ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February2020

An Improved Smart Contract Model for Distributed Ledgers using Multi-modal Biometrics

May Stow[1]

Research Scholar, Department of Computer Science, Federal University, Otuoke, Bayelsa State, Nigeria[1]

ABSTRACT:Transactions between parties in current systems are usually conducted in a centralized form which requires the involvement of a trusted third-party. This could create serious security issues such as single point of failure and high transaction cost. Distributed ledger technology emerged to tackle these issues by allowing un-trusted parties to interact with each other without the need for a third-party intermediary. In this study, an Improved Smart Contract Model for Distributed Ledgers using Multi-modal Biometrics was developed using Structured System Analysis and Design Methodology (SSADM). Furthermore, the study recommended the importance of verified distributed ledger systems using biometrics. Verified distributed ledgers have the potential to reduce costs of transactions. Experts also believe that a distributed ledger technology is much more secure because each node of the network holds records, thereby creating a system that's more difficult to manipulate or successfully attack. In addition, this study could be useful to stakeholders in Ecommerce, Financial Institutions and any researcher with penchant for smart contracts.

KEYWORDS:Distributed Ledger, Multi-modal Biometrics, Smart Contract, SSADM, Transactions

I. INTRODUCTION

Transactions between parties in current systems are usually conducted in a centralized form which requires the involvement of a trusted third-party. This could create serious security issues such as single point of failure and high transaction cost. Distributed ledger technology emerged to tackle these issues by allowing un-trusted parties to interact with each other without the need for a third-party intermediary. Distributed platforms have attracted a lot of attention from individuals, commercial organizations, national and international institutions, thereby enhancing the possibility of securing record of information in a distributed way. Building on this, it is highly possible to construct distributed databases and also to record the results of transactions that have financial value, especially in crypto-currencies.

A smart contract is an executable program (written in some programming language like, Java, C++, Solidity, Go, etc.) that is deployed on a blockchain to mediate contractual interactions between two or more parties. A smart contract knows details about itself (properties) and how to interact with other objects (methods). However, major setbacks on smart contracts are due to an inefficient verification scheme. Certain anomalies such as insecurity, data privacy and jurisdictional issues, record retention risks and issues of confidentiality among un-trusted parties can be traced to lack of an improved verification scheme when executing smart contracts. TRON is an ambitious project dedicated to the establishment of a truly decentralized Internet and its infrastructure. The TRON Protocol, one of the largest blockchain-based operating systems in the world, offers public blockchain support of high throughput, high scalability, and high availability for all Decentralized Applications (DApps) in the TRON ecosystem. The July 2018 acquisition of BitTorrent further cemented TRON's leadership in pursuing a decentralized ecosystem. The introduction of Bitcoin in 2009 revolutionized society's perception of the traditional financial system in the wake of the Great Recession (2007-2008). As centralized hedge funds and banks collapsed from speculation in opaque financial derivatives, blockchain technology provided a transparent universal ledger from which anybody could glean transaction information. The transactions were cryptographically secured using a Proof of Work (PoW) consensus mechanism, thus preventing double spend issues. In late 2013, the Ethereum white paper proposed a network in which smart contracts and a Turing-complete Ethereum Virtual Machine (EVM) would allow developers to interact with the network through Digital Applications. However, as transaction volumes in Bitcoin and Ethereum peaked in 2017, it was apparent from the low

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February2020

transaction throughput times and high transaction fees that cryptocurrencies like Bitcoin and Ethereum in their existing state were not scalable for wide spread option. Thus, TRON was founded and envisioned as an innovative solution to these pressing scalability challenges. Analyzing verification of processes in smart contracts involves the application of Digital Signature Algorithm. According to Prince [1], "the digital signature algorithms uses some sort of complex operations aims to prevent the data from being accessible only for the authorized users, and computing such operations could exhaust the systems with limited computational resources"; the problem statement affects the integrity of the data directly and minimizes the security level to facilitate the process of penetration, then the algorithms must be selected depending on the degree to maintain the integrity of the information regardless of the type of device. Security is implemented directly by using a digital signature in each Named Data Network (NDN) data packets, and then it's important to check the efficiency of these implemented protocols. The data packet could carry any type of information: credit cards number, personal information, and passwords, top secret information etc., then the role of the digital signature is to keep the data packet away from the cyber-attacks.

II. RELATED WORK

Kosba et.al [2] designed Hawk, a blockchain cryptography and privacy-preserving smart contracts tool. It provides a framework for private smart contracts using zkSNARKs with strong privacy goals that include hiding the amounts of monetary transfers and contract state from non-participants and supporting private inputs that are hidden even from the other participants in the contract.

The major drawbacks in their work using the HAWK tool, includes;

1. lack of scalability as each contract requires kilobytes of data to be put on-chain.
2. No absolute privacy-preserving guarantee with Hawk tool since it relies on trusting a third-party manager who gets to see all the private data.
3. SNARKS require a peer-circuit trusted setup which means that every distinct program that a contract implements, a new trusted set up is required. Multi-party computation can be included to reduce trust in the setup, which is infeasible to perform on a per-circuit basis as required by Hawk.

Luu et al [3] proposed Oyente which was the first tool to apply symbolic execution in finding potential security bugs such as transaction ordering dependency, re-entrancy and unhandled exceptions in smart contracts. The tool takes as input the byte-code of a smart contract and a state of the Ethereum blockchain. It emulates the EVM and explores the different paths of the contracts it then uses the Z3 SMT solver to decide the satisfiable conditions which would make the program vulnerable in the current path. It also formulates the security bugs as intra-procedural properties and uses symbolic execution to check these properties. Out of the 19,366 existing Ethereum contracts at that time, Oyente flags 8,833 of them as being vulnerable, including the vulnerability responsible for the Distributed Autonomous Organization (DAO) attack. However, Oyente does not perform inter-procedural analyses to check inter-procedural or trace properties as sCompile tool does.

Hirai [4] proposed using a theorem prover environment to formally verify properties of a smart-contract. The author encoded EVM instructions semantics in Coq and later in Isabelle. He performed a formal verification of Ethereum smart contract and defined the complete instruction set of the Ethereum Virtual Machine (EVM) in Lem, a language that can be compiled for interactive theorem provers, which enables proving certain safety properties for existing contracts. Their framework allows a developer to prove the properties of his smart-contracts on the bytecode level inside a theorem prover. Being the most foundational among all other approaches, this method gives the highest guarantees on correctness of producing artefacts, but it takes a lot of time and effort.

Tikhomirov et.al [5] designed a tool called SmartCheck. Like ZEUS tool, SmartCheck analyses the high-level solidity source code of the smart contract to detect vulnerabilities. It is also able to find a wide range of vulnerabilities such as re-entrancy, unhandled exceptions, locked Ether, integer overflows and many more. SmartCheck transforms the solidity contract in an intermediate representation (IR) and uses an XML-based. XPaths patterns-checks for security properties in the contract intermediate representation (IR). This approach makes the system to lose precision for

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February2020

vulnerabilities which naturally cannot be expressed as XPaths, such as re-entrancy but more efficient for smart contracts vulnerability detection.

Andreas et al [6] researched on a comprehensive reference model for blockchain-based distributed ledger technology. The work compared four blockchain technology platforms and focused on their business level properties which included actors and roles, services and process data models. Furthermore, the authors compared their results using a reference model, which could potentially guide the business analysts, system analysts and software developers when developing new blockchain platforms or their supported implementations. In addition, the accuracy of their proposed reference model was validated by considering it against selected blockchain technologies. However, the authors did a good job but could not further improve the verification aspect of their system using biometrics. The application of biometrics to their model will ensure robustness in the systems' verification and validation of distributed ledger transactions.

III. DISTRIBUTED LEDGER TECHNOLOGY (DLT)

Blockchain is a domain in the field of distributed ledger technology which is currently well-covered in existing literature especially from a cryptographic point of view. DLT has been defined by different researchers from different perspectives. Mercy Corps [7] defined distributed ledger technology (DLT) as a trust layer where peer-to-peer networks, cryptography and hash technology are combined to eliminate the need for a trusted third-party intermediary. According to Coulouris[8], a distributed system is defined as a system in which hardware and software components located at networked computers communicate and coordinate their actions only by message passing. There are various types of distributed systems today, such as Clusters, Grids, P2P (Peer-to-Peer) networks, distributed storage systems and so on, each aimed at solving different kinds of problems. DLT is also defined as a series of networks of databases that allow participants to create, disseminate and store information in an efficient and secure manner. These networks of databases can operate smoothly and securely without the need for any central party or central administrator that every participant knows and trusts. DLT operations are designed in such a way that information stored and communicated through the networks has a high level of trustworthiness, and every participant in the network can get simultaneous access to a common view of the information. Unauthorized changes to the information and its history are very difficult.

IV. MULTI-MODAL BIOMETRICS: AN OVERVIEW

Recently there has been an extensive growth in the use of biometrics for person identification applications .Biometrics which is defined as anatomical / physiological (fingerprint, iris, face) and behavioural (ridges, gait) characteristics are used by FBI (Federal Bureau of Investigation), law enforcement and intelligence departments for the identification or authentication of an individual. Biometric identification systems which use a single biometric trait of the individual for identification and verification are called uni-modal systems. Biometric identification systems which use or are capable of using a combination of two or more biometric modalities to identify an individual are called multimodal biometric systems. The most important reason behind using multimodal biometric systems is these systems depend on multiple sources of information and thereby improve the recognition rate. In order to choose multimodal biometric technology for identification, a study on multimodal biometric system is required.

Biometrics is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are then distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioural characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioural characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behavior metrics to describe the latter class of biometrics. Biometric identification systems which use or are

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February2020

capable of using a combination of two or more biometric modalities to identify an individual are called multimodal biometric systems. The block diagram and workings of a multimodal biometric system are shown in figures 1 and 2. Biometric systems which rely on Unimodal authentication system rely on single source of information like face, fingerprint, voice, gait, iris, retina, etc. These systems lack level of accuracy due to noisy data, intra-class variations, inter-class similarities, non-universality and spoofing. It leads to considerably high False Acceptance Rate (FAR) and false rejection rate (FRR), limited discrimination capability, upper bound in performance and lack of permanence. These disadvantages imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity.

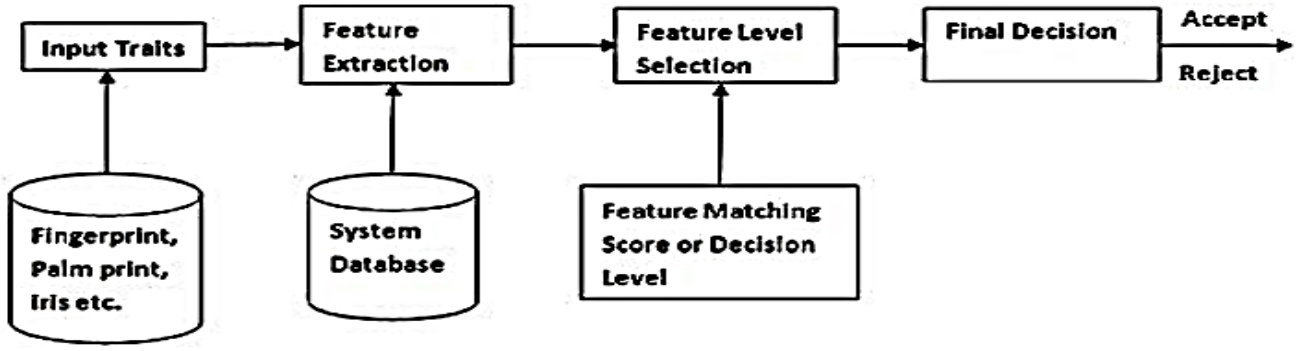

Fig. 1: Block Diagram of a Multi-modal Biometric System
(**Source:** [6])

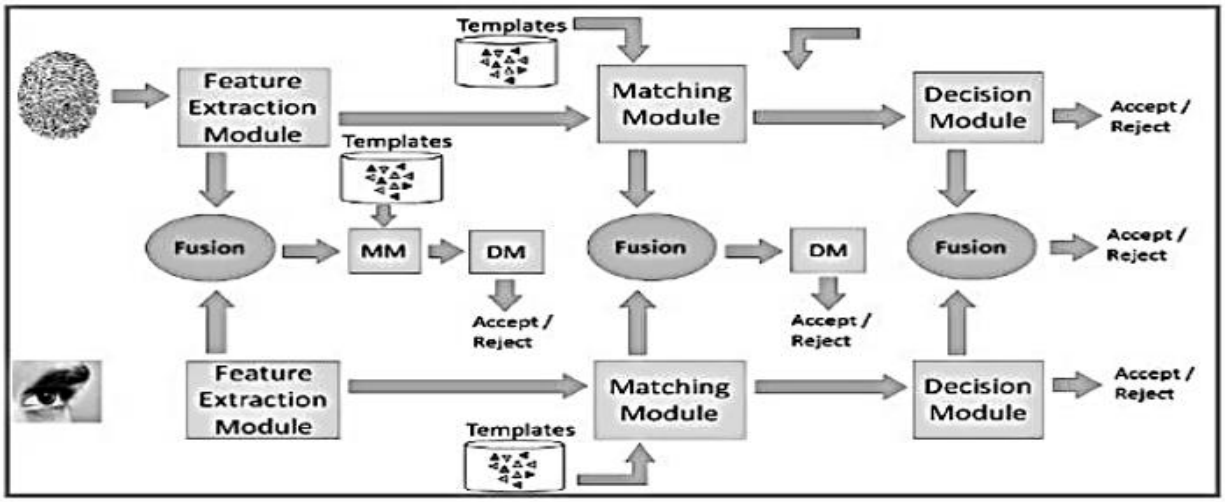

Fig. 2: Workings of Multimodal Biometric System
(**Source:** [6])

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February2020

These systems allow the integration of two or more types of biometric systems known as multimodal biometric systems. These systems are more reliable due to the presence of multiple, independent biometrics. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge response type of mechanism by requesting the user to present random subset of biometric traits thereby ensuring that a "live" user is indeed present at the point of data acquisition.

V. RESULTS AND DISCUSSION

5.1 Methodology

The Methodology for the Proposed Model Design is Structured System Analysis and Design Methodology (SSADM). Structured Systems Analysis and Design Methodology is a systems approach to the analysis and design of information systems. SSADM was produced for the UK government office concerned with the use of technology in government, from 1980 onwards. System design methods are a discipline within the software development industry which seeks to provide a framework for activity and the capture, storage, transformation and dissemination of information so as to enable the economic development of computer systems that are fit for purpose.

The Methodology application to the proposed system involved the following stages:

- **Stage One:**
  Analyzing Existing ways deployed to tackle the issue:
  There was in-depth analysis on current performance of the Existing System in Recommending reliable information to users.
- **Stage Two:**
  Existing System Performance and Identification of Anomalies:
  This phase involved studying result performance of the Existing System in order to spot any anomaly that should be corrected.
- **Stage Three: Review of any spotted anomaly from the Existing System:** This phase involved the deployment of the proposed system algorithm to any spotted anomaly from the Existing System Performance.
- **Stage Four:**
  Comparison of the Existing and Proposed Systems Performance Result: This phase involves comparing results of the Proposed and Existing Systems Performance.
- **Stage Five:**
  This phase involves the adoption of the most efficient result that tackles the mentioned issue due to the outcome of the comparison between the Existing and Proposed Systems.

5.2 Analysis of the Existing Model

The Existing System is a model for blockchain-based distributed ledger technology as developed by [6]and further illustrated in figure 3. The work compared four blockchain technology platforms and focused on their business level properties which included actors and roles, services and process data models. Another common process of the existing system is the Mining process (Block generation process). Mining is based on the proof-of-work. A miner will build a new block, add collected unverified transactions and metadata, and calculate the computationally exhaustive proof-of-work for the block. If he is the first one to solve the task and mine the block, he can submit the block to the network and receive a reward for that work. In Ethereum, the mining process also requires a state transition process, since it keeps a state of the blockchain.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February2020

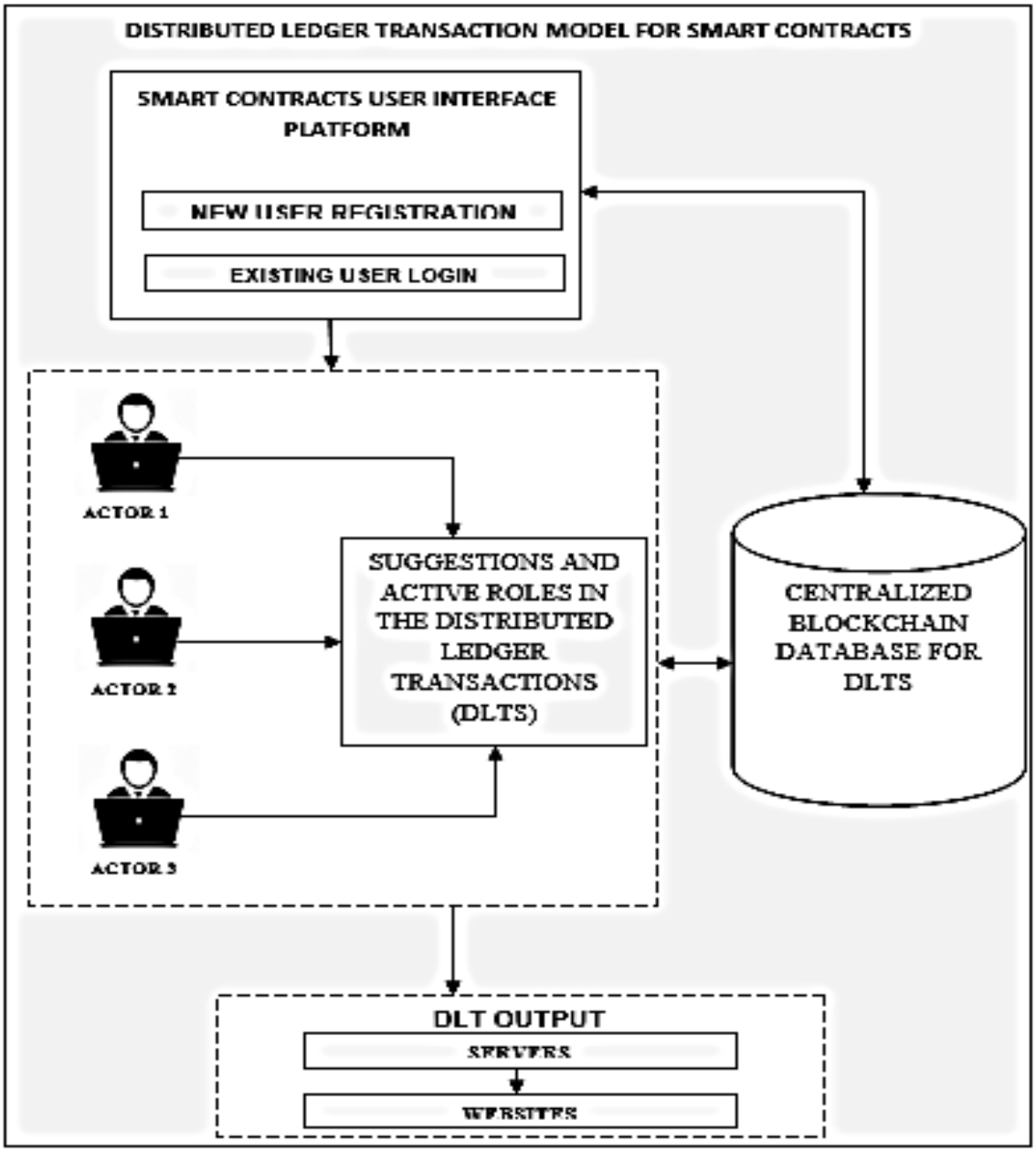

Fig. 3: Reference Model for Blockchain-based Distributed Ledger Technology
(Existing System Architecture)
(**Source:** [6])

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February2020

5.3 Explanation of the Existing Model

The following components of the Existing Model include the

- *Smart Contract User Interface Platform:*
  This platform enables newly system users to register in order to be assigned a unique username and corresponding password.
- *Actors/Active Roles:*
- These are individuals that interact with the blockchain through the creation of Distributed Ledger Transactions.
- *Centralized Blockchain Database for DLTs:*
- This is a central storage platform that contains associated rules for the DLTs managed by the actors of the Smart Contracts. Furthermore, the central storage platform also contains profile details of the registered users.
- *DLT Output:*
  This platform outputs the transaction performances of the transactions to witnesses and stake holders of the DLT.

5.3 Disadvantages of the Existing Model

The following disadvantages of the Existing Model encompass failure for improvement of the verification aspect of their system using biometrics. Every transaction to be implemented on the blockchain must be verified since the actors on the platform are untrusted. The application of biometrics to their model will ensure robustness in the systems' verification and validation of distributed ledger transactions.

5.4 Analysis of the Proposed Model

Our approach for improving the existing model encompasses the addition of an enhanced verifier platform that uses multimodal biometric technique (see figure 4). The need for the improvement is due to the fact that smart contracts testing is complicated because of the critical nature of applications and its immutability if deployed on a blockchain. Secondly, manual test generation is likely to form an important component but inevitably is limited; there is a need for effective automated test generation and execution techniques. Currently available options to test and verify contracts are:

1. deploy the contract to live (the real) Ethereum main network and execute it. This costs about 5 minutes and real money to deploy and execute.
2. deploy the contract to the test-net Ethereum network (for developers' usage) and execute it. This costs about 2 minutes to deploy and free ether.
3. deploy the contract to an Ethereum network (local) simulator and execute it. This costs about 3 seconds and is free but limited interaction and no realistic test of network related issues.

There are many automated test generation approaches that might have value. A number of these use formal approaches, such as those based on symbolic execution or search based methods to produce test cases that provide code coverage. Code coverage approaches may still have value but not to be sufficient on their own. An alternative approach is to base test automation on a model; an approach that is typically called model-based testing (MBT). Writing specifications manually tends to be complicated and error prone, AI can learn specifications from runtime traces.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February2020

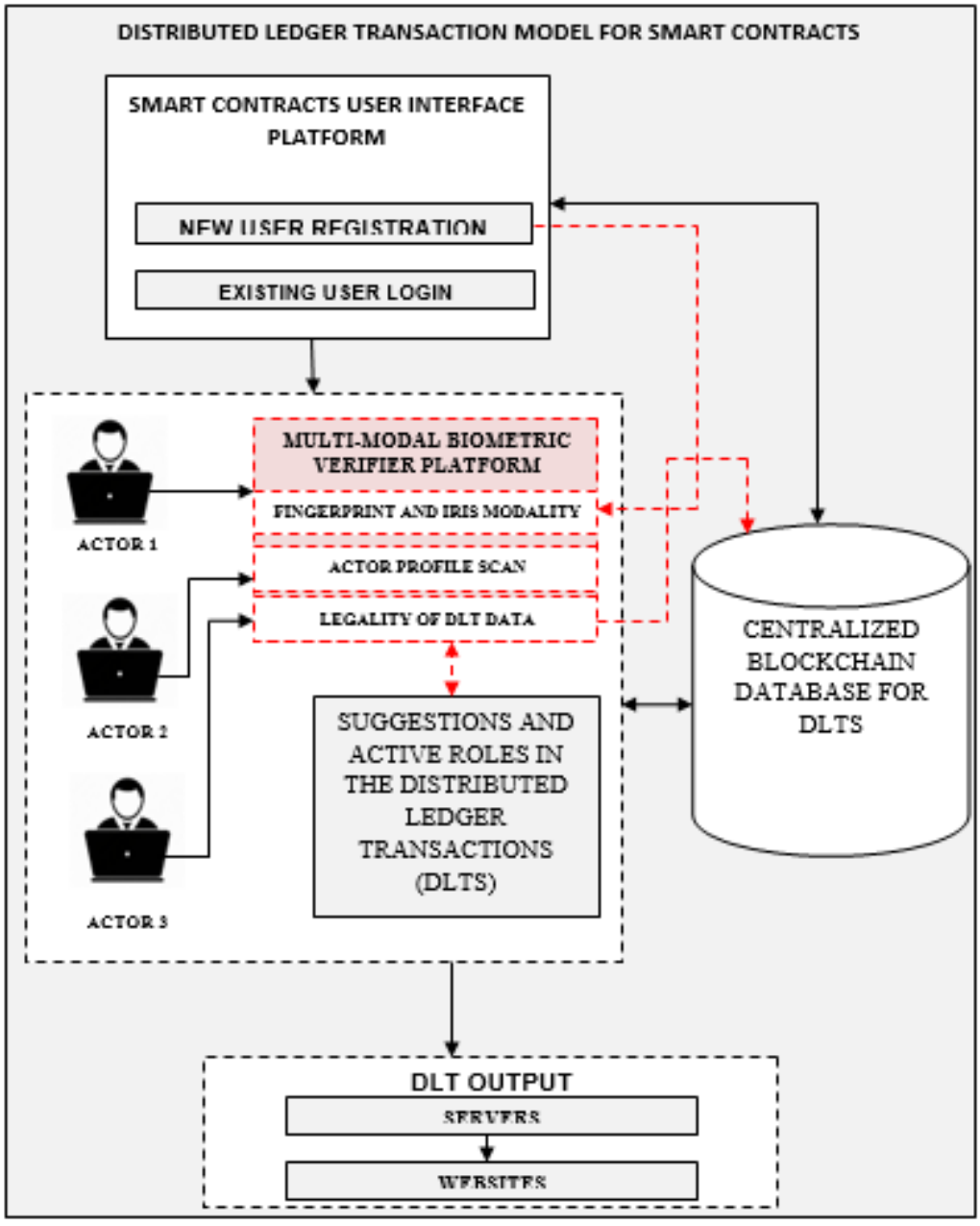

Fig. 4: An Enhanced Reference Model for Blockchain-based Distributed Ledger Technology using Multi-Modal Biometric
(Proposed System Architecture)

5.5 Explanation of the Proposed Model Components

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February2020

The following components of the Proposed System include the

- *Smart Contract User Interface Platform:*
  This platform enables newly system users to register in order to be assigned a unique username and corresponding password.
- *Actors/Active Roles:*
  These are individuals that interact with the blockchain through the creation of Distributed Ledger Transactions.
- Multi-modal Biometric Verifier Platform:
  This component aids efficient and robust verification process that relies on a hybridized biometric process which includes fingerprint and iris technology. Secondly, there are other sub-components such as actor-profile scan and legality of the shared DLT data. The actor-profile scan involves verifying the profile of the actors when there is suspicion of any actor with malicious intent in the system. Furthermore, DLTs are backed-up by certain ethics and conditions. Hence, the legality of DLT data is a unique platform that also verifies whether any shared transaction does not compromise the existing ethics and condition.
- *Centralized Blockchain Database for DLTs:*
  This is a central storage platform that contains associated rules for the DLTs managed by the actors of the Smart Contracts. Furthermore, the central storage platform also contains profile details of the registered users.
- *DLT Output:*
  This platform outputs the transaction performances of the transactions to witnesses and stake holders of the DLT.

5.6Advantages of the Proposed Model

The following advantages of the proposed model include

- Improved verification process for of Distributed Ledger Transactions
- Latency Reduction
- Security via Multimodal Biometric Technique

VI. CONCLUSION

In this study, we have developed an Improved Smart Contract Model for Distributed Ledgers using Multi-modal Biometrics.The importance of multimodal biometrics to distributed ledger systems encompasses verification and security. The defence and intelligence communities require automated methods capable of rapidly determining an individual's true identity as well as any previously used identities and past activities, over a geo-spatial continuum from set of acquired data. Furthermore, the study recommended the importance of verified distributed ledger systems. Verified distributed ledgers have the potential to reduce costs of transactions.

REFERENCES

[1] Prince L.S., T. SimonandM. Darryl, Scripting smart contracts for distributedledger technology. University of Kent, UK, 1 – 7, 2015.
[2] Kosba A. E. Miller, Z. Shi,Wen and C.Papamanthou, Hawk: The blockchainmodel of cryptography and privacy-preserving smart contracts, IEEE Symposium on Security and Privacy, 839-858, 2016.
[3] LuuL., D.H. Chu, H. Olickel, P. SaxenaandA. Hobor, Oyente: Making smartcontractssmarter.In: Proceedings of the 23rd ACM SIGSAC Conference onComputer and Communications Security (CCS), ACM, 54–269, 2016.
[4] Hirai Y., Defining the Ethereum Virtual Machine for interactive theorem, Provers, International Conference on Financial Cryptography and DataSecurity. Springe 520–535, 2017.
[5] TikhomirovS.,E.Voskresenskaya, I. Ivanitskiy, R. Takhaviev, R. MarchenkoandY. Alexandrov, SmartCheck: Static analysis of Ethereum smart contracts. IEEE/ACM Proceedings and Workshop on Emerging Trends Software Engineering Blockchain (WETSEB), 9-16, 2018
[6] Andreas A., M. Chanson and A. Meeuw, A decentralised sharing app running a smart contract on the ethereum blockchain. In Proceedings of the 6th International Conference on the Internet of Things. 177-178, 2016.
[7] Mercy V.Smart contracts and licensingin Business Innovation ThroughBlockchain.101- 124, 2017.
[8] Coulouris G., DollimoreJ.and T. Kinberg, Distributed SystemsConcepts and Design. Addison-Wesley. UK. 45-63, 2011