Blockchain Based Secure Communication Application Proposal: Cryptouch

Recep Ahmet Sarıtekin[1], Eren Karabacak[1], Zübeyir Durğay[1], Enis Karaarslan[1]
Department of Computer Engineering, Mugla Sitki Kocman University
Mugla, Turkey

***Abstract*— The convergence which brought with the globalizing world, highly affects the network and the communication sectors. Mostly closed source and centralized systems are used for network and communication. This contradicts with the information security principles and privacy. These centralized systems can not fully meet the concept of transparent, reliable, fast and uninterrupted communication. Distributed, decentralized and also transparent communication is possible with the blockchain technology. In this study, a communication application which is based on blockchain technology is proposed. InterPlanetary File System (IPFS) is preferred to overcome the limits of the blockchain. A prototype implementation called Cryptouch is proposed. Application features and potential benefits are discussed.**

***Index Terms*— Blockchain, Decentralized Systems, Information Security, Cyber Security, IPFS**

I. INTRODUCTION

Communication is an inevitable and important dimension of the human life. The evolution of the communication from the past to today, has reached a global area through the digitalization. The data that give name to the our era, gave the opportunity to collect large data in the communication sector; making this the center of attention by the central systems like states and firms that manage the sector. This global power is monopolized by centralized systems with closed (proprietary) software. Non-transparent, centralized applications are inadequate as we are in an era that the personal and organizational information security is important. Controlled and centralized systems do not satisfy the flexibility for the user. The centralized platforms also do have a single point of failure. Decentralized and transparent platforms must be developed as a solution. Blockchain technology is a candidate for that.

The blockchain technology empowers users to control their own digital identity, share and communicate with trust. Communication applications which are based on blockchain technology; use asymmetric ciphers and consensus-based algorithms and using P2P network structure. These applications can solve the needs of the user. In this study, an application called Cryptouch is proposed which is a blockchain based communication application; the working principles and the potential benefits are discussed in detail.

In the next section, fundamentals of blockchain and the IPFS will be given. In the third section, model and the prototype of the blockchain based communication application Cryptouch is presented. In the fourth chapter, the result and likely future work will be mentioned.

978-1-5386-3449-3/18/$31.00

II. FUNDAMENTALS

A. Blockchain System

Blockchain technology keeps a continuous, fixed record list, called blocks, that are linked and secured using cryptographic functions. Each block usually contains transaction data, timestamp and hash which is a pointer to the previous block. It is an open and distributed ledger that can record transactions between two parties effectively, verifiably and permanently[1].

The system is durable against tampering by design. Blockchain is managed by a peer-to-peer network that is collectively linked to a protocol to verify new blocks. Any recorded block data can not be changed without changing all the subsequent blocks. This process is managed by the consensus protocols and requires that the majority of the network communicate and agree on a joint decision[1].

The blockchain was developed as a solution to the Byzantine generals problem[2]. It is secure by design and is an example of a transparent and fast distributed computing system. There is a potential for using it in identity management, transaction records, documentation of resources, food traceability, voting systems and similar record management activities[3]. Blockchain systems are widely used for the cryptocurrency today. The identity verification (authentication) is mostly done by asymmetric cryptology[4]. The public wallet address is the public key and the private key is formed by implementing cryptographic functions. These keys are used for the key distribution of the session key which will be used to encrypt the communication (confidentiality) and signing the transactions (integrity and authenticity)[5].

Blockchain technology is not feasible for all problems. It is appropriate to use this technology for a solution in environments where it is necessary to provide trust between multiple parties and share data[6].

B. IPFS (InterPlanetary File System)

IPFS[7] is an hypermedia distribution protocol created to make the web faster, safer, and more open. It is designed to provide a decentralized alternative to the current HTTP protocol that is censorship resistant and much more efficient.

IPFS is a peer-to-peer distributed file system that aims to connect all computing devices with the same file system.

IPFS can be seen as a BitTorrent[8] community that exchanges objects in a Git repository. There is no mutual trust between nodes as it is in BitTorrent. IPFS provides a block storage model with content-rich bridges that contain highly efficient content.

IPFS utilizes the blockchain protocols and the network infrastructure that Bitcoin uses to store immutable data in these blocks, remove duplicated files from the network, search for files on the network and obtain address information. IPFS benefits can be summarized as[9-10]:

- Availability: No single point of failure
- Reliability: Trusting the content without trusting the peers that served it[11]
- Bandwith optimization
- Security: Content-addressing and content-signing prevents the DDoS attacks that HTTP is exposed to.

III. RELATED WORKS

Blockchain technology started to be used before enough academic studies show the way for better solutions and standardization. The development has been conducted mostly out of the academia.

Communication applications that aim to satisfy the data security concern are started to be developed. These applications are using asymmetric ciphers, consensus algorithms and blockchain technology. Decentralized messaging nodes use P2P network for connection. There are applications like filecoin (https://filecoin.io), uport (https://www.uport.me), ujomusic (https://ujomusic.com) which use IPFS and blockchain, but they are not used for communication.

In the "E-chat" (https://echat.io) application; IPFS, P2P and blockchain technologies are used together. When one user sends a message to another; if connection to P2P network and instant access is not needed at that moment, all information is intended to be stored in the IPFS based decentralized storage network. In order to send this data on the Blockchain system, it stores the URL of the data (e-chat message or file) directly in IPFS.

"CrypViser" (https://ico.crypviser.net), is another application which has automated end-to-end encryption models and authentication algorithm that provides decentralized distribution of public keys over the blockchain. Crypviser can prevent any kind of manipulation, interceptions and "man-in-the middle" (MITM) attacks on all communication levels by providing encryptions key identification.

In order to increase communication safety, there are also some academic studies. In a recent study [12], multi-link concurrent communication model based on trust degree and novel integrated factor communication tree (IFT) algorithm are proposed to improve reliability. It is shown that, a routing scheme based on the IFT algorithm for the communication of the blockchain can increase communication efficiency by ensuring the reliability.

Even E-chat and CrypViser seem to be communication applications, it seems that sending crypto coins is the main purpose. To our knowledge, an academic study about this topic and an open source communication application which uses IPFS for a blockchain system was not proposed or implemented before. Cryptouch will aim enterprise solutions.

IV. CRYPTOUCH SYSTEM AND GUI DESIGN

Cryptouch is designed as a communication application that uses a distributed system model that uses both blockchain and IPFS technologies. It is designed to meet corporate, social and personal communication needs. It is envisaged to use a private and allowed blockchain system. The main aims are such as:

- Providing an intermediary, distributed, open source, secure, transparent and uninterrupted communication to its users with its free software philosophy.
- Accomplishing a user-to-user messaging, file transfer, video meeting and announcement system without a mediation by using a new technology such as IPFS.
- Providing a continuous, redundant and secure communication environment in the network where the application is used.

The model of the proposed system is shown in Figure 1. The application is designed to work only between the users of the same network. Private networks are preferred as an enterprise solution. Message creation and transfer/reception are created using a decentralized private backbone. The private network will be preferred by the corporations as E2E network security processes will be easily applied.

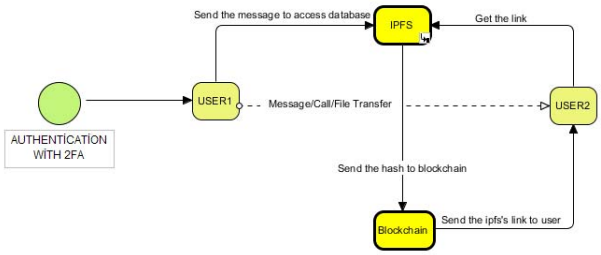

Fig. 1. Proposed System Model

The functionality can be summarized as the following steps shown in Figure1:

1) First, the user logs in to their account via mobile or web app
2) The following can be started with the normal messaging feature in the application:
   - Video-to-speech meetings by IPFS
   - User-specific, private and encrypted speech
3) The data load that can occur in the blockchain is reduced, and direct uninterrupted communication is ensured with IPFS.

A. Why IPFS with Blockchain ?

IPFS with blockchain is preferred. Blockchain technology is not fit to store large amounts of data. IPFS is selected to overcome this and the system will be designed to be used as a publicly accessible database. On the ipfs each file submitted

to the network is given a unique cryptographic hash that allows the IPFS network to automatically delete duplicates and track version history for every file. Historic versioning prevents information from being easily erased. Since the files are provided by distributed nodes, download speeds are higher.These characteristics make the IPFS a perfect place to store data, which can be referenced and time stamped with blockchain technology.

B. GUI Design

The user interfaces are given in Fig 2.

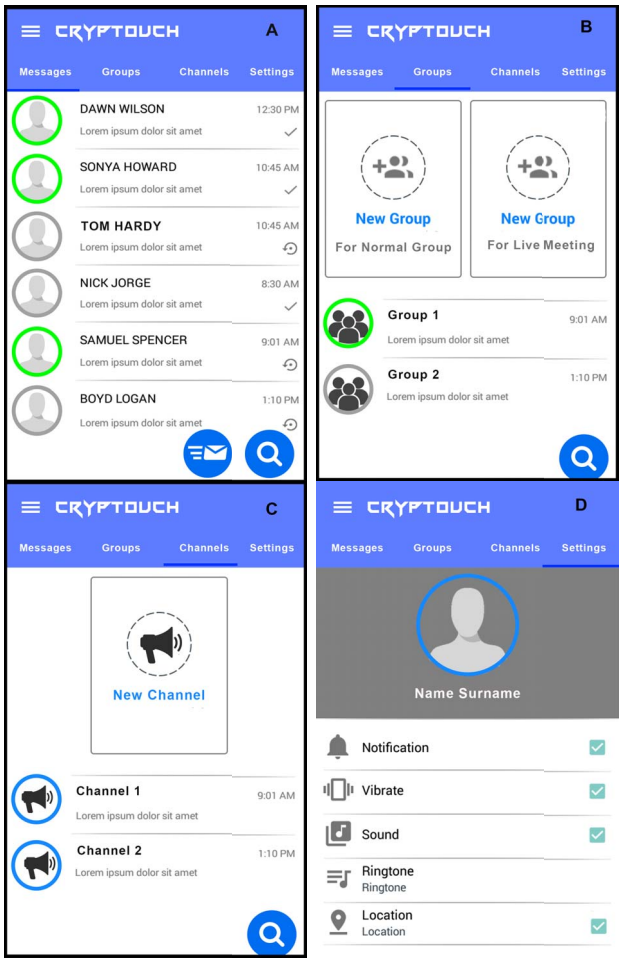

Fig. 2. Figure2(a)(b)(c)(d). Sample User Screens

The screens can be described as follows:

- Main Screen: This is the main screen when the users open the application. Users can see private messages, groups, channel history and settings. They can create the new private messages and make a text search on the application. It is shown in Fig 2.a.
- Chat Lists: Users can reach and read their private messages, history and the user's status. They can also see the message status as forwarded or read. It is shown in Fig 2.a.
- Group Screen: Users can create a new group with each other for chat or live meeting. The group can also be created to be valid only for that call. The users will be able to see their call histories.It is shown in Fig 2.b.
- Channel Screen: Users can create new channels and see the history of the subscribed channels. They can broadcast the messages to the subscriber.It is shown in Fig 2.d.
- Setting Screen: Users can edit username, change notifications settings and location settings.

C. Development Process of the Application

Today, there are many platforms to develop blockchain technology. It is planned to use Hyperledger Fabric from the Linux Foundation, which is both fast and mature, as well as a lot of programming language and company support. It adds flexibility to the application development phase with its module insertion and extraction features.

The use of Meteor as a back-end is being tested. Even development process has some difficulties, it is possible to develop both mobile and web applications for the written code at the same time. This will help to save time and workforce. The application is initially planned to be published as an application in free software operating systems, also web application and mobile application (Android / IOS).

D. Application Features

Institutions and organizations can openly and privately set up communication applications within their needs.Here are some things that can be done in practice:

- Private Message: Private messaging between employees of the organization
- File Sharing: File sharing among company members
- Channel System: Departments and workgroups can communicate with their employees by opening special communication channels
- Announcement System: Publish announcements of company or workgroup managers
- Records Management: Blockchain can make the registration of company data more convenient and stable. This technology ensures the personal privacy and privacy of private data.

V. Discussion

The proposed application Cryptouch is compared with similar applications in Figure 3. Cryptouch will also have the enterprise solution capability.

KEY FEATURES	Glide	Skype Qik	Snapchat	WhatsApp	LINE	WeChat	CRYPTOUCH
Video Messaging	Yes	Yes	Yes	Yes	No	Yes	Yes
Length of Video Message	300 seconds	42 seconds	10 seconds	90 seconds	N/A	45 seconds	N/A
Text Messaging	Yes	No	Yes	Yes	Yes	Yes	Yes
Video Calling	No	No	Yes	Yes	Yes	Yes	Yes
Streaming vs. Download?	Streaming	Download	Download	Download	Download	Download	IPFS
Where Are Your Videos Stored?	Cloud	Device Cache	Device Cache	Device Cache	Device Cache	Device Cache	IPFS
Group Messaging	Yes (<50)	Yes	Yes	Yes (<50)	Yes	Yes	Yes
Share Videos to Social Networks	Yes	No	Yes	No	No	No	No

Fig. 3. Comparison of Cryptouch with similar products

Potential benefits of the implementation can be given as:

- Increased Trust: The immutable ledger and the mining (data verifying with multiple nodes) process increases

the trust. Reliability: As the data is stored in multiple locations, consensus protocols will only allow information to be changed when all parties agree on it. The confidence of the information in the system is thus ensured.

- Auditability: The system will have multiple ledgers that can be accessed to track the transaction history and ensure consistency. Security: Abusing data encryption is more difficult because it is stored in a distributed database. It is unlikely to seize or misuse all of them. We'd also like to note that the security of the blockchain model should be studied in detail.
- Confidentiality/Privacy: The user can be anonymous using his/her encryption keys or prevent other people from viewing his/her private information
- Increased flexibility against Spam and DDOS attacks: The cost of cyber security measures can be reduced by the high level of durability and security provided by the blockchain system.
- Availability and speed: Information is stored in a number of places which facilitate access and increase the access speed. Anyone on the network will be able to access this information.
- Transparency: The users will have accessibility to the ledgers. Users can see all operations and each node has an overview of the operations.
- Avoiding fraud and manipulation: Hacking activities or unauthorized changes are difficult to do without noticing in this system. Information is difficult to manipulate because it is stored in multiple, decentralized ledgers.
- Reduction of costs: The costs to perform and verify an operation will probably be reduced as there is no need for centralization in the blockchain.

VI. CONCLUSION

Cryptouch, a communication application based on blockchain technology is modeled and a prototype is being developed. InterPlanetary File System(IPFS) is used to overcome the data storage limits of the blockchain. IPFS based tests have been made.

This application can be used to ensure the availability, confidentiality and privacy of the private data that is shared between the users of an organization. Details of the application is made available at our web site (http://cryptouch.io).

Future work will include enabling all the functions mentioned in the paper and enrichment of the application. Enterprise solutions which allow E2E communication is planned to be developed. We believe this study can lead to more sophisticated products.

ACKNOWLEDGMENT

This study is carried out by the Muğla Sıtkı Koçman University Blockchain Research Group (MSKU Blockchain Research Group) (MSKU BcRG).

REFERENCES

[1] Benet, J., "IPFS - Content Addressed, Versioned, P2P File System", arXiv:1407.3561, 2014
[2] Karaarslan E., Akbaş, M.F., "Blockchain Based Cyber Security Systems" (Turkish), UBGMD Journal, Cilt 3, Sayı 2, Pages 16 - 21, DOI: 10.18640/ubgmd.373297,
[3] Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." International Workshop on Open Problems in Network Security. Springer, Cham, 2015.
[4] Durğay Z., Karaarslan E., "Usage of Blockchain Technology in the E-Government Applications: Preliminary Study" (Turkish), Akademik Bilişim 2018, 2018
[5] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". 2008., https://bitcoin.org/bitcoin.pdf
[6] Ghassan Karame. 2016. On the Security and Scalability of Bitcoin's Blockchain. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). ACM, New York, NY, USA, 1861-1862. DOI: https://doi.org/10.1145/2976749.2976756
[7] Karl Wüst and Arthur Gervais, "Do you need a Blockchain?", IACR Cryptology ePrint Archive 2017 (2017): 375. [Online]. Available:https://eprint.iacr.org/2017/375
[8] Benet, J., "IPFS - Content Addressed, Versioned, P2P File System", arXiv:1407.3561, 2014
[9] Bernaille, Laurent, and Renata Teixeira. "Early recognition of encrypted applications." International Conference on Passive and Active Network Measurement. Springer, Berlin, Heidelberg, 2007.
[10] "IPFS is starting to replace HTTP!"(Turkish), Chip Online, Available: www.chip.com.tr/haber/ipfs-httpnin-yerine-gecmeye-hazirlaniyor.html, 2016
[11] "IPFS Protocol Selects Ethereum Over Bitcoin, Prefers Ethereum Dev Community". Cointelegraph.com. Retrieved 25 October 2017, Available: cointelegraph.com/news/ipfs-protocol-selects-ethereum-over-bitcoin-prefers-ethereum-dev-community
[12] Juan Benet, "IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3)", IPFS Whitepaper, 2014
[13] J Li, G Liang, T Liu, "A Novel Multi-link Integrated Factor Algorithm Considering Node Trust Degree for Blockchain-based Communication", KSII Transactions on Internet and Information Systems, 2017