe

The University of Texas at San Antonio, Nicole.Beebe@utsa.edu

Kim-Kwang Raymond Choo*

The University of Texas at San Antonio, raymond.choo@fulbrightmail.org

In the United States and around the world, gun violence has become a long-standing public safety concern and a security threat, due to violent gun-related crimes, injuries, and fatalities. While legislators and lawmakers have attempted to mitigate its threats through legislation, research on gun violence confirms the need for a comprehensive approach to gun violence prevention. This entails addressing the problem in as many ways as possible, such as through legislation, new technological advancements, re-engineering supply, and administrative protocols, and so on. The research focuses on the technological, supply, and administrative aspects, in which we propose a manner of managing gun-related data efficiently from the point of manufacture/sale, as well as at points of transfers between secondary sellers for the improvement of criminal investigation processes. Making data more readily available with greater integrity will facilitate successful investigations and prosecutions of gun crimes. Currently, there is no single and uniform platform for firearm manufacturers, dealers, and other stakeholders involved in firearm sales, dissemination, management, and investigation. With the help of Blockchain technology, gun registry, ownership, transfers, and, most importantly, investigations, when crimes occur, can all be managed efficiently, breaking the cycle of gun violence. The identification of guns, gun tracing, and identification of gun owners/possessors rely on accuracy, integrity, and consistency in related systems to influence gun crime investigation processes. Blockchain technology, which uses a consensus-based approach to improve processes and transactions, is demonstrated in this study as a way to enhance these procedures. This is the first study to explore and demonstrate the utility of Blockchain for gun-related criminal investigations using a design science approach.

CCS CONCEPTS • Information systems • Information systems applications • Decision support systems

Additional Keywords and Phrases: Blockchain, Smart Contract, Gun Violence, Crisis Management

1 INTRODUCTION

In 2020, for example, a report by the Center for Disease Control (CDC) quantified firearm-related fatalities to nearly 45,000 in the United States alone, which is over one hundred people per day[1]. According to data from the National Institute of Justice (NIJ)[2] and the Bureau of Justice Statistics (BJS)[3], firearms were

* Corresponding Author.

[1] https://www.cdc.gov/violenceprevention/firearms/fastfact.html

[2] https://bjs.ojp.gov/content/pub/pdf/hus11.pdf

[3] https://bjs.ojp.gov/content/pub/pdf/cv15.pdf

2158-656X/2022/1-ART1 $15.00
http://dx.doi.org/10.1145/3571290

reportedly used in 71% of murders, 41% of robbery offenses and 24% of assault offenses. These statistics raise important questions about existing gun-related systems, processes, protocols, and practices surrounding firearm administrations, purchases, ownership, transfers, usage, and related investigative procedures. A number of measures have been put in place to tackle gun violence and abuse, including social and legislative measures. At the time of this research, for example, the U.S. President had announced a number of executive actions on gun control[4].

In addition to legislative approaches, there have also been approaches to utilize Information Technology (IT) artifacts to facilitate gun control and firearm-related investigations. Examples include the National Integrated Ballistic Information Network (NIBIN) [1], databases linked to the Firearms Tracing System (FTS) [2], microstamping techniques [3], and the National Tracing Center's e-Trace (a web-based tool that is currently being used to track crime guns for investigative purposes). Forensic ballistics, the examination of evidence relating to guns, bullets, or casings found at crime scenes [4], is supported by NIBIN, the database for storing millions of digitized images of shell casings discovered at crime scenes. The theory behind firearm identification is that microscopic striations and impressions are left on bullets and cartridge cases when a gun is fired. These markings are unique, reproducible, and therefore, like "ballistic fingerprints" can be used to identify a gun.

Hence, if investigators recover bullets or cartridge cases from a crime scene, forensic examiners can test-fire a suspect's gun to see if it produces ballistic fingerprints that match the evidence [4]. In other words, the forensic ballistic procedure allows gun crime investigators to link shell casings recovered at crime scenes to digitized shell casing images stored in a database, with NIBIN and other microstamping technologies. The existing FTS system runs on multiple centralized databases and legacy systems such as the "Sales Reports" database (a registration record with specific firearms and owner name and address), databases on "Suspect Gun" (whereby guns "suspected" of being used for criminal purposes but not recovered by law enforcement are stored), databases on "Traced guns" (a registration record which includes names and addresses of the first retail seller and purchaser), "Out of Business Records" (data manually collected from paper Out-of-Business records (or input from computer records) and entered into the trace system by The Bureau of Alcohol, Tobacco and Firearms ATF), and databases on "Theft Guns" (firearms reported as stolen to ATF) [2]. The FTS databases interface with the current e-Trace system, a web-based environment that facilitates law enforcement and authorized investigators in electronically tracking crime gun data and its exchange. In other words, the e-Trace system aids in gun tracking when a gun is recovered from a crime scene, whereby its origin and ownership is traced to a registered owner through a trace procedure coordinated by the US Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) [5].

There are, however, a number of limitations in existing systems, and this work aims to address several of these limitations: First, microstamping is a newer technological trend in smart gun manufacturing and hence may be found only in certain, newer firearm types, such as semi- automatic rifles, rather than older and/or less sophisticated guns [3]. Hence, this technology does not help investigations involving older

[4] https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/07/fact-sheet-biden-harris-administration-announces-initial-actions-to-address-the-gun-violence-public-health-epidemic/

firearms. Additionally, the technological trend is only useful to the extent of identifying a gun that has been involved in a crime since microstamping and NIBIN on their own can only help identify the weapon based on the unique markings or "fingerprints" identified on the casing (rather than providing information such as documented gun sales, transfer, and other supportive information for accuracy, consistency, and authenticity). Second, with NIBIN, the time and process required to identify a crime gun through the comprehensive comparative analysis can be lengthy; thus, making it inefficient for time-sensitive investigations. Third, the current e-Trace system that links to the FTS databases to fulfill trace requests assume that gun dealers submit all sales documents to the ATF, and so do manufacturers; whereby this information is kept intact and then queried or manually searched to verify a gun's identity when needed. This means if gun sellers and manufacturers fail to submit accurate and consistent information regarding the guns they sell or manufacture, the ATF's search process could be futile leading to the un identification of a gun crime perpetrator.

A search could also be futile if the gun being investigated had been 'unofficially' transferred, sold, trafficked, or stolen. This is because all of these events usually happen without proper documentation making traceability along a gun's chain of custody difficult due to the fact that they are traceable only to the original owner, rather than the last owner or potential crime suspect. In our analysis, we have determined that the primary issues with current systems are data inconsistencies, and their absence, as well as the fact that investigators can encounter unavailability of information during gun-related investigations. The current fragmentation of data collection, storage, and maintenance mechanisms in the firearm domain is partly responsible for this. Since firearm manufacturers, dealers, law enforcement agencies, and other stakeholders do not have access to a single, uniform platform to capture and manage firearm-related data, they must rely on numerous systems and mechanisms to capture, store, and maintain firearm-related data. As a result, firearm crime investigations often have difficulty tracing firearm-related information.

Table 1: Gaps in Current Systems

Entity	Current Process	Limitations and Potential Gaps
Firearms Dealer	Licensed entities, also known as Federal Firearms Licensees (FFLs), are authorized to sell guns to individuals who pass the required background check.	Since gun owners' information is not centrally stored in a single database, tracing (e.g., during an investigation) and auditing can be challenging. Change of ownership is not recorded in any database, which can be used for tracing and auditing.
ATF (The Bureau of Alcohol, Tobacco, and Firearms)	Responsible for performing background checks of firearms sellers and issuing of licenses.	Maintains information about sales (through multiple databases), generally incomplete, and other information relating to smuggled weapons and weapons involved in criminal investigations (e.g., arm trafficking). ATF runs on old technology and searching on the database is not possible due to lack of indexing [a]. ATF runs on old technology and searching on the database is not possible due to lack of indexing [b].

[a] https://www.npr.org/2013/05/20/185530763/the-low-tech-way-guns-get-traced.
[b] https://www.thetrace.org/2016/08/atf-non-searchable-databases/

Based on these identified gaps in current trace procedures and firearm-related investigations, this research aims to address some of the existing challenges in current systems and procedures, such as the lack of standard documentation frameworks for gun sales and transfers, and a lack of a single and uniform platform for the capturing and management of firearm data from the manufacturers, dealers, and investigative stakeholder fronts, with integrity and assurance. Specifically, our study aims to answer the following research questions:

RQ1: On the basis of identifying information (e.g., the serial number), how can the chain of custody of a crime-related weapon be traced to a crime suspect?

RQ2: How can the progressive ownership of a crime-related weapon be successfully traced along its chain of custody, if important identifying information such as the serial number is missing (e.g., older weapons that do not follow finger-printing rules)?

RQ3: How can we maintain the integrity of gun ownership using a decentralized architecture that does not require data storage to be confined to a single location while maintaining data integrity?

RQ4: How can an integrated environment for gun-related crime investigations be created, that is secure, immutable (data integrity), highly efficient, and available 24 hours a day, 7 days a week?

We propose a Blockchain-based integrated model that not only captures gun ownership and chain of custody, with an integrated gun tracing mechanism to address the research questions. Consequently, we propose an enhancement to the gun-crime investigative process by implementing a holistic and robust blockchain-based gun-crime tracing mechanism based on Nakamoto's underlying technology [6], for crime gun-related investigations specifically firearms tracking, information sharing and suspect identification. Due to its inherent features, such as decentralization, immutability, integrity, transparency, and

standardization, Blockchain, a technology that implements a consensus-driven approach to transactions, provides an appropriate framework. The solution seeks to solve the above three challenges in gun-related investigations. By streamlining and standardizing the process of gun sales, ownership and tracking, the proposed blockchain-based framework will provide significant advantages of improving and expediting crime gun tracing from the manufacturer to a licensed dealer along its custody chain, and especially to the most current firearm custodian or suspect of gun crime. Hence, the blockchain-based framework, provides a powerful tool that aids gun crime investigations, thus reducing gun violence.

To represent our idea in a structured and systematic format, we use the design science approach [7], demonstrating the use of a permissioned blockchain-based platform based on the Ethereum smart contract [8]. Our study is the first to present a design science approach-based study that explores the utility of blockchain in facilitating the investigation of gun-crime related investigations.

2 RESEARCH BACKGROUND

In this section, we provide background information related to technological advancements in government processes (e.g., government information systems) aimed at improving trust, transparency, and integrity. We also explain the importance of adopting Blockchain (also known as distributed ledger technology) for purposes of improving processes related to gun criminal investigations with the hope of reducing gun violence.

2.1 Related Works in Government Processes

Research on government information systems generally began in the 1970s when computers first surfaced [9–11], continuing thereafter to cover important aspects of government processes such as transparency in governing, trust between officials and citizens, accountability, and integrity among others [12–15]. One system examined on this basis, and positioned as a facilitator of transparency and open communication between governments and citizens is social media, a platform utilized to provide avenues for official and unofficial communications from governments directly to the citizens in real time [16]. As an electronic communication platform generally used for the dissemination of information, social media helps to bridge information gaps, hence improving communication, transparency and accountability, which also leads to an improvement in the participatory culture in certain government processes [12,17]. Hence social media changes the communication dynamics between governments and citizens from that of a "closed" format to an "open and inclusive" format by improving information assimilation, close collaboration between governments and citizens, and a generally open governance model [12, 18–21].

When it comes to transparency, integrity and trust, a technology of similar promise is Blockchain, based on its characteristics of immutability, decentralization and transparency [22]. Such characteristics align well with important requirements of government processes such as gun-related criminal investigations [23]. Work such as [8, 24, 25] have acknowledged the potential of improving gun-related criminal investigation processes, and demonstrated how Blockchain characteristics and properties can be leveraged via context specific designs to address current challenges such as secure information sharing across different departments, and overall transparency in information sharing [24, 26, 27]. Similar research by [25] demonstrate how Blockchain can be applied in e-governance via an e-residency program

that aids secure access control through "self-sovereign identity authentication". Additional related works in e-governance [15] also discuss its potential applicability and areas of exploration in government processes that include asset registry, digital identity mechanisms, money tracing, marital status registry, e-voting, and criminal records management. The present study is inspired by, and builds upon such existing works and past implementations and applications of the Blockchain technology in data or information-intensive domains (e.g. the Internet of Things, IoT and healthcare) where Blockchain is positioned as part of remedies to data and information security threats [28–34] to improve data integrity and authenticity through inbuilt decentralization and tamper resistance properties [31] to enhance privacy and embedded access control mechanisms [30], and non-repudiation during collaborative and interorganizational interactions [33]. The distributed ledger technology makes it possible for organizations to keep track of records of transactions making it suitable in situations in which multiple parties are involved in a transaction [15]. Under these circumstances, participating organizations can jointly create, 'modify' and keep track of an immutable history of transactions, as needed in cases related to gun investigations. Additionally, as these processes involve numerous sources or stakeholders and deals in sensitive information, a permissioned blockchain helps streamline the actions of numerous authoritative and non-authoritative stakeholders to ensure integrity, trust, and confidence in such processes. In past research [35], the use of such a permissioned Blockchain-based framework is demonstrated for identity and access control in a consortium-like environment with multiple stakeholders such as the one we propose in the current paper.

2.2 The Importance of Adopting Blockchain for Process Optimization in Gun Related Criminal Investigations to Combat Gun Violence

In gun-related investigations, there are multiple stakeholders that include criminal investigators, gun dealers/sellers, manufacturers, and owners among others. A Blockchain-based system with specifically agreed protocols for gun sale, ownership, and transfer aids with expediting the investigation process in general, and specifically the identification of a potential crime suspect within reduced times and in an efficient manner. With such a distributed ledger of shared information that offers higher integrity, consistency and secure accessibility to sensitive information, participating entities and affected individuals can have confidence in gun related investigations as every entity involved in the investigation such as the NIBIN, the ATF, the manufacturers', the firearm shops, law enforcement, etc., knows how information is being managed on a particular case and also has access to an accurate copy of each transaction or record on gun sales, transfers, management, and their metadata. Over the past few years, Blockchain has become integral to a series of solutions to problems, ranging widely from climate change through renewable energy initiatives [36], to the IoT data security [37]. Additionally, Blockchain has also already been widely implemented in finance and the healthcare, hence can be leveraged to provide similar desirable outcomes of information security and integrity in criminal investigation initiatives, specifically gun related.

A distributed ledger with desirable features that include transparency and tamper resistance through encryption, Blockchain uses cryptographic mechanisms to authenticate all participants on a network [6]. This implies that to be able to modify transactions already added to the chain of blocks in a network, every participant would be notified and additionally, would need to validate and verify that transaction before it gets added to the previous transactions with a unique hash, requiring a lot of resources to change the hash.

Additionally, and importantly, this makes it almost impossible to secretly update or delete information from a ledger without others on the network knowing of it. Noteworthy also is the fact that all information stored on the blockchain are made available to all members of the network, ensuring transparency among participants, and integrity of data [36–39].

Gun violence, an enduring challenge of the century, requires a holistic approach to its remediation, including regulations, grassroots advocacies and awareness, as well as successful criminal prosecution of gun related crimes. Blockchain is a viable tool in tackling the gun violence crisis by improving the criminal investigation processes of gun related crimes, such as by facilitating transparent tracking of crime suspects and crime-related guns along their chains of custody.

When a gun-related crime occurs in the United States for example, it is extremely difficult to zero in on a suspect in a timely fashion, partly due to the limitations in existing systems for gun sales, documentations and tracking, that consequently lead to data inconsistencies and missing gun information. Additionally, the gun culture in some countries such as the United States allow most people to access guns, legally or even illegally. The un-streamlined sale and transfer procedures introduce inconsistencies in gun related data and the multitudes of unregistered guns out in circulation all make it difficult to identify a gun used to commit a crime, as well as a gun crime suspect. A bottom-up system that streamlines the investigative process of gun related crimes providing a decentralized, consortium-like platform for efficient gun sales and transfer management might be one of the needed recipes for successful gun crime suspect tracing and the eventual successful investigations and prosecutions of related crimes. A blockchain-based platform to track guns along their chains of custody, and crime suspects; over traditional centralized or manual databases is beneficial in various aspects that include secure data handling, quality assurance, fault tolerance, etc. (see Table 2).

Table 2: Security, Integrity, Transparency, and Immutability Properties of Blockchain (BC)

Properties	Benefits	References
Immutability, Security, and Integrity through cryptographic validations	Through the use of public key encryption (which identifies and validates the identity of transacting parties before executing exchanges), BC provides secure information access and exchange. With cryptographic validation of interactions and immutable time-stamped ledgers, BC helps to prove information integrity, provenance, and accountability.	[22, 40–42]
Decentralization in ownership & management.	Due to its decentralization property, BC is controlled by a network of participants rather than a single actor. Because no central authority is involved, there is less chance of a single point of failure or censorship if a node fails.	[15, 40, 41, 43]
Transparency & trust	Blockchain networks allow anyone to view the full history of transactions, making it challenging to hide transactions from authorized participants, and easy to audit, to keep the network "honest" and reliable.	[43–46]
Standardization & efficiency	In comparison to current centralized systems, disparate applications created in silos to support related functions, or pen and paper records management processes at the dealers' which require duplication of data or cause human error, digitizing via BC yields improved operational efficiency. A BC network in this instance enables interoperability and standardization, as well as secure data sharing between systems.	[8, 15, 24, 25, 47]

3 METHODOLOGY

In this section, we will first introduce the case study, which will briefly describe the specific problems in related systems that we aim to address through a methodological approach to improve gun-related crime investigation processes. We then present the proposed design of our Blockchain-based platform, which will include smart contracts to handle two types of functionalities: one to handle firearm sales and the other to handle firearm tracing for gun violence investigation. Finally, we go over the design science research approach used to evaluate the developed artifacts in detail.

3.1 Existing Gun Sales and Tracing Architecture using Legacy Systems

The National Tracing Center (NTC) of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) is a United States crime-related gun-tracking facility. Among its many responsibilities, in addition to detecting firearms trafficking by following the movement of crime guns across state and national borders or lines, the NTC also traces firearms associated with crimes and provides investigative leads to responsible agencies as one of its responsibilities. Firearm tracking expedites the investigation process and assists federal, state, and local law enforcement agencies involved in the process. At the moment, the primary challenge with tracing firearms is not having a central digital mechanism for the capturing fragmented firearm sales and change of ownership documentations across the jurisdictions. First, there are multiple laws in place, both for and against the documentation of firearm sales and records that vary by state. This already introduces loopholes that may hinder accurate data capture that can be used for future firearm

tracing. Additionally, a lack of trust in current systems that store these transactions and the possibility of data leaking into the wrong hands compound the challenges. Existing firearm transaction tracing systems, such as the e-trace system at the National Tracing Center, NTC, still run on outdated technologies (e.g., legacy database-type systems) that are not easily scalable. Moreover, investigators also have to manually input gun sale documentation into the tracing website upon receipt from dealers and sellers, who usually use manual mechanisms to keep such information, information into the website whenever a trace is needed, making comprehensive tracing lengthy and potentially inaccurate because of un-streamlined and un-standardized document management systems that exist at the various gun sale and transfer points. Firearm purchase records, potentially critical to tracing guns used in crimes, are usually submitted in manual formats such as in paper formats which arrive at the National Tracing Center in scores of cardboard boxes and shipping containers awaiting to be inputted into the tracing website. Such records can be lost, tempered with or simply destroyed, making them inaccessible to investigation teams. There are also various legal restrictions on gun purchasing and ownerships to curb the illicit sale of firearms to convicted felons, juveniles, and other high-risk groups. Even with the current limits, there are many sources from which offenders can obtain firearms as firearm transfers and secondary sales without proper documentation as this process is currently not organized. Studies on types and origins of the guns [48, 49] tend to suggest that the lack of integrated tracking systems that streamline the purchasing of firearms by firearms dealers and buyers who purchase multiple firearms facilitates the easy trading of illicit firearms.

In analyzing the firearms tracking case study, we argue that there is an urgent requirement to have a trustworthy system for the management of such sensitive information at this time in history where information technology innovations are exponentially growing. The ideal system should record all the firearms transactions on all fronts: from the dealer's front, manufacturer's front, law enforcement front, and so forth, with detailed information such as the date of manufacturer, sale or transfer, buyer information and firearm type. Such a secured system should further be set up to provide data only to a controlled group working on a firearm-related crime investigation, quickly and on a need-to-know basis. The proposed system would capture and consequently be able to quickly make available firearms sales information, change of ownership, and further enhance the tracing of firearms during crime investigations involving firearms with trust, reliability, and adequate transaction speed.

Taking these factors into account, we proposed and evaluated the use of Blockchain technology, specifically permissioned Ethereum-based Blockchain, as an instantiation of this system for our research. Following a review of the existing review and the case study on firearm sales and tracing, the Blockchain proposal is appropriate to address issues related to gun related data collection in adequacies in current systems, data management and maintenance as explained in the introduction, as well as issues of stakeholder trust and transaction speed as explained below:

1. Trust – Transactions made on the Blockchain boost trust due to the immutability and transparency of the Blockchain. Furthermore, with the permissioned Blockchain, a specific number of nodes on the Blockchain operate as key transaction validators. In the Ballistic Analysis scenario, the permissioned Blockchain is a far more realistic choice for increasing confidence because important nodes of the Blockchain may be designated as representatives from numerous parties and stakeholders increasing the trust in the system. In the investigation of weapons offences, the NTC, ATF, NIBIN, FTS, and local police are all involved. They

should have access to firearms records in order to trace ownership, and hence stakeholders from these departments should have access to firearm sales records alongside firearms merchants and manufacturers.

2. Delays in Firearms Tracing during crime – Due to the involvement of multiple stakeholders, the current process of ballistic analysis faces multiple bottlenecks, and most of the time the delay involves connecting the firearm to the suspect and the order of events. The process can be streamlined by implementing processing logic on Blockchain smart contracts. The transaction time on Blockchain, on the other hand, is determined by the consensus mechanism. The current protocol for permissionless networks, such as Ethereum Mainnet, is PoW (Proof of Work), which relies on all possible network nodes validating transactions, causing significant delays. In the case of permissioned Blockchain networks, the consensus mechanism is generally a lightweight protocol such as the Proof-of-Authority protocol or the Hyperledger protocol, which speeds up the transaction creation process. In a permissioned Blockchain, network nodes are pre-authenticated, and block generation rights can only be granted to specific nodes, known as validating nodes. If a node is unavailable for an extended period of time, it can be removed from the list of validating nodes, allowing other stakeholder nodes to take their place. Such a protocol aids in determining which stakeholder nodes are active and which are not.

Due to the nature of the problem that we are addressing in this study, we follow a design science approach to develop and evaluate a prototype for a blockchain-based solution that embodies our proposed solution for secure and timely firearms tracing during related criminal investigations.

3.2 Proposed Blockchain-Based Platform

To demonstrate the functionalities of the Blockchain-based system proposed in this study, we develop Ethereum-based smart contract to optimally capture the sale and tracking of firearms transactions. Successful firearm tracing begins with complete, accurate and immutable documentation of firearm related metadata and sales data. We present the process involved in the sale of firearms, its documentations, tracing, and the multiple stakeholders that could be involved in firearm-related investigations and the Ballistic Analysis process in the Blockchain smart-contract architecture diagram in Figure 1.

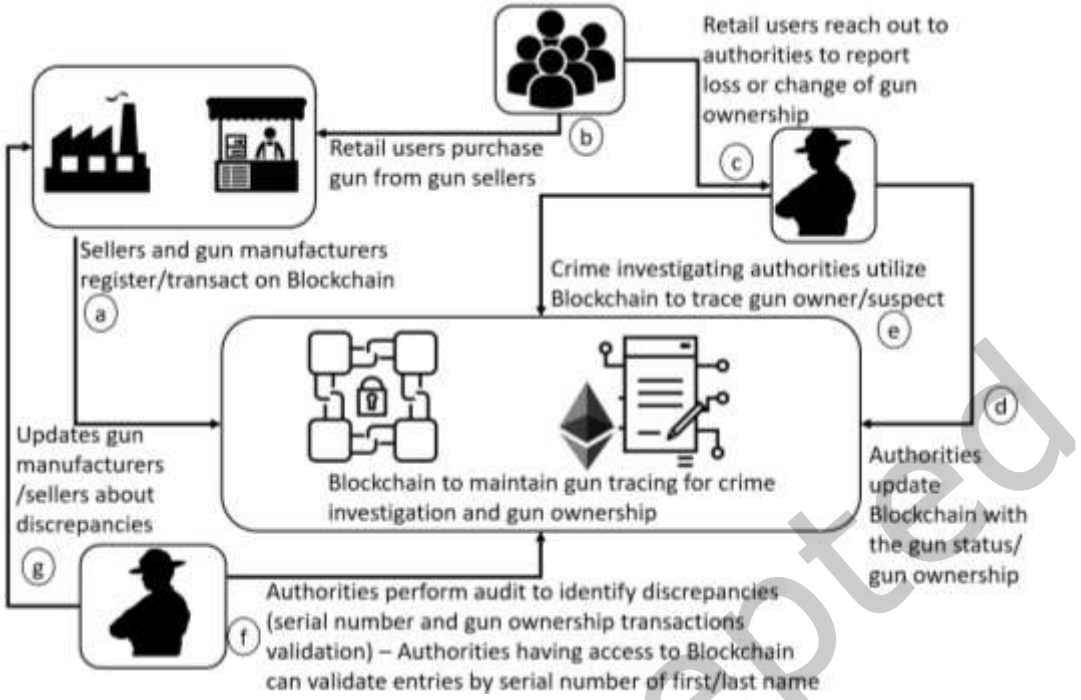

Figure 1: Gun Ownership and Tracing Smart Contract Architecture

The Firearms ownership part of the smart contract addresses the primary issue of capturing the sale of firearms for accountability. There is currently no single and uniform platform available to both firearm manufacturers and dealers involved in the sale of firearms. Due to the lack of a uniform platform for registering the purchase of firearms, the tracking of firearms becomes difficult when a crime is committed using an unregistered weapon. Any firearm dealer or manufacturer involved in the sale of firearms will need to be registered on the permissioned Blockchain. Then all sales of firearms are captured on the Blockchain. The Smart Contract validates each registered arms dealer or manufacturer before enabling the seller to record firearm sales on the Blockchain. The current process for registering firearm sales requires a background check through NICS (National Instant Criminal Background Check System) and the sales information is manually submitted to ATF as physical paperwork, complicating the process of tracing firearms transactions. To avoid disassociating the customer whose background has been verified from the purchaser of firearms, the smart contract first verifies whether the seller selling the firearm is already registered, and then updates the customer information on the Blockchain to complete the transaction. This mechanism provides an additional layer of security for illegal firearms dealers or manufacturers to create false entries or to manipulate existing entries on the Blockchain. The Firearms Ownership part of the contract performs multiple functions including creating new sales, capturing information about the firearm owner upon receipt of identification information, updating the firearm status, providing direct search functionality using multiple criteria on the Blockchain. The Firearm tracing portion of smart contract, which is the core process of criminal investigation, demonstrates the processes involved in optimally tracking a crime-related weapon through its chain of custody; this entails registrations to the

Blockchain of new users with the role as investigators and all other potential stakeholders in firearm related investigation processes (firearms sellers, manufacturers, regulators, crime investigators, and so forth.). The management of firearm ownership and transfers, access control (each registered user on the Blockchain is assigned appropriate access by the permissioned Blockchain administrator, the firearms seller receives seller access, and the local investigating agency receives investigator access), status updates and the eventual tracing/searching of crime-related weapons through their chains of custody, ownership and the supply, are additional functionalities of the smart contract.

A demonstration of each of the above described processes/procedures and their representative functionalities are captured in the smart contact whose details are shown in Table 3. It should be noted that the presented smart contract functionality overviews are only for demonstration purposes.

Table 3: Functionalities implemented in the Smart Contract

Firearm Tracing Functionalities	Crime Investigation Functionalities
registerUser Step 1: Deploy the private blockchain Step 2: Receive request to register as a firearms manufacturer, as a retail seller, or a investigating officer Step 3: Validate information Step 4: If primary validation is successful, confirm registration and provide tokens for the manufacturer or retail seller providing approval to carry out sales Else fail registration End Procedure	*newTraceInvestigation* Step 1: Identify the firearm serial number using ballistic imaging Step 2: Create a new investigation case using the serial number and the suspect information Step 3: Submit new case for processing End procedure
UpdateAccessPrivileges Step 1: Restrict procedure to blockchain management Step 2: Add privileges for additional users to perform audit on manufacturer or retail seller End procedure	*updateFirearmsStatus* Step 1: Identify the firearm serial number that requires status update Step 2: Select the new status for the weapon and update status Step 3: Submit case weapon status for processing End procedure
newFirearmsSale Step 1: Capture the identification information of the firearms user Step 2: Create a new firearms entry with the user identification information and the new firearm make, model, and serial number Step 3: Validate information Step 4: Update firearm status as NEW and complete transaction End procedure	*updateTraceSuspect* Step 1: Select the serial number for which prime suspect information is available Step 2: Search for any existing crime cases using the firearm serial number Step 3: Search for firearms owner information querying firearms ownership contract using the weapon serial number or by using suspect personal information Step 4: If search returns a valid contact update firearms tracing system using the search results Else If Any other suspect details available, update suspect End Step 5: Update prime suspect End procedure
updateFirearms (Owner/status – Restricted procedure for local police department)	*UpdateCaseStatus* Step 1: Identify the case that requires status update

Firearm Tracing Functionalities	Crime Investigation Functionalities
Step 1: Restrict the procedure to local police department Step 2: Receive request to update firearm status or change of ownership Step 3: Verify identification information Step 4: Update firearm status/owner information and complete transaction End procedure	(Search for case either by firearm serial number or case id) Step 2: Select the new case status and submit case status for processing End procedure
searchGunBySerial and *searchGunByName* Step 1: Identify the search criteria (Search by serial number or using first name, last name, zip code) Step 2: If search by serial then "Enter the serial number of the weapon in the serial number field" Else "Enter first name, last name, and zipcode in the respective search fields" Step 3: Submit search End procedure	*updateAdditionalTraces* Step 1: Identify the case that has more details Step 2: Enter case details Step 3: Submit case request End procedure

Per the demonstrations, the firearm tracing functionality of the contract provides for a mechanism to search for a possible firearm-related crime suspect using a firearm transaction record when a firearm or its shell casing is recovered at a crime scene. Even if no serial number information is readily available but with probable suspect details, including, say, demographics such as first and last names and zip code; the blockchain will return a list of possible suspects to initiate further investigations. Specifically, the processing on the Blockchain should be optimized, and in order to keep the transactions optimized, the gas price and the amount of gas used by each transaction will be utilized. In the case of a permissioned Blockchain, gas price standards are irrelevant; however, to prevent transaction failures, optimal execution logic should be implemented in the smart contract, resulting in less gas consumption. As the search process on the Blockchain is costly and consumes a large volume of gas for the transaction to be carried out, we provide a mechanism for obtaining one to one mapping for the extraction of possible suspect information. In many private networks, such as our case study of implementing ballistic analysis on a permissioned blockchain, network participants act as validators and are not compensated with gas. For networks that do not require gas as an incentive, the gas price is typically set to zero (that is, free gas). However, some private networks may allocate Ether and maintain a non-zero gas price in order to control resource consumption. As a result, gas prices remain significant, and the performance of smart contracts must be considered. For demonstration purposes, two different criteria were used, one using a serial number of weapons, and the other using a first name, last name, and zip code combination. However, this can be extended to multiple search criteria without compromising the gas cost through our design approach. The firearm tracing contract performs a number of functions, such as creating a new investigation request using the serial number of the weapon received through ballistic imaging, updating the status of the weapon, updating the case for prime suspect details, updating the status of the case and adding additional details to the case. Sample data for the involved parties are shown below in Table 4:

Table 4: Sample data in the Smart Contract Structure

Authorized User	Gun Owner	Gun Trace – Transaction
Role: 1 (Seller of firearms). sellerName: Grab a Gun totalGunSales: 1000 The role field may contain additional values. For instance, 2 for a Blockchain auditor who is not permitted to sell a weapon and 3 for law enforcement agencies conducting criminal investigations	seller: 0x5c6B0f7Bf3E7ce046039 Bd8FABdfD3f9F5021678 (SHA256 hex address) Name: John Doe physicalAddress: 123 Main St, Anytown, USA dob: 01011990 zipcode: 12345 serial: 331-12345 ownerId: 999 gunStatus: 1 gunStatus field can take multiple values such as 2 for stolen and 3 for turned in.	seller: 0x5c6B0f7Bf3E7ce046039 Bd8FABdfD3f9F5021678 (SHA256 hex address) suspectName: Uncle Tom1 physicalAddress: 125 Back St, Newtown, USA dob: 02021992 zipcode: 12346 serial: 331-12346 ownerId: 998 gunStatus: 2 caseStatus: 1 caseId: 888 caseStatus field can take multiple values such as 2 for closed and 3 for suspended.

3.3 Overview of the Design Science Research Methodology

Our research follows a Design Science Research Methodology (DSR) process model introduced by Peffers et. al [50], to demonstrate the utility of Blockchain in the streamlining of firearm sales, tracking and crime-related investigations. Consequently, multiple smart contracts are developed as earlier discussed, to optimize the processing logic of the sale, transfer, acquisition and importantly tracking of firearms using multiple search mechanisms on a Blockchain. The relevance of the artifacts is justified on the basis of the absence of a single, uniform, secure system or platform that allows manufacturers, dealers, law enforcement officials, and crime investigators to gather, maintain, and trace fire-arm information when investigating firearm crimes involving numerous stakeholders, while ensuring data integrity. The artifacts that we have developed are, hence, solutions in accordance with the DSR guidelines, through registration, maintenance and search processes that draw on existing knowledge. The DSR process requires a rigorous assessment of the utility, benefits, quality, and efficacy of the artifacts, which we have presented in parallel and later in subsequent sections. Utility is demonstrated by scenario-inspired "functionalities" that we posit will address the key issues in firearm related investigations. We have in tandem verified that the proposed artifacts can be scaled to handle an increasing volume of data. Figure 2 below presents a map of the design process followed in our research.

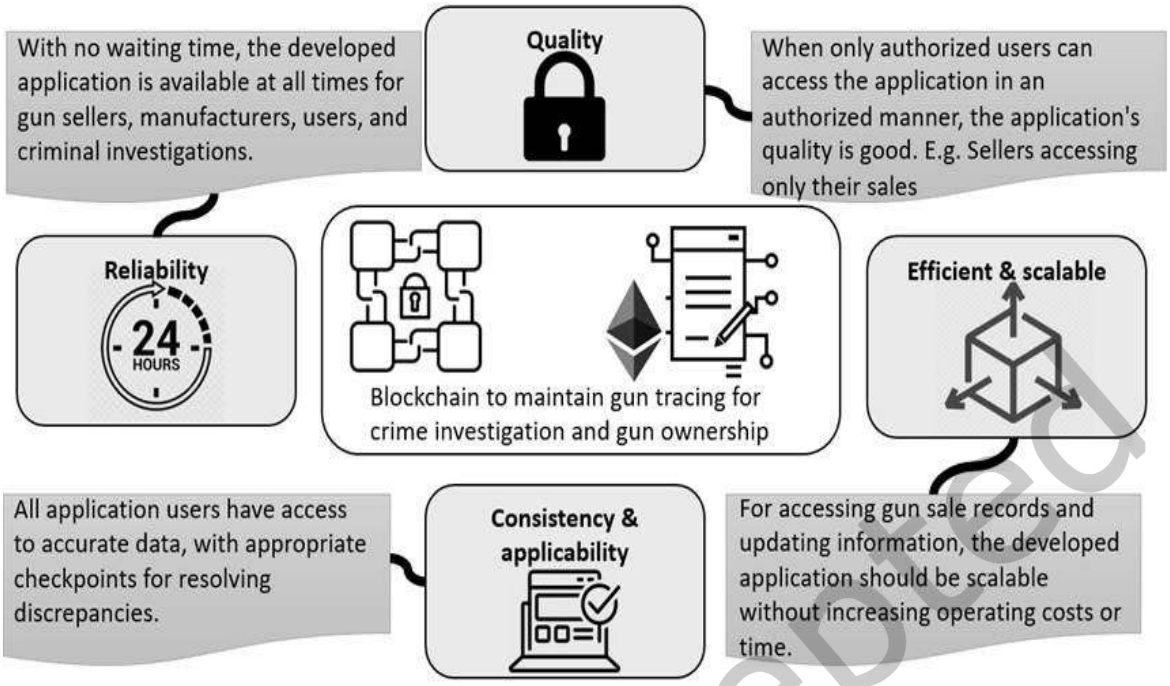

Figure 2: Design Science Research – Process Stages

3.4 Demonstration of Value of Designed Artifact

We develop a set of comprehensive strategies to demonstrate the value of our methodological artifacts. We present strategies from the perspective of various stakeholders in our blockchain, such as manufacturers or retailers, the local police department, criminal investigation teams and the private blockchain auditing team. Also, as the audit process is an essential quality check process to ensure smooth operations, our smart contracts provide two demonstrations. However, this can be customized depending on the need. To conduct an audit using the data stored on our private Blockchain, the administrator can either use the index on the entries for the Blockchain's registered users, Gun users or the Blockchain can be searched using the names of the owners or the zip code. These strategies have been developed from our review on the existing body of knowledge of current systems such as the ATF'S e-Trace and Firearm Tracing System [2], as well as their current limitations, thus justifying the approach of design science research. DSR is a problem-solving paradigm that has its roots in engineering and the sciences of the artificial [51], and seeks to enhance human knowledge via the creation of innovative artifacts. It seeks to enhance technology and science knowledge bases via the creation of artifacts to solve real-world problems and improve the environment in which they are instantiated. The outcomes of using DSR include both the newly designed artifacts and design knowledge that provides understanding of why the artifacts enhance existing applications [52], and in our context we ensure that the insights gained from the current tracing systems at ATF (e.g., e-Trace and FTS) are incorporated in our developed artifacts. These strategies are presented in Table 5.

Table 5: Strategies Demonstrating the Value of Artifacts

Manufacturer or Retail seller	Local police department	Crime investigation department
1) Should be able to register on the Blockchain	6) Should be able to update the firearm status	10) Should have access to all the manufacturers or retail sellers
2) Should be able to create new sales transaction on the Blockchain	7) Should be able to update the owner information	11) Should have access to all the owners and transactions
3) The new transaction on the blockchain should have the firearm status as new	8) Should have access to all the manufacturers or retail sellers	12) Should be able to search the Blockchain efficiently using multiple search criteria – using serial number of firearm, using seller information, and buyer details
4) Should not be able to access any other manufacturer/retail seller sales information	9) Should have access to all the owners and transactions	13) Should be able to link the serial number and create a new criminal investigation
5) Should not be able to update the firearm status or ownership after initial sales		14) Should be able to create a new crime investigation with new serial number of weapon irrespective of the weapon on blockchain

3.5 Demonstration of Utility Through Exploratory and Confirmatory Focus Group

Utility is one of the key requirements and is part of the Design-Science paradigm meta-requirements proposed by Peffers et. [50]. The artifacts that we are developing should allow easy access to the registration of multiple stakeholders on our platform, reducing delays in the investigation of firearms. Following previous research in formulating a design approach, we designed our study through an initial exploratory approach by conducting a focus group meeting to understand the current challenges and assumptions in the existing systems. After framing an initial design approach to all the necessary conditions, we proceeded towards a confirmatory process. Based on the design principles, a confirmatory focus group discussion involving former police officers from a southern US state police department was used to assess the design of the conceptual artifact [53]. From the details of our proposed design the former police officers were asked for insights on the several functionalities proposed in our design, as well as how the proposed design aligns with real insights from law enforcement Intel. The objective was to align our design and to validate it based on insights from personnel with real hands-on knowledge and experience. Feedback was used to further improve the design.

3.6 Demonstration of Design Quality

The quality of the artifact is another key assessment criterion for the DSR studies [54]. In the case of smart contract artifacts, we have developed, the quality is measured in terms of gas costs. We measured the gas units consumed for the "update transactions" functionality by simulating the total number of arms sales in multiples of 50 starting from 10 to 1000 and inserting them into the Blockchain. Read transactions are created as a "view" type of transactions in which case no gas cost is required. We have not seen any significant deviations in the average gas cost of transactions (measured in Gwei) as shown in the figure 3.

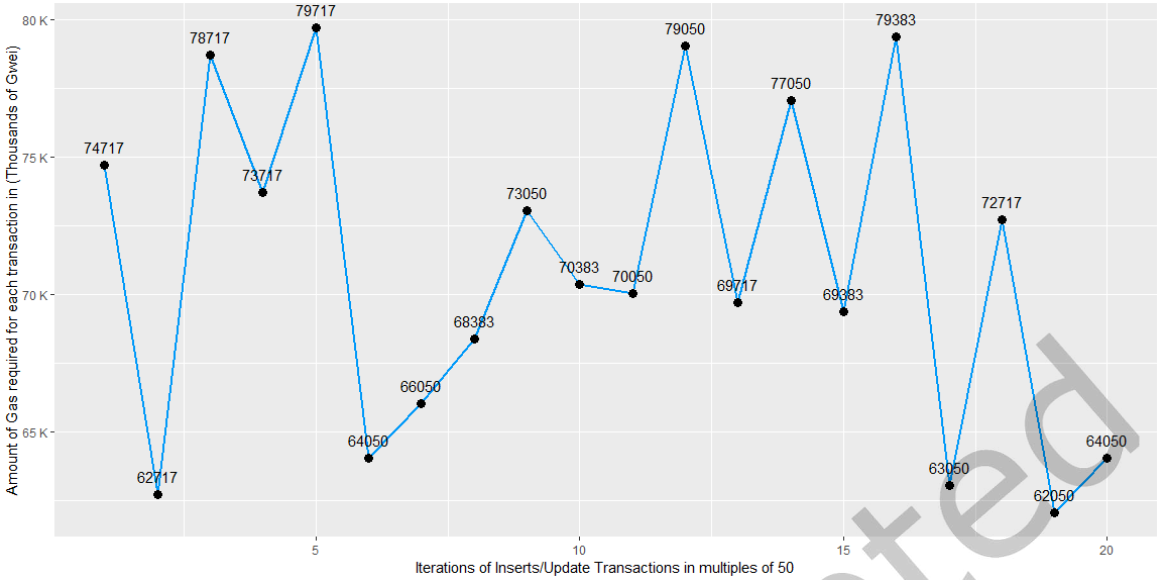

Figure 3: Average Gas Cost of Various Transactions on Blockchain

3.7 Demonstration of Design Efficiency

Efficiency is another meta-requirement for design science research that directly addresses the ease of use and timeframe needed to deliver results. In terms of time dimensions, we assessed our artifacts against the data that our artifacts can handle. We have simulated data for multiple stakeholders and different volumes of transactions. We have captured the simulated data in the blockchain we've developed. We then captured the time it takes for us to capture the data and the time it takes for us to search for the information that we have already stored, using the various search criteria that we are proposing. We reported the time to capture information and extract information from our blockchain by increasing the amount of data we store on blockchain. We measured the time needed to insert 10 records at once and repeated the process of capturing the time for 10 times. Average time remained the same throughout the process, confirming that the smart contract developed is scalable.

4 DISCUSSION AND LIMITATIONS

Firearm tracing is one of three paramount activities in firearm-related investigations. Successful investigation of gun-related crimes is essential to reducing gun violence. Firearm tracing success relies on the integrity, consistency and accuracy of input sales, transfer and ownership data for successful tracking of crime-related weapons along their chains of custody. Current protocols, processes and technologies that include centralized databases and semi-automated record management techniques are outdated, untrustworthy and inconsistent, making them insufficient for the nature of law enforcement Intel. This study presents and evaluates the feasibility of a permissioned blockchain-based solution based on the smart contract Ethereum, to overcome current loopholes in the gun tracking process. We present a design based on DSR, modeling a smart contract framework capable of handling functionalities from both

firearms sales and criminal investigations, drawing on existing knowledge on firearm sales and tracing to optimize the processing logic of respective functions in the gun sales, transfer, and search process. As such, the proposed system captures contextual firearm-related transactions in several representative procedures and functionalities: sales, update, search and access control. The relevance of the artifact is justified on the basis of identified gaps in current processes and trace-procedures; while its benefits, quality and efficacy are assessed using scenario-based case information, simulated data and focused group discussions, demonstrating that the proposed design is scalable with the ability to handle increasing volumes of data. Although the developed system will not solve every loophole in firearm-related investigation, our study demonstrates a feasible and positively consequential technological improvement that leverages the heralded potentials of the Blockchain to bring about enhancements in the weapon investigative process through efficient tracking, timely information sharing and expedited weapon-related crime suspect identification. Consistent with the nature of Blockchain, a consensus-driven mechanism is, hence, introduced into foundational firearm investigative processes, bringing about trust, consistency, integrity and overall efficiency.

The contribution of this study must be considered in light of its limitations, which also build the basis for future research. While we argue that the proposed prototype could be applied to U.S. gun crime intelligence and investigation procedures for the improvement of established sales, transfer and ownership processes, our system is developed and evaluated based on assumptions that it is possible to accommodate existing laws concerning firearm sales, manufacturing, and ownership. Hence, generalizability depends on, and may be limited by such existing laws which may differ between jurisdictions. Additionally, the presented blockchain-based solution is evaluated using simulated data as access to such sensitive federal systems that capture data on weapon sales, transfer and ownership is challenging. Future studies can build on our research by leveraging such data for wholesome conclusions on system functionality. Our system is also subject to additional functional limitations (e.g., our study does not address the case of willful entering of incorrect information, even though the "update" process enables correction of data discrepancies).Our study only presents certain functionalities of the proposed system as this research effort is mainly for demonstration purposes. For example, we implement the search function based on limited search criteria that include "serial number", "first name", and "last name", which means that the full functionality of the system has not been shown in this study. We note that additional criteria and functionalities of the system can be demonstrated using a similar approach as in the study. Lastly, our study is limited to the implementation of smart contract on the primary chain with the same Blockchain carrying all the transactions, smart contract, and the data that the smart contract can access. The amount of data that a smart contract can store has no theoretical upper limit, and both the smart contract and the data the smart contract uses are shared across all nodes of the Blockchain network independently. The smart contract's queries, updates, and validation are not resource-intensive processes as a result by avoiding tracing the blocks of a Blockchain. However, as the amount of data that smart contracts store grows, it may become necessary to offload the smart contract data from the on-chain network using sidechains or L2 scaling [55] to the off-chain network. Future research can expand on our framework to connect the Blockchain separately and expand off-chain data using sidechains. Nevertheless, by moving the smart contract data off-chain, certain security issues must be resolved

5 PRACTICAL RELEVANCE AND IMPLICATION

A blockchain-based framework is proposed for use in gun-related investigations, specifically crime-gun tracing. Conducting a trace is standard gun crime investigative work, and data inconsistencies and inaccuracies can hamper this process, leading to reduced success rates or failed investigations. A recent report released by the U.S. Government Accountability Office [5](2022, p. 29), for example, reinforced the importance of having a robust gun-tracing and monitoring system – "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", as well as the importance of information sharing across national borders. The proposed blockchain based framework seeks to support the above-discussed functionalities, by improving data integrity, trust, and overall success in gun related investigations. When data accuracy and integrity is upheld in systems used in gun-related documentations, it becomes easier to successfully track the path of a crime gun along its chain of custody to a potential crime suspect. This provides a powerful tool that aids gun crime investigations, consequently leading to reductions in gun violence.

6 CONCLUSION

Blockchain has been touted in the extant literature for its ability to ensure trust, transparency, and enhanced information integrity in data-intensive domains such as healthcare and the Internet of Things (IoT). Our study reinforced the potential of blockchain in reducing gun violence through enhanced, efficient and expedited crime-gun tracing and overall related investigations. By mitigating limitations in current methods (e.g., lack of standardized documentation frameworks for firearm sales and transfers sellers, manufacturers, owners and investigators that result in data integrity issues, inconsistencies, incompleteness or missing records), the proposed blockchain-based framework enhances and expedites crime gun tracing along its chain of custody from the manufacturer to a licensed dealer, and importantly to the most current firearm custodian or suspect.

APPENDICES

Appendix A. Smart Contract Code

```
pragma solidity >=0.7.0 <0.9.0;

/**
 * @title Ballistic Information Processing
 * @dev This Smart Contract captures the firearm sales and tracing of gun crimes
 */
contract gunRegistrationAndTracing {
    address admin = 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4;
    uint idxTest = 99;
    /**
```

[5] https://www.gao.gov/assets/gao-22-104680.pdf

```
 * This structure holds the address of all the registered users and their roles
*/
struct authorizedUser {
    address user;
    // A value of 1 in role is for seller and 2 is to trace the firearm
    uint role;
    uint userNumber;
    string sellerName;
    uint totalGunSales;
}

struct gunOwnerStruct {
    address seller;
    string name;
    string physicalAddress;
    uint dob;
    uint zipcode;
    string serial;
    uint ownerId;
    uint gunStatus;
}

struct gunTraceStruct {
    address seller;
    string suspectName;
    string physicalAddress;
    uint dob;
    uint zipcode;
    string serial;
    uint ownerId;
    uint gunStatus;
    uint caseStatus;
    uint caseId;
}
```

```
    /**
     * This structure holds the index values of gunOwner corresponding to the gunSeller
     * The key here is the serial number the owner holds
    */
    struct gunOwnerSellerStruct {
        address seller;
        string serial;
    }
    mapping(string => uint) public ownerSellerIdx;
    mapping(string => uint) public ownerSellerNameIdx;
    mapping(address => uint) public userIdx;



    authorizedUser[] public allUsers;
    gunOwnerStruct[] public gunOwners;
    gunTraceStruct[] public gunCases;

    /**
     * This register function first checks if the contract creater is the one who is trying to register users
     * Once the initial validation completes, the function registers a user with the respective role
     */
    function registerUser(address _userAddress, uint _role, string memory _sellerName) public {
        require (msg.sender == admin);
        authorizedUser memory newUserStruct = authorizedUser ({
            user: _userAddress,
            role: _role,
            userNumber: allUsers.length + 1,
            sellerName: _sellerName,
            totalGunSales: 0
        });
        allUsers.push(newUserStruct);
```

```
        userIdx[_userAddress] = allUsers.length;
    }

    /**
     * This update function first checks if the contract creater is the one who is trying to update the registered users. Once the initial validation completes, the function updates the privileges of the user with the respective role. There are two variations of the functions provided for reference. The address of the user can be directly used to update the records or the user number (Taken as a sequence for simplicity is used for updating the user)
     */
    function updateUser(uint _role, uint _userNumber, string memory _sellerName, uint _totalGunSales) public {
        require (msg.sender == admin);
        authorizedUser memory updateUserStruct = allUsers[_userNumber - 1];
        //updateUserStruct.user = _userAddress;
        updateUserStruct.role = _role;
        updateUserStruct.sellerName = _sellerName;
        updateUserStruct.totalGunSales = _totalGunSales;
        allUsers[_userNumber - 1] = updateUserStruct;
    }

    function updateUserUsingAddress(address _userAddress, uint _role, string memory _sellerName, uint _totalGunSales) public {
        require (msg.sender == admin);
        uint _userNumber = userIdx[_userAddress];
        idxTest = _userNumber;
        authorizedUser memory updateUserStruct = allUsers[_userNumber - 1];
        updateUserStruct.user = _userAddress;
        updateUserStruct.role = _role;
        updateUserStruct.sellerName = _sellerName;
        updateUserStruct.totalGunSales = _totalGunSales;
        allUsers[_userNumber - 1] = updateUserStruct;
    }
    /**
```

```
     * This UpdateAccessPrivileges function first checks if the contract creater is the one
who is trying to update the registered users. Once the initial validation completes, the
function updates the privileges of the user with the respective role. Requires userNumber.
User address could also be used to update the access privileges similar to
updateUserUsingAddress function.
     */
    function UpdateAccessPrivileges(uint _role, uint _userNumber) public {
        require (msg.sender == admin);
        authorizedUser memory updateUserStruct = allUsers[_userNumber - 1];
        updateUserStruct.role = _role;
        allUsers[_userNumber - 1] = updateUserStruct;
    }

    /**
     * This newFirearmsSale function first checks if the role of the user requesting to
sell a Gun is a registered seller
     * Using the address and the userNumber passed
     */
    function newFirearmsSale(address _userAddress, uint _userNumber, string memory _name,
string memory _physicalAddress,
    uint _dob, uint _zipcode, string memory _serial, uint _gunStatus) public {
        authorizedUser memory currentUserStruct = allUsers[_userNumber - 1];
        require (currentUserStruct.role == 1);
        require (currentUserStruct.user == _userAddress);
        currentUserStruct.totalGunSales += 1;
        allUsers[_userNumber - 1] = currentUserStruct;
        gunOwnerStruct memory newGunOwnerStruct = gunOwnerStruct ({
            seller: _userAddress,
            name: _name,
            physicalAddress: _physicalAddress,
            dob: _dob,
            zipcode: _zipcode,
            serial: _serial,
            ownerId: gunOwners.length + 1,
            gunStatus: _gunStatus
```

```
        });
        gunOwners.push(newGunOwnerStruct);

        ownerSellerIdx[_serial] = gunOwners.length;
        ownerSellerNameIdx[_name] = gunOwners.length;
    }

    /**
     * This update Gun function first checks if the role of the user requesting to sell a Gun is a registered seller. Using the address and the userNumber passed. Only the records of the registered gun seller are updated. OwnerId is required to update the correct record
     */
    function updateFirearms(address _userAddress, uint _userNumber, string memory _name, string memory _physicalAddress,
    uint _dob, uint _zipcode, string memory _serial, uint _gunStatus, uint _ownerId) public {
        authorizedUser memory currentUserStruct = allUsers[_userNumber - 1];
        require (currentUserStruct.role == 1);
        require (currentUserStruct.user == _userAddress);
        gunOwnerStruct memory currentGunOwnerStruct = gunOwners[_ownerId - 1];
        currentGunOwnerStruct.name = _name;
        currentGunOwnerStruct.physicalAddress = _physicalAddress;
        currentGunOwnerStruct.dob = _dob;
        currentGunOwnerStruct.zipcode = _zipcode;
        currentGunOwnerStruct.serial= _serial;
        currentGunOwnerStruct.gunStatus = _gunStatus;
        gunOwners[_ownerId - 1] = currentGunOwnerStruct;
    }

    /**
     * This update Gun function first checks if the role of the user requesting to sell a Gun is a registered seller. Using the address and the userNumber passed, the records of the registered gun seller alone are updated. OwnerId is required to update the correct record
     */
```

```
    function updateFirearmsStatus(address _userAddress, uint _userNumber, string memory
_serial, uint _gunStatus, uint _ownerId) public {
        authorizedUser memory currentUserStruct = allUsers[_userNumber - 1];
        require (currentUserStruct.role == 1);
        require (currentUserStruct.user == _userAddress);
        gunOwnerStruct memory currentGunOwnerStruct = gunOwners[_ownerId - 1];
        currentGunOwnerStruct.serial= _serial;
        currentGunOwnerStruct.gunStatus = _gunStatus;
        gunOwners[_ownerId - 1] = currentGunOwnerStruct;
    }

    /**
     * This search Gun function first checks if the role of the user requesting to search
records is admin or a user with trace authority. Using the address and the userNumber
passed. Required parameters: 1. user address is the address of the user trying to record
the gun sale, 2. The gun serial number. There is a second version possible, with the user
number based search instead of passing the user address
     */

    function searchGunBySerial(address _userAddress, string memory _serial)
    public view returns  ( string memory, string memory, uint, uint, string memory, uint )
{
        uint _userNumber = userIdx[_userAddress];
        authorizedUser memory currentUserStruct = allUsers[_userNumber - 1];
        require (msg.sender == admin || currentUserStruct.role == 2);
        require (currentUserStruct.user == _userAddress);
        gunOwnerStruct memory currentGunOwnerStruct;
        uint _gunOwnerNumber = ownerSellerIdx[_serial];
        currentGunOwnerStruct = gunOwners[_gunOwnerNumber];
        return (currentGunOwnerStruct.name,
                currentGunOwnerStruct.physicalAddress,
                currentGunOwnerStruct.dob,
                currentGunOwnerStruct.zipcode,
                currentGunOwnerStruct.serial,
                currentGunOwnerStruct.gunStatus);
```

```
    }
    /**
     * This search Gun function first checks if the role of the user requesting to search records is admin or a user with trace authority. Using the address and the userNumber passed, search the Blockchain by first and last name (Currently, the structure is having a single variable _name for simplicity)
     */

    function searchGunByName(address _userAddress, string memory _name)
    public view returns ( string memory, string memory, uint, uint, string memory, uint ) {
        uint _userNumber = userIdx[_userAddress];
        authorizedUser memory currentUserStruct = allUsers[_userNumber - 1];
        require (msg.sender == admin || currentUserStruct.role == 2);
        require (currentUserStruct.user == _userAddress);
        gunOwnerStruct memory currentGunOwnerStruct;
        uint _gunOwnerNumber = ownerSellerNameIdx[_name];
        currentGunOwnerStruct = gunOwners[_gunOwnerNumber - 1];
        return (currentGunOwnerStruct.name,
                currentGunOwnerStruct.physicalAddress,
                currentGunOwnerStruct.dob,
                currentGunOwnerStruct.zipcode,
                currentGunOwnerStruct.serial,
                currentGunOwnerStruct.gunStatus);
    }

    function compareStrings(string memory a, string memory b) public pure returns (bool) {
        return (keccak256(bytes(a)) == keccak256(bytes(b)));
    }
    /**
     * This create a new gun trace record function. The first check is if the creater is a registered user with trace role
     * Once the initial validation completes, the function creates a new crime investigation case
     */
```

```
    function newTraceInvestigation(uint _userNumber, address _seller, string memory
_suspectName,
    string memory _physicalAddress, uint _dob, uint _zipcode, string memory _serial, uint
_ownerId, uint _gunStatus, uint _caseStatus ) public {
        authorizedUser memory currentUserStruct = allUsers[_userNumber - 1];
        require (msg.sender == admin || currentUserStruct.role == 2);
        require (currentUserStruct.user == msg.sender);
        gunTraceStruct memory newTraceStruct = gunTraceStruct ({
            seller: _seller,
            suspectName: _suspectName,
            physicalAddress: _physicalAddress,
            dob: _dob,
            zipcode: _zipcode,
            serial: _serial,
            ownerId: _ownerId,
            gunStatus: _gunStatus,
            caseStatus: _caseStatus,
            caseId: gunCases.length + 1
        });
        gunCases.push(newTraceStruct);
    }

    /**
     * This update trace request function first checks if the role of the user is a
registered user with trace role using the address and the userNumber passed. The caseId is
required to update the correct record (Update Case Status)
     */

    function updateTraceCaseStatus(uint _userNumber, uint _caseStatus, uint _caseId) public
{
        authorizedUser memory currentUserStruct = allUsers[_userNumber - 1];
        require (msg.sender == admin || currentUserStruct.role == 2);
        require (currentUserStruct.user == msg.sender);
        gunTraceStruct memory currentGunTraceStruct = gunCases[_caseId - 1];
        currentGunTraceStruct.caseStatus = _caseStatus;
```

```
        gunCases[_caseId - 1] = currentGunTraceStruct;
    }

    /**
     * This update trace request function first checks if the role of the user is a registered user with trace role, using the address and the userNumber passed. The caseId is required to update the correct record (Update Prime Suspect)
     */
    function updateTraceSuspect(uint _userNumber, string memory _suspectName, uint _caseId) public {
        authorizedUser memory currentUserStruct = allUsers[_userNumber - 1];
        require (msg.sender == admin || currentUserStruct.role == 2);
        require (currentUserStruct.user == msg.sender);
        gunTraceStruct memory currentGunTraceStruct = gunCases[_caseId - 1];
        currentGunTraceStruct.suspectName = _suspectName;
        gunCases[_caseId - 1] = currentGunTraceStruct;
    }

    /**
     * This update trace request function first checks if the role of the user is a registered user with trace role using the address and the userNumber passed. The caseId is required to update the correct record
     */
    function updateAdditionalTraces(uint _userNumber, address _seller, string memory _suspectName, string memory _physicalAddress,
    uint _dob, uint _zipcode, string memory _serial, uint _ownerId, uint _gunStatus, uint _caseStatus, uint _caseId) public {
        authorizedUser memory currentUserStruct = allUsers[_userNumber - 1];
        require (msg.sender == admin || currentUserStruct.role == 2);
        require (currentUserStruct.user == msg.sender);
        gunTraceStruct memory currentGunTraceStruct = gunCases[_caseId - 1];
        currentGunTraceStruct.seller = _seller;
        currentGunTraceStruct.suspectName = _suspectName;
        currentGunTraceStruct.physicalAddress = _physicalAddress;
        currentGunTraceStruct.dob = _dob;
```

```
        currentGunTraceStruct.zipcode = _zipcode;
        currentGunTraceStruct.serial= _serial;
        currentGunTraceStruct.ownerId= _ownerId;
        currentGunTraceStruct.gunStatus = _gunStatus;
        currentGunTraceStruct.caseStatus = _caseStatus;
        gunCases[_caseId - 1] = currentGunTraceStruct;
    }
}
```

REFERENCES

[1] E. R. Maguire, W. R. King, M. C. Matusiak, and B. Campbell, "Testing the Effects of People, Processes, and Technology on Ballistic Evidence Processing Productivity," Police Q., vol. 19, no. 2, pp. 199–215, Jun. 2016, doi: 10.1177/1098611115618374.

[2] A. Pattavina, Information Technology and the Criminal Justice System. SAGE, 2005.

[3] T. E. Lizotte and O. Ohar, "Forensic firearm identification of semiautomatic handguns using laser formed microstamping elements," in Optical Technologies for Arming, Safing, Fuzing, and Firing IV, Sep. 2008, vol. 7070, pp. 180–194. doi: 10.1117/12.796521.

[4] W. R. King, B. A. Campbell, M. C. Matusiak, and C. M. Katz, "Forensic Evidence and Criminal Investigations: The Impact of Ballistics Information on the Investigation of Violent Crime in Nine Cities," J. Forensic Sci., vol. 62, no. 4, pp. 874–880, 2017, doi: 10.1111/1556-4029.13380.

[5] D. Lambert, "Intelligence-Led Policing in a Fusion Center," FBI Law Enforc. Bull., vol. 79, no. 12, pp. 1–6, 2010.

[6] S. Nakamoto, "A Peer-to-Peer Electronic Cash System," p. 24.

[7] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," MIS Q., vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.

[8] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," in 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Mar. 2018, pp. 1–7. doi: 10.1109/ISDFS.2018.8355340.

[9] K. V. Anderson and H. Z. Henriksen, "The First Leg of E-Government Research: Domains and Application Areas 1998-2003," Int. J. Electron. Gov. Res. IJEGR, vol. 1, no. 4, pp. 26–44, Oct. 2005, doi: 10.4018/jegr.2005100102.

[10] J. N. Danziger and K. V. Andersen, "The Impacts of Information Technology on Public Administration: An Analysis of Empirical Research from the 'Golden Age' of Transformation," Int. J. Public Adm., vol. 25, no. 5, pp. 591–627, Apr. 2002, doi: 10.1081/PAD-120003292.

[11] Å. Grönlund and T. A. Horan, "Introducing e-Gov: History, Definitions, and Issues," Commun. Assoc. Inf. Syst., vol. 15, no. 1, Jun. 2005, doi: 10.17705/1CAIS.01539.

[12] S. Arshad and S. Khurram, "Can government's presence on social media stimulate citizens' online political participation? Investigating the influence of transparency, trust, and responsiveness," Gov. Inf. Q., vol. 37, no. 3, p. 101486, Jul. 2020, doi: 10.1016/j.giq.2020.101486.

[13] J. C. Bertot, P. T. Jaeger, and J. M. Grimes, "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies," Gov. Inf. Q., vol. 27, no. 3, pp. 264–271, Jul. 2010, doi: 10.1016/j.giq.2010.03.001.

[14] "Promoting transparency and accountability through ICTs, social media, and collaborative e-government | Emerald Insight." https://www.emerald.com/insight/content/doi/10.1108/17506161211214831/full/html (accessed Oct. 27, 2022).

[15] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," Gov. Inf. Q., vol. 34, no. 3, pp. 355–364, Sep. 2017, doi: 10.1016/j.giq.2017.09.007.

[16] Z. Tang, A. S. Miller, Z. Zhou, and M. Warkentin, "Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations," Gov. Inf. Q., vol. 38, no. 2, p. 101572, Apr. 2021, doi: 10.1016/j.giq.2021.101572.

[17] G. Pernagallo and B. Torrisi, "A logit model to assess the transparency of Italian public administration websites," Gov. Inf. Q., vol. 37, no. 4, p. 101519, Oct. 2020, doi: 10.1016/j.giq.2020.101519.

[18] G. A. Porumbescu, M. Cucciniello, and J. R. Gil-Garcia, "Accounting for citizens when explaining open government effectiveness," Gov. Inf. Q., vol. 37, no. 2, p. 101451, Apr. 2020, doi: 10.1016/j.giq.2019.101451.

[19] B. Faber, T. Budding, and R. Gradus, "Assessing social media use in Dutch municipalities: Political, institutional, and socio-economic determinants," Gov. Inf. Q., vol. 37, no. 3, p. 101484, Jul. 2020, doi: 10.1016/j.giq.2020.101484.

[20] R. Dekker, P. van den Brink, and A. Meijer, "Social media adoption in the police: Barriers and strategies," Gov. Inf. Q., vol. 37, no. 2, p. 101441, Apr. 2020, doi: 10.1016/j.giq.2019.101441.

[21] Q. Chen, C. Min, W. Zhang, G. Wang, X. Ma, and R. Evans, "Unpacking the black box: How to promote citizen engagement through government social media during the COVID-19 crisis," Comput. Hum. Behav., vol. 110, p. 106380, Sep. 2020, doi: 10.1016/j.chb.2020.106380.

[22] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing,"

Future Gener. Comput. Syst., vol. 95, pp. 420–429, Jun. 2019, doi: 10.1016/j.future.2019.01.018.

[23] S. Stoughton, "Law enforcement's warrior problem," vol. 128, pp. 225–234.

[24] H. Hou, "The Application of Blockchain Technology in E-Government in China," in 2017 26th International Conference on Computer Communication and Networks (ICCCN), Jul. 2017, pp. 1–4. doi: 10.1109/ICCCN.2017.8038519.

[25] C. Sullivan and E. Burger, "E-residency and blockchain," Comput. Law Secur. Rev., vol. 33, no. 4, pp. 470–481, Aug. 2017, doi: 10.1016/j.clsr.2017.03.016.

[26] C. Feng et al., "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," IEEE Netw., vol. 35, no. 1, pp. 130–137, Jan. 2021, doi: 10.1109/MNET.011.2000223.

[27] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-Enhanced Data Sharing With Traceable and Direct Revocation in IIoT," IEEE Trans. Ind. Inform., vol. 17, no. 11, pp. 7669–7678, Nov. 2021, doi: 10.1109/TII.2021.3049141.

[28] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," in 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Dec. 2016, pp. 1392–1393. doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.

[29] M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, "Data governance: Organizing data for trustworthy Artificial Intelligence," Gov. Inf. Q., vol. 37, no. 3, p. 101493, Jul. 2020, doi: 10.1016/j.giq.2020.101493.

[30] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," Comput. Secur., vol. 88, p. 101653, Jan. 2020, doi: 10.1016/j.cose.2019.101653.

[31] R. A. Michelin et al., "SpeedyChain: A framework for decoupling data from blockchain for smart cities," in Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York, NY, USA, Nov. 2018, pp. 145–154. doi: 10.1145/3286978.3287019.

[32] Md. A. Rahman, Md. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City," IEEE Access, vol. 7, pp. 18611–18621, 2019, doi: 10.1109/ACCESS.2019.2896065.

[33] D. B. Rawat, L. Njilla, K. Kwiat, and C. Kamhoua, "iShare: Blockchain-Based Privacy-Aware Multi-Agent Information Sharing Games for Cybersecurity," in 2018 International Conference on Computing, Networking and Communications (ICNC), Mar. 2018, pp. 425–431. doi: 10.1109/ICCNC.2018.8390264.

[34] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, Jan. 2018, doi: 10.1016/j.csbj.2018.07.004.

[35] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Oct. 2017, pp. 1–5. doi: 10.1109/PIMRC.2017.8292361.

[36] J. Bao, D. He, M. Luo, and K.-K. R. Choo, "A Survey of Blockchain Applications in the Energy Sector," IEEE Syst. J., vol. 15, no. 3, pp. 3370–3381, Sep. 2021, doi: 10.1109/JSYST.2020.2998791.

[37] S. S. Seshadri et al., "IoTCop: A Blockchain-Based Monitoring Framework for Detection and Isolation of Malicious Devices in Internet-of-Things Systems," IEEE Internet Things J., vol. 8, no. 5, pp. 3346–3359, Mar. 2021, doi: 10.1109/JIOT.2020.3022033.

[38] R. M. Parizi, A. Dehghantanha, A. Azmoodeh, and K.-K. R. Choo, "Blockchain in Cybersecurity Realm: An Overview," in Blockchain Cybersecurity, Trust and Privacy, K.-K. R. Choo, A. Dehghantanha, and R. M. Parizi, Eds. Cham: Springer International Publishing, 2020, pp. 1–5. doi: 10.1007/978-3-030-38181-3_1.

[39] J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," IEEE Access, vol. 7, pp. 36500–36515, 2019, doi: 10.1109/ACCESS.2019.2903554.

[40] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telemat. Inform., vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[41] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," IEEE Consum. Electron. Mag., vol. 7, no. 2, pp. 18–21, 2018.

[42] L. Soltanisehat, R. Alizadeh, H. Hao, and K.-K. R. Choo, "Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review," IEEE Trans. Eng. Manag., 2020.

[43] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Comput. Secur., vol. 78, pp. 126–142, 2018.

[44] K. Francisco and D. Swanson, "The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency," Logistics, vol. 2, no. 1, p. 2, 2018.

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

[46] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," Future Gener. Comput. Syst., vol. 91, pp. 527–535, 2019.

[47] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability," Comput. Struct. Biotechnol. J., vol. 16, pp. 224–230, 2018.

[48] D. M. Hureau and A. A. Braga, "The trade in tools: The market for illicit guns in high-risk networks," Criminology, vol. 56, no. 3, pp. 510–545, 2018.

[49] G. E. Tita and M. Barragan, "Understanding the illicit gun market in Los Angeles: A review of the empirical evidence," Gun Stud., pp. 75–94, 2018.

[50] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," J. Manag. Inf. Syst., vol. 24, no. 3, pp. 45–77, 2007.

[51] H. A. Simon, "Artificial intelligence: an empirical science," Artif. Intell., vol. 77, no. 1, pp. 95–127, 1995.

[52] J. vom Brocke, A. Hevner, and A. Maedche, "Introduction to design science research," in Design science research. Cases, Springer, 2020, pp. 1–13.

[53] M. C. Tremblay, A. R. Hevner, and D. J. Berndt, "Focus groups for artifact refinement and evaluation in design research," Commun. Assoc. Inf. Syst., vol. 26, no. 1, p. 27, 2010.

[54] J. Venable, J. Pries-Heje, and R. Baskerville, "FEDS: a framework for evaluation in design science research," Eur. J. Inf. Syst., vol. 25, no. 1, pp. 77–89, 2016.

[55] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," J. Netw. Comput. Appl., vol. 149, p. 102471, 2020.