Chapter 14

A BLOCKCHAIN MODEL FOR SHARING INFORMATION IN CRIMINAL JUSTICE SYSTEMS

Pardon Ramazhamba and Hein Venter

Abstract Criminal justice systems around the world, including in South Africa, encounter missing case dockets and digital evidence. Problems are also posed by the mechanisms used to share criminal case data, especially email and paper documents that provide exposure to illegal data alteration.

This chapter describes a blockchain model for sharing criminal case data securely and efficiently with authorized criminal justice system entities. The model is implemented using Hyperledger Fabric and promising results were obtained during the simulation experiments. The model enables entities to access criminal case data in real time, which helps speed up the delivery of justice. Moreover, the model improves collaboration among the various entities, especially when it comes to joint operations and investigations involving law enforcement and prosecutors. The model also stores credible evidence because the underlying data is immutable and cannot be deleted.

Keywords: Criminal justice system, digital evidence sharing, blockchain

1. Introduction

Information and communications technologies have significantly advanced the collection, storage, processing and analysis of digital information. Interactions with digital information tend to leave digital footprints or evidence of what happened, when and where. When a crime is committed, a forensic investigator creates a report that seeks to ascertain what occurred, where it occurred, when it occurred and who might be involved, and suggests why it occurred and attempts to explain how it occurred. These issues play critical roles in the criminal justice process because they seek to prove that a subject is linked to a specific criminal activity. Preserving such crucial information that may convict or acquit a subject requires innovative information and communications technology solutions that are secure and efficient.

In parliamentary questioning, the South African Police Service revealed that 688 criminal case dockets went missing between April 2008 and February 2009 [10]. The South African Police Service rolled out its Integrated Case and Docket Management System to address the problems posed by lost or stolen case dockets or evidence. In 2020, a docket archive store assessment conducted by the South African Department of Community Safety reported that approximately 63% of the case dockets in the Western Cape were lost in the archiving system and 14% of the dockets were lost in court [17, 25]. Also in 2020, the South African Broadcasting Corporation reported that almost 400 corruption, theft and fraud cases involving the South African Police Service were under investigation [22]. In 2022, Carte Blanche [5] reported that case dockets were sold by a corrupt South African Police Service official before they could be entered into the Integrated Case and Docket Management System.

These reports and others indicate that a different approach is required to ensure that criminal case data and digital evidence are secure and shareable. Indeed, The Sunday Times (South Africa) [10] reported that the Integrated Case and Docket Management System did not curb the loss or theft of case dockets in certain high-profile criminal cases. In other instances, case data was unavailable because the applications were designed to share information in a centralized manner. However, decentralization using gateway ports enables nefarious individuals to secretly share information with interested parties outside organizational boundaries.

This chapter proposes a blockchain model for securely preserving and sharing criminal case data during its lifecycle with all the entities in the South African criminal justice system. The novelty of the model lies in its integration of blockchain technology with the applications used by South African criminal justice system entities.

2. Background

This section presents a conceptual model of the South African criminal justice system and describes the blockchain technology employed in this work.

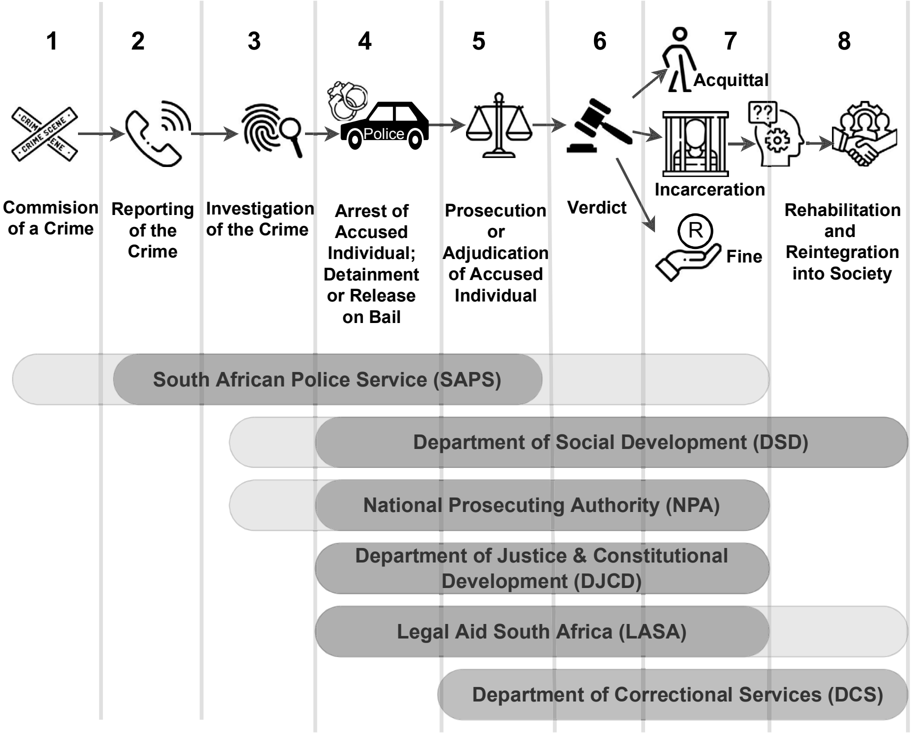

1
2
3
4
5
6
7
8
CRIME SCENE
Police
Acquittal
Incarceration
Fine
R
??
Commision of a Crime
Reporting of the Crime
Investigation of the Crime
Arrest of Accused Individual; Detainment or Release on Bail
Prosecution or Adjudication of Accused Individual
Verdict
Rehabilitation and Reintegration into Society
South African Police Service (SAPS)
Department of Social Development (DSD)
National Prosecuting Authority (NPA)
Department of Justice & Constitutional Development (DJCD)
Legal Aid South Africa (LASA)
Department of Correctional Services (DCS)

Figure 1. South African criminal justice processes [24].

2.1 Conceptual Model

The South African criminal justice system covers the eight processes shown in Figure 1, where each process may involve one or more entities. The first process is the commission of a crime (1) that is reported to the South African Police Service (2). The South African Police Service then opens a criminal case docket and assigns it to an investigating officer. During the investigation process (3), witnesses are identified, evidence is acquired, secured and analyzed, and the accused individual is identified. The accused individual is then arrested by the South African Police Service and detained or released on bail (4).

The arrest and subsequent detention or release of an accused individual involve other entities as required by the South African Constitution. The participating entities include the National Prosecuting Authority (NPA), Department of Justice and Constitutional Development (DJCD), Legal Aid South Africa (LASA) and Department of Social Development (DSD). The National Prosecuting Authority handles the prosecution.

The Department of Justice and Constitutional Development handles the court proceedings [7]. Legal Aid South Africa assists individuals who cannot afford legal representation. The Department of Social Development handles social support programs for vulnerable individuals such as victims of crime, poor people, elderly people and children.

The fifth process (5) is the prosecution of the accused individual, which may involve adjudication instead of a trial. The National Prosecuting Authority accepts the case for prosecution if the evidence is strong enough for court proceedings. This leads to the accused individual being handed over to the Department of Correctional Services (DCS) for pretrial detention, if necessary [6]. The next process is the trial in a court of law that concludes with a verdict (6), resulting in one of three outcomes, acquittal, incarceration or fine (7). The Department of Correctional Services is responsible for incarcerating the convicted individual as well as providing post-sentence rehabilitation and reintegration into society (8).

The six entities use various applications to interact with criminal case data:

- The South African Police Service uses its Integrated Case and Docket Management System to maintain and manage case dockets and forensic evidence.
- The National Prosecuting Authority uses its Electronic Case Management System (ECMS) to handle cases that are ready for prosecution.
- The Department of Justice and Constitutional Development uses its Integrated Case Management System (ICMS) for court proceedings.
- Legal Aid South Africa uses its Electronic Legal Aid Application (eLAA) to assist individuals who cannot afford legal representation.
- The Department of Social Development uses its Child Protection Register (CPR) to assist individuals younger than 18 years old.
- The Department of Correctional Services uses its Integrated Inmate Management System (IIMS) to manage incarceration and post-sentence rehabilitation and reintegration into society.

Figure 2 presents a conceptual view of the integrated South African justice system. The solid lines represent the information flows in the integrated justice system whereas the dotted lines represent information flows of the applications used by the various entities in the integrated

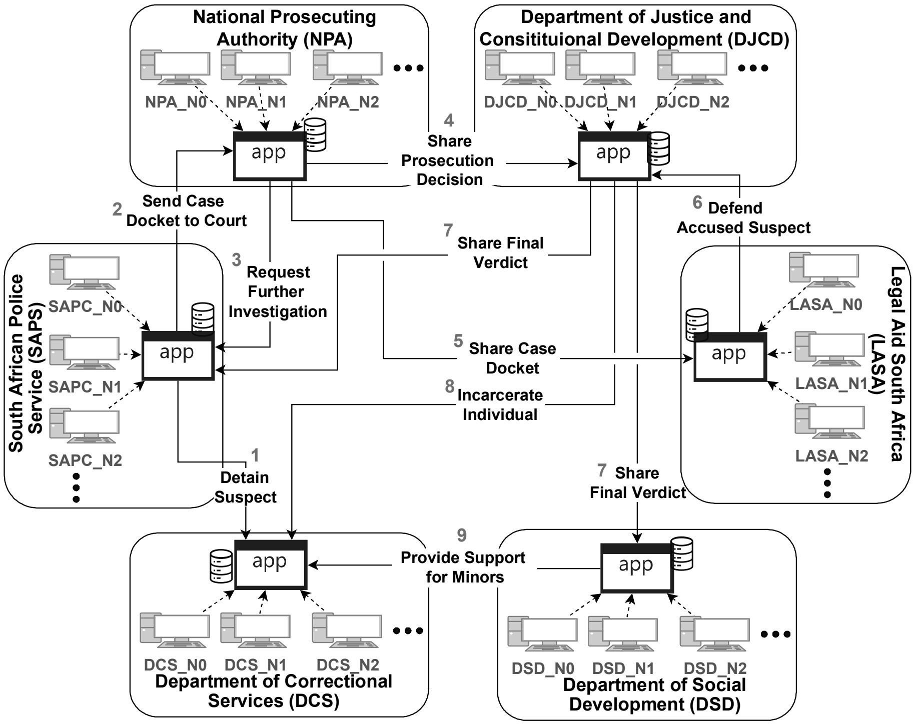

National Prosecuting Authority (NPA)
NPA_N0
NPA_N1
NPA_N2
app
Department of Justice and Consitituional Development (DJCD)
DJCD_N0
DJCD_N1
DJCD_N2
app
4 Share Prosecution Decision
2 Send Case Docket to Court
3 Request Further Investigation
7 Share Final Verdict
6 Defend Accused Suspect
South African Police Service (SAPS)
SAPC_N0
SAPC_N1
SAPC_N2
app
5 Share Case Docket
8 Incarcerate Individual
Legal Aid South Africa (LASA)
LASA_N0
LASA_N1
LASA_N2
app
1 Detain Suspect
7 Share Final Verdict
9 Provide Support for Minors
app
DCS_N0
DCS_N1
DCS_N2
Department of Correctional Services (DCS)
app
DSD_N0
DSD_N1
DSD_N2
Department of Social Development (DSD)

Figure 2. Integrated South African justice system.

justice system. Key to the integration is a gateway portal that shares criminal case data with authorized entities.

2.2 Blockchain Technology

Blockchain technology is employed to implement distributed shared ledger systems that store diverse assets and transactions [9]. Blockchain technology is part of the larger class of distributed ledger technology (DLT) that employs distributed ledger systems to store and share information with various entities. Specifically, blockchain technology groups transactions into blocks that are linked in a chain-like data structure called a blockchain. The principal advantage of distributed ledger technology is that it automatically eliminates problems associated with single points of failure experienced by centralized systems. In a criminal case data management scenario, distributed ledger technology also eliminates problems posed by an entity with centralized power over the data, especially when the entity is reluctant to share the data with other entities. For example, a prosecutor with the National Prosecuting Authority may be reluctant to share information about an accused individual with a representative from Legal Aid South Africa who is assisting the individual with his/her legal defense.

Another benefit of distributed ledger technology is that it enforces trust among entities even when they do not trust each other. This is because all the network nodes provide access to the same data as identical copies of the ledger containing criminal case data are replicated across multiple geographical locations [23]. Therefore, it would not be possible to alter data without it being detected. Distributed ledger technology employs cryptographic techniques to add and append new transactions to achieve the immutability of data across the network. Every interaction stores information governed by its smart contract that self-executes whenever the conditions associated with a transaction are met.

Several blockchain frameworks such as Bitcoin, Ethereum, Quorum, HydraChain, Hyperledger Fabric (HLF) and MultiChain are employed in distributed ledger systems. However, some of the frameworks, namely Bitcoin, Ethereum, Quorum, HydraChain and MultiChain, employ cryptocurrency or mining algorithms to add new transactions to the network. The proposed solution seeks to share criminal case data among entities that are known to each other. Therefore, a private blockchain that does not use cryptocurrency or mining algorithms to add new transactions is adequate.

Hyperledger Fabric was chosen to implement the proposed integrated justice system. Hyperledger Fabric is a private blockchain framework that implements cross-industry blockchain solutions [15]. Hyperledger Fabric employs a membership service provider feature that enrolls participants. Its distributed ledger system incorporates two components, a world state (WS) and transaction log (TL) [13]. The world state stores the data that describes the network state whereas the transaction log records all the transactions that manifest the current state of the ledger.

3. ShareCrimE Model

Figure 3 presents an overview of the proposed blockchain-based ShareCrimE model for sharing criminal case data. The model comprises four components:

- **Users/Agents:** Users and agents are members of the entities that play critical roles in the South African criminal justice system.

- **Applications:** Applications are mechanisms employed by users/agents to interact with the ShareCrimE model.

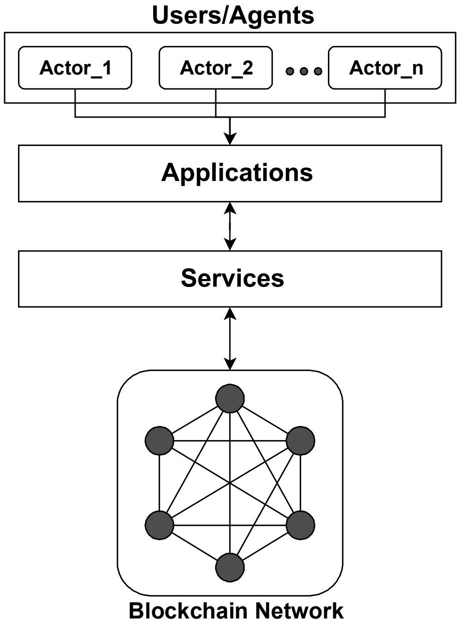


Figure 3. ShareCrimE model.

- **Services:** Services are mechanisms used by applications to interact with the data stored in the blockchain network in the ShareCrimE model.

- **Blockchain Network:** The blockchain network stores and distributes criminal case data to nodes in the ShareCrimE model.

Creating the ShareCrimE model involves five steps: (i) identifying users/agents, (ii) establishing applications, (iii) establishing services, (iv) establishing the blockchain network and (v) integrating the four components created in the previous four steps in the ShareCrimE model.

3.1 Identifying Users/Agents

This step identifies the users/agents in the ShareCrimE model. The South African criminal justice system has six types of users/agents (i.e., entities) that have specific roles in the ShareCrimE model:

- **South African Police Service:** Creates or scans criminal case dockets, appends digital evidence, shares and accesses criminal case data.

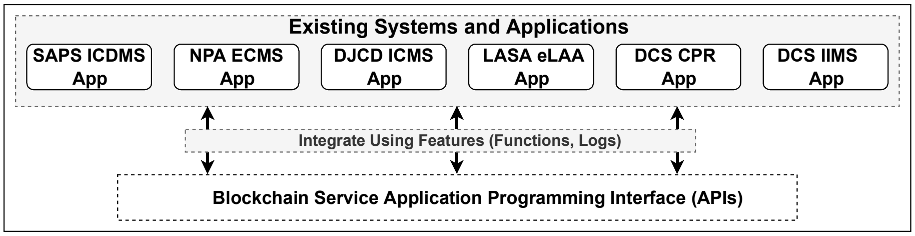

Existing Systems and Applications
SAPS ICDMS App
NPA ECMS App
DJCD ICMS App
LASA eLAA App
DCS CPR App
DCS IIMS App
Integrate Using Features (Functions, Logs)
Blockchain Service Application Programming Interface (APIs)

Figure 4. ShareCrimE model application layer.

- **National Prosecuting Authority:** Creates chargesheets, and shares and accesses criminal case data.
- **Department of Justice and Constitutional Development:** Enters verdicts, and shares and accesses criminal case data.
- **Legal Aid South Africa:** Accesses criminal case data and verdicts, and shares some data with the National Prosecuting Authority.
- **Department of Social Development:** Accesses criminal case data to identify the victims associated with criminal cases.
- **Department of Correctional Services:** Accesses criminal case data and verdicts.

3.2 Establishing Applications

This step identifies the applications employed by users/agents to interact with criminal case data and digital evidence. Figure 4 shows the applications in the ShareCrimE model application layer. The applications are integrated with the blockchain service application programming interface (API) using features such as functions and logs. Integrating the currently-used applications instead of creating new applications saves considerable time and money. The integration also facilitates the implementation of data security. The data stored in the model can be trusted because it is immutable by default, meaning that it cannot be changed or altered for unauthorized purposes.

3.3 Establishing Services

This step identifies the services that implement the interactions between the application layer and blockchain network. The services include identity management, wallet management and network gateway:

- **Identity Management:** This service manages the identities of various resources (e.g., nodes, applications and administrators) in the ShareCrimE model [14]. Each resource is associated with a digital identity or certificate that is used by the blockchain network to control access. Note that the membership service provider in Hyperledger Fabric uses X.509 certificates as identities that rely on a public key infrastructure (PKI) hierarchical model [14].

- **Wallet Management:** This service manages the identities of users/agents that participate in the blockchain network [11]. The service is embedded in the applications employed by users/agents as they interact with the network. The process is initiated when a user/agent logs into an application and submits valid credentials to connect with the blockchain network via a specific channel associated with its identity. The channel is essentially a private blockchain overlay that enables a user/agent to share data secretly.

- **Network Gateway:** This service manages all the interactions between the blockchain network and applications employed by users/agents [11]. Note that an application uses a connection profile to configure a gateway that handles its interactions because it describes a set of components associated with various nodes (i.e., peer nodes and ordering nodes) and certificate authorities [11]. Additionally, the connection profile contains the channel and information about users/agents that use the components [11]. The certificate authority issues public key infrastructure certificates to users/agents.

3.4 Establishing the Blockchain Network

Figure 5 shows the blockchain network used by the ShareCrimE model. The network comprises four components, certificate authorities, raft ordering service, main channel and peer nodes:

- **Certificate Authorities:** The ShareCrimE model comprises six certificate authorities corresponding to the six entities: South African Police Service (SAPS_CA), National Prosecuting Authority (NPA_CA), Department of Justice and Constitutional Development (DJCD_CA), Legal Aid South Africa (LASA_CA), Department of Social Development (DCS_CA) and Department of Correctional Services (DSD_CA).

- **Raft Ordering Service:** The ShareCrimE model comprises six ordering nodes (node_1, . . . , node_6). The raft ordering service

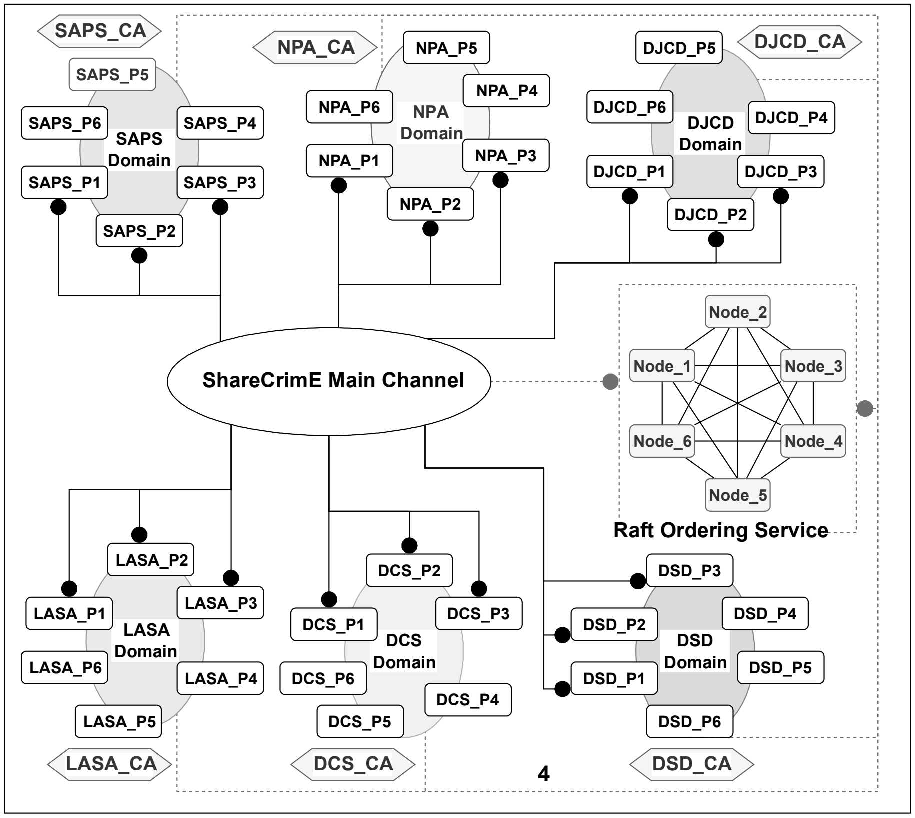


Figure 5. ShareCrimE blockchain network.

collects all the transactions in the network and groups them into blocks [13].

- **Main Channel:** The ShareCrimE model has one main channel that connects to the raft ordering service and six entity domains, integrating the various peer nodes belonging to the six domains. The main channel provides mechanisms that enable the entities to share criminal case data securely and use the private blockchain configurations efficiently. In particular, the channel uses the raft ordering service to group its transactions into blocks and distribute the blocks to relevant peer nodes in the blockchain network.

- **Peer Nodes:** Each entity has six peer nodes, all six connected with their domains and three of the nodes connected directly to the main channel. The 18 peer nodes connected directly to the main channel are called anchor peer nodes because they can send data outside their domain boundaries (e.g., sharing data in nodes in the South African Police Service domain with nodes in the National Prosecuting Authority domain) [13].

An anchor peer node is like a TV anchor who sits in a studio, collects the latest news feeds from journalists in various locations and broadcasts the news to viewers. For example, nodes SAPS_P1, SAPS_P2 and SAPS_P3 may be anchor peers whereas nodes SAPS_P4, SAPS_P5 and SAPS_P6 may be normal peer nodes. Note that all the peer nodes, including anchor peer nodes, have smart contracts and distributed ledger systems. This setup applies to all the entities in the blockchain network.

3.5 Integrating Model Components

Figure 6 shows a high-level representation of the ShareCrimE model obtained by integrating the users/agents, applications, services and blockchain network established in the first four steps. The information flows start when users/agents submit criminal case data using various applications. The ShareCrimE model functionality is embedded in these applications via mechanisms such as features and functions. The identities of users/agents that request access to data in the ShareCrimE model are verified by services to ensure data confidentiality, integrity and availability. The blockchain network used by the ShareCrimE model comprises six certificate authorities, a raft ordering service and 36 peer nodes.

4. ShareCrimE Model Design

This section discusses two key elements of the ShareCrimE model design, information flows and main channel sequence diagram.

4.1 Information Flows

Figure 7 shows the information flows in the ShareCrimE model, including how the components interact with criminal case data and how digital forensic evidence is accessed. The information flows begin when users/agents submit their transactions to the blockchain network in the ShareCrimE model. Transactions are accepted by the ShareCrimE model upon checking that they meet all the predefined conditions stipulated in their smart contracts. Following this, the raft ordering service collects all the accepted transactions, groups them into a block and distributes them to all the nodes in the network. As mentioned above, the distributed ledger system has two components, a world state and a transaction log. The world state stores the data that has resulted in

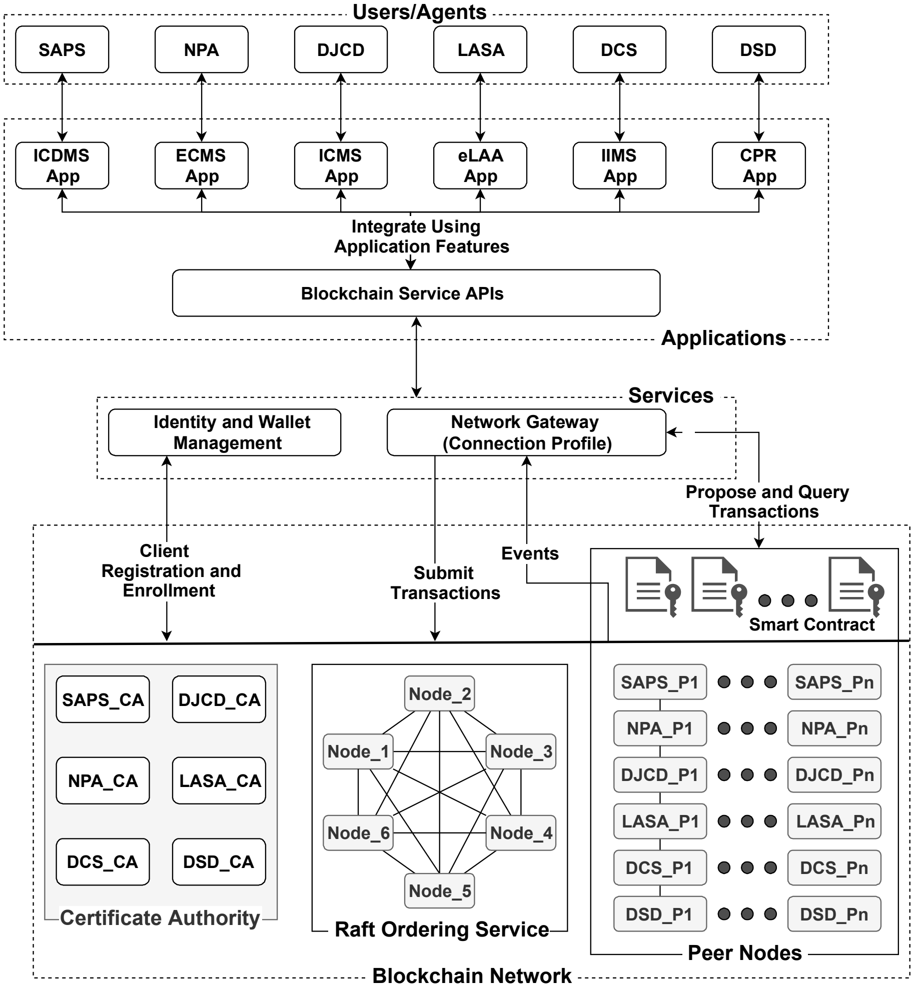


Figure 6. High-level ShareCrimE model.

the current state of the network whereas the transaction log stores data that can be used by forensic investigators or other actors to verify what has transpired for a particular criminal case. Transaction log data is available to law enforcement agencies as well as lawyers and judges.

4.2 Main Channel Sequence Diagram

Figure 8 shows a sequence diagram associated with the main channel. The main channel shares criminal case data among applications used by different entities. The SAPS app in the figure shares criminal case

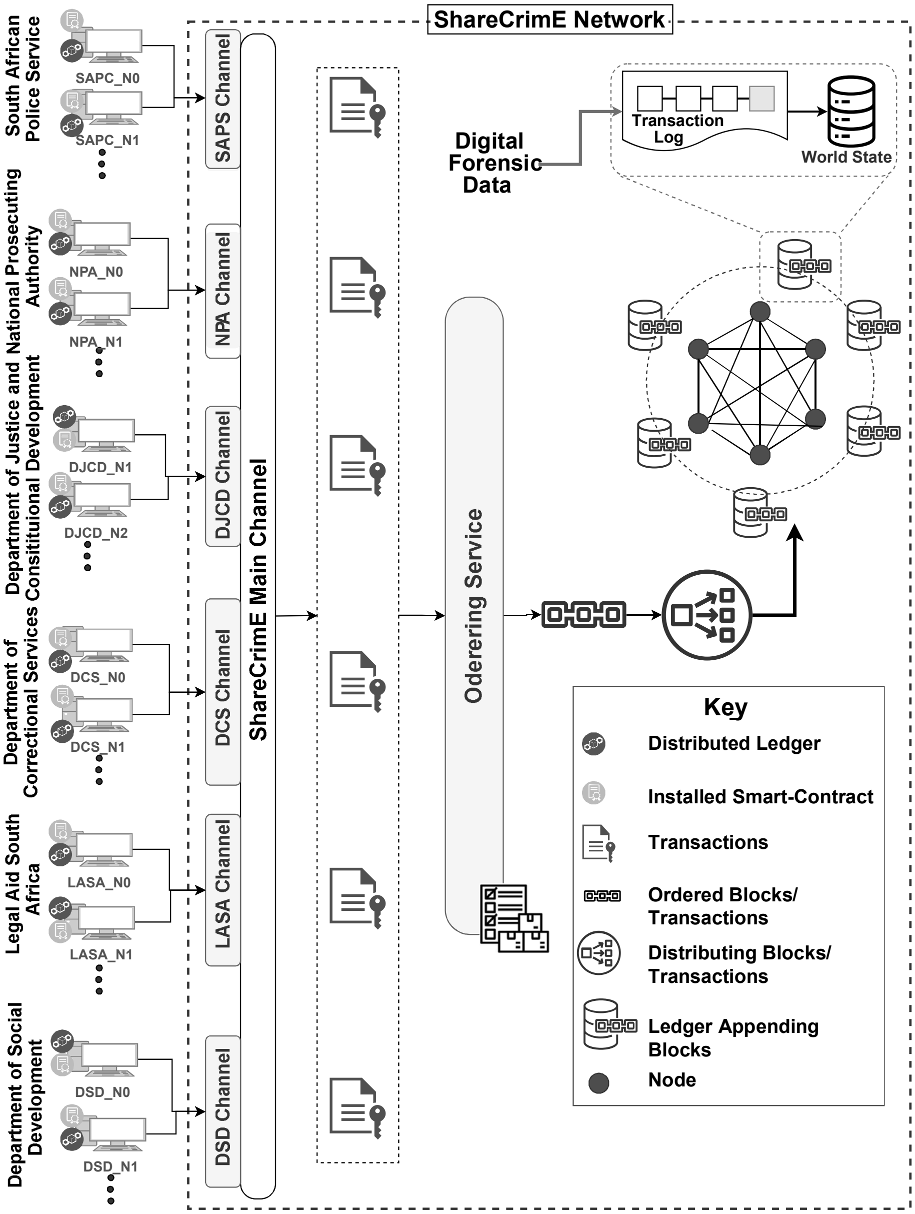


Figure 7. ShareCrimE model information flows.

data about arrested individuals. The process of sharing starts when the SAPS app seeks to create or share criminal case data pertaining to an individual under arrest. Note that all the accepted transactions

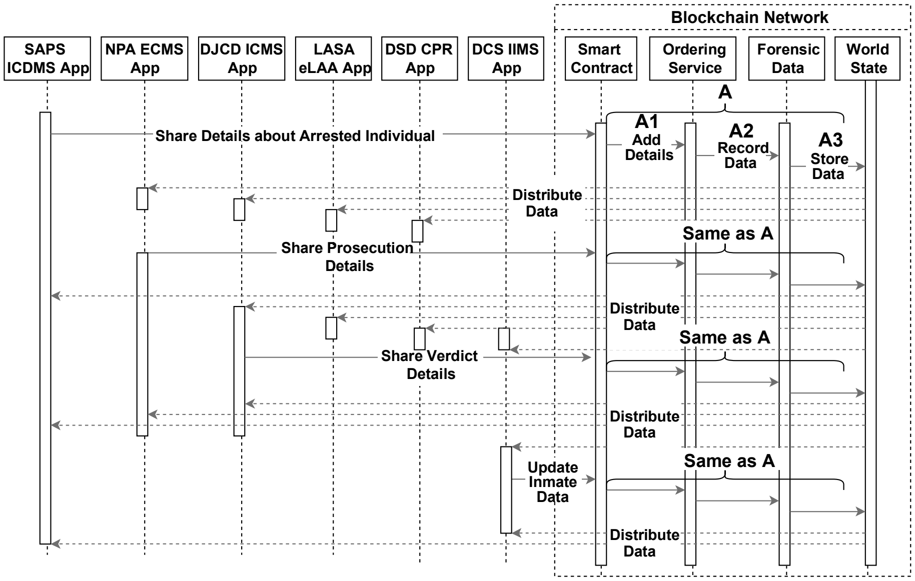


Figure 8. Main channel sequence diagram.

associated with the arrest are grouped into blocks (represented by A1) and distributed to all the nodes in the network. The transactions are stored in transaction logs (represented by A2) and the actual data is stored in the world state (represented by A3). Thereafter, the NPA app shares the prosecution details associated with the same criminal case. The recording and storing of evidence is handled by the blockchain network in the same way as shown for the SAPS app.

After sharing the prosecution details with relevant entities, the DJCD app shares the verdict by submitting it with a smart contract. Next, the blockchain network handles another process involving digital evidence storage and distributes the details to other entities. After the verdict provided by the DJCD app is associated with the incarceration, the details of the individual are shared with the DCS app, including the sentence given to the individual. The DCS app then shares its records with all its members and the SAPS app as part of its role to maintain the records of its inmates.

5. ShareCrimE Prototype Results

A ShareCrimE model prototype was implemented using Hyperledger Fabric v2.2 on a virtual machine with two CPU cores, 6 GB RAM and 60 GB secondary storage. Note that Hyperledger Fabric requires the in-

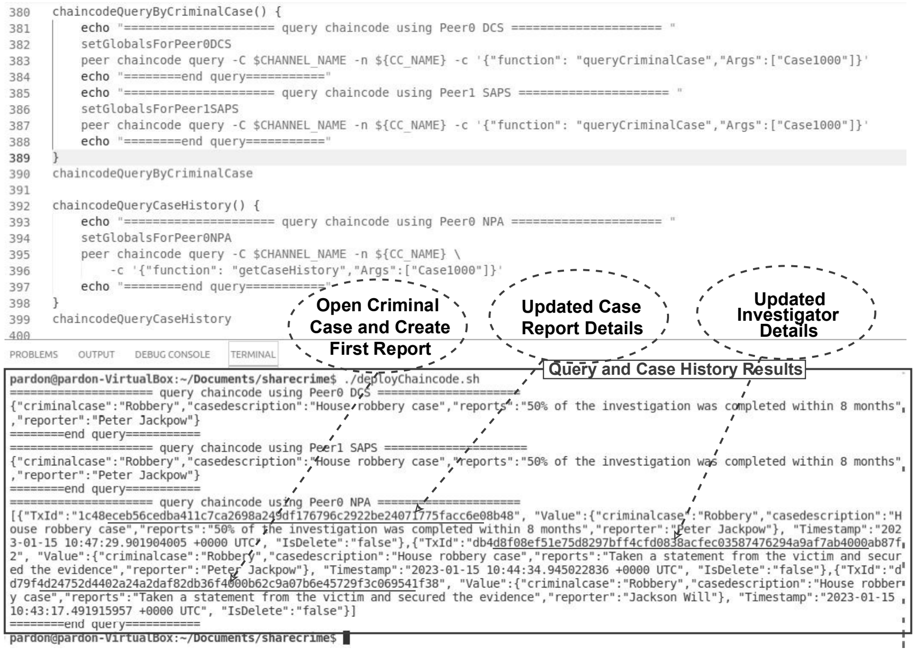
Algorithm 1: ShareCrimE model algorithm.

```
Data: Criminal Case Reports with Digital Evidence
Result: Criminal Case Data Shared with Authorized Entities
Initialize Criminal Case (Report Crime to SAPS) ← 0
if Establishing Blockchain Network then
    Configuration Results
end
if Interacting with Blockchain Network (Operational Results) then
    if Criminal Case is not yet opened then
        Open/Create Criminal Case and add it to the Blockchain Network
    end
    else
        Enable Various Nodes to Access or Query Criminal Case Reports
        if Update Criminal Case Data then
            Update Assigned Reporter/Investigator
            Update Criminal Case Reports
        end
        Query Criminal Case History
    end
end
```

stallation of several packages as prerequisites [12]. After all the prerequisites were met and Hyperledger Fabric was executing, the implementation of the ShareCrimE network was initiated and various processes were executed.

Algorithm 1 specifies the processes involved in the ShareCrimE model simulation. Various results are generated during the simulation. Some results are associated with configuring the blockchain network whereas others are associated with the operation of the ShareCrimE model. The algorithm only produces the results generated during the operational testing phase that involves the creation, modification and querying of criminal case data.

Figure 9 shows the results generated by the two types of query operations, query updated criminal case data and query criminal case history. Query updated criminal case data yields the latest results or updates added to the blockchain network whereas query criminal case history yields the results of all the transactions that sought to create or modify criminal case data in the blockchain network. The results of transactions are marked using TxId in the figure. Lines 380–390 in Figure 9 specify a function used by two peer nodes (Peer0 of DCS and Peer1 of SAPS) to query the latest results of criminal case Case1000. Lines 392–399 specify a function used by Peer0 of NPA to query the entire history of the criminal case Case1000. The results generated by these functions are depicted as query and case history results. The query criminal case



```
chaincodeQueryByCriminalCase() {
    echo "==================== query chaincode using Peer0 DCS ==================== "
    setGlobalsForPeer0DCS
    peer chaincode query -C $CHANNEL_NAME -n ${CC_NAME} -c '{"function": "queryCriminalCase","Args":["Case1000"]}'
    echo "========end query=========="
    echo "==================== query chaincode using Peer1 SAPS ==================== "
    setGlobalsForPeer1SAPS
    peer chaincode query -C $CHANNEL_NAME -n ${CC_NAME} -c '{"function": "queryCriminalCase","Args":["Case1000"]}'
    echo "========end query=========="
}
chaincodeQueryByCriminalCase

chaincodeQueryCaseHistory() {
    echo "==================== query chaincode using Peer0 NPA ==================== "
    setGlobalsForPeer0NPA
    peer chaincode query -C $CHANNEL_NAME -n ${CC_NAME} \
        -c '{"function": "getCaseHistory","Args":["Case1000"]}'
    echo "========end query=========="
}
chaincodeQueryCaseHistory
```

PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
Open Criminal Case and Create First Report
Updated Case Report Details
Updated Investigator Details
Query and Case History Results

```
pardon@pardon-VirtualBox:~/Documents/sharecrime$ ./deployChaincode.sh
==================== query chaincode using Peer0 DCS ====================
{"criminalcase":"Robbery","casedescription":"House robbery case","reports":"50% of the investigation was completed within 8 months",
,"reporter":"Peter Jackpow"}
========end query==========
==================== query chaincode using Peer1 SAPS ====================
{"criminalcase":"Robbery","casedescription":"House robbery case","reports":"50% of the investigation was completed within 8 months",
,"reporter":"Peter Jackpow"}
========end query==========
==================== query chaincode using Peer0 NPA ====================
[{"TxId":"1c48eceb56cedba411c7ca2698a249df176796c2922be24071775facc6e08b48", "Value":{"criminalcase":"Robbery","casedescription":"H
ouse robbery case","reports":"50% of the investigation was completed within 8 months","reporter":"Peter Jackpow"}, "Timestamp":"202
3-01-15 10:47:29.901904005 +0000 UTC", "IsDelete":"false"},{"TxId":"db4d8f08ef51e75d8297bff4cfd0838acfec03587476294a9af7ab4000ab87f
2", "Value":{"criminalcase":"Robbery","casedescription":"House robbery case","reports":"Taken a statement from the victim and secur
ed the evidence","reporter":"Peter Jackpow"}, "Timestamp":"2023-01-15 10:44:34.945022836 +0000 UTC", "IsDelete":"false"},{"TxId":"d
d79f4d24752d4402a24a2daf82db36f4000b62c9a07b6e45729f3c069541f38", "Value":{"criminalcase":"Robbery","casedescription":"House robber
y case","reports":"Taken a statement from the victim and secured the evidence","reporter":"Jackson Will"}, "Timestamp":"2023-01-15
10:43:17.491915957 +0000 UTC", "IsDelete":"false"}]
========end query==========
pardon@pardon-VirtualBox:~/Documents/sharecrime$
```

Figure 9. ShareCrimE model results.

history outlines three transactions used to create or modify data stored in the blockchain network.

6. Evaluation

This section discusses the benefits and limitations of the ShareCrimE model.

Benefits. The ShareCrimE model provides enhanced information security. The mechanisms used to secure criminal case data from unauthorized parties include the use of a distributed ledger system, cryptography, secure communications channels, timestamps and immutable transactions.

Increased transparency is provided by the distributed nature of the model and the processes used to create and modify criminal case data. Creation or modification of criminal case data by rogue parties would be visible because all the authorized entities have access to the entire criminal case data history. This also ensures the integrity of the stored data and evidence.

The ShareCrimE model supports parallel, real-time investigations by the South African Police Service and National Prosecuting Authority. It reduces delays because the National Prosecuting Authority can rapidly determine if case dockets are ready for trial. Additionally, all the authorized entities have seamless access to criminal case data that enables them to complete their reports quickly, ensuring the timely delivery of justice. Also, the ShareCrimE model supports collaboration by users/agents in different geographical locations.

Limitations. A limitation of the ShareCrimE model is the difficulty integrating criminal case data applications used by some entities in the South African criminal justice system. This is especially true for current criminal case data applications that are rendered as services by third parties.

A second limitation is the possible lack of political will. Most of the high-ranking positions in the participating entities are political appointees and it would be a slow process to gain approvals for an advanced technological system from all the stakeholders.

7. Related Work

Lone and Mir [21] have proposed a blockchain-based forensic chain of custody system that is intended to maintain the integrity of criminal case data and evidence. However, their solution employs Hyperledger Composer, which is a deprecated system. Elgohary et al. [8] also employ Hyperledger Composer, but their application is focused on maintaining the chain of custody in image forensic investigations. Other researchers, including Ahmad et al. [1], Bonomi et al. [3], Li et al. [20] and Yunianto et al. [26], adopt the Ethereum framework as their foundation. The problem is that the Ethereum framework employs native cryptocurrency and mining algorithms to add new transactions to their networks, which require considerable computational resources.

The proposed ShareCrimE model bears similarities to the work of Lone and Mir [21], Li et al. [20], Khan et al. [19] and Alruwaili [2] in that they also propose blockchain models for criminal justice systems. The model of Khan et al. [19] is implemented using Hyperledger Sawtooth [16] that employs practical Byzantine fault tolerance and proof of elapsed time consensus algorithms. Hyperledger Sawtooth supports private and public blockchain solutions, but it relies on a third-party (Intel for its Software Guard Extensions) [18].

Table 1 compares the ShareCrimE model with four prominent models in terms of eight key features. The ShareCrimE model stands out from the other models because it accommodates all eight features. Addition-

Table 1. Comparison of the ShareCrimE model with related models.

Model Features	**Lone and Mir [21]**	**Ahmad et al. [1]**	**Bonomi et al. [3]**	**Khan et al. [19]**	**ShareCrimE Model**
Support of private blockchain	✓	✓	✓	✓	✓
No cryptocurrency/mining algorithms required to add transactions			✓		✓
Integration of existing applications					✓
Support of multiple criminal justice system entities	✓	✓	✓	✓	✓
Based on the South African criminal justice system					✓
Sharing of criminal case data and evidence	✓	✓	✓	✓	✓
No third-party reliance	✓	✓		✓	✓
Use of Hyperledger Fabric					✓

ally, it is only one of two models that does not rely on cryptocurrency or mining algorithms to add new transactions.

8. Conclusions

The ShareCrimE model demonstrates how blockchain technology can be adapted to securely share criminal case data among the various authorized entities in a criminal justice system. The ShareCrimE model promotes greater transparency and accountability. Creation or modification of criminal case data by rogue parties would be visible because all the authorized entities have access to the entire criminal case data history. The stored evidence and underlying data are immutable and cannot be deleted, ensuring their security, integrity and availability. All the authorized entities have seamless access to criminal case data that enables them to compile reports and complete tasks quickly, ensuring the timely delivery of justice. The model also enhances collaboration especially when it comes to joint operations and investigations involving law enforcement and prosecutors.

The ShareCrimE model was developed using the South African criminal justice system as a case study. However, the model is generic enough to be customized to criminal justice systems in other countries.

Acknowledgment

This research was supported by the University of Pretoria.

References

[1] L. Ahmad, S. Khanji, F. Iqbal and F. Kamoun, Blockchain-based chain of custody: Towards real-time tamper-proof evidence management, *Proceedings of the Fifteenth International Conference on Availability, Reliability and Security*, article no. 48, 2020.

[2] F. Alruwaili, CustodyBlock: A distributed chain of custody evidence framework, *Information*, vol. 12(2), article no. 88, 2021.

[3] S. Bonomi, M. Casini and C. Ciccotelli, B-CoC: A Blockchain-Based Chain of Custody for Evidence Management in Digital Forensics, arXiv: 1807.10359v1 (arxiv.org/abs/1807.10359v1), 2018.

[4] A. Carstensen and J. Bernhard, Design science research – A powerful tool for improving methods in engineering education research, *European Journal of Engineering Education*, vol. 44(1-2), pp. 85–102, 2019.

[5] Carte Blanche, Dockets for sale, YouTube (`www.youtube.com/watch?v=s1L8j50Sgz0`), April 10, 2022.

[6] Department of Correctional Services, Mission/Vision/Values, Republic of South Africa, Pretoria, South Africa (`www.dcs.gov.za/?page_id=174`), 2023.

[7] Department of Justice and Constitutional Development, Strategic Plan for the Period 2011-2016: Annual Review 2011/12, Document no. RP45/2011, Republic of South Africa, Pretoria, South Africa (`www.gov.za/sites/default/files/gcis_document/201409/mtsf0.pdf`), 2011.

[8] H. Elgohary, S. Darwish and S. Elkaffas, Improving uncertainty in chain of custody for image forensic investigation applications, *IEEE Access*, vol. 10, pp. 14669–14679, 2022.

[9] Hong Kong Applied Science and Technology Research Institute, Whitepaper on Distributed Ledger Technology, Hong Kong, China (`www.astri.org/tdprojects/whitepaper-on-distributed-ledger-technology`), 2022.

[10] G. Hosken and S. Masombuka, A hole in Pistorius conman case docket, *Sunday Times (South Africa)*, March 23, 2016.

[11] Hyperledger Fabric, Application Design Elements, San Francisco, California (`hyperledger-fabric.readthedocs.io/en/release-2.2/developapps/designelements.html`), 2023.

[12] Hyperledger Fabric, Getting Started – Install, San Francisco, California (`hyperledger-fabric.readthedocs.io/en/release-2.5/getting_started.html`), 2023.

[13] Hyperledger Fabric, Glossary, San Francisco, California (`hyperledger-fabric.readthedocs.io/en/latest/glossary.html?highlight=ledger\#`), 2023.

[14] Hyperledger Fabric, Identity, San Francisco, California (`hyperledger-fabric.readthedocs.io/en/release-2.2/identity/identity.html?highlight=certificate\%20authority\#what-is-an-identity`), 2023.

[15] Hyperledger Foundation, About Hyperledger Foundation, San Francisco, California (`www.hyperledger.org/about`), 2023.

[16] Hyperledger Foundation, Hyperledger Sawtooth, San Francisco, California (`www.hyperledger.org/use/sawtooth`), 2023.

[17] L. Isaacs, DA demands in-field training for SAPS officers in the Western Cape, *Eyewitness News (Cape Town)*, March 4, 2022.

[18] S. Kaur, S. Chaturvedi, A. Sharma and J. Kar, A research survey on applications of consensus protocols in blockchain, *Security and Communication Networks*, article no. 6693731, 2021.

[19] A. Khan, M. Uddin, A. Shaikh, A. Laghari and A. Rajput, MF-ledger: Blockchain Hyperledger-Sawtooth-enabled novel and secure multimedia chain-of-custody forensic investigation architecture, *IEEE Access*, vol. 9, pp. 103637–103650, 2021.

[20] M. Li, C. Lal, M. Conti and D. Hu, LEChain: A blockchain-based lawful evidence management scheme for digital forensics, *Future Generation Computer Systems*, vol. 115, pp. 406–420, 2021.

[21] A. Lone and R. Mir, Forensic-chain: Blockchain-based digital forensics chain of custody with PoC in Hyperledger Composer, *Digital Investigation*, vol. 28, pp. 44–55, 2019.

[22] L. Matya, Almost 400 corruption cases involving SAPS members being investigated, *SABC News (South Africa)*, November 3, 2020.

[23] H. Natarajan, S. Krause and H. Gradstein, Distributed Ledger Technology and Blockchain, FinTech Note no. 1, World Bank, Washington, DC (`hdl.handle.net/10986/29053`), 2017.

[24] Select Committee on Security and Justice, Progress Report: Integrated Justice System (IJS) Programme, Department of Justice and Constitutional Development, Republic of South Africa, Pretoria, South Africa (`static.pmg.org.za/170531IJSReport.pdf`), 2017.

[25] Republic of South Africa, MEC Albert Fritz on e-docket software not being effectively used by SAPS and courts, Media Statement, Pretoria, South Africa, March 5, 2020.

[26] E. Yunianto, Y. Prayudi and B. Sugiantoro, B-DEC: Digital evidence cabinet based on blockchain for evidence management, *International Journal of Computer Applications*, vol. 181(45), pp. 22–29, 2019.