e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

MOBILE TRACKING THROUGH BLOCKCHAIN APPLICATION

SM Waqas Ayub Shah[*1]

[*1]Department Of Computer Systems Engineering, University Of Engineering And Technology, Peshawar, Pakistan.

ABSTRACT

Today's technological equipment must have availability, confidentiality, and integrity. We anticipate that mobile devices, including smartphones and tablets, will support numerous security levels. Mobile devices should be safeguarded against all of the risks that they face. This publication's goal is to assist the government or organization in safeguarding mobile device ownership. This publication does not cover laptops or PCs, nor does it cover mobile devices with little processing power. In addition to explaining the security risks associated with using mobile devices, this book offers suggestions for choosing, deploying, and utilizing decentralized technology (Blockchain) and offers advice on how to keep smartphones safe throughout their life cycles. This paper will also outline the differences between Hyperledger Fabric and Ethereum as well as the benefits of Hyperledger Fabric. Additionally, we offer a novel user-centered data sharing solution that uses a decentralized, permissioned blockchain to improve identity management through the membership service supported by the blockchain and safeguard smartphone ownership and privacy through a channel formation scheme.

Keywords: Integrity, Security, Blockchain.

I. INTRODUCTION

There seem to be more and more applications for blockchain technology being discovered every day. Massive information, computer-based intelligence, systems administration, IoTs, budgetary establishment, and many other endeavors are finding that either the blockchain will advance them to the next level or it will ultimately become their biggest risk.

In late November 2008, a thesis on a digital currency system that was sent to a US mailing list of cryptographers with the help of some and a competition for PC developers under the pseudonym Satoshi Nakamoto is where the term "blockchain" first appeared. Starting from the beginning, the term includes a few implications: In actuality, the blockchain is a distributed duplicate database that permits proof exchanges between two components without the need for a specialized expert. In one instance, professionals and analysts use this term to identify the entire innovative environment behind the career of computerized sources among participants on a comparable system, excluding any mediators [1].

Let's examine the real example in accordance with difficulty editing to better understand Blockchain science. Because our financial systems are largely centralized, they have a center of failure. If bank regulations are not followed, transactions will no longer be possible, or all customer records will not be accessible to the individual user. Additional issues include the fact that each bank charges a portion of each transaction, which causes customers to be held up for unnecessary expenses during each transaction [2]. Another essential problem is that starting and completing a calculation requires a lot of paperwork, and financial institutions' capabilities are no longer available around-the-clock; they are typically limited to holidays. As a result, if someone is unfairly using the data over the entire bank,

In order to comprehend it, let's assume that the network is not decentralized and that there are four friends in it. One of the four tries to communicate data to another buddy. This indicates that there is only one copy of the data; if one friend sends a corrupted copy, the other friends in the network are unaware of it. However, if the network is decentralized and each user has a copy of the data, then corrupting one copy will alert all users to the corrupted data [3]. Like how blockchain technology operates, if one user transfers tainted data to another user, other users in the network alert and reject the transaction.

Security is one of the many domains that have discovered a good relationship with blockchain. We shall look into this relationship in this proposal. Before continuing, it is important to understand what blockchain and flexible proprietorship are.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

Currently used for phone calls, cell phones have evolved into essential and universally specialized devices that can also be used to access the Web, send instant messages, and record the world. Unfortunately, cell phones were not designed with security and safety in mind. They not only do a bad job of protecting your correspondence, but they also expose you to additional types of observation risks, namely area following. In addition, there is a risk that all of the information will be accessible if the phone is misplaced or stolen [4].

II. RELATED WORK

Similar to optional applications like property vaults, the concept of decentralized digital currency has been around for a while. After making money by correctly solving computational puzzles through decentralized consensus, Wei Dai's B-cash emerged in 1998 as one of the most significant affirmations. However, at the time, there was little consideration given to specifics, such as whether decentralized consistency should actually be maintained. Hal Finney's 2005 thinking about reusable proofs over work included a dictation that used concepts from b-money along with Adam Back's computationally challenging Hashcash puzzles to generate an idea because of a cryptocurrency. However, this was once again done too quickly by relying too heavily on computing, specifically a backend [5].

First, it offered a simple yet very accurate consistency mechanism that enabled nodes in the network to collectively decide on a consensus over a canonical update in imitation of the Bitcoin ledger's ruler [6]. Second, it provided a way to allow equitable participation in the songwriting process, resolving the political conundrum of determining who has the ability to influence the consensus while also preventing Sybil assaults. It accomplishes this by using a financial block in conjunction with a configuration barrier to mimic participation, such as the requirement to remain registered as having a special status with regard to a specific list. The ounce of a single node into the consensus voting process is instantly proportional following the increase in processing power [7].

This system would be easy to build if we had access to a reliable centralized service; it should basically be implemented as described, utilizing the additional robust capability of a communal server to expose the regime. In any event, Bitcoin and we are mercurial in creating a decentralized foreign currency system. Next, we combine the government's change of condition rule with a tuning provision so that, based on assurances, everyone agrees to the trades [8]. The decentralized agreement process of Bitcoin necessitates that nodes in the system continuously try to create "blocks," or programs of transactions.

Generally speaking, Ethereum can support three different kinds of apps [9]. The first category consists of financial applications, which give users more effective means of handling and making financial transactions. Lastly, there are uses that are completely unrelated to finance, such decentralized government and online voting. We will use mobile ownership tracking, which falls within the third category. Mobile devices have several issues, particularly in terms of security [10].

III. METHODOLOGY

This section will describe the research methodology used in this investigation. In addition to providing a summary with detailed reflections on the approach/method, it will cover the research design, data collection, data analysis, and presentation.

After examining several blockchain systems, we have decided to construct our blockchain application on Hyperledger Fabric. There are many benefits and drawbacks to this platform, however the following are the main justifications for choosing Hyperledger Fabric as a development platform:

- Permissioned Blockchain
- Organization Based Certificate Authority
- Organization Based Access
- Support for Channels
- Flexible Architecture
- No Transaction Fees

There are various methods for creating chaincode, and Hyperledger Fabric offers docker images for various components. Hyperledger Fabric offers support for chaincode development in NodeJS and Go. Additionally,

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

Hyperledger Fabric offers Java and NodeJS Software Development Kits (SDKs) for creating client apps. Since these were the only options available at the start of this development, we decided to employ the Go programming language for chaincode development and NodeJS SDK for user application development.

We currently have a Hyperledger Fabric blockchain network with a channel that all organizations have joined. The last thing these organizations need is a chaincode, also known as a smart contract, that they can use to conduct network transactions. In order to issue and verify IMEIs, we will be installing and instantiating chaincode. Any business can use this chaincode to issue IMEI certificates on this blockchain network. Chaincode peer are

->github.com/chaincode/smartchain/go/

This command installs the smartchain chaincode on the peer. After installing, the chaincode needs to be initialized.

peer chaincode instantiate -o orderer.example.com:7050 --tls --cafile

/opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/

ordererOrganizations/example.com/orderers/orderer.example.com/

msp/tlscacerts/tlsca.example.com-cert.pem -C docchain -n smartchain -v

1.0 -c '{"Args":[""]}' -P "AND

('ProvinceMSP.peer','DistMSP.peer','TehsilMSP.peer','VillageMSP.peer')"

We took into consideration the Hyperledger Fabric blockchain framework when designing our network's architecture.

Our network's participants are given designated roles, specifically those that are supported by Hyperledger Fabric. Every node is viewed as a certificate authority and an agency. Every branch pertaining to a province is a department inside an agency that maintains at least one comrade node. Even if it is no longer required, this is covered in order to improve the network. As previously stated, each branch is viewed as an employer in our blockchain network. A department then maintains a certificate or authority, a few orderers, and few peers. Each of these components' functions and purposes are covered in detail. Every department has imitated joining a shared channel.

Each organization has a certificate authority that provides other users or participants with countersigned certificates. This user or participant may be a department's PTA section, another intermediate certificate authority, or a province administrator. We have just taken into account the KP PTA's IMEI maintenance area, where certificates are granted for the relevant department, for network simplicity.

District Admin

District Admin uses client certificate signed by root certificate of organization with an attribute "Dist_admin=true". District admin can register tehsil on the blockchain.

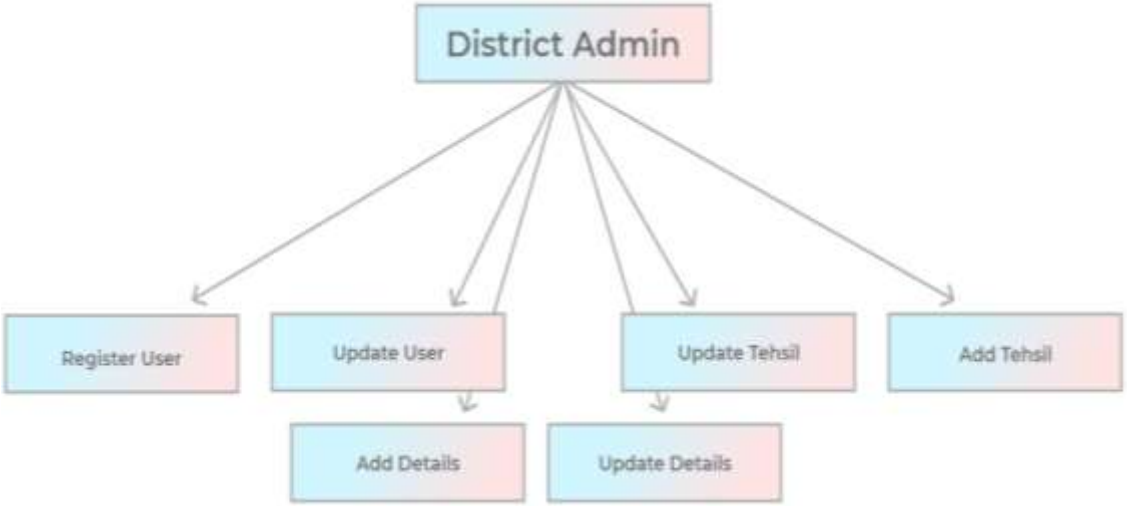

Figure 1: Flowchart for District Admin.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

Tehsil Admin

After registration of tehsil, tehsil admin can register villages, programs and specializations offered by each department. This structure is later used by village admin to issue certificate to smart phone user.

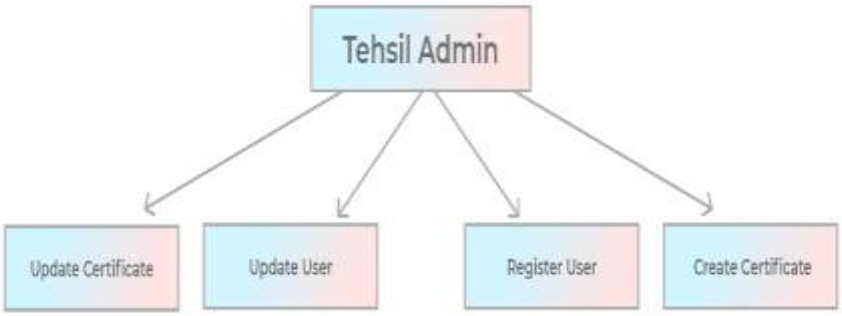

Figure 2: Flowchart for Tehsil Admin.

Village Admin

Village Admin uses a client certificate signed by root certificate of organization with two specific attributes, "village_admin=true" and "tehsil=Tehsil Name". The Tehsil attribute used in this certificate allows the admin to issue certificate for a specific user.

Figure 3: Flowchart for Village/User

IV. EFFICIENCY OF BLOCKCHAIN SYSTEM

Blockchain technology is a foundational technology that has excellent potential for use across all industries. On the one hand, the fin-tech sector uses it extensively, leading people to believe that it is only about coins and money. On the other hand, it is used in a variety of other industries, including land transfers, transportation, and mobile. Blockchain technology has the potential to completely transform payment transfer technology, and the elimination of the banking system may result in increased fund transfer efficiency.

Is it possible to envision a world where mobile transfer contracts are recorded in shared databases and integrated in digital code? Yes, we can prevent data from being erased, changed, or revised by using blockchain applications. We are able to recognize, verify, store, and

All government data is stored in a data structure in a standard database. Databases offer a flat file hierarchy system for easy information collection and storage. Relationship models, which are arranged by database management systems, allow us to look for similar data in other tables and relate it in various ways. Tables are typically used by databases to store data. An administrator is a single person who has the ability to alter, oversee, and regulate a database. A user or administrator controls the database in a typical database. This user has the ability to add, remove, edit, and modify any entry in the database.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

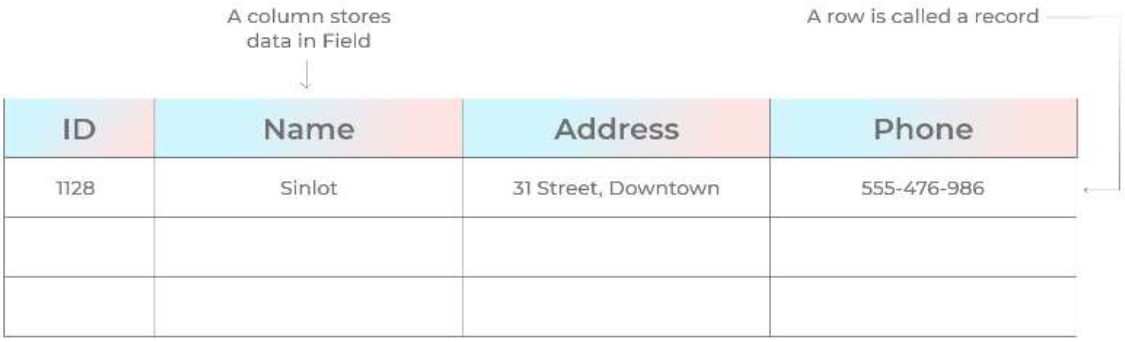

Figure 4: Table of database.

Admin assign certain role to different user that they can do certain process, so the bottom line is an admin can alter any record in database.

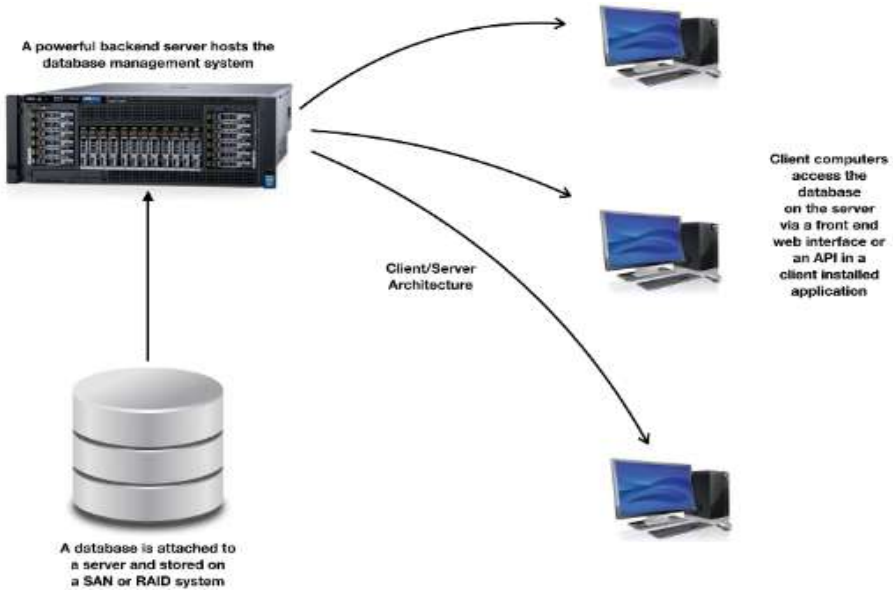

Figure 5: A Client /Server Architecture

Advantages of Database:

a) Customizability for User Friendliness

b) Stability

c) Transaction Speed and Volume

Problems with Databases

a) Single Point of Failure

b) Administrator Account

c) Security Issues

Stability is the strength of database system and enterprise networks still use it. It is more user friendly as compare to blockchain. Blockchain is normally used to establish transparency and trust.

A Database Is Ideal For:

- Data that need continuous updating, like monitoring and sensors
- Fast Online transaction processing
- Confidential information (non-transparent to the public)
- Data that does not require verification
- Standalone applications that store data
- Relational data

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

A Blockchain Is Ideal For:

- Monetary transactions
- Transfer of value
- Verification of trusted data (identity, reputation, credibility, integrity, etc.)
- Public Key Verification
- Decentralized applications (DApps)
- Voting systems

So here are the facts which I point out and it not about which system is better, but which system suits you. They both having their purpose, but in our project, we chose Blockchain because for transfer of value and verification of trust.

Our system will keep record of previous IMEI holder, there identity, time period, and price, which is a main concern of a buyer.

V. CONCLUSION

Using smartphone security as a case study, this paper introduced several Blockchain ideas. The first successful blockchain implementation is Bitcoin. Blockchain technology is now being used in several industries where trust is sought without the involvement of a centralized authority. We have created a blockchain application for verifying smartphone switches.

As an organization, each community district employs a Detach application. Considering the privileges of various governmental authorities, we allocate distinct privileges. After implementing successful chaincode in Go, we used the Hyperledger framework of the NodeJS Software Development Kit (NodeJS SDK) to create the application interface.

Compared to centralized systems, blockchain architectures are more transparent and safer. Any log-in information is saved. This makes it simple to observe someone making unauthorized changes to data and comply with audit reports. Every transaction on the blockchain is signed by the client using cryptographic certificates, so we can identify any updates to where and when.

The issue of mobile leave-out use will be successfully addressed by this approach. The process of confirming smartphone ownership will be quick, simple, safe, clear, and affordable if this approach is used.

VI. REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[2] V. Buterin et al., “Ethereum white paper, 2014,” URL https://github.com/ethereum/wiki/wiki/White-Paper, 2013.
[3] N. van Saberhagen, “Cryptonote v 2.0, 2013,” URL: https://cryptonote.org/whitepaper.pdf . White Paper. Accessed, pp. 04–13, 2018.
[4] D. Schwartz, N. Youngs, A. Britto et al., “The ripple protocol consensus algorithm,” Ripple Labs Inc White Paper, vol. 5, 2014.
[5] O. Jacobovitz, “Blockchain for identity management,” The Lynne and William Frankel Center for Computer Science Department of Computer Science. BenGurion University, Beer Sheva Google Scholar, 2016.
[6] A. Ebrahimi, “Identity management service using a blockchain providing certifying transactions between devices,” Aug. 1 2017, uS Patent 9,722,790.
[7] K. Korpela, J. Hallikas, and T. Dahlberg, “Digital supply chain transformation toward blockchain integration,” in proceedings of the 50th Hawaii international conference on system sciences, 2017.
[8] S. Shang, N. Memon, and X. Kong, “Detecting documents forged by printing and copying,” EURASIP Journal on Advances in Signal Processing, vol. 2014, no. 1, p. 140, 2014
[9] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Surveys Tutorials, vol. 18.
[10] NRI, “Survey on blockchain technologies and related services,” Tech. Rep., 2015.
URL: http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf.