Blockchain And Cryptocurrency Module

Critical Evaluation of Blockchain-Based Fintech Solution

Prototype:

I-Mart

By

Salisu Abdullahi

C2224671

Table of Contents

1.0 Introduction

With blockchain platforms going through the trough of disillusionment in the Gartner HypeCycle of 2022, interests in new blockchain solutions have waned. This is due to many consumers only interested in cryptocurrency and blockchain wallets which have seen them move through to the slope of enlightenment. Despite that, consumer applications like NFT games and commerce are driving innovation making enterprises gradually begin to realize business value and pushing the tipping point for adoption (Litan, 2022). Progress have been made in expanding the scope of use of blockchain-based solutions beyond cryptocurrency, with new enterprise in education, ticketing and sales and food safety using NFTs and smart contracts to manage them. As more innovations are introduced covering more aspects of life, it is only a matter of time before the mainstream adoption of blockchain based solutions in all aspects of life, one of which is the gadget resale ecosystem. Gadgets are among the top 5 stolen items in the UK with mobile phones, computer accessories and laptops being a major component of this (Shaw *et al*, 2015). Also, the increase in substandard used devices in the gadget market has created consumer problems affecting the brands as well. The prototype, I-Mart employs the use of blockchain technologies to handle and manage resale of gadgets by creating a transparent process which prioritizes authenticity, value, and true ownership.

2.0 Reflection on Underlying Technologies

I-mart used Nguyen (2023) ideals needed to stay ahead (smart world, productivity revolution, transparency and privacy, and new critical technology enablers) as a source of reference in creation of the technologies of the app.

2.1 Distributed Ledger Technology

I-mart used multi-party distributed ledger technology based on the Ethereum blockchain ensuring that there is accuracy and transparency in ownership transfer and authenticity of the gadget in real time. Recently, adoption of distributed ledger technologies

by companies have reshaped existing markets and created new ones (Hyperledger, 2022) ensuring accuracy in reporting, managing logistics, preventing fraud, and identifying inaccuracies (Franklefield, 2023). Blockchain technology is fast becoming the transformative distributed ledger technology of recent times with wide application in bitcoin and Ethereum (Khan, Jung and Hashmani, 2021a). Multi-party blockchain based distributed ledgers create a single source of truth which every party can relate to (Hill, 2023a) (see appendix I).

2.2 Consensus Mechanism and Transaction Speed

To improve the speed of doing transactions, I-mart uses Polygon technology due to its scalability which is a challenge hindering optimal blockchain solutions (Khan, Jung and Hashmani, 2021b) (see appendix I). I-mart faster processing is based on proof-of stake consensus mechanism which uses low energy and required no special computing equipment (McKinsey and company, 2023) with validators nodes owned by Apple, the Broker store and I-mart.

2.3 Smart Contracts

The prototype use of smart contracts made transaction completion easy, and ownership transfer seamless. Smart contracts are beneficial for facilitating or creating trust between parties improving efficiency and reducing reliance on third parties thereby enhancing the integrity of business dealings (Sinha *et al*, 2022). (See Appendix I)

2.4 Cryptoassets

Introducing token capabilities to I-mart made it possible to create digital twins of real-world assets, transfer value, create tokenized incentives, or fractionalize ownership of assets (Hill, 2023b) thereby making it easier to automate our processes around them and improve our application efficiency (see Appendix I). Also, I-mart integrates payment merchants like Moonpay onto the chain to help with easy exchange between fiat currency and cryptocurrency for customers who wants their payment in either of both currencies.

3.0 Reflection on Security and Ethics

3.1 Access Control

We decided to use private permissioned blockchains as they can restrict access or permission to the network and transactions. Permission state of any blockchain is important in the security of any application which uses the blockchain. This is because public blockchains create privacy issues as the information on them is accessible to all network's nodes and users (Williams, 2022), thereby risking personal data of users. The prototype use of validation nodes manages access to user's data further making it safe (See Appendix II). Many businesses or enterprise applications require access controls or other limitations, such as restricting data content or store locations (Shah *et al*, 2019a). The application use attribute-based access controls (ABAC) to manage access by using smart contract authenticate the roles and challenge-protocol for user verification making the gadget ownership and authentication process seamless (see Appendix II).

3.2 Data Privacy

The broad definitions of personal data with respect to blockchain have made it impossible to avoid adhering to privacy and data protection laws especially as the prototype uses user data for financial settlement, logistics management and ownership management. Therefore, to ensure compliance with data protection and privacy laws, a few solutions were considered and implemented in the prototype based on Shah *et al* (2019b). These include avoiding sharing of user personal data on the chain and using the blockchain as only pointers to the ownership history using usernames, using encryption keys during item delivery to prevent reidentification, and change of asset code upon transfer of ownership of asset to another user.

4.0 Reflection on Personal Contribution

Personally, my interest in the prototype was high as used gadget resale is a thriving market in my country, Nigeria. What is worrying however, is the chances that most UK-used gadgets sold are stolen items. A report by Parker and Sullivan (2018) highlighted that there was 446,000 phone theft in 2016 alone and most of the phones end up in Nigeria. This puts

at risk, buyers of used phones both in the UK and in Nigeria who are not aware that the phones are stolen and end up being arrested or persecuted. Thus, it was important to me that we were able to design a prototype that can help curb and reduce this. Also, during the presentation, the prototype got impressive reviews from the audience, but one concern was noted regarding there being a way for users to trust the legitimacy of any device they are buying ensuring that they were not stolen or used for fraudulent activities. I had not considered that outcome and was unable to sufficiently provide an answer as blockchain validation of the device software may not be able to provide such information. One of the module tutors helped in providing an answer by suggesting that we could use a combination of each gadget's unique IMEI or device number, and Mandatory Access Control (MAC) handled by the gadget parent company to check usage logs and determine if gadget has been used fraudulently and wiped. I read up on the use of MAC more and learnt about how it can be used to establish controls that cannot be changed by users, but only through administrative action (Hu *et al*, 2017) providing only administrators (gadget owners) with system resource and information and restrict user access to change owner of the gadget. Hence, this can be deployed in the prototype to also protect the user and ensure that only through ownership transfer can the phone information be wiped, and ownership changed.

5.0 Reflection on Teamwork

During the initial stages and just after the group has been shared. We took a test on 123test (https://www.123test.com/team-roles-test/) to assess our individual team identities. Based on Belbin team role attributes (https://www.belbin.com/about/belbin-team-roles), the outcome showed that the group was made of one resource investigator, two implementer and one team worker. This will be important in highlighting our team's journey in creating the prototype using Tuckman's theory (1965). We did not spend time on the forming stage as we were quick to identify a number of ideas we wanted to create a prototype for. They included goods authenticity verification application for importers and exporters, a price validation application for food items and a gadget resale authentication and ownership transfer application. As a result, we decided to go and make individual research about each of our ideas and come back to brainstorm on which we thought was

best. After brainstorming, we decided to pitch our ideas to the module tutor for professional insights into which of them will be best and we finally concluded to design a gadget resale authentication and ownership transfer application. The storming stage took longer as we kept changing ideas and features of how our prototype should look like and the appropriate technologies to use. Most notable conflicts that arose include deciding the distributed ledger to use, deciding how to handle cross-currency trade, what software features to authenticate on the chain and whether the need for a wallet was necessary or not. However, the group was able to overcome these by applying some conflict resolution techniques such as group participation in solving the problem by collectively evaluating alternative solutions which have a common goal (stevens and campion, 1994a). We also used the study technique of communication to determine features to authenticate by listening to each other's view of features that are important when purchasing a gadget. With the conflicts out of the way, the norming and performing stages were quickly attained using planning, task coordination and expectation techniques (stevens and campions, 1994b) to identify the tasks that needed to be done and assigned the design of the user framework, smart contract coding, user interface design and business ethics consideration to different members while also working together to ensure harmonization of all our task.

Finally, based on the feedback and review of our presentation, we discovered that it would have been advantageous to our creation process if we had a team member with a specialist attribute (based on Belbin team role attribute) and thus will be perfecting it based on the feedback from the presentation hence we have not attained the adjourning stage yet. We are holding out for the future value of the prototype and hope we will get the chance to implement a real-world use of the application.

APPENDIX

Appendix I

Ethereum: is a decentralized blockchain platform that runs on a network of computers and uses smart contracts to reduce any chances of downtime or interference. Handling of the gadget ownership transfer process involves events from multiple sources (Apple, Broker, and I-Mart) making Ethereum the perfect distributed ledger to use.

Proof of Stake Consensus Algorithm: is a way in which the legitimacy of a data or transaction that is to be added to a blockchain is verified. This uses a network of computers (nodes) to validate transactions and add them to the blockchain.

Smart Contract: is a digital contract that is automatically executed when predetermined conditions are met on a blockchain network. These smart contracts can be used to facilitate the exchange of anything in a wide variety of contexts such as the trading of assets with valid ownership transfer (Szakiel, 2022) with automatic execution once the specified conditions are met. Here, Trust is not an issue as smart contracts and consensus algorithms automate the addition, modification, and verification of data into the system (Hill, 2023c)

Tokenization: made it possible for us to create a digital representation of our gadget using both the picture and its asset code to mint a 3D non-fungible token (NFT).

Polygon Technology: is a Layer 2 scaling solution for Ethereum which provides faster and cheaper transactions through a separate blockchain (sidechain) connected to the main blockchain through a two-way peg facilitating the transfer of data and assets between the main chain and the side chains (Makori, 2023). Scalability, high energy, and transaction cost have been identified as a crucial challenge hindering provision of optimal solutions to businesses with direct or indirect dependency on consensus mechanism (Khan, Jung and Hashmani, 2021b) used by the blockchain. Using polygon technology deals with these issues as it provides the advantages of low transaction cost, and a faster rate of minting the NFTs created as a digital twin of the gadget (Antier Solutions, 2022).

Appendix II

Validation Nodes: are computers that synchronize with a blockchain or DLT network participating in consensus, and are responsible for verifying, voting on, and maintaining a record of transactions. They are distributed across the data owners and are selected based on the amount of stake delegated to them by Data Owners (Apple, I-mart, and broker stores) who support the security of the network by selecting the best validators to stake.

Data Owners: are the organizations (token holders) who play crucial roles in the blockchain and ensure seamless operation. They are selected in the chain using an endorsement policy which determines who has access to a particular process and can validate if the process is a valid one (Islam and Madria, 2019).

Attribute-based access control: provides an integration between the ABAC distribution model and a Blockchain, offering a method to easily find and access digital assets consisting of three components: Asset Security, Secure Asset Issuance, and Distributed Permissions (Golightly *et al*, 2023). Based on Cruz et al (2018), I-mart implements a smart contract with roles such as addUser or removeUser to assign a role to or revoke a role from a specific user; addEndorser or removeEndorser to add or remove endorser and function changeStatus() to change the status of deactivated smart contracts. Challenge-response protocol is utilized for the authentication of the broker, who request a service from the gadget owner. This protocol has five steps: declaration, information check, challenge response, and response verification.

REFERENCES

1. Antier Solutions (2022). 'What is Polygon Blockchain? Why Should You Use it?', *Medium*, 3 February. Available at: https://antiersolutions.medium.com/what-is-polygon-blockchain-why-should-you-use-it-29a95fceb8c6 (Accessed: 3 May 2023).
2. Cruz J.P. *et al*. (2018). 'RBAC-SC: Role-Based Access Control Using Smart Contract', *IEEE Access*, 6 (2018), 12240–12251. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8307397 (Accessed: 5 May 2023).
3. Franklefield J. (2023). *Distributed Ledger Technology (DLT): Definition and How It Works.* Available at: https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp (Accessed: 3 May 2023).
4. Golightly L. *et al* (2023). 'Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN', *Cybersecurity and Applications,* Volume 1. Available at: https://www.sciencedirect.com/science/article/pii/S2772918423000036 (Accessed: 3 May 2023).
5. Hill K. (2023a). 'Multi-Party Systems in Blockchain Explained', *Kaleido* 17th February. Available at: https://www.kaleido.io/blockchain-blog/multi-party-systems-in-blockchain (Accessed: 3 May 2023).

6. Hill K. (2023b). 'Multi-Party Systems in Blockchain Explained', *Kaleido* 17th February. Available at: https://www.kaleido.io/blockchain-blog/multi-party-systems-in-blockchain (Accessed: 3 May 2023).
7. Hill K. (2023c). 'Multi-Party Systems in Blockchain Explained', *Kaleido* 17th February. Available at: https://www.kaleido.io/blockchain-blog/multi-party-systems-in-blockchain (Accessed: 3 May 2023).
8. Hu V.C. *et al* (2017). 'Verification and Test Methods for Access Control Policies/Models', *National Institute of Standards and Technology Special Publication 800-192,* Gaithersburg, MD, June 2017. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-192.pdf (Accessed: 3 May 2023).
9. Hyperledger (2022). *Hyperledger Foundation.* Available at: https://www.hyperledger.org/ (Accessed: 3 May 2023).
10. Islam A. and Madria S. (2019). 'A Permissioned Blockchain based Access Control System for IOT', *IEEE International Conference on Blockchain.* Missouri, USA. Available at: https://www.researchgate.net/profile/Azharul-Islam-4/publication/338365055_A_Permissioned_Blockchain_Based_Access_Control_System_for_IOT/links/5e43324a458515072d932533/A-Permissioned-Blockchain-Based-Access-Control-System-for-IOT.pdf (Accessed: 5 May 2023).
11. Khan D., Jung L.T., and Hashmani M.A (2021a). 'Systematic Literature Review of Challenges in Blockchain Scalability', *Applied Sciences,* 11(20). doi: https://doi.org/10.3390/app11209372
12. Khan D., Jung L.T., and Hashmani M.A (2021b). 'Systematic Literature Review of Challenges in Blockchain Scalability', *Applied Sciences,* 11(20). doi: https://doi.org/10.3390/app11209372
13. Litan A. (2022). 'Gartner Hype Cycle for Blockchain and Web3, 2022', Gartner, 22 July. Available at: https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/ (Accessed: 3 May 2023).
14. Makori J. (2023). 'Polygon vs. Ethereum: DeFi, NFTs, Gas Fees, and More', *CoinGecko,* 19th April. Available at: https://www.coingecko.com/learn/polygon-vs-ethereum#.ZFUAH2EH8Y4.link (Accessed: 5 May 2023).

15. McKinsey and Company (2023). *What is proof of stake?* Available at: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-proof-of-stake (Accessed: 3 May 2023).
16. Nguyen T. (2023). *4 Emerging Technologies You Need to Know About*. Available at: https://www.gartner.com/en/articles/4-emerging-technologies-you-need-to-know-about (Accessed: 3 May 2023).
17. Parker N. and Sullivan M. (2018). 'Nigerian gangs making MILLIONS from phones nicked in UK phone theft epidemic', *The Sun,* 2 April. Available at: https://www.thesun.co.uk/news/5957717/nigeria-black-market-fuels-britain-moped-theft/ (Accessed: 3 May 2023).
18. Shah P. *et al* (2019a). 'Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies', *Practice Law*, W-021-8235. Available at: https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf (Accessed: 3 May 2023).
19. Shah P. *et al* (2019b). 'Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies', *Practice Law*, W-021-8235. Available at: https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf (Accessed: 3 May 2023).
20. Shaw O. *et al* (2015). *Crime and the value of stolen goods*. Research Report 81. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/468003/horr81.pdf (Accessed: 3 May 2023).
21. Sinha A. *et al* (2022). *Smart Contracts Could Improve Efficiency and Transparency in Financial Transactions*. Available at: https://www.spglobal.com/_division_assets/images/special-editorial/smart-contracts-could-improve-efficiency-and-transparency-in-financial-transactions/0922_smartcontracts.pdf (Accessed: 3 May 2023).
22. Stevens M. and Campion M. (1994a). 'The Knowledge, Skill, and Ability Requirements for Teamwork: implications for Human Resource Management', *Journal of Management,* 20(2), 503-530. Available at:

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9eb1c2ca0cc41e3749152a1e7972bb2f0fc65b2b (Accessed: 5 May 2023).

23. Stevens M. and Campion M. (1994b). 'The Knowledge, Skill, and Ability Requirements for Teamwork: implications for Human Resource Management', *Journal of Management,* 20(2), 503-530. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9eb1c2ca0cc41e3749152a1e7972bb2f0fc65b2b (Accessed: 5 May 2023).
24. Szakiel P. (2022). *How Smart Contracts Are Changing the Way We Do Business*. Available at: https://www.g2.com/articles/smart-contracts (Accessed: 3 May 2023).
25. Tuckman, B. W. (1965). 'Developmental sequence in small groups', *Psychological Bulletin*, 63(6), 384–399. https://doi.org/10.1037/h0022100 (Accessed: 5 May 2023).
26. Williams T. (2022). 'Top Disadvantages of Blockchain Technology', *The Knowledge Academy*, 19 December. Available at: https://www.theknowledgeacademy.com/blog/blockchain-disadvantages/ (Accessed: 3 May 2023).