ISSN 2278-3091

Volume 9, No.1.3, 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1491.32020.pdf

https://doi.org/10.30534/ijatcse/2020/1491.32020

A Refuse Management System and Blockchain: A Practical View

Rohana Sham[1], Amir A'Atieff Hussin[2], Noranita Abdamia[3], Suhana Mohamed[4], Won Jet Rou[5]

[1] Assistant Professor, Logistics Department, UCSI University, Malaysia, rohana@ucsiuniversity.edu.my

[2] Assistant Professor, Department of Information Technology, International Islamic University, Malaysia, amiraatieff@iium.edu.my

[3]Senior Lecturer, Department of Economics, Universiti Teknologi Mara, Malaysia, noran801@uitm.edu.my

[4] Senior Lecturer, Department of Finance, Universiti Teknologi Mara, Malaysia, suhan291@uitm.edu.my

[5] Logistics Department, UCSI University, Malaysia, 1001439293@student.ucsiuniversity.edu.my

ABSTRACT

The refuse management in Malaysia had experienced high degradation, and this had caused a massive loss of ecosystem services due to significant pollution. Added with low community engagement to clean the environment, a lot of refuse management system being developed through apps is left unattended by them. One of the significant drawbacks of today refuses management system are still lacking in terms of the identity protocol for identifying individual especially those who have signed up for the app's usage. Apart from that, leakage of user identity has become a critical issue affecting users' certain level to use the app as main tools under a refuse management system. As a result, most of the service providers need to build and maintain their own databases of user information for all kind of system they developed. Therefore, the objective of the study is to identify major security issue and inadequacy of the current blockchain mechanism in the refuse management system and to explore why blockchain mechanism should be used as a mechanism for higher authentication security in refuse management system. Thus, this project will demonstrate the potential of why blockchain should be used as a mechanism for in cleaning up the environment. The ultimate outcome looks at the potential blockchain application in refuse management system for the utilizing of the surrounding committee to clean the environment.

Key words: Authentication, Blockchain, Refuse Management, Security

1. INTRODUCTION

Blockchain is a digitized, decentralized, and public ledger of all cryptocurrency transactions. All the transaction using blockchain technology are recorded in a chronological order to monitor the transaction of the digital currency without any central control [1]. They have also agreed that in blockchain technology, every computer in the network is called a node in the network and every node in the system receives a duplicate information of the transaction that automatically gets downloaded. The blockchain technology is used to develop protocol for automated access-control while not requiring a central third- party management [2]. He also describes the growth in research and industry concerning with how blockchain technology can provide security and privacy in the peer to peer network. According to [3], among the most popular blockchain systems include Ethereum, bitcoin, Monero, and the security threats for blockchain in real-time scenarios was deliberates. Thus, the main objectives of the paper are divided into 2. The first objective is to explore the significant security issues of inadequacy of the current blockchain mechanism in the refuse management system. The second objective is to explore on why the blockchain mechanism should be used as a mechanism for higher authentication security in a refuse management system.

2. PROBLEM STATEMENT

A. High Pollution

In Malaysia, major environmental management issues are all linked to refuse management quality. The problem is worsened when community engagement in environmental cleaning effort is degrading as well. In the global economy, engaging the community as part of the plan to reduce pollution has become a central issue [4]. They summarized that in the past two decades, extreme efforts had been made to promote environmental performance measurements and market-based instruments by winning and involving all society in addressing the environmental issues. As the target of this research is to encourage community engagement towards environment cleaning, having a suitable way to secure information on members of the community who wish to participate is essential. Blockchain is one of the best-known methods of security which be used to secure both IoT and user data [5]. However, some challenges still remain towards integrating this technology with IoT [6].

B. Authentication Issues

Information security is widely studied in area of computing that has recently received wide attention from the research community [7]-[9]. User authentication is one of the main methods of securing information by ensuring only users with necessary rights have access to acquired data. Authentication is used to confirm that specific data claimed true by a particular party to be true. This differs with identification which only attests to the identity of someone or something. Authentication is meant instead to verify or confirm that identity. Authentication confirms the identity using various ways such as document validation, source authenticity and most recently, digital certificates [10]. A common form of authentications are passwords, and it is one of the oldest and most widely used methods of verifying a user's identity [11]. Being first introduced in 1961 by researchers at the Massachusetts Institute of Technology (MIT) while building a time-shared computer they dubbed the Compatible Time-Sharing System (CTSS). After their research focus on Since then efforts have been made to increase the security of this vulnerable method such that the introduction of secure encryption using cryptography [12] together with best practices to improve the formulation of password on the user's side to something not easily known [13]. Even with enhancements, underlying vulnerabilities of this type of authentication remains an issue. The fact remains as passwords can easily be surmised because ordinary things such as words and personal details (date of birth etc.) are used. With the processing power of personal computers increasing by the day together with introduction of ever faster distributed parallel processing network, using brute for attacks [14] to figure out a password becomes more feasible as it can be done faster than before [15].

C. Lack of Transparency in Current Transaction

Even without using computational power, passwords can be easily obtained when it is irresponsibly written down and even through simple observation by someone in the proximity of user. Some users use their password across several platforms leading to a higher likelihood of being hacked [16]. Another weakness of passwords is that most of them are stored in a central location making an attack much easier to be a focus on as is with other modes of authentication such as digital certificates and centrally stored public or private encryption keys. Avoiding a centralized authentication method is the key to making blockchain more secure than others. Admittedly, alternatives to password-only systems do exist. Newer technology such as biometrics and multi-factor authentication provides better security than passwords. However, for these systems to be effective, the existing centralized authentication used in many of these systems needs to be replaced to avoid the likelihood of security breach. Instead of having one big bullseye to be attacked, create redundant mirrors of the same data that only blockchain out if the entire network of mirrors is taken down. This is the solution provided by blockchain. Blockchain was built on the notion that a decentralized system offers better security than a centralized one[17].Having multiple shared copies of information that is publicly available across a chain which consists of blocks of such data that is replicated at a specific frequency makes this method almost impossible to hack. This is because taking down one server will not compromise the data because another server in the chain contains the same data as well. For example, in the case of biometric authentication, to change an individual's biometric record, the perpetrator must hack all the blocks in the blockchain which is extremely difficult since every block is encrypted with their unique security encryption [18].

D. Information Leakage

While passive mobile apps [19] have existed for some time, the inadequacy of the blockchain mechanism application is still low. Apart from that, the issues of information leakage that happens had resulted in the trust of the apps has gone down. With high utilization of app among users, this phenomenon had also indirectly showed that the users are tasked with providing their own identity, entering credentials for online and cloud service that they access. This act has generated a massive amount of user data in which the majority of them face higher chances of getting leak. Their details, MyKad numbers, addresses and mobile phone numbers which have been used to register as a member before using any apps may have fallen into the wrong hands [20].

3. SECURITY ISSUES IN BLOCKCHAIN

Any electronics or electrical devices which is connected to internet are known as 'Internet of objects' or 'Internet of Things' [21]. Being connected to the internet exposes these IoT to a myriad of threats. Significant security and privacy issues can stem from the essential traits of IoT itself which generally consists of heterogeneous devices that are dynamic and applied to multiple domains sometimes with undefined perimeters. This makes finding a comprehensive solution for the current security challenges difficult [22].

Consequently, when considering these challenges, is of utmost importance to approach analyzing, understanding and finally defining requirements for blockchain-based systems with extreme caution. Each domain where an IoT device interacts comes with its own set of peculiarities that needs to be considered to maximize protection of privacy and security. Experience can be gathered from others who have ventured into this field such as those have conducted in-depth analysis to produce concrete specifications that meet required security and privacy environment such as the work of [23].

Similarly, we intend to conduct our research in to improve upon likewise applying it for a secure authentication and activation system to help towards a pollution-free environment by utilizing an IoT-based infrastructure secured with Blockchain Technology. We aim to use blockchain and IoT technology to contribute to fulfilling the United Nation's current sustainable development goals. While our project only focused on the pollution-free environment, we will draw upon ideas and experiences towards using blockchain community benefiting purposes such as those studied by [24]. Research has also shown that blockchain can contribute to smart cities in different ways including in taking care of the environment [25]. This research tends to make the same concept to a whole new level in the case of Malaysia, to convince the community to engage by feeling secured with blockchain authentication. The blockchain mechanism is known to increase trust as is supported by several research found in the literature [26]-[28]. The question is whether this trust can translate into higher engagement and activation of a community that will lead to pollution-free environment. Trust is known to be to an essential catalyst towards community engagement as was found by [29],[30]. The basis of blockchain security is decentralized trust which relies on the notion of a stable source of the truth. The main problem with IoT is that the system cannot be fully trusted. Thus, Blockchain is needed as it can help to create something called a Trusted execution environment (TEE) for the IoT devices. This is because all the data that was stored on blockchain is immutable and traceable. Thus, a blockchain create a unique and pure source of IoT data.

4. BLOCKCHAIN ISSUES AND GAP ANALYSIS

Blockchain could be applied to create a better and trusted network from all stakeholder in many possible areas. A research done by [21] had concluded that among the application of the blockchain is as follow:

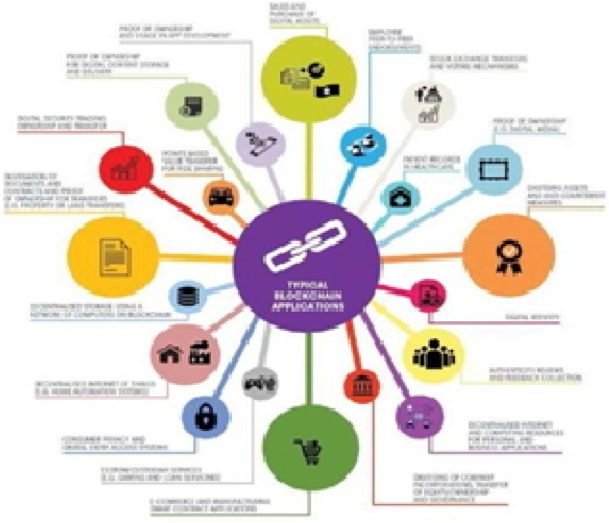

Figure 1: Example of Blockchain Application [21]

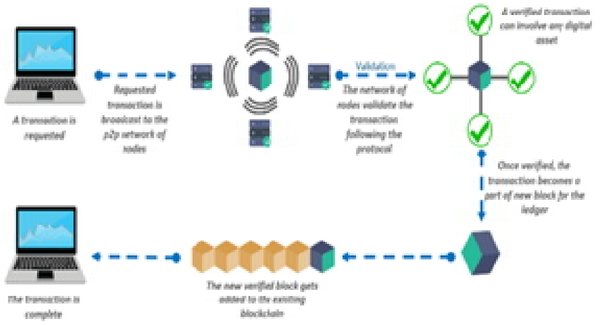
A transaction is requested
Requested transaction is broadcast to the p2p network of nodes
Validation
The network of nodes validate the transaction following the protocol
A verified transaction can involve any digital asset
Once verified, the transaction becomes a part of new block for the ledger
The new verified block gets added to the existing blockchain
The transaction is complete

Figure 2: Blockchain Technology Transaction [21]

Figure 1 and 2 explain on possible application of blockchain and blockchain technology transaction. There are many successful non-monetary domains where Blockchain technology is successful. This include the supply chain, healthcare system, proof of location, cloud storage and human resource management. Thus, to run a successful blockchain application, the features shall be included are contract of transaction is triggered by participant through digital ledger and the block is where pool of data was collected, recorded on correct sequence and timestamp.

A detail analysis of blockchain application found that lack of discussion was made to refuse management system using blockchain. Thus, this paper tries to fill up the gap by looking at the possibility of the blockchain in a refuse management system. However, to understand the blockchain system well, several applications of blockchains were discussed.

A.Blockchain in Supply Chain

Internet of Things (IOT) raise needs on tools for centralized organizations as organizations can track locations of goods and increase operations transparency but normally organization is opaque and causes limited control and lack of inner details known by users [31]-[33].

Issues in supply chain includes information not asymmetry and data isolation, contributing lower trust towards suppliers, causing negative influence as issues of low quality and counterfeit products would arise, leading to information fraud and pressure for member in supply chain [34],[35].According to [36], use of blockchain with multiagent system, issues on linear supply chain can be solved due to decentralization.

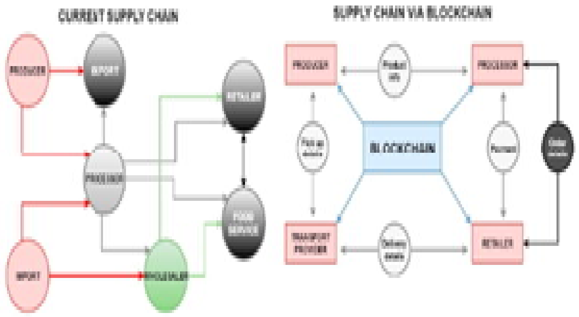

Figure 3: Comparison on supply chain with traditional approach and with blockchain [36]

The figure above shown with blockchain, all process entered in supply chain can be read by users if they have direct connections. Access of blocks can be shared to users enables users to check origins of information. Blockchain increases trust and integrity of information as blockchain identify integrity of data, reduce duplicate data and reconcile data collected to increase trustworthiness of data [32]. Below show improvements of blockchain towards supply chain management where transparency, accuracy and efficiency can be achieved:

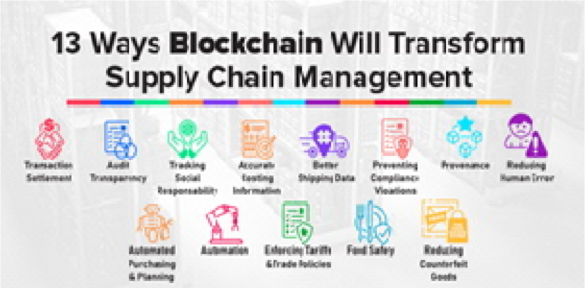
13 Ways Blockchain Will Transform
Supply Chain Management
Transaction Settlement
Audit Transparency
Tracking Social Responsability
Accurate Costing Information
Better Shipping Data
Preventing Compliance Violations
Provenance
Reducing Human Error
Automated Purchasing & Planning
Automation
Enforcing Tariffs & Trade Policies
Food Safety
Reducing Counterfeit Goods

Figure 4: Blockchain in Supply Chain [37]

Integration of blockchain with procurement system would provide smoothness in supply chain through increasing effectiveness in operations [65], [66].

B.Blockchain in Health

Electronic Health Record (EHR) is used to collect patient's data and contributed to researches [38]-[41]. Issues such as missing data and non-standard medical coding schemes would lead to incorrectness and impreciseness of data [42],[43].

The study [44] had proposed use of Ethereum blockchain [45] and smart contract to store data in blockchain with ease of storing and retrieving data for patients, thus patients' previous record would store in cloud and enables hospitals to retrieve information even patient has visited another hospital. Cryptographically signed instructions are provided by blockchain to ensure data integrity as cryptographic hash of records remove possibility of moderating to achieve security and immutability of data [44]. Patients could share information using private blockchain and participated parties able to access information in blockchain, level of privacy can be controlled and provide sufficient information [46],[47].

C.Blockchain In Finance

Interbank and cross-border payment are inefficient as process handled by intermediary clearing firms require series of complicated process within parties involved, causing higher cost and delay in payment [48]. Issues in finance including cybersecurity issues as it involved online transactions which enables faster process and wider reach in transactions, but cybersecurity risk arise and financial institutes require to preventing cyberattacks, cybercrime, cyber espionage [49].

Blockchain record every transaction where it is identified and verified by members in blockchain, thus intermediary to protect the transaction is unnecessary [50]. Transactions are done in real-time will increase efficiency. According to [51], cybersecurity issues can be improved by use of blockchain with mechanism of cybersecurity relating to the organization as blockchain provides data ownership, transparency and auditability on data, and fine-grained access controls [51].

D.Blockchain In Refuse Management System

Issues relating to refuse management system were identified such as lack of proper collection of refuse item and storage, lack of waste recovery and treatment system while the researcher proposed model for levers and options in waste management system to develop plans and managing waste effectively [52].There is a need to develop different model for e-waste management system in countries such as Germany, Switzerland, Japan and India are compared, showing that high producers' participation would result in lower participation cost in E-waste management and application of Advance Recycling Fee (ARF) is heartened to be cast-off in countries. The researchers proposed that India could follow concept of "Design of Environment" (DOE) from Japan where practice of e-waste management is done by producers voluntarily [53].

Furthermore, there is a proposal on collaborating on e-hailing application with waste collection ststem to reduce the cost on waste collection as well as achieving the 11th sustainable goals to make the environment green [54].

According to the model of [55], the use of the mixed-integer linear programming (MILP) mathematical model can be used to collect and disposal of municipal solid waste (MSW) by bearing in mind pollution emissions where this model could increase the efficiencies and reduce uncertainties. The study also minimizes cost of systems including cost of establishments, operations, transportation, pollutions and non-collected wastes [55]. Sustainable Development Goals (SDG) can be achieved by integrating blockchain with refuse management system [56]. Furthermore, use of blockchain can contributes to ensure the integrity of the systems for related parties and at the same time reducing fraud or loss of cash closing as no printed cards would be used during process.

Blockchain in waste management system would manage waste collection and trading of waste towards third parties as it increases trust between stakeholders and no accounting records needed to be kept by farmers thus enable to spread the system to farmers in the system [56].

Practices from past and future of refuse management system are studied and proposed on integrating technologies with refuse management for data collection where researchers studied process of locating, cleaning and utilizing environmental data, however, implementation on blockchain on refuse management system is not provided [57].

Blockchain is important as challenges in refuse management identified are lack of awareness and enforcement on waste management, issues in waste segregation at source, unnecessary generations, lack of scientific landfills, no technology on tracking flow of waste and lack of accountability between related parties [58]. The researchers proposed the use of Thui-mychain on Internet of Things (IOT), Artificial Intelligence (AI) and use of cryptocurrency to address issues identified by the researchers above [58]. Use of blockchain could not effectively reduce opportunities of fraud, manual processes and increase technology knowledge as in study of [59], researchers identified that issues of fraud and manipulation of parties depending with each other's in refuse management system cannot be solved by use of blockchain. It can be solved by other methods before blockchain is implemented, researchers argued that blockchain is a tool to prevent error or loss of information and helps increasing control.

5. METHODOLOGY

A. Phase 1

The first phase of the research aims to investigate the current security issues of the inadequacy of the blockchain mechanism in a refuse management system, especially on the authentication issues of the users who are willing to participate. This phase begins with a thorough investigation of different authentication strategies used and frameworks proposed for the online services offered. This is in line with the technique used by [60] where a comprehensive evaluation was performed to provide maximum effectiveness and applicability of the proposed technology. On top of that, the security challenges of online apps authentication [61] and the Internet-of-Things (IoT) [62] are then further explored. It is then followed by data collection and analysis. This phase ends with a summarization of the investigation above and analysis to formulate the problem of the inquiry.

B. Phase 2

This phase concentrates on identifying the inadequacy issues of blockchain mechanism in a refuse management system based on problems identified in the literature [6]. This phase begins with a detailed study on why the blockchain mechanism still faces the challenge of inadequacy in terms of the application. It is then followed by the flow diagram of how a user interacts with a service provider smart contract which is deployed to the blockchain mechanism through the activated apps. Then, the final design will cover the transactions user can make using the smart contract in the blockchain network in a refuse management system. This technique was adopted from [63] where a new derivation scheme using blockchain was demonstrated through the simulation results to verify the performance enhancement.

C. Phase 3

This phase focuses on the critical issues of blockchain mechanism in a refuse management system. Through an investigation on the current problems of the blockchain, the tool is determined. Once the issues identified, the proposed mechanism is tested through the execution of the smart contract. This stage will carefully be observed on data confidentiality, integrity, and reliability. The procedure will be strictly found on the information leakage that usually happens when the IoT data is not secured by the blockchain mechanism. All activities in this phase will be evaluated with a formal security proof with consideration on the issues and challenges reported by [64].

D. Phase 4

The final phase concentrates on the documentation of the research and realizes model formulation on how blockchain could be integrated into the refuse management system to engage community surrounding for a better environmental cleaning purpose. In this stage, proper testing and validation to activate an ecological friendly refuse management system using blockchain mechanism are involved.

6. RESULT AND DISCUSSION

Current State of Refuse Management Workflow

If you have ever come across any of the recycle bin in your residential area, the bin is always not known, or they refuse item is usually not declared by the owner. Added to this the municipal council had allocated only once a week of a collection that created a worse scenario to most of the residential area especially during the festive season where the refuse item will be double and left unattended in front of their home. In some residential area, there will be individual vendors coming from house to house asking for the refuse item to be sold. This phenomenon had created great potential for high carbon release. Added to that is the personal security issues, where the identity of the vendors are not known. This has resulted in an insecure feeling by the house owner to participate or even communicate with them. Thus the refuse item is still left at their home and create unhealthy living and environment.

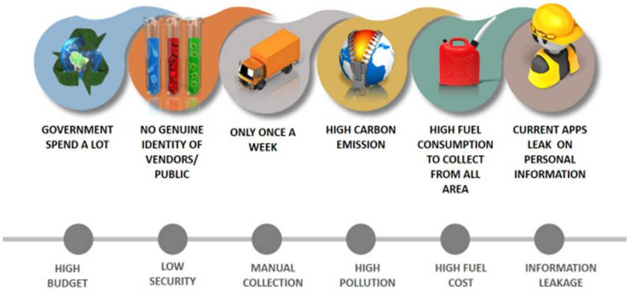

Figure 5: Current State of Refuse Management Flow

With all these states of current operating condition, a blockchain technology was suggested to enable a zero-knowledge proof for waste management. Apart from the current state of refuse management workflow that needs to be understood. The current state of refuse management waste collection is also needed to be further details out. Thus, the following Figure 6 further details out the current refuse management system collection.

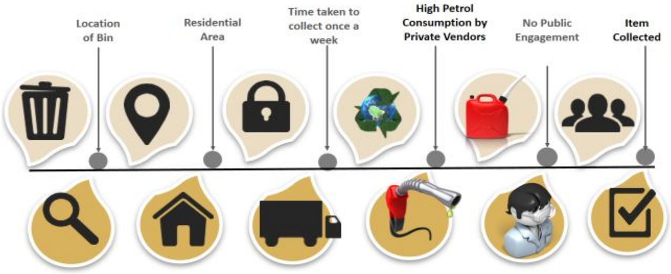
Location of Bin
Residential Area
Time taken to collect once a week
High Petrol Consumption by Private Vendors
No Public Engagement
Item Collected

Figure 6: Current Refuse Collection Workflow

Current State of Refuse Management Workflow

All refuse management users are members of one or more ecosystems. The platform users can access to these ecosystems are by using their private keys. In the refuse management ecosystem, any entity, person or asset (bin) is assigned unique digital identity credentials (public key number or hash code). Thus, is created a unique relationship that links all society in a bigger globe ecosystem mode. These credentials can be used to participate in global identity verification exchange where all citizen can participate without having to reveal the real identity of them when dealing with refuse management.

Refuse Management using a blockchain technology choose the ecosystem model for the creation of applications to link all the stakeholder in a chain or node because such a model enables implementation of several types of business, social, governmental and other activities autonomously.

These ecosystems consist of:

1. Encompass actors which include a large number of applications, users, vendors and a municipal council (who create and use these applications to track the movement of refuse item).
2. Include a system to manage all user roles (public, vendors and municipal) and access rights for applications and user's participation from all parties.
3. Are self-sufficient systems which can operate on their own; if there is a need to connect and integrate with another ecosystem, that is also possible.
4. Can be created by any individual, vendors or government with wallet owner.

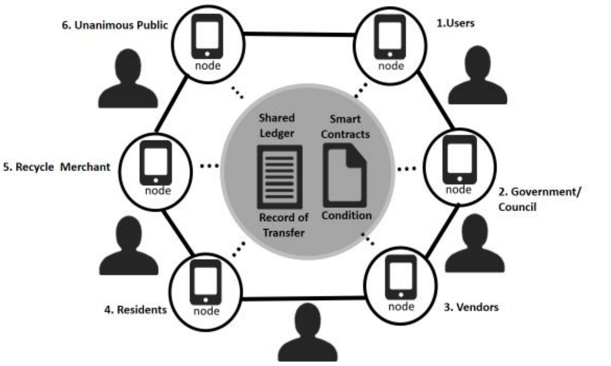

Figure 7: Refuse Management Ecosystem

The creator of an ecosystem is known as an ecosystem founder or administration.

By default, an ecosystem founder normally holds the complete set of rights for controlling the whole ecosystem: creating and editing applications, user roles, permissions, modifying ecosystem parameters, etc. However, control of these rights can be transferred to other members of the ecosystem. The procedure for accepting new members into an ecosystem is defined by its founder.

However, the system can be set to be an autonomy. In order to achieved this, the ecosystem founder, along with its members, creates a set of rules to control the operations within the ecosystem. In this refuse management system, these rules are known as smart laws. The smart law system establishes the rules for modification of access rights and other regulations that should be met before the total refuse system can be connected or work.

Smart Contract

The total smart contract being established will then constitute the legal system of the ecosystem. In general, is an agreement between parties that binds them to something happening in the future. The "smart" comes from the automatic execution of these digital contracts. Simply speaking they consist of many "if, then" statements that are written in and enforced by code. In this refuse management system, only when users alert their bin, then only the rest of the actors will get notified and can act accordingly. To the vendor side, only those with legal hash can access to the information and react to the refuse management system in the system. So does the municipal council where the alert will be sent when all info met the smart laws and consensus are met. In this case, consensus always involves group-lead decision making. Hence, consensus protocol used in a blockchain network tells a lot about its degree of security, decentralizable and transparency. Thus, using the blockchain to manage the refuse management system create a more secure environment and more transparent giving more opportunity for the public to participate in cleaning the environment together.

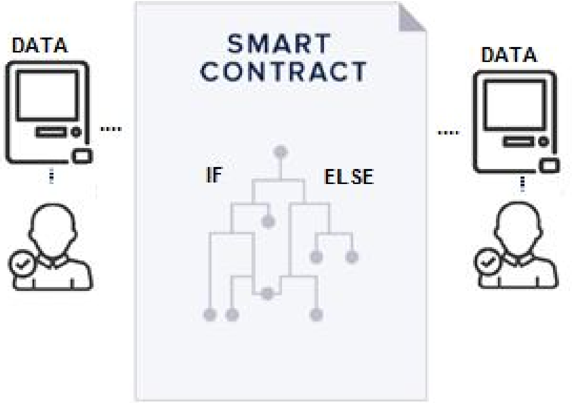

Figure 8: Smart Contract for Refuse Management System

7. CONCLUSION

This paper concluded that using blockchain technology in managing refuse management will help more society to participate as the transaction becomes more transparent and secure. Information management will be more confident and controlled in the most cost-effective ways. The future extension of Blockchain application should be focus on the supply chain sector where critical decision and human errors happen daily and decrease the total effectiveness of the entire supply chain network.

ACKNOWLEDGMENT

Authors special thanks goes to Ministry of Higher Education for the grant of Fundamental Research Grant Scheme

(FRGS/1/2019/ICT04/UCSI/02/1) and UCSI University for the resources given to complete this paper.

REFERENCES

1. A. P. Joshi, M. Han, and Y. Wang. **A survey on security and privacy issues of blockchain technology**, *Mathematical Foundations of Computing,* vol. 1, no. 2, pp.121-147, 2018.
2. C. C. Agbo, Q. H. Mahmoud and J. M. Eklund. **Blockchain Technology in Healthcare: A Systematic Review,** *Healthcare*, vol.7, no.2, pp.1-30, 2019.
3. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen. **A survey on the security of blockchain systems**, *Future Generation Computer Systems*, 2017.
4. H. Borhan and E.M. Ahmed. **Green Environment: Assessment of Income and Water Pollution in Malaysia**, *Procedia - Social and Behavioral Sciences,* vol. 42, no. July 2010, pp.66–174, 2012.
5. N. Kshetri. **Blockchain's roles in strengthening cybersecurity and protecting privacy,** *Telecommunications Policy,* vol. 4, no. 10, pp.1027-1038, 2017.
6. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz. **On blockchain and its integration with IoT. Challenges and opportunities,** *Future Generation Computer Systems*, vol. 88, pp.173-190, 2018.
7. N. S. Safa, C. Maple, T. Watson, and R. Von Solms. **Motivation and opportunity-based model to reduce information security insider threats in organisations**, *Journal of Information Security and Applications,* vol. 40, pp.247-257, 2018.
8. F. Bélanger, S. Collignon, K. Enget, and E. Negangard. **Determinants of early conformance with information security policies,** *Information & Management*, vol. 54, no. 7, pp.887-901, 2017.
9. S. Hong, S. Park, L. W. Park, M. Jeon, and H. Chang. **An analysis of security systems for electronic information for establishing secure internet of things environments: Focusing on research trends in the security field in South Korea,** *Future Generation Computer Systems*, vol. 82, pp.769-782, 2018.
10. L. O'Gorman. **Comparing passwords, tokens, and biometrics for user authentication**. *Proceedings of the IEEE*, vol. 91, no. 12, pp.2021-2040, 2003.
11. R. McMillan. **The World's first computer password, it was useless too**, *Wired. com,* pp.1-27, 2012.
12. M. Bellare and V.T. Hoang. **Adaptive Witness Encryption and Asymmetric Password-Based Cryptography**, *In: Katz J. (eds) Public-Key Cryptography -- PKC 2015,* PKC 2015, Lecture Notes in Computer Science, vol. 9020, Springer, Berlin, Heidelberg. 2015.
13. L. Zhang-Kennedy, S. Chiasson, and P. Van Oorschot. **Revisiting password rules: facilitating human management of passwords**, In *2016 APWG symposium on electronic crime research (eCrime)*, pp. 1-10, IEEE, June 2016.
14. A. Abdou, D. Barrera, and P. C. Van Oorschot. **What lies beneath? Analyzing automated SSH bruteforce attacks**. In *International Conference on Passwords*, pp. 72-91, Springer, Cham, December 2015.
15. E. Tirado, B. Turpin, C. Beltz, P. Roshon, R. Judge, and K. Gagneja. **A new distributed brute-force password cracking technique,** In *International Conference on Future Network Systems and Security*, pp. 117-127, Springer, Cham, July 2018.
16. C. Luevanos, J. Elizarraras, K. Hirschi, and J. H. Yeh. **Analysis on the security and use of password managers**, In *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pp.17-24, IEEE, December 2017.
17. J.M. Woodside, F.K. Augustine Jr, and W. Giberson. **Blockchain technology adoption status and strategies,** *Journal of International Technology and Information Management,* vol. 26, no. 2, pp. 65-93. 2017.
18. P. Garcia. **Biometrics on the blockchain,** *Biometric Technology Today*, vol. 2018, no. 5, pp.5-7, 2018.
19. Cornerstone Corporation Sdn Bhd. **ROL Citizen's Eye (1.0.7) [Mobile application software]**, Available: http://www.klriver.org/, 2018.
20. S. Zulhuda and A. Ibrahim. **The state of e-government security in Malaysia: reassessing the legal and regulatory framework on the threat of information theft**, In *1st Taibah University International Conference on Computing and Information Technology (ICCIT 2012)*, pp.812-817, March 2012.
21. H. Miraz and M. Ali. **Blockchain Enable Enhance IoT Ecosystem Security**, *International Conference on Emerging Technologies in Computing 2018 August*, pp.1-9, August 2018.
22. A. Ouaddah. **A blockchain based access control framework for the security and privacy of IoT with strong anonymity unlinkability and intractability guarantees**, *Advances in Computers*, 2018.
23. A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman. **Access control in the Internet of Things: Big challenges and new opportunities**, *Computer Networks*, vol. 112, pp.237-262, 2017.
24. B. Kewell, R. Adams, and G. Parry. **Blockchain for good?** *Strategic Change*, vol. 26, no. 5, pp. 429-437, 2017.
25. J. Sun, J. Yan, and K. Z. Zhang. **Blockchain-based sharing services: What blockchain technology can contribute to smart cities**. *Financial Innovation*, vol. 2, no. 1, pp.26, 2016.
26. M. M. Schöner, D. Kourouklis, P. Sandner, E. Gonzalez, and J. Förster. **Blockchain technology in the pharmaceutical industry**. Frankfurt, Germany: Frankfurt School Blockchain Center, 2017.
27. G. Wolfond. **A blockchain ecosystem for digital identity: improving service delivery in Canada's**

public and private sectors. *Technology Innovation Management Review*, vol. 7, no. 10, 2017.

28. N. Kshetri and J. Voas. **Blockchain-enabled e-voting**, *IEEE Software*, vol. 35, no. 4, pp.95-99, 2018.
29. M. R. Habibi, M. Laroche, and M. O. Richard. **The roles of brand community and community engagement in building brand trust on social media**, *Computers in Human Behavior*, vol. 37, pp. 152-161, 2014.
30. C. P. Hsu, Y. F. Chiang, and H. C. Huang. **How experience-driven community identification generates trust and engagement**, *Online Information Review*, vol. 36, no. 1, pp. 72-88, 2012.
31. K. Francisco and D. Swanson. **The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency**, *Logistics*, vol. 2, no. 1, pp. 2, 2018.
32. P. Helo and Y. Hao. **Blockchains in operations and supply chains – a review and reference implementation**. *Proceedings of International Conference on Computers and Industrial Engineering, CIE*, vol. 2018-Decem, no. July, pp.242–251, July 2018.
33. K. Korpela, J. Hallikas, and T. Dahlberg. **Digital Supply Chain Transformation toward Blockchain Integration**, *Proceedings of the 50th Hawaii International Conference on System Sciences*, pp.4182–4191, 2017.
34. S. A. Abeyratne and R. P. Monfared. **Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger**. *International Journal of Research in Engineering and Technology*, vol. 05, no. 09, pp. 1–10. 2016.
35. F. Tian. **An agri-food supply chain traceability system for China based on RFID & blockchain technology**. *13th International Conference on Service Systems and Service Management (ICSSSM),* pp.1–6, 2016. https://doi.org/10.1109/ICSSSM.2016.7538424
36. R. Casado-Vara, J. Prieto, F. D. L Prieta, and J. M. Corchado. **How blockchain improves the supply chain: Case study alimentary supply chain**, *Procedia Computer Science*, 2018. https://doi.org/10.1016/j.procs.2018.07.193
37. S. Mire. **Blockchain in Supply Chain Management: 13 Possible use Cases**, *DMCA Report*, 2018.
38. I. R. Bardhan and M. F. Thouin. **Health information technology and its impact on the quality and cost of healthcare delivery**, *Decision Support Systems*, vol. 55, no. 2, pp. 438–449, 2013. https://doi.org/10.1016/j.dss.2012.10.003
39. A. Gupta and R. Sharda. **Improving the science of healthcare delivery and informatics using modeling approaches,** *Decision Support Systems*, vol. 55, no. 2, pp. 423–427, 2013. https://doi.org/10.1016/j.dss.2012.10.001
40. M. P. Johnson, K. Zheng, and R. Padman. **Modeling the longitudinality of user acceptance of technology with an evidence-adaptive clinical decision support system**. *Decision Support Systems*, vol. 57, no. 1, pp. 444–453, 2014. https://doi.org/10.1016/j.dss.2012.10.049
41. G. Van. Valkenhoef, T. Tervonen, T. Zwinkels, B. D. Brock, and H. Hillege. **ADDIS: A decision support system for evidence-based medicine**. *Decision Support Systems*, vol. 55, no. 2, pp. 459–475, 2013.
42. B. K. Beaulieu-Jones, D. R. Lavage, J. W. Snyder, J.H. Moore, S. A. Pendergrass, and C.R. Bauer. **Characterizing and Managing Missing Structured Data in Electronic Health Records: Data Analysis**, *JMIR Medical Informatics*, vol. 6, no. 1, (2018). https://doi.org/10.2196/medinform.8960
43. G. Jetley and H. Zhang. **Electronic health records in IS research: Quality issues, essential thresholds and remedial actions**, Decision *Support Systems*, vol. 126, no. May, pp. 113-137, 2019. https://doi.org/10.1016/j.dss.2019.113137
44. D. Dhagarra, M. Goswami, P. R.S. Sarma, and A. Choudhury. **Big Data and blockchain supported conceptual model for enhanced healthcare coverage: The Indian context,** *Business Process Management Journal*, 2019.
45. G. Wood. **Ethereum: A Secure Decentralised Generalised Transaction Ledger**. *Ethereum Project Yellow Paper, (August 1, 2017),* pp. 1–32, (2014). https://gavwood.com/paper.pdf
46. G. Yang, C. Li, and K. E. Marstein. **A blockchain□based architecture for securing electronic health record systems**. *Concurrency and Computation: Practice and Experience*, vol. March, pp. 1–10, 2019. https://doi.org/10.1002/cpe.5479
47. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang. **Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control**, *Journal of Medical Systems*, vol. 40, no. 10, 2016.
48. P. Rosati and Č. Tilen. **Blockchain Beyond Cryptocurrencies.** *Disrupting Finance*, pp. 149–170, 2019.
49. S. Henry and A. F. Brantly. **Countering the Cyber Threat**, *The Cyber Defense Review*, vol. 3, no. Spring 2018, pp. 47–56, 2018.
50. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman. **Blockchain technology: beyond Bitcoin**, *Applied Innovation Review*, vol. 2, pp. 71, 2016.
51. K. J. Smith and G. Dhillon. **Assessing blockchain potential for improving the cybersecurity of financial transactions**, *Managerial Finance*, 2019.
52. B. G. Mwanza, C. Mbohwa, and A. Telukdarie. **Municipal solid waste management in Kitwe City: An engineering management perspective**. *Management of Environmental Quality: An International Journal*, vol. 29, no. 6, pp. 1075–1092, 2018. https://doi.org/10.1108/MEQ-10-2017-0120
53. K. Chaudhary and P. Vrat. **Case study analysis of e-waste management systems in Germany,**

Switzerland, Japan and India: a RADAR chart approach, *Benchmarking: An International Journal*, vol. 25, no. 9, pp. 3519–3540, 2018.

54. S. Rohana, A.H. Amir Hussin, A. Noranita, and M.M. Marhani. **Developing a Pollution Free Environment Framework through Technology Integration(e-HailingApp)**, *Environment-Behaviour Proceedings Journal*, vol. 4, no. 10, pp.161-167, 2019.
55. E. B. Tirkolaee, I. Mahdavi, M. M. S. Esfahani, and G. W. Weber. **A robust green location-allocation-inventory problem to design an urban waste management system under uncertainty**, *Waste Management*, vol. 102, pp. 340–350, 2020.
56. D. Zhang. **Application of blockchain technology in incentivizing efficient use of rural wastes: A case study on Yitong System**, *Energy Procedia*, 2019.
57. J. P. Howell, K. Schmidt, B. Iacone, G. Rizzo, and C. Parrilla. **New Jersey's waste management data: retrospect and prospect,** *Heliyon*, vol. 5, no.8, pp. 1-8, 2019.
58. P. Gopalakrishnan and R. Ramaguru. **Blockchain based waste management,** *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, pp. 2632–2635, 2019.
59. G. Ongena, K. Smit, J. Boksebeld, G. Adams, Y. Roelofs, and B. Smart. **Association for Information Systems AIS Electronic Library (AISeL) Blockchain-based Smart Contracts in Waste Management: A Silver Bullet? Recommended Citation**, *BLED 2018 Proceedings*, pp.345–356, 2018.
60. Q. Qiang, I. Nurgaliev, M. Muzammal, C. S. Jensen, and J. Fan. **On Spatio-temporal blockchain query processing,** *Future Generation Computer System*, vol.98, pp. 208-218, 2019.
61. A. P. Joshi, M. Han, and Y. Wang.**A survey on security and privacy issues of blockchain technology**, *Mathematical Foundations of Computing*, vol. 1, no. 2, pp. 121-147, 2018.
62. M. A. Khan and K. Salah. **IoT security: Review, blockchain solutions, and open challenges,** *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.
63. L. Han and M. Ma. **Blockchain based mobility management for 5G,** *Future Generation Computer System*, 2019.
64. A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito. **Blockchain and iot integration: A systematic survey,** *Sensors*, vol. 18, no. 8, pp. 2575, 2018.
65. A. Thio-ac, A. K. Serut, R. L. Torrejos, K. D. Rivo, and J. Velasco. **Blockchain-based System Evaluation: The Effectiveness of Blockchain on E-Procurements,** *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 5, pp. 2673-2676, 2019. https://doi.org/10.30534/ijatcse/2019/122852019
66. A. Thio-ac, E. J. Domingo, R.M Reyes, N. Arago, R. J. Jorda, and J. Velasco. **Development of a Secure and Private Electronic Procurement System based on Blockchain Implementation,** *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 5, pp. 2626-2631, 2019. https://doi.org/10.30534/ijatcse/2019/115852019