МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

ІНСТИТУТ КОМП'ЮТЕРНИХ СИСТЕМ

МАТЕРІАЛИ ДЕВ'ЯТОЇ МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ СТУДЕНТІВ ТА МОЛОДИХ ВЧЕНИХ

присвячена 55-річчю
ІНСТИТУТУ КОМП'ЮТЕРНИХ СИСТЕМ

" Сучасні інформаційні технології 2019 "

" Modern Information Technology 2019 "

23-24 травня

Одеса
«Екологія»
2019

УДК 004.42

BLOCKCHAIN BASED MESSENGER FOR PROVIDING A SECURE PEER TO PEER COMMUNICATION FACILITIES

Kilichenko Hlib, Komleva Nataliia
Ph.D., Assoc.Prof. of System Software Department Komleva N.
Odessa National Polytechnic University, Ukraine

ABSTRACT. This work is concerned with evaluating the applicability of blockchain technology for achieving secure private communication between peers. Standard client-server architecture proved to be efficient for that purpose, yet a central point of control undermines the privacy of the parties involved. Therefore, it is necessary to explore ways of tackling this problem in a distributed system.

Introduction. Distributed systems underwent a massive change in the past decade. Not in the least because of the rise of Blockchain technology which expanded the ways in which network nodes could interact and reach consensus. Therefore, to address the issue of communication between nodes it would be useful to understand the possibilities and limitations of blockchain technology [1].

Objectives. The main point of this work is to assess possible means of building robust and secure distributed communication systems without intermediate parties controlling the information flow and also suggest technologies capable of simplifying the development of such systems.

Main part of the work. There are two general software architectures for organizing data exchange over the standard network stack: centralized and decentralized. Former is today's de facto approach for solving most business tasks: they are straightforward, modifiable and highly efficient. Yet central unit of control is not faultless and inclined to corruption due to a human factor. With the rising concern for data privacy also grown an interest in decentralized data exchange. The core problem of this approach is reaching a distributed consensus on the state of the system. Blockchain is the implementation of the distributed ledger technology which stores data in a chain of cryptographically linked blocks and reaches consensus through incentivising nodes of the network to follow its protocol.

In general case of popular messaging apps like Telegram, WhatsApp, Viber or Facebook Messenger, full privacy could not be guaranteed with chats providing the cloud-based backup of the messaging history. But with End-to-end encryption (E2EE) things are more complicated and depend on whether the code base is open and actually secure and also on the key exchange protocol used. In the case of Telegram, Diffie–Hellman key exchange procedure is used, making it a highly secure communication channel. The problem is that it could not be backed up and restored on any other device. And that what we will try to find out. The core attribute of the blockchain technology relevant to building a decentralized communication system is the ability for nodes to share a state without having to rely on a central authority. The first and most famous application of blockchain technology today is Bitcoin, a decentralized cryptocurrency.

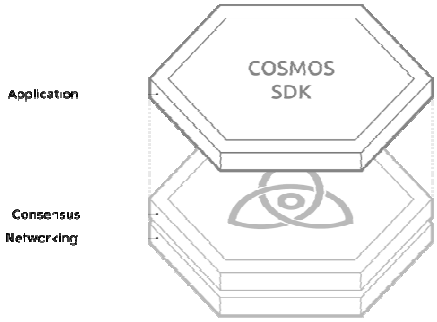
The first feature, shared by the third generation of blockchains is a reliance on a new consensus mechanism called Proof-of-Stake (PoS). In PoS-based cryptocurrencies the creator of the next block is chosen via various combinations of random selection and wealth or age of the node. That allows to concentrate computing power on validation of actual transactions and therefore to achieve higher scalability reaching thousands of transactions per second. Another feature common for the third generation of blockchains is the ability to process cross-chain transactions by creating protocols for cross-chain interactions, such as IBC.

In this way, it could be said that communications system could be built upon a blockchain satisfying third generation requirements. Storing any data inside transactions is very costly - information is replicated across all the full nodes of the network. One way to use blockchain architecture for p2p communication while not storing data in transactions is to use a distributed system for storing and accessing files, such as IPFS. IPFS file sharing is similar to the one in torrent systems. It allows to get a hash of any file and address this file inside the system by that hash. This hash could

be stored in blockchain transactions significantly reducing the amount of information stored on blockchain. IPFS could also be used for maintaining a distributed hash table for peer look up.

Building a third generation blockchain from scratch is time intensive. Blockchain architecture could be split into three main layers (pic. 1) where networking layer and consensus layer could be isolated by a third party solution so that development could be centered to the dApp itself. Stack that is suggested for that purpose consists of Tendermint ecosystem and Cosmos SDK [2, 3].

Tendermint consists of two chief technical components: a blockchain consensus engine and a generic application interface. The consensus engine, called Tendermint Core, ensures that the same transactions are recorded on every machine in the same order. The application interface, called the Application BlockChain Interface (ABCI), enables the transactions to be processed in any programming language. And the Cosmos SDK is a generalized framework that simplifies the process of building secure blockchain applications on top of Tendermint Core.



Pic. 1 – Layers of blockchain architecture

Conclusions. A secure p2p communication could be achieved using a blockchain system satisfying third generation requirements and a distributed file sharing system, such as IPFS. On its basis distributed hash table of peers could be built and maintained to allow peers to discover each other. Data storage could be handled though the IPFS protocol. Questions of cost efficiency and scalability remain open, but such a system build upon open-source technologies could provide a high level of data privacy as long as the underlying cryptography is robust.

REFERENCES

1. Blockchain Architecture [Online]. Available: https://www.pluralsight.com/guides/blockchain-architecture.[Accessed: 29-April-2019].

2. Tendermint Documentation [Online]. Available: https://www.tendermint.com/.[Accessed: 29-April-2019].

3. Build your custom blockchain app today [Online]. Available: https://cosmos.network/sdk/.[Accessed: 29-April-2019].