informatics

MDPI

*Article*

# Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections

**Olawande Daramola * and Darren Thebus**

Department of Information Technology, Cape Peninsula University of Technology, Cape Town 8000, South Africa; 209236183@mycput.ac.za

* Correspondence: daramolaj@cput.ac.za

Received: 1 April 2020; Accepted: 12 May 2020; Published: 20 May 2020

**Abstract:** E-voting is one of the valid use cases of blockchain technology with many blockchain e-voting systems already proposed. But efforts that focus on critical analysis of blockchain e-voting architectures for national elections from stakeholders' perspectives are mostly lacking in the literature. Therefore, government decision-makers and election stakeholders do not yet have a sufficient basis to understand the potential risks, challenges, and prospects that are associated with blockchain e-voting. This paper demonstrates how the use of the Architecture Trade-off Analysis Method (ATAM) can enable stakeholders in national elections to understand the risks, prospects, and challenges that could be associated with a blockchain e-voting system for national elections. By using a study context of South Africa, a proposed blockchain e-voting architecture was used as a basis to aid election stakeholders to reason on the concept of blockchain e-voting to get them to understand the potential risks, security threats, critical requirements attributes, and weaknesses that could be associated with using blockchain e-voting for national elections. The study found that blockchain e-voting can prevent many security attacks, internal vote manipulation, and promote transparency. However, voter validation and the security of the blockchain architecture are potential weaknesses that will need significant attention.

**Keywords:** blockchain; smart contracts; electronic voting; Architecture Trade-off Analysis Method (ATAM), requirements engineering; software architecture

## 1. Introduction

Credible elections are the foundation for lasting democracy and good governance. Elections in many developing countries are historically marred with difficulties, errors, and institutional manipulations which reduces their credibility. E-voting has been proposed as a solution for many of the challenges of paper-based voting to ensure error-free and bias-free elections [1]. Conventional e-voting systems mostly rely on centralised system architectures, which make them susceptible to cyberattacks that target central infrastructures, such as distributed denial of service attacks (DDOS). In recent times, e-voting has been identified as one of the valid use cases of blockchain technology. The decentralised nature of blockchain, and its attributes of anonymity, and transparency make it a suitable approach to handle many of the difficulties associated with conventional e-voting systems [2]. Blockchain-based e-voting architecture can potentially address most of the challenges of traditional voting systems and conventional e-voting. These include issues of voter's authentication, verification of votes, protection of voter's privacy, the security of votes, and integrity of election results.

Several novel designs of blockchain e-voting systems and architectures have been proposed in the literature. In fewer cases, prototype implementations of blockchain e-voting systems have been reported while evaluations of blockchain e-voting systems were conducted, albeit on a small scale. All of these do not offer the guarantee that blockchain e-voting will succeed if applied in the context of national elections. Thus far, proposals of blockchain e-voting that have focused on national elections are limited. The few cases that have been reported so far include Estonia, Turkey, India, and South Korea [3]. Moreover, studies that focused on the critical analysis of blockchain e-voting systems from the perspectives of real election stakeholders in the context of requirements of national elections rarely exist, this has created a situation where government decision-makers and election stakeholders do not have sufficient basis to understand the potential risks, challenges, and prospects of blockchain e-voting on a national scale. The research question of interest is: *How can election stakeholders and decision-makers be enabled to understand the risks, prospects, and challenges of blockchain e-voting for elections in specific national contexts*? The need to answer this question is a theoretical gap that requires the attention of researchers.

Thus far, several proposals that advance the merits of blockchain e-voting have been reported. However, most of these are not derived from communal engagements with election stakeholders, and domain experts in a way that promoted collective reasoning on the potential risks, challenges, and prospects of blockchain e-voting for national elections. Conceptually, most of the research efforts on blockchain e-voting have followed a methodical approach that entails the following (i) formulate an idea/concept (ii) design/implement a proof of the idea; (iii) show or explain how the idea/system will work (iv) in fewer cases, perform an evaluation; and (v) draw a conclusion that the idea/system is good. This conceptual approach to the topic of blockchain e-voting is not sufficient to enable election stakeholders, and government decision-makers to understand the potential risks, challenges, and prospects of blockchain e-voting for national elections. There is currently, a lack of a stakeholder-centric, and participatory approach to the design of blockchain e-voting solutions in a way that involves the participation of stakeholders, or elicits communication among election stakeholders. Thus, it is necessary to devise more stakeholder-centric approaches for the planning, design, and implementation of blockchain e-voting systems. It is particularly valuable if these approaches are applied at the very early stages of system planning and construction, such as requirements and architecture modelling, because more non-technical persons will be able to participate. This will promote shared understanding and collective ownership of the project objectives, and ultimately help to save costs [4]. It is easier to engage with stakeholders and less technical people at the level of requirements engineering and architecture design than the later stages of development that are more technically-oriented. The use of a stakeholder-centric approach can enable the participation of government-decision makers, election stakeholders, which will promote their understanding of the potential risks, prospects, and challenges of blockchain e-voting. This will ultimately equip them with the capacity to make informed decisions on issues of blockchain e-voting adoption.

A very pragmatic way to promote communal engagement on the quality attributes of a system and associated risks is to employ the Architecture Trade-off Analysis Method (ATAM) [4,5]. ATAM uses elicited requirements to determine the extent and the potentialities of a system to satisfy its expected quality attributes through critical analysis by domain experts from an architectural perspective. The results of ATAM are quite useful for cost and benefit analysis, improvement of system design, and guidance in system implementation, software project management, and project-based decision making when it is used as a precursor to the actual system development process.

Thus, in contrast to previous studies on blockchain e-voting, this paper introduces a stakeholder-centric approach that enables critical analysis of the suitability of blockchain-based e-voting for national elections. As a contribution, it demonstrates how ATAM can be used to enable election stakeholders to reason on the potential risks and critical quality attributes that are essential for successful blockchain e-voting implementation at a very early stage of planning. By selecting the nation of South Africa as a case study, this paper demonstrates how a rigorous, but yet lightweight, architecture-centric evaluation method can be applied at the formative stage of planning for decision-making on the adoption of blockchain for e-voting in context of national elections, which will be useful for government decision-makers.

The rest of this paper is organised as follows: Section 2 gives an overview of the background and related work. Section 3 describes the adopted research design and presents a description of the blockchain-based architecture for national e-voting system (BANES). Section 4 is the report of the ATAM evaluation, while Section 5 discusses the findings of the ATAM evaluation. We present detailed security analysis of the BANES in Section 6, while the implications of the study is presented in Section 7. The paper is concluded in Section 8 with a brief note and an overview of future work.

## 2. Background and Related Work

In this section background information, the topics of e-voting for national elections, and blockchain technology are presented. It closes with a review of related work.

### *2.1. E-Voting for National Elections*

E-voting is appealing for national elections in many countries because of its potential to eliminate many of the challenges that are associated with traditional paper-based elections. It affords among others the following: (i) ease of voting with heavy investment in paper-based electoral materials, and the logistics of transporting them from place to place; (ii) quick voting process and automatic tallying of votes, and collation of results; (iii) elimination of human error and bias in the recording and compilation of valid votes; (iv) to some extent can also protect voter's privacy and confidentially of their voting choices [1,2].

Thus far, some countries are known to have utilised e-voting systems for national elections. These include Estonia, Norway, and Switzerland [3]. However, the design of most e-voting systems are based on centralised coordination that makes them vulnerable to cyberattacks, and distributed denial of service (DDOS) attacks, which may impair the outcome of elections. Many e-voting implementations across the world have been criticised for their shortcomings in the areas of security, privacy, and transparency, which has made some countries such as Australia, Finland, Germany, and the Netherlands to jettison e-voting and go back to the use of the paper ballot system [6]. Additionally, although e-voting systems have been implemented in countries like Brazil, Estonia, India, and the USA, several shortcomings have been observed [2,6].

Elections in Africa are particularly problematic because of various socio-economic problems and high levels of illiteracy among the population. This situation of underdevelopment generally makes Africa a very complex setting for e-voting to thrive. However, the enormity of the challenges and problems of traditional voting systems in most African countries makes it compelling to consider the prospects of adopting e-voting. In terms of e-readiness for e-voting adoption, South Africa ranks highest among African countries because of its more advanced ICT infrastructure, and Internet technology diffusion per population. This is mostly the basis for selecting South Africa as the case study in this paper.

### *2.2. Overview of Blockchain Technology*

A blockchain consists of a chain of blocks that are interconnected in a way that each block has a unique hash value for its identification. The blocks are interlinked by ensuring that each block contains the hash value of its preceding block, thereby creating a continuous chain in the form of a distributed digital ledger [6–8]. The blocks in a blockchain are distinct and independent computing nodes that interacts based on a cryptographic protocol. All transactions in a blockchain are validated by other nodes before it is recorded in the blockchain. A new block can only be created based on a predefined consensus protocol, which defines the rules of interaction amongst the nodes of blockchain. The creation of a new block and the validation of transactions are done by the consensus algorithm. The most common consensus algorithms include proof of work, proof of stake, and delegated proof of stake [9], which are used to authenticate all transactions in the blockchain to prevent illegal manipulation by external agents.

Thus, blockchain architecture enables data integrity, data security, data privacy, and immutability, which makes it viable for realising efficient and reliable e-voting systems [2]. A blockchain network is immutable in that it allows an append-only ledger of transactions to be recorded on multiple nodes of the blockchain. Bitcoin, which is a cryptocurrency transaction system, is the first occurrence of blockchain technology. Blockchain technology is composed of three main components which include: private key cryptography, a peer to peer network, and a blockchain protocol [6]. The key attributes and capabilities of blockchain technology such as transparency, autonomy, immutability, and anonymity are enabled by the combination of these technologies. The three main types of blockchain technology are permissionless (public) blockchain, permissioned (private) blockchain, and consortium (hybrid) blockchain. A permissionless blockchain is readily accessible to the public and open for reading, download, or membership for anyone interested. Bitcoin and Ethereum are examples of a public blockchain. A permissioned (private) blockchain is privately owned by an individual or organisation, and access to its resources and membership are based on very strict protocols; while a consortium blockchain possesses the characteristics of both public and private blockchains because it enables read-only access for members of the public, and has a partially decentralised nature.

### *2.3. Related Work*

Our review of related work focused mainly on blockchain e-voting with smart contracts which is the category to which the blockchain e-voting architecture that is proposed in this paper belongs. A smart contract is an executable code that enables untrusted parties in a blockchain to directly interact and perform transactions with one another without needing a centralised authority [10].

Several Ethereum-based e-voting platforms that implement smart contracts have been reported before now. The Ethereum platform is used as an e-voting protocol because of its many use cases, and its capacity to support smart contracts when compared to the Bitcoin platform, which can only be used to verify the correctness of transactions. Examples of Ethereum-based blockchain e-voting so far reported include [8], where a system that supports self-tallying of votes with maximum voter privacy was proposed. The system was designed to support small-scale boardroom elections and was tested in an election that involved 40 participants, which is a much smaller scale compared to a national election. In [11], the application of e-voting as a service for the implementation of distributed voting systems on a national scale was evaluated by using a case study in Iceland. The approach was based on the use of a private Ethereum blockchain and depended on a particular ID authentication company in Iceland to ensure the verification of voter's identity. The authors claimed that the system is capable of supporting cost-efficient elections while protecting voter privacy. However, the design and execution of the study seem quite suitable for blockchain elections in small-sized countries like Iceland, unlike the countries with big populations.

In [12] the feasibility of Votereum as a blockchain e-voting system was assessed by deploying it to the Rinkeby testing network. It was designed to enable an open and secure election on a national scale that also protects the privacy of voters. Votereum was found to support basic requirements such as robustness, ballot privacy, individual verifiability, and universal verifiability, but not capable of ensuring receipt-freeness and resisting coercion. It was also found to be potentially prone to scalability problems because it relied on Ethereum, which is a public blockchain with an enormous number of transactions of its own apart from those that will come from hosting a national election. In [13] a prototype implementation and evaluation of the costs, efficiency, and scalability of a blockchain e-voting system was present. The Truffle web framework was used to debug its smart contracts which were written in the Solidity language; the deployment and testing of the smart contracts were done by using Ganache; while the voters' accounts were managed by MetaMask. The framework was presented as scalable and suitable for both small community and country-wide elections, and an improvement on previous efforts. However, the details of the type of requirements that the system could handle were not specified in the paper. Ques-Chain [14] ensures that authentication during blockchain e-voting can be done without hurting confidentiality and that anonymity of voters can be protected without problems of scams at the same time. The system is reckoned as capable of being used in all instances that require high information security requirements, be it for national referendums or elections in corporate settings. A potential drawback of Ques-Chain is the scalability of the system when used for national elections because it relies on Ethereum because of the vast number of transactions per day of its own. Other Ethereum-based e-voting proposals with smart contracts include [3,6–8,15–19]. However, none of these approaches was based on engagement with election stakeholders on the quality attribute requirements of blockchain e-voting system or the viability of the proposed solution in the context of national elections.

E-voting systems that are based on permissioned blockchain architectures have also been reported recently. In [20] a consortium blockchain that uses the Hyperledger Fabric was used for e-voting. The Chaincode of the Hyperledger Fabric implements smart contracts, which facilitates secure and efficient voting transactions and protects the privacy of voters. The Hyperledger Fabric provided a modified blockchain protocol that enables traditional paper-based voting and e-voting to take place. The design of the system was not based on explicit requirements that were captured from stakeholders but general e-voting requirements. The TrustedEVoting (TeV) framework [21] is based on a conceptual design that combines cryptography and permissioned blockchain to ensure secure and verifiable e-voting. TeV supports voter's anonymity and post-election vote checking by a voter. However, there was no actual implementation or evaluation of the TeV in the context of a national election. In [22] the Fujioka, Okamoto, and Ohta (FOO) blockchain e-voting protocol was presented. It is based on the Hyperledger Fabric, and uses smart contracts. It also implements blind signature, and a consensus mechanism for the security of the blockchain. Experimental results show that the blockchain-based FOO e-voting protocol is suitable, and efficient for large-scale elections, with many functional attributes. However, a specific application of the FOO blockchain e-voting in the context of a national election was not the focus of the paper.

In [23], a decentralised e-voting system that is based on blockchain and homomorphic encryption was proposed. The authors argued that e-voting was realised without a third party and that the system can promote the transparency of elections. The design of the system focused on the different phases of an election but did not target specific quality requirements. In [24], the authors presented a blockchain-based e-voting system that ensured the anonymity of voter by using Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARKs) to achieve voter unlinkability to their votes. The system used digital signatures to provide message authentication, cryptographic hashes to create hash chains, and provided resistance to coercion, the integrity of vote cast, voter authentication, voter confidentiality, and other quality attributes. The system was not based on any form of engagement with stakeholders. In [25], a system that relies on a blockchain and smart contract to support the dual activities of decentralised electronic voting and bidding was presented. The concept of oblivious transfer and homomorphic encryptions were used to ensure the protection of the privacy of voters and bidders. The system was rated as efficient in terms of ensuring anonymity, the privacy of data, and reliability and verifiability of data. It is also found to be safer than comparable systems. The author in [26] described how an anonymous decentralised e-voting system can be developed by using ring signature and blockchain technology. The aim is to guarantee verification of voting rights, anonymity, the correctness of the vote cast, and prevention of double waste attacks. The architecture of the system was described, but there was no implementation and evaluation of the proposed concept.

In [27], a blockchain system for decentralised e-voting that uses Elliptic Curve Digital Signature Algorithm (ECDSA) and hash code to encrypt data, and fingerprint biometric authentication of voters was presented. A hardware implementation of the fingerprint recognition module was described but discussion on other aspects of the system was not elaborated. The system was adjudged by the authors as capable of ensuring election credibility and increasing voter confidence. A framework that used an adjusted blockchain to block creation and block sealing to curtail the problems associated with the aspect of e-voting such as the polling process, selection of hash algorithm, voting data management, and security during elections was presented in [28]. Process modelling was used to understand election requirements that should be addressed, while logical argument was only to justify the proposed approach after its implementation. The system even though was addressed to national elections did not involve engagement with election stakeholders. In [29], reports the implementation of a secured blockchain e-voting system by using the AngularJS framework for creating the front-end web app, and MongoDB as the database. The blockchain was created with Python, while the hash for each block was generated by using the SHA256 algorithm. The authors argue that blockchain voting will guarantee a safe and secure election. However, no form of evaluation was done to assess the proposed system.

Other blockchain e-voting systems that implement smart contracts that have been reported include [30–32], while a comprehensive review of blockchain-based smart contracts is presented in [33]. As a departure from previous efforts, this paper presents a stakeholder-centric approach to the design of blockchain e-voting system that enabled the participation of election stakeholder at early stages of development which are at the level of requirements gathering and evaluation of the software architecture. This will enable relevant stakeholders to understand the potential risks, and prospects of blockchain e-voting. It is also the first study on blockchain e-voting from the South African context. Table 1 gives a summary of the conceptual orientation of the most recent approaches (papers between 2017 and 2020) on blockchain e-voting. The analysis of these approaches reveals that most authors used domain analysis, which entails studying the requirements of existing e-voting systems to compose the requirements of their system. In some other cases, authors have arbitrarily selected requirements that they judged important and used them as a basis for the design of their system. There are only two cases where evaluative feedbacks [8,19] were sought from users, while there is no instance where election stakeholders/users were engaged to elicit requirements. This picture reveals that, despite the several studies on blockchain e-voting so far, very little has been done to promote the involvement of election stakeholders, which has limited their ability to understand the risks and prospects of blockchain e-voting.

**Table 1.** Summary of approaches used for blockchain e-voting research.

| **Authors** | **S.E** | **Req.** | **D/I** | **S.F** | **Eval.** |
|---|---|---|---|---|---|
| Bulut et al. [3]; Ayed [6]; Zhang et al. [14]; Teja et al. [18]; | ✗ | DA | ✓ | ✗ | ✗ |
| Pawade et al. [19] | ✗ | DA | ✓ | ✓ | PE |
| Murtaza et al. [24] | ✗ | DA | ✓ | ✗ | PE |
| Zinh Vo-Cao et al. [12]; Hjlmarsson et al. [11]; Tso et al. [25] | ✗ | DA | ✓ | ✗ | SA |
| Zhang et al. [30] | ✗ | DA | ✓ | ✗ | SA + PE |
| Vewer et al. [20] | ✗ | DA | ✓ | ✗ | Use Cases |
| Braghin et al. [13] | ✗ | EP | ✓ | ✗ | PE |
| Lai et al. [14]; Hsaio et al. [23] | ✗ | EP | ✓ | ✗ | SE |
| Shahzad & Crowcroft [28] | ✗ | PM | ✓ | ✗ | Argument |
| McCorry et al. [8] | ✗ | ✗ | ✓ | ✓ | PE |
| Yavuz et al. [7] | ✗ | ✗ | ✓ | ✗ | ✗ |
| Sadia et al. [31] | ✗ | ✗ | ✓ | ✗ | SA |
| Canessane et al. [17]; Naphade et al. [16]; Kurbatov et al. [26]; Nimje & Bhalerao [27]; Leema et al. [29] | ✗ | SR | ✓ | ✗ | ✗ |
| Kirillov et al. [20]; Zhou et al. [22]; Li et al. [32] | ✗ | SR | ✓ | ✗ | SA |

S.E—Stakeholder Engagement for requirements; Req.—Requirements Identification; D/I—Design or Implementation; S.F—Stakeholder Feedback; Eval.—Evaluation; DA—Domain Analysis; SR—Selected Requirements. PE—Performance Evaluation; SE—Security Analysis; PM—Process modelling; EP—Focus on Election Phases

## 3. Research Design

The adopted research design for the study involves elicitation of the e-voting requirements, formulation of a blockchain e-voting architecture, an architecture-based evaluation using the Architecture Trade-off Analysis Method (ATAM), the analysis of the results, the overall security analysis of the proposed system, and a report of the findings. The key activities of the research design are described next.

### *3.1. Overview of Elicited E-voting Requirements for South Africa*

To elicit e-voting requirements, we had a semi-structured interview session with two top officials of the South African Independent Electoral Commission (IEC). The feasibility study report on e-voting for South Africa in 2013 and the Seminar Report on E-voting done by the IEC were also reviewed [34]. Four persons that had participated in two previous elections in South Africa were also interviewed to gain information from the voter's perspective. The requirements elicitation process yielded the following key requirements:

(i) *Trust*: All stakeholders must have confidence and trust in the e-voting system. This will depend on multiple aspects such as security, transparency, auditability, verifiability and other essential attributes.

(ii) *Transparency*: The system should support the casting of votes and tally of votes by all stakeholders, as well as allow them to verify this easily.

(iii) *Verifiability*: The system must enable voters to check that their votes were cast and recorded as valid votes for a candidate of their choice without any error or internal manipulation.

(iv) *Auditability*: The system must be able to support any process that may necessitate the rechecking and recounting votes in the event of electoral disputes.

(v) *Availability*: The system must have sufficient mechanisms in place to forestall instances of down-time during the period of elections.

(vi) *Performance*: The system must ensure that all operations are handled speedily and efficiently. Efficiency depends on the overall system's throughput such as the number of transactions per time (seconds/minutes), and the response time to user queries.

(vii) *Non-coercion of voters: The* system must minimise the risk of voters being coerced to vote in certain ways by preventing manipulation and intimidation of voters. The system must be able to conceal the identity of voters, and the choices made during voting.

(viii) *Socio-economic influences*: Politicians should not be able to exploit the poor socio-economic status of some voters to unduly influence them to vote in a particular way. This is a particularly significant problem in South Africa, and indeed in many elections in Africa.

(ix) *Socio-political factors*: The e-voting system should not be vulnerable to socio-political manipulations that can compromise the integrity of the voting process.

### *3.2. A Proposed Blockchain Architecture for National Elections*

Based on the identified requirements, a blockchain-based architecture for national e-voting system (BANES) was proposed (See Figure 1). It is a layered architecture that consists of four layers which are [35,36]:

**Client layer**: this layer contains the various electronic devices and systems with which users interact with the blockchain e-voting system. These devices are the peer nodes of the e-voting blockchain that interact via smart contracts, referred to as "chaincode" in the Hyperledger Fabric. The different types of peer nodes and their assigned responsibilities are:

(i) *E-Voting nodes*: The primary purpose of these nodes is to enable voters authentication and casting of votes, and to ensure that all blockchain transactions are recorded.

(ii) *Administrator nodes*: These nodes are used to configure blockchain network channels, assign roles to the nodes of the blockchain, grant permissions, and set the level of access control for specific nodes.

(iii) *Public nodes*: These are the nodes that enable view-only public access to transactions of the e-voting blockchain.

(iv) *Vote validation*: These nodes are responsible for vote validation. They are also used to ensure the authenticity of transactions that are included in a block.

(v) *Committing nodes*: These are the nodes that validate and commit new blocks to the blockchain.

**Application Service Layer**: this consists of a set of services that are available in the e-voting system. The level of access control and the defined permissions level determines the type of services that a node can access in the blockchain.

**Blockchain Layer**: this is composed of the Hyperledger Fabric V2.0, which is a modular blockchain architecture framework that facilitates blockchain information system solutions. It supports the creation of permissioned blockchain networks that have in-built properties such as security, and privacy protection [37]. The Hyperledger Fabric has "ordering nodes" which ensures consistency of the blockchain by ensuring that only ordered blocks of an endorsed transaction are made available to the committing peer nodes before they are added to the blockchain [37].

**IEC Data Storage Layer**: this contains the relevant databases that store information on the profile of registered voters, political offices being contested for, and all political candidates. This database is used as the basis to authenticate and authorise voters to vote.

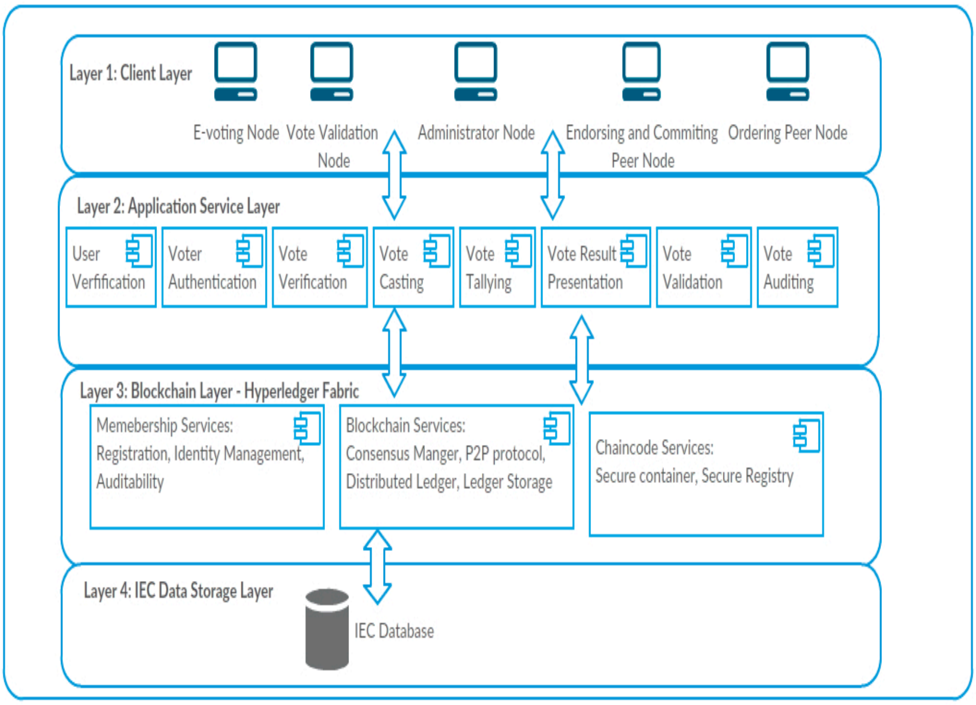
Layer 1: Client Layer
E-voting Node
Vote Validation Node
Administrator Node
Endorsing and Commiting Peer Node
Ordering Peer Node
Layer 2: Application Service Layer
User Verfification
Voter Authentication
Vote Verification
Vote Casting
Vote Tallying
Vote Result Presentation
Vote Validation
Vote Auditing
Layer 3: Blockchain Layer - Hyperledger Fabric
Memebership Services: Registration, Identity Management, Auditability
Blockchain Services: Consensus Manger, P2P protocol, Distributed Ledger, Ledger Storage
Chaincode Services: Secure container, Secure Registry
Layer 4: IEC Data Storage Layer
IEC Database

**Figure 1.** A schematic view of the blockchain-based architecture for national e-voting system (BANES).

### *3.3. Other Vital Aspects of the Blockchain Architecture*

By design effective operations of the BANES is premised on two key concepts, which are smart card technology and the zero-knowledge protocol.

**Smart Card Technology for Voter Authentication**. This is used to eliminate impersonation and to ensure that only valid voters can vote [38]. During the voter registration exercise before election time, a smart card shall be given to each voter by the central electoral authority. The smart card will contain the voter's public key for identification, which will be combined with a personal identification number (PIN) for voters' authentication.

**Zero-knowledge Protocol for Voter Authentication and privacy protection**. The zero-knowledge protocol was applied in the BANES to ensure that when an authorised voter casts a vote, the blockchain knows that a valid vote has been cast and nothing more. The identity of the voter and voter's choice is not revealed [39].

### *3.4. A Process View of the Blockchain Architecture for E-Voting (BANES)*

For efficiency, it is assumed that the casting of votes will take place at designated polling units to protect voters from being coerced to vote in certain ways by politicians and their agents. With the BANES, the e-voting procedure will follow the procedure below [28]:

(i) The voter inserts the personal smart card into the voting node and supplies a password.

(ii) Authentication and authorisation of the votes take place via the IEC database.

(iii) If successful, a digital ballot is generated by the IEC system. A digital ballot consists of a set of candidate public keys and a unique ballot ID

(iv) Voter submits a vote for the preferred candidate.

(v) The ballot ID is assigned to the preferred candidate through their public key. The transaction is authenticated by using the digital signature of the private key.

(vi) The transaction is sent to all nodes and stored on the blockchain.

An overview of the e-voting process that is based on the blockchain architecture is presented in Figure 2.

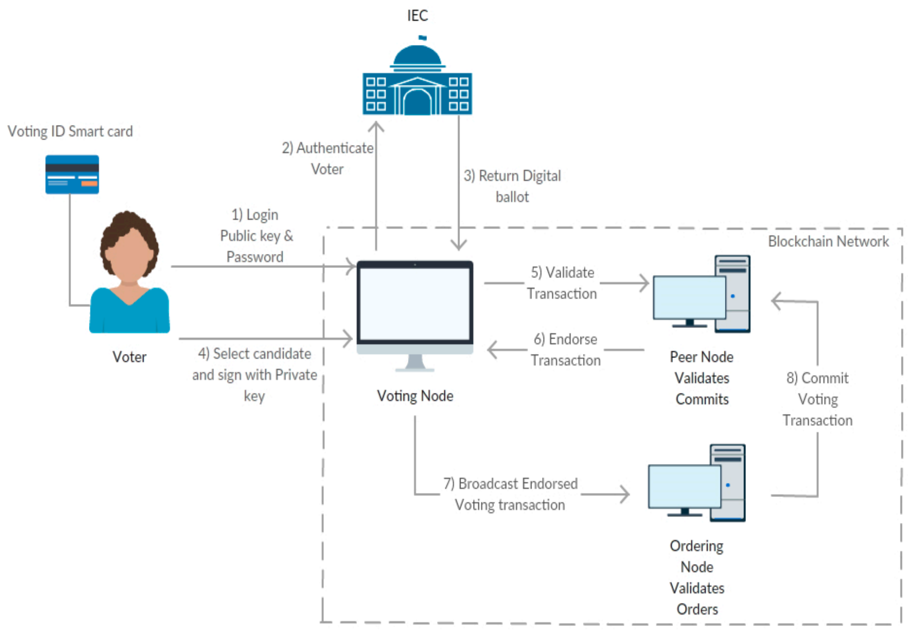
IEC
Voting ID Smart card
2) Authenticate Voter
3) Return Digital ballot
1) Login Public key & Password
Blockchain Network
5) Validate Transaction
6) Endorse Transaction
Voter
4) Select candidate and sign with Private key
Voting Node
Peer Node Validates Commits
8) Commit Voting Transaction
7) Broadcast Endorsed Voting transaction
Ordering Node Validates Orders

**Figure 2.** A high-level view of the e-voting process using the BANES.

## 4. ATAM Evaluation

The report of the Architecture Trade-off Analysis Method (ATAM) evaluation of the BANES is present in adjoining subsections. ATAM was selected for the evaluation of the proposed blockchain architecture because it is arguably the best scenario-based architecture method. A comparative analysis of scenario-based architecture evaluation methods which included the Scenario-Based Architecture Analysis (SAAM), the Architecture Trade-off Analysis Method (ATAM), the Performance Assessment of Software Architecture (PASA), and the Architecture Level Modifiability Analysis (ALMA) as reported in [40] revealed that ATAM is the only scenario-based architecture evaluation method that provides comprehensive process support for the architecture evaluation process. This is the main motivation for using ATAM.

### *4.1. Assessing Blockchain E-voting Architecture Using the Trade-Off Analysis Method (ATAM)*

ATAM is used to evaluate software architectures by using scenarios. The objective of ATAM is to assess the degree to which a system is likely to be able to satisfy its expected quality attributes by analysing it from an architectural perspective. ATAM allows the risks, sensitivity points, and trade-off points of a system to be identified [4,5]. In ATAM, risks are a potentially problematic architectural decision, a sensitivity point is a property of one or more components that is necessary to attain a specific quality attribute response, while a trade-off point is a property that affects more than one attribute and is a sensitivity point for more than one attribute. ATAM results are particularly useful for cost and benefit analysis, improvement of system design, and guidance in system implementation, and software project management. The ATAM evaluation for the proposed BANES was done in two phases with a set of stakeholders comprising domain experts and ordinary end-users: election stakeholders.

A panel of three experts was used for the first phase, which focused on architecture analysis. The experts include (i) an information system (IS) solutions architect with 14 years' experience of industry practice (ii) a senior IT personnel with experience in blockchain use cases and blockchain development. He also has a doctorate qualification in mathematics and encryption, and (iii) a third expert is a researcher in software engineering with over 15 years' experience in software design and development. Three participants who are non-experts participated in Phase 2 of the ATAM. The three were end-users and voting stakeholders that were given the task to verify the outcome of the first phase. The description of the activities that were undertaken during the ATAM is shown in Table 2.

**Table 2.** Outline of Activities of the ATAM Evaluation.

| S/N | Phase 1 | Description of Activity |
|---|---|---|
| 1. | Present ATAM | A quick overview of the process, techniques, and expected outputs of ATAM was presented to the panel of experts in the first phase and then to all participants in the second phase together in the same session. The techniques used are:<br>Utility tree generation; Architectural approach-based; elicitation/analysis; and; scenario brainstorming/mapping.<br>The outputs of ATAM are:<br>• Elicited and prioritised scenarios<br>• Questions used to understand/evaluate the architecture to produce a utility tree<br>• Utility tree—describing and prioritising the critical architectural requirements<br>• Set of discovered risks and non-risks<br>• Set of discovered sensitivity points and trade-offs |
| 2. | Present Business Drivers | A description of various business drivers (see Section 3.1) that relate to e-voting was presented to the participants to give them a better understanding of the system they are evaluating. |
| 3. | Present Architecture | The BANES was presented to the participants using the 4 + 1 architectural view model of Kruchten [41], which prescribes a logical view, development view, process view, physical view, and also scenarios descriptions.<br>• The Logical View was illustrated with a UML class diagram<br>• The Process View was illustrated with a UML activity diagram<br>• The Development View was illustrated with a UML component diagram<br>• The Physical View was illustrated with a UML deployment diagram<br>• Snapshots of the Process View and the Development View are shown in Figures 3 and 4. |

**Table 2.** *Cont.*

| S/N | Phase 1 | Description of Activity |
|---|---|---|
| 4. | Identify Architectural Approaches | The architectural approaches that have been adopted and the rationale for adopting them were explained. The summary of quality attributes and the approach/component that seeks to address them is presented as follows:<br>• Voters Smart card—Identification, Authentication, and Authorisation<br>• Zero-knowledge protocol—Security<br>• Hyperledger Fabric Blockchain:<br>➢ Public/private key Encryption—Security, Functional Suitability<br>➢ Modular Architecture—Reliability<br>➢ REST API's—Reliability, Security, Performance<br>➢ Permissioned Blockchain network—Security, Functional Suitability<br>➢ Isolation of system services—Performance, Security<br>➢ Distributed processing—Security<br>➢ Decentralised processing and storage—Functional Suitability, Reliability<br>➢ Immutability—Security, Functional Suitability |
| 5. | Generate Quality Attribute Utility Tree | The quality attribute utility tree was generated from the questions from the participating experts in their attempt to further understand the architecture design and process, together with stated concerns and scenario discussion and elicitation. The utility tree allows for the prioritisation of specific quality attribute requirements, as they relate to the scenarios. |
| 6. | Analyse Architectural Approaches | The prioritised list of scenarios, which is the output of the previous step is used to probe the architectural approaches to realise the important quality attributes. This step was used to identify any risks, sensitivity points, and trade-offs within the design architecture. The 3 highest priority scenarios were mapped to the relative architectural approach. The approaches were analysed by identifying risks, scenarios that were concerned with more than one approach was identified as a sensitivity point.<br>The following scenarios were included:<br>*Scenario 1*—Connections outside of the blockchain network are hampered by a Man-in-the-middle attack.<br>*Scenario 2*—Vote verification introduces the risk of coercion.<br>*Scenario 3*—High volumes of traffic is affecting accessibility and reliability. |
| | Phase 2 | |
| 7. | Brainstorm and Prioritise Scenarios | The discussion included both sets of stakeholder representatives to elicit new scenarios that the expert group may have thought of and to identify any other scenarios from an end-user, voters, perspective. The generated utility tree from Step 5, aided in the discussion and elicitation of a larger set of scenarios. |
| 8. | Analyse Architectural Approaches<br>Present Results | This step is a reiteration of step 6 if the highest-ranked scenarios of the first iteration of step 6 differ from the highest-ranked scenarios identified in step 7. In the case of our ATAM, the highest priority scenarios of step 6 remained the same. |
| 9 | Present Results | This is the step where the results of the evaluation are presented. From the result of the ATAM evaluation, the major trade-off is the aspect of vote validation. To forestall the possibility of voters' coercion the vote validating nodes should be restricted to only secure locations. |

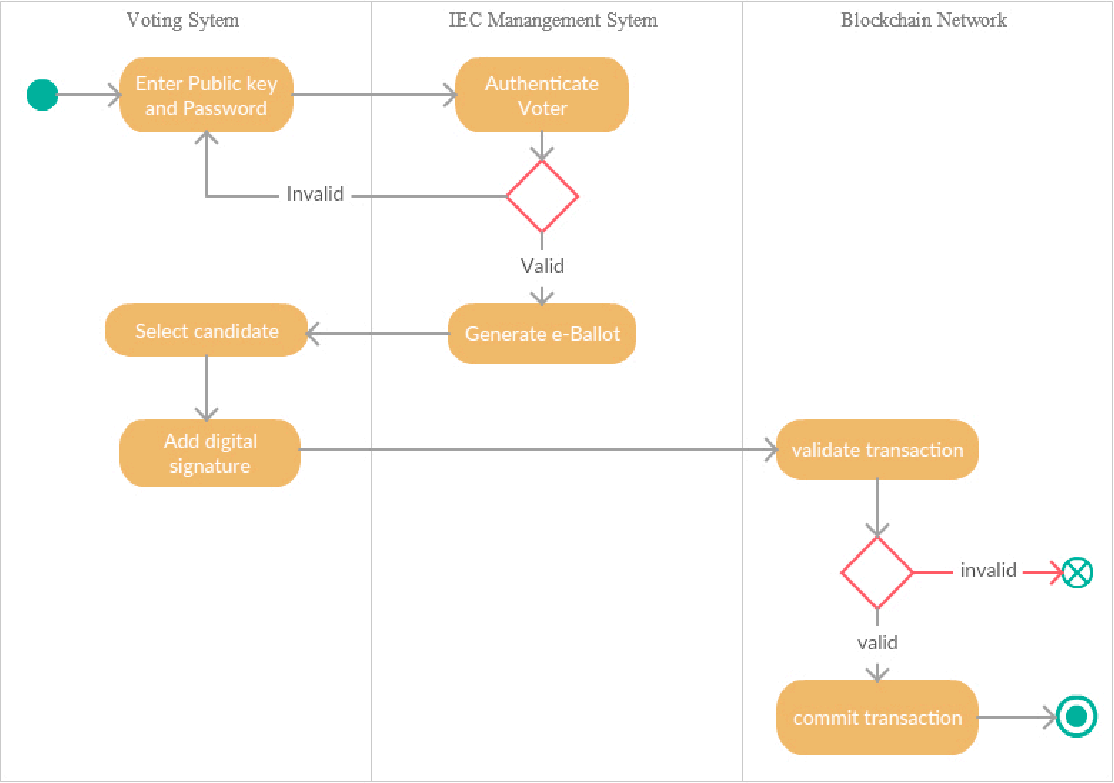

**Figure 3.** Process View—UML activity diagram of BANES.

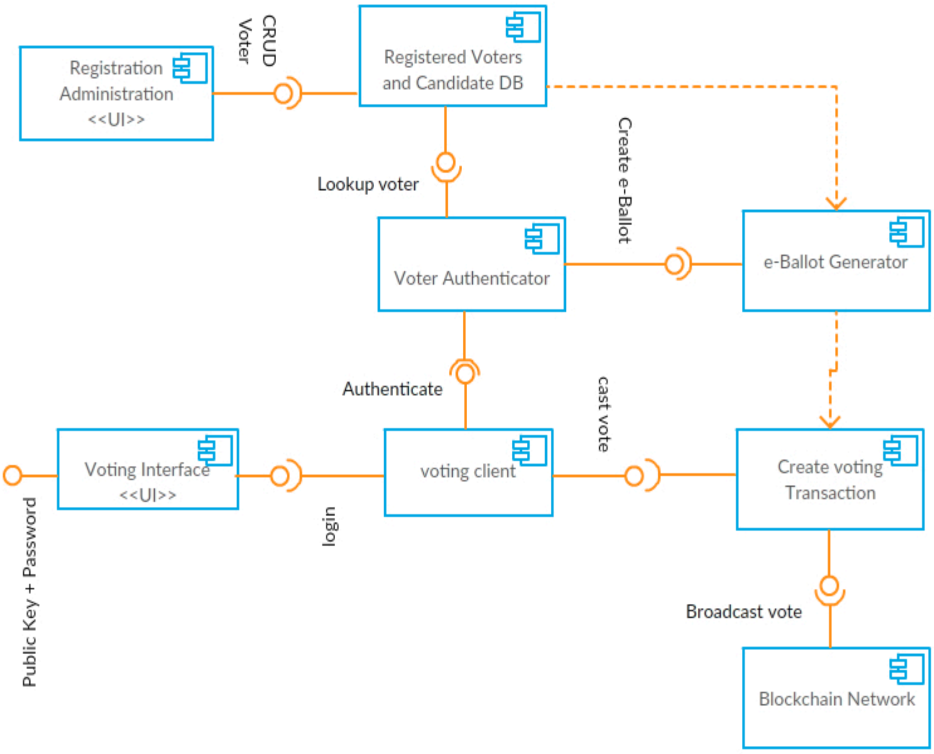

**Figure 4.** Development View—UML component diagram of BANES.

### *4.2. Use of Scenarios for evaluation of Business Drivers and Quality Attributes*

From the elicited requirements, the most important business drivers of national e-voting in South Africa are the need to (i) reduce the huge cost associated with the use of ballot papers, and the distribution of electoral materials; (ii) increase the transparency of the electoral process; (iii) have a faster procedure for efficient voting and counting; (iv) have credible results; (v) increase voters' accessibility; (vi) minimise carbon footprint; (vii) reduce the costs expended on elections; and (viii) increase participation of voters. The panel of experts considered the attributes of security, performance, and functional suitability as deserving of the highest priority because of the identified core business drivers. Security deals with the ability of the system to mitigate threats that may be harmful to its operations, performance is concerned with the speed and accuracy of system operations, while functional suitability is assessed based on the level of auditability, availability, transparency, and verifiability of the system. We derived specific scenarios to assess these important attributes (see Table 3).

**Table 3.** ATAM attributes and scenarios (Thebus and Daramola, 2019).

| Attributes | Scenarios |
|---|---|
| Security | Keeping a voter's choice private and concealed in all circumstances |
| | Only one vote per voter is allowed |
| | There is a Man-in-the-middle attack during voting |
| Performance | There is a high volume of transactions which could affect the speed of processing and reliability |
| Functional Suitability (Transparency, verifiability, Auditability) | Stakeholders want to view the process to be sure of transparency |
| | After voting, stakeholders want to verify election result |
| | A voter wants to verify his/her vote without the risk of coercion |

### *4.3. Observations Based on ATAM Activities and Scenarios*

As stipulated in the applied ATAM guideline, a detailed analysis of the proposed architecture (BANES) was undertaken by the experts in a brainstorming session (see Figure 1) to identify potential risks, non-risks, sensitivity points, and trade-off points.

The most critical quality attributes that have the highest priority were analysed by using the specified scenarios (see Table 2). The concept of the 4+1 views of architecture that was proposed by Kruchten was used to engender other perspectives of the proposed architecture and enable a better understanding of the vision, composition, and capabilities of the proposed architecture. The 4 + 1 Views approach was also intended to engender a thorough analysis of the proposed architecture by the experts. The findings from the brainstorming and interaction of the experts are presented below.

**Security**: Security is reinforced by the use of smart card technology. A voter is expected to use a smart card and personal identification number (pin) to log in, with a combination of a public key and private key, which will ensure that only a valid voter can vote. Additionally, it will be possible to establish the validity of a vote cast without having to reveal the identity of the voter. This will be accomplished through the zero-knowledge protocol that was adopted in the architecture (see Section 3.3). With this, the anonymity of a voter will always be maintained when votes are to be audited. This is one of the critical rights of a voter that should be protected in an election. The threat of a man-in-the-middle attacks for connections that are outside of the blockchain network can be mitigated by the fact that another private key encryption component can be added to protect the communication between the blockchain and the components that are external to it. The use of smart cards for identification, authentication, and authorisation of voters eliminates the threats of a man-in-the-middle attack. Therefore, although security is a potential risk, and sensitivity point in issues of e-voting, the provisions of the architecture seems adequate to generally cater to the envisaged security risks and threats. A security analysis of how the blockchain architecture could respond to potential security threats as enabled by the Hyperledger Fabric is presented in Section 6.

**Performance**: Naturally a national election will result in a vast amount of traffic and a high volume of transactions. A way to minimise these challenges is to allow voting days to span over one or two weeks so that everyone does not have to vote on a specific day. Despite this, huge traffic and a high volume of transactions will have ample impact on accessibility, availability, performance, and reliability of an e-voting system. However, the use of the Hyperledger Fabric for the blockchain layer of the BANES (see Section 3.1), which supports decentralised and distributed modular functionalities based on the specified permission, roles, and blockchain channel will help to alleviate the risk associated with this scenario.

**Functional Suitability**: An e-voting process must satisfy the requirements of transparency, verifiability, confidentiality, and auditability to facilitate a credible election. The use of zero-knowledge protocol will cater for confidentiality and auditability of votes without revealing the identities of the voters. However, the verifiability of votes carries an implicit risk of coercion, whereby voters may be influenced in certain ways as they try to verify if their votes were correctly assigned to their candidate of choice and counted. This situation could compromise the integrity of the voting process. To mitigate this threat, designated peer nodes can be tasked with the role of vote validation instead of allowing all nodes to handle vote validation. This could be designated by using access points such as IEC outlets that have the required level of security to ensure that voters are not coerced in any way as they attempt to verify their votes. The main trade-off point was functional suitability, which can be mitigated by ensuring that votes are only verified at designated nodes and not on just on any node of the blockchain.

## 5. Discussion of Findings from ATAM Evaluation

The findings from the engagement with stakeholders, including electoral officials and voters, reveal a positive disposition to the use of e-voting for national elections in South Africa. The stakeholders believe e-voting is feasible but should also be combined with a paper-based approach to cater to persons with low levels of literacy, and those that lack access to smartphone technology. There is also a quest to have more assurance that e-voting will work and not fail at critical times. There was a great deal of emphasis by the stakeholders on the need to ensure that specific basic requirements, such as availability, performance, security, usability, reliability, and functional suitability (consist of auditability, transparency, transparency, and verifiability), are met. Findings from the ATAM evaluation reveal that the experts consider the conceptual design and composition of the BANES to be a good template for the development of a plausible national e-voting system for South Africa. The BANES could adequately cater for the core systems attributes such as security, performance, and functional suitability. However, necessary adaptations and customisations will be required if the BANES is to be used to cater for the requirements from other developing countries.

The findings of the ATAM shows that a blockchain e-voting architecture for e-voting can be generally more resistant to DDOS attacks when compared to a centralised system that can be more vulnerable. Although blockchain is not entirely immune to hacker's activities, it can be more resistant to security attacks which are good for the sanctity of the elections. The BANES has the potential to engender more transparent elections and is less vulnerable to manipulation by partisan human agents within a centralised election monitoring organisation that may comprise the integrity of votes cast by the voters. The adoption of the state-of-the-art blockchain technologies, such as the Hyperledger Fabric and zero-knowledge protocol, provides a solid basis for a robust blockchain e-voting system to be implemented. It was also evident that the success of a system based on the BANES could also be enhanced by adopting proactive procedures such as the use of smart card technology for voting, and scheduling of the election to span over multiple days for vote casting and tallying of votes instead of just on a single day. These procedures would help to reinforce security and minimise excessive network traffic during the entire election period. It was also discovered that vote validation is a sensitivity point and a trade-off point that would require attention whenever blockchain e-voting is to be implemented. To address this, designated nodes will have to be located in very secure environments to handle voters' validation.

Although this study used a relatively small number of stakeholders, whereas using a larger pool of stakeholders could have provided a stronger basis for more robust conclusions, we believe that, generally, the results of the ATAM provides a good basis to make quick and sound decisions at a very early stage of system development on the prospects of a blockchain-based architecture for e-voting in South Africa. However, it was obvious that, apart from the core technology aspects, adequate procedural and policy support will be required to realise blockchain-based e-voting for national elections. This should be in the form of the effective distribution of smart cards to registered voters by the central electoral authority, hosting designated nodes for vote validation, and ensuring that the elections are adequately spaced over multiple days so that the technology infrastructures are not overstretched due to voting traffic congestion. This will increase the probability of a successful implementation of blockchain e-voting for national elections.

## 6. Security Analysis of the Hyperledger Fabric for National E-Voting

In this section, we present a security analysis of the BANES, which largely depends on the Hyperledger Fabric (HF) as its blockchain infrastructure. Our goal is to assess the capabilities of HF to secure the e-voting system in the circumstances of an attack. Some studies have shown that the HF could outperform the Bitcoin and Ethereum architectures across all assessment benchmarks, particularly in the areas of throughput and latency [42,43]. The HF is typically a distributed ledger technology that does not include a cryptocurrency component by default, unlike Ethereum and Bitcoin. This makes it adaptable to several enterprise applications that do not involve cryptocurrency transactions, which reduces the security threat. However, national elections are high-stake ventures for politicians in Africa, thus, the security and reliability of an e-voting system for elections will surely be tested. By design, the BANES is bound to inherit the strengths and weaknesses of its underlining components and technologies. Thus, securing an e-voting system will require a holistic strategy that transcends the security features that are provided at the level of the Hyperledger Fabric alone [44]. Other network security measures, such as securing the network with firewall and password protection, and securing the data storage are essential. In the sequel subsections, we shall present the possible threats at various layers of the BANES and how the in-built features of the HF can mitigate them. Also, we shall highlight additional security measures that would be required to secure the blockchain e-voting system. The layers discussed in the context of the BANES are the Application Layer, Blockchain Layer (containing the Smart Contract Layer, Consensus Layer, and Network Layer) and the Data Layer.

### *6.1. Attack on the Application Layer*

**Illegal Access to Application Layer Servers**. The threats of illegal access to e-voting servers at the application layer could be in the form of unauthorised access, password intrusion attack, phishing, and spoofing attacks. The e-voting nodes, vote validation nodes, and endorsing nodes are likely targets because a successful attack on this layer will yield a handsome reward for the attacker [44]. The Hyperledger Fabric (HF) can mitigate the threat of password intrusion attack, phishing, and spoofing through the use of cryptographic encryption based on either the Secure Hash Algorithm-256 bit (SHA256) and the Elliptic Curve Digital Signature Algorithm (ECDSA) to make tampering impossible. Unauthorised access can also occur at the Application Layer and the Smart Contract Layer. However, this threat can be mitigated because the HF has a certificate authority (CA) that generates X.509 certificates for its members to identify unauthorised access/intrusion of any form either through spoofing and phishing. However, to ensure stronger security at the application layer, additional measures such as the following will still be necessary:

- Ensure effective real-time monitoring of the system through data encryption storage protection, and proactive security threat detection in the blockchain. The invention by Signorini et al. [45] (U.S. Patent) enables the detection of security threat within a blockchain or distributed ledger system by (i) adding forked chains discarded at a device to a standard blockchain to enhance the structure of the original chain; (ii) inspecting all forked chains that have been added; (iii) anomaly detection based on patterns in the added forked chains in enhanced blockchain, and (iv) a review of all transactions that involved the forked chain in the enhanced blockchain structure.

- Prevent both internally- and externally-induced attacks.
- Forestall repetitive intrusion attacks. The network administrator must ensure that a list of revoked membership certificates to ensure that members that are once revoked cannot re-join the network.

**Compromised Insider/Employee Attack on Election Servers.** This is the threat of insider attack in the form of tampering, or illegal manipulation of data. To mitigate this, the Hyperledger Fabric has features to track who did what through digital signatures to ensure non-repudiation.

**Distributed Denial of Service of Attack (DDoS)**. DDoS makes it impossible for multiple legitimate nodes to gain access to value network resources by spamming them. Ordinarily, a blockchain network that is based on peer-to-peer interaction of several thousand nodes will discourage this. However, nodes in a permissioned blockchain are susceptible to DDoS. Although the effect of DDoS may be minimal on the entire voting process if only ordinary nodes are targeted because the ordering protocol of the blockchain will ensure that crashed nodes are isolated while the other nodes continue interacting until the crashed nodes are ready to join the blockchain again. However, for the HF it is possible an attacker to identify strategic nodes such as endorsers within a channel and direct DoS attacks to them. This can obstruct endorsers from endorsing key transactions, like tallying of votes, voter validation and so on, which will adversely affect the performance of the e-voting system. Since the identities of endorsers are known within a channel, a wormhole attack is also possible. A wormhole attack will compromise a node in the channel, and leak transaction information of the entire channel to an external party. To mitigate this threat, the HF security protocol must be augmented with extra features to ensure stronger protection against DDoS attacks and wormhole attacks to which it is currently vulnerable. However, there are mechanisms to augment the HF with techniques that will ensure randomised selection of endorsers, and the use of pseudonyms to protect the identity of endorsers to shield them from DDoS attacks. Wormhole attacks can also be prevented by using a group signature algorithm to anonymize a sender's identity, while a receiver's anonymity is achieved through bilinear pairing [46].

### 6.2. Attack on the Smart Contract Layer

The Hyperledger Fabric smart contracts—Chaincode is prone to enemy attack. Mostly attacks on smart contracts stem from vulnerabilities in the smart contract code that could be exploited by attackers to cause harm to assets in the system. In the case of e-voting, assets to target could be the vote verification and vote tally operations to manipulate or corrupt results data. Yamashita et al. [47] identified 13 potential risks of the HF smart contracts that can be exploited. The risks were categorised into five categories which are (i) non-determinism arising from language instructions; (ii) non-determinism arising from accessing outside of the blockchain; (iii) state database specification; (iv) Hyperledger Fabric specification, and (v) common practices. To mitigate these risks, vulnerabilities in the smart contracts codes must be avoided by giving significant attention to quality assurance through code inspection and certification. HF smart contracts can be written by using general-purpose programming languages, like Java, Go, and Node.js, which means the programmers rely on their expertise in these languages to quickly develop smart contract codes. However, unlike a domain-specific language that is designed primarily for writing smart contracts, such as Solidity, general-purpose languages lack specific restrictions, which make them less safe for writing smart contracts. The use of static code verifiers can help to improve the quality of smart contract codes and ensure better quality assurance. Examples of such code verifier tools include *Chaincode Scanner*, *Gosec*, and *Golint* [47]. Smart contracts cannot be changed once they are deployed, and their results are irrevocable, hence, the only away to forestall exploitable vulnerabilities in smart contracts is to certify them to be of good quality before they are deployed.

### 6.3. Attack on the Consensus Layer

In a blockchain, the consensus protocol ensures that all nodes act in agreement to the specific rules that guides conduct in the network. The consensus algorithm regulates the endorsement, ordering, and validation of transactions in a blockchain. These core activities that are dependent on the consensus algorithm can be crippled by attacks that target the consensus algorithm, such as a Sybil attack. This is when an attacker creates a large number of fake nodes to gain undue influence over legitimate nodes. To mitigate a Sybil attack, the Hyperledger Fabric (HF) will have to rely on its certificate authority to identify fake nodes and deny them membership. Additionally, the HF offers support for a pluggable consensus protocol that can be customised to fit specific use cases and trust models. Currently, the HF implements the Crash Fault Tolerant (CFT) ordering service that is based on the Raft protocol to bypass any faulty node and reach a consensus [37]. For blockchain e-voting, a Byzantine fault-tolerant (BFT) consensus algorithms which can deal with random or malicious replication faults will be an ideal option of a consensus algorithm.

### 6.4. Attacks on the Network Layer

A blockchain is an interconnection of peer nodes, hence, there are attacks at the network layer that could also target individual nodes in the e-voting blockchain. Examples of these are Eclipse attack and Broader Gateway Protocol (BGP) hijacking attack. The goal of an Eclipse attack is to control all the outgoing connections of the target to isolate it. The HF can forestall this by enforcing Transport Layer Security (TLS) client authentication on peer nodes. This will provide support for secure communication between peer-to-peer nodes. Broader Gateway Protocol (BGP) hijacking involves diverting network traffic to an attacker. For this, the HF can use native encryption for transmission to prevent hijacking. Other mechanisms to strengthen security at the network layer include the use of reliable encryption for data transmission, and strengthening the security of data transmission in the network using firewalls, and other network security protocols to prevent external attacks.

### 6.5. Attacks on the Data Layer

The security threat to the Data Layer can target key electoral data servers to corrupt them, and causing harm to the electoral process. Attack examples include malicious information attacks and attacks on the signature and encryption method. The HF can mitigate this with the use of cryptographic encryption (SHA256, ECDSA) that is used to make tampering extremely difficult.

Summarily, from the security analysis, we argue that the Hyperledger Fabric (HF) can sufficiently secure a blockchain e-voting system against many of the security challenges in the context of a real national election. Generally, the security of blockchain technology is not perfect but still evolving with so many new threats emerging, and efforts being made to devise adequate mitigation mechanisms [44]. Indeed, there are other security protocols for decentralised peer-to-peer networks that could also be used to realise secure decentralised e-voting. For example, the decentralised trust and reputation system—StR, reported in [48]—offers strong security features like privacy protection. However, the obvious attributes of blockchain technology such as decentralisation, trustless configuration, anonymity, and immutability makes it appealing as a viable solution for e-voting, hence its popularity in recent times. Although it still far from being a silver bullet, the interest of big consortiums in open source enterprise blockchain projects like the HF holds significant promise for the future. The Hyperledger Fabric is particularly designed as a permission blockchain to enable a trustless business to business interaction within an enterprise environment. Thus, our preference to select the HF as the backbone of the proposed blockchain architecture for national e-voting in the South African context is reasonable.

## 7. Implications of the Study

This study has both managerial and social implications which are outlined in sequel sections.

### *7.1. Managerial Implication*

Generally, elections in Africa are problematic from the planning stage to the implementation and post-election periods. Many countries in Africa are looking for solutions to this problem, and e-voting has featured prominently as part of the consideration. With the surge of interest in blockchain technology, a large number of proposals on the use of blockchain for e-voting have been proposed. However, these proposals are mostly theoretical postulations that are grounded in engineering and mathematical concepts to convince of the accuracy or correctness of the proposed models. There is the need to devise approaches that can communicate the nuances, and affordances of blockchain e-voting in a less formal way that will allow government decision-makers who are not necessarily technically inclined to relate to the issues of blockchain e-voting, and the associated potential risks, challenges, and prospects. This study offers a first attempt of this by demonstrating how a lightweight approach that is rooted in qualitative scenario-based evaluation method (ATAM) can be used to assess the plausibility of blockchain for e-voting. It introduces a way of thinking about blockchain e-voting architecture to make decisions even when an actual system has not been developed. The outcome of this type of ATAM process involving government decision-makers, managers and electoral officials would provide valuable guidance that can help in the area of quick decision-making, cost and benefit analysis, improvement of system design, system implementation, and project planning on issues of blockchain e-voting for national elections.

### *7.2. Practical Implications*

In most developing countries, voters have lost confidence in elections because elections results are no longer trusted due to fraud and other challenges. This study demonstrates a new conceptual approach to issues of blockchain e-voting in way that can encourage more participation of election stakeholders in the design of e-voting systems. This kind of system is more likely to meet the critical requirements of voters and be more adaptive to user needs. Additionally, by introducing the use of scenario analysis, system developers and election stakeholders would be able to:

- Reason collectively on the desirable quality attribute requirements, risks, and probable challenges of blockchain e-voting to find a mutually agreeable solution;
- Formulate, review, and revise architecture documentations and in the process find the best fit for the proposed system.
- Promotes mutual reasoning and buy-in, and better project planning eventually leading to improved systems implementation and performance.

All of this will inspire the confidence of voters in the electoral process and increase participation in the national democratic process. This is because blockchain e-voting can help to eliminate many of the challenges associated with poor elections of the past.

Socially, for Africa, healthy e-voting could lead to the appointment of credible leaders, which could translate to good governance, improved democracy. This will ultimately lead to the improvement of the socio-economic condition of people, and the country as a whole.

## **8. Conclusions**

In this paper we show that despite several efforts that have been made to propose novel designs and system implementations of blockchain e-voting, adequate attention has not been given to the adoption of a stakeholder-centric approach. This has provided an insufficient basis for government decision-makers and key election stakeholder to be able to make an informed decision on the merits of blockchain e-voting for national elections. To address this gap, we demonstrated how the architecture trade-off analysis method (ATAM) could be used to enable election stakeholders to understand the potential risks, challenges, and prospects of blockchain e-voting through a participatory architecture assessment and documentation process.

To do this, we adopted an approach that is based on interaction with electoral officials, documentations on national elections, and voters to identify the key requirements that are critical for a national e-voting system. This is a departure from how most of the existing e-voting systems derived their requirements. Based on the elicited requirements, a blockchain architecture for the national e-voting system (BANES) was proposed. The BANES was then evaluated by using the ATAM, which is a standard procedure for preliminary evaluation of software architectures that enabled the participation of users, election stakeholders, and domain experts. This provided an opportunity for the stakeholders to gain a good knowledge of blockchain e-voting, and an understanding of the potential risks, quality attributes, weaknesses, and capabilities of a blockchain e-voting system that may be developed based on the architecture presented to them. The results of the ATAM revealed that BANES satisfied all the key quality attributes of e-voting in the South African context. It was adjudged as capable of engendering a secure e-voting system that has good performance and is functionally suitable for use for national elections. A sensitive and trade-off point in the aspect of voter validation was also identified. Voter validation and security were spotted as aspects that will require significant attention during development. We also presented a security analysis of BANES as enabled by the Hyperledger Fabric (HF) and argued that with adequate collaboration and supplementary security mechanisms, the HF can adequately protect the BANES from security threats during a national election.

As a contribution, this study presents a first attempt to assess the plausibility of blockchain e-voting through a critical analysis process that is stakeholder-centric. The analysis is done at the early stages of development, lightweight-oriented to facilitate the participation of non-technical persons, and enables communal understanding of the potential risks, challenges, and prospects of blockchain e-voting.

In future work, we shall delve more into how we can devise a more detailed design for the BANES through engagement with a larger pool of stakeholders that is more diversified. This will enable the elicitation of more requirements including both explicit and implicit (hidden/unspoken) requirements that pertain to e-voting in the South African context. This will enable a more robust basis for the accurate design of a blockchain e-voting system and its proof of concept implementation. We shall also look more into how we can identify the best supplementary security protocol that can be used to fortify the security of our blockchain-based system architecture.

**Author Contributions:** Conceptualisation: O.D. and D.T.; methodology: O.D.; experimentation: D.T.; validation: O.D., D.T.; writing—original draft preparation: O.D.; writing—review and editing: O.D. and D.T.; supervision: O.D. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Acknowledgments:** The authors of this paper appreciate the support of the Cape Peninsula University of Technology (CPUT).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Ayo, C.; Daramola, O.; Azeta, A. Developing A Secure Integrated E-Voting System. In *Handbook of Research on E-Services in the Public Sector: E-Government Strategies and Advancements*; IGI Global: Hershey, PA, USA, 2011; pp. 278–287.
2. Osgood, R. The Future of Democracy: Blockchain Voting'. COMP116: Information Security. Available online: http://www.cs.tufts.edu/comp/116/archive/fall2016/rosgood.pdf (accessed on 14 May 2020).
3. Bulut, R.; Kantarci, A.; Keskin, S.; Bahtiyar, S. Blockchain-Based Electronic Voting System for Elections in Turkey. In Proceedings of the 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11–15 September 2019; pp. 183–188.
4. Kazman, R.; Klein, M.; Clements, P. *ATAM: Method for Architecture Evaluation*; Defense Technical Information Center (DTIC): Pittsburgh, PA, USA, 2000.
5. Carvalho, M.B.; Bellotti, F.; Berta, R.; De Gloria, A.; Gazzarata, G.; Hu, J.; Kickmeier-Rust, M. A case study on Service-Oriented Architecture for Serious Games. *Entertain. Comput.* **2015**, *6*, 1–10. [CrossRef]

6. Ben Ayed, A. A Conceptual Secure Blockchain Based Electronic Voting System. *Int. J. Netw. Secur. Appl.* **2017**, *9*, 1–9. [CrossRef]
7. Yavuz, E.; Koc, A.K.; Çabuk, U.C.; Dalkiliç, G. Towards secure e-voting using ethereum blockchain. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–7. [CrossRef]
8. McCorry, P.; Shahandashti, S.; Hao, F. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. In *International Conference on Financial Cryptography and Data Security*; Springer Science and Business Media LLC: Cham, Switzerland, 2017; pp. 357–375.
9. Zhang, S.; Lee, J.-H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2019**. [CrossRef]
10. Bartoletti, M.; Carta, S.; Cimoli, T.; Saia, R. Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact. *Futur. Gener. Comput. Syst.* **2020**, *102*, 259–277. [CrossRef]
11. Hjalmarsson, F.P.; Hreioarsson, G.K.; Hamdaqa, M.; Hjalmtysson, G. Blockchain-Based E-Voting System. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 983–986.
12. Thuy, L.V.-C.-; Cao-Minh, K.; Dang-Le-Bao, C.; Nguyen, T.A. Votereum: An Ethereum-Based E-Voting System. In Proceedings of the 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF), Danang, Vietnam, 20–22 March 2019; pp. 1–6.
13. Braghin, C.; Cimato, S.; Cominesi, S.R.; Damiani, E.; Mauri, L. Towards Blockchain-Based E-Voting Systems. In Proceedings of the New Information and Communication Technologies for Knowledge Management in Organizations; Springer Science and Business Media LLC: Cham, Switzerland, 2019; pp. 274–286.
14. Zhang, Q.; Xu, B.; Jing, H.; Zhang, S.; Zheng, Z. Ques-Chain: An Ethereum Based E-Voting System. In Proceedings of the 9th International Conference on Computer Science and Information Technology (CCSIT 2019), Sydney, Australia, 29–30 June 2019.
15. Lai, W.-J.; Hsieh, Y.-C.; Hsueh, C.-W.; Wu, J.-L. DATE: A Decentralized, Anonymous, and Transparent E-voting System. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 24–29.
16. Naphade, S.; Dubbewar, H.; Patil, M.; Tambave, S. Ethereum Blockchain Based E-Governance System. Available online: http://www.ijrti.org/papers/IJRTI1905057.pdf (accessed on 14 May 2020).
17. Canessane, R.A.; Srinivasan, N.; Beuria, A.; Singh, A.; Kumar, B.M. Decentralised Applications Using Ethereum Blockchain. In Proceedings of the 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, Tamil Nadu, 14–15 March 2019; pp. 75–79.
18. Teja, K.; Shravani, M.; Simha, C.Y.; Kounte, M.R. Secured voting through Blockchain technology. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1416–1419.
19. Pawade, D.; Sakhapara, A.; Badgujar, A.; Adepu, D.; Andrade, M. Secure Online Voting System Using Biometric and Blockchain. In *Advances in Intelligent Systems and Computing*; Springer Science and Business Media LLC: Cham, Switzerland, 2019; pp. 93–110.
20. Kirillov, D.; Korkhov, V.; Petrunin, V.; Makarov, M.; Khamitov, I.M.; Dostov, V. Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain. In Proceedings of the Applications of Evolutionary Computation; Springer Science and Business Media LLC: Cham, Switzerland, 2019; pp. 509–521.
21. Verwer, M.B.; Dionysiou, I.; Gjermundrod, H. TrustedEVoting (TeV) a Secure, Anonymous and Verifiable Blockchain-Based e-Voting Framework. In Proceedings of the Education and Technology in Sciences; Springer Science and Business Media LLC: Cham, Switzerland, 2019; pp. 129–143.
22. Zhou, Y.; Liu, Y.; Jiang, C.; Wang, S. An improved FOO voting scheme using blockchain. *Int. J. Inf. Secur.* **2019**, 1–8. [CrossRef]
23. Hsiao, J.-H.; Tso, R.; Chen, C.-M.; Wu, M.-E. Decentralized E-Voting Systems Based on the Blockchain Technology. In *Lecture Notes in Electrical Engineering*; Springer Science and Business Media LLC: Cham, Switzerland, 2017; Volume 474, pp. 305–309.
24. Murtaza, M.H.; Alizai, Z.A.; Iqbal, Z. Blockchain Based Anonymous Voting System Using zkSNARKs. In Proceedings of the 2019 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 27–29 August 2019; pp. 209–214.
25. Tso, R.; Liu, Z.-Y.; Hsiao, J.-H. Distributed E-Voting and E-Bidding Systems Based on Smart Contract. *Electronics* **2019**, *8*, 422. [CrossRef]

26. Kurbatov, O.; Kravchenko, P.; Shapoval, O.; Poluyanenko, N.; Malchyk, M.; Sakun, A.; Kovtun, V. Anonymous decentralized e-voting system. In Proceedings of the 2019 International Workshop on Conflict Management in Global Information Networks (CMiGIN), Lviv, Ukraine, 29 November 2019; pp. 12–22.
27. Nimje, R.; Bhalerao, D.M. Blockchain Based Electronic Voting System Using Biometric. In Proceedings of the Lecture Notes on Data Engineering and Communications Technologies; Springer Science and Business Media LLC: Cham, Switzerland, 2019; pp. 746–754.
28. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access* **2019**, *7*, 24477–24488. [CrossRef]
29. Leema, A.A.; Gulzar, Z.; Padmavathy, P. Trusted and Secured E-Voting Election System Based on Block Chain Technology. In Proceedings of the International Conference on Computer Networks, Big Data and IoT (ICCBI—2019), Madurai, India, 19–20 December 2019; Springer Science and Business Media LLC: Cham, Switzerland, 2020; pp. 81–88.
30. Zhang, S.; Wang, L.; Xiong, H. Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *Int. J. Inf. Secur.* **2019**. [CrossRef]
31. Sadia, K.; Masuduzzaman, M.; Paul, R.K.; Islam, A. Blockchain Based Secured E-Voting by Using the Assistance of Smart Contract. *arXiv* **2019**, arXiv:1910.13635.
32. Li, P.; Lai, J. LaT-Voting: Traceable Anonymous E-Voting on Blockchain. In Proceedings of the Applications of Evolutionary Computation; Springer Science and Business Media LLC: Cham, Switzerland, 2019; pp. 234–254.
33. Alharby, M.; Van Moorsel, A. Blockchain Based Smart Contracts: A Systematic Mapping Study. In Proceedings of the 3rd International Conference on Artificial Intelligence and Soft Computing, Zakopane, Poland, 3–7 June 2017; pp. 125–140.
34. IEC. *2014 Report on the National and Provincial Elections*; Technical Report; Independent Electoral Commission: Centurion, Pretoria, South Africa, 2014.
35. Thebus, D.; Daramola, O. E-voting System for National Elections Using a Blockchain Architecture. In *Pan African International Conference on Science, Computing and Telecommunications Book of Proceedings*; University of Swaziland: Kwaluseni, Swaziland, 2019.
36. Daramola, O. A Process Framework for Semantics-Aware Tourism Information Systems. In Proceedings of the International Conference on Web Engineering, Vienna Austria, 5–9 July 2010; Volume 6385, pp. 521–532.
37. Hyperledger: Hyperledger Fabric—Hyperledger. Available online: https://www.hyperledger.org/projects/fabric (accessed on 26 October 2018).
38. Gupta, A. Design and Implementation of Public Key Infrastructure on Smart card Operating System. Ph.D. Thesis, Indian Institute of Technology, Department of Computer Science, Kanpur, India, 2008.
39. Goldwasser, S.; Micali, S.; Rackoff, C. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.* **1989**, *18*, 186–208. [CrossRef]
40. Babar, M.; Gorton, I. Comparison of Scenario-Based Software Architecture Evaluation Methods. In Proceedings of the 11th Asia-Pacific Software Engineering Conference, Busan, Korea, 30 November–3 December 2005; pp. 600–607.
41. Kruchten, P. The 4+1 View Model of architecture. *IEEE Softw.* **1995**, *12*, 42–50. [CrossRef]
42. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]
43. Qassim, N.; Qasse, I.A.; Abu Talib, M.; Bou-Nassif, A. Performance Analysis of Hyperledger Fabric Platforms. *Secur. Commun. Netw.* **2018**, *2018*, 1–14. [CrossRef]
44. Wang, H.; Wang, Y.; Cao, Z.; Li, Z.; Xiong, G. An Overview of Blockchain Security Analysis. In Proceedings of the Education and Technology in Sciences; Springer Science and Business Media LLC: Singapore, 2019; pp. 55–72.
45. Signorini, M.; Di Pietro, R.; Kanoun, W. Blockchain-Based Security Threat Detection Method and System. U.S. Patent 16/325,564, 13 June 2019.
46. Andola, N.; Raghav; Gogoi, M.; Venkatesan, S.; Verma, S. Vulnerabilities on Hyperledger Fabric. *Pervasive Mob. Comput.* **2019**, *59*, 101050. [CrossRef]

47. Yamashita, K.; Nomura, Y.; Zhou, E.; Pi, B.; Jun, S. Potential Risks of Hyperledger Fabric Smart Contracts. In Proceedings of the 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Hangzhou, China, 24–24 February 2019; pp. 1–10. [CrossRef]
48. Dimitriou, T.; Michalas, A. Multi-party trust computation in decentralized environments in the presence of malicious adversaries. *Ad Hoc Netw.* **2014**, *15*, 53–66. [CrossRef]