УДК 004.75

Alexander Ivanov, Yevhenii Babichenko, Hlib Kanunnikov,
Paul Karpus, Leonid Foiu-Khatskevych, Roman Kravchenko,
Kyrylo Gorokhovskyi, Ievhen Nevmerzhitskyi

TECHNICAL COMPARISON ASPECTS OF LEADING BLOCKCHAIN-BASED PLATFORMS ON KEY CHARACTERISTICS

Blockchain as a technology is rapidly developing, finding more and more new entry points into everyday life. This is one of the elements of the technical Revolution 4.0, and it is used in the field of supply, maintenance of various types of registers, access to software products, combating DDOS attacks, distributed storage, fundraising for projects, IoT, etc.

Nowadays, there are many blockchain-platforms in the world. They have one technological root but different applications. There are many prerequisites to the fact that in the future the number of new decentralized applications will increase. Therefore, it is important to develop a methodology for determining the optimal blockchain-based platform to solve a specific problem. As an example, consider the world-famous platforms Ethereum, Nem, and Stellar. Each of them allows to develop decentralized applications, issue tokens, and execute transactions. At the same time, the key features of these blockchain-based platforms are not similar to one another. These very features will be considered in the article.

Purpose. *Identify the key parameters that characterize the blockchain-based platforms. This will provide an opportunity to present a complex blockchain technology in the form of a simple and understandable architecture. Based on these parameters and using the expertise of the article's authors, we will be able to develop a methodology to be used to solve the problems of choosing the optimal blockchain-based platform for solving the problem of developing smart contracts and issuing tokens.*

Methods. *Analysis of the complexity of using blockchain-based platforms. Implementation of token issuance, use of test and public networks, execution of transactions, analysis of the development team and the community, analysis of the user interface and the developer interface.*

Discussion. *By developing a platform comparison methodology to determine optimal characteristics, we can take the development process to a new level. This will allow to quickly and effectively solve the tasks.*

Results. *Creation of a methodology for comparison blockchain-based platforms.*

Keywords: blockchain, token, consensus, smart contract, crypto currency, decentralized applications, blockchain-based platform.

Introduction

The emergence of Distributed ledger technology (DLT), which also includes Blockchain technology and smart contracts, is a natural evolutionary stage in the development of digital technologies.

An important feature of these technologies is the possibility of creating a new type of assets: crypto-tokens (crypto-currency). At its core, crypto-token is a programmable asset, that is, an asset whose behavior can be established at the program level.

Appearance of this kind of assets has opened the possibility of creating new models of economic relations between participants in various economic and social systems and provided a number of unique properties of these systems that were tokenized on the basis of distributed ledger technology:

- Blockchain provides an opportunity for guaranteed personalization (identification) of assets and business processes provided by these assets;
- Protocols, built on the Blockchain technology to implement the transfer of values, ensure a reduction in transaction costs due to the absence of the third-party guarantor and a reduction in the number of interim operations; in this case, the cryptographic algorithm of consensus performs the role of guarantor;
- Crypto-tokens and smart-contracts provide an opportunity for instant, transparent monetization of value streams;
- Smart contracts are a mechanism that provides the participants' confidence, backed up by economic incentive mechanisms that implement Nash equilibrium.

This study focuses on the review and comparative analysis of Blockchain-based platforms that provide tools for tokenization of business processes and monetization of value streams.

In order to compare the Blockchain platforms we need to clearly define the following questions:

- what tasks are to be solved with the use of these platforms;
- do we need additional resources for our product or service launching, support, and development, or do we have our own sufficient funds;
- in case of ICO crowdfunding, are we going to use our tokens as permanent cryptocurrency reflecting our real assets or do we need them for one time finding our business;
- who are our customers and participants to use our service and products with the use of blockchain platform;
- what kind of transactions do we have;
- in which aspects do we want to achieve 100 % confidence of our potential customers and participants using distributed ledger for transactions;
- do we want to expand our business worldwide, or are we focusing on the local level?

As soon as we know our products in an excellent way, it will not be difficult to answer the questions mentioned above, knowing about blockchain technology only one indisputable thing: it is the way of making transactions and recording information which cannot be faked without destroying all the system.

Using the platform comparison methodology below, we will be able to conclude which platform out of the investigated will be better. Similarly, any industry or business will be able to analyze different platforms that are more suitable for individual use.

1. Ethereum

Ethereum is the first platform to implement the virtual machine for processing smart-contracts on blockchain (Ethereum Virtual Machine – EVM). Ethereum has become the standard in the world of smart-contracts, and EVM is the leading industrial standard for smart-contracts implemented on many different platforms [14].

1.1. Tokens and standards

The basic and most popular standard for issuing tokens on Ethereum is ERC20. Basically, this is a specification of a smart-contract interface which includes functions for checking balances, transferring tokens, and allowing to do pull transaction with the help of *transferFrom* function. It is worth noting that the standard contains only general descriptions of what each function should to do, and implementation can vary in a wide range [5].

A widely discussed issue with this standard is that in Ethereum there is basically no difference between addresses of users and smart-contracts. This leads to a situation when a user can send tokens to some address by mistake, and if this address was in use by a smart-contract, tokens cannot be withdrawn from this smart-contract if it does not have this functionality implemented.

Another issue is that ERC20 standard does not provide:

1) a possibility for a smart-contract to be triggered by a token transfer to its address while pure ETH transfers do so (this is called "fallback function");

2) a possibility to attach any data to a transaction.

To address these issues, several new standards were developed:

1) ERC223. This standard extends ERC20 and allows to handle transactions to smart-contracts by using *tokenFallback* function. This function should be called every time the transaction is sent to a smart-contract. If a smart-contract does not provide this function, the transaction will fail. Also, this standard provides a possibility to attach messages to transactions.

2) ERC777 provides nearly the same functionality but with major changes to the interfaces making it incompatible with ERC20 standard.

But currently the majority of wallets do not have support for the full functionality of the new standards [9].

1.2. Consensus

Currently Ethereum uses Proof-of-Work based on Ethash algorithm which aims to work against ASIC miners (Bitmain announced ASICs for this algorithm). The major problems with this algorithm are as follow:

1) This protocol is relying on high amounts of computations, which leads to higher energy consumption.

2) The throughput of the entire system is limited by the time needed to perform computations against a block. Currently an effective throughput is about 30 TPS, and blocks are issued every 14–15 seconds, but in fact the block is built much faster and, according to Ethereum developers, the effective throughput can be up to 875 TPS [4].

These issues will be solved by migrating to Proof-of-Stake algorithms, which is planned during 2018.

1.3. Decentralized applications (DApps)

The basic goal of Ethereum is to be an open platform for creating decentralized applications. The benefits of using DApps are immutability of state (no one can modify the state as it is persisted on the blockchain) and fault tolerance (as there is no single application server that will fail).

Other application parts (front-end and back-end, for instance) can interact with Ethereum via JSON RPC API. The most popular way of interaction is by using Web3.js library built on top of this API [2].

With this API, users can read data stored on the blockchain and submit transactions. In Ethereum, a transaction is any action that involves changes in on-chain state. This includes ETH transfers, calls to smart-contracts, and so on.

When submitting a transaction, a user should pay fees. Fees are calculated in gas – a special unit which defines the basic price of transaction, prices for every operation in EVM, and the price for storing additional data within the transaction body. The price of gas (in ETH) is not fixed and can vary over time.

1.4. Our contributions

Our team (482.solutions) contributed to Ethereum by reporting some minor bugs. One of the examples is go-ethereum/#14359 [3] issue. The issue itself was caused by the lack of testing. When one specifies a large value of network ID (used to distinguish different networks one from another), it may have got cut down to 16 or 32 bits causing errors in communication. Such problems are usually caused by a lack of static checks. Also, tests involving networkId were using only values from 0 to 3, so they could not have covered all corner cases.

2. NEM

New Economy Movement, or **NEM,** is a corporate-level solution for managing the blockchain-based economy system.

The NEM blockchain platform is built out of a network of nodes, all running NEM’s core node server software. In summary, these nodes provide a powerful, easy-to-use, stable, and secure platform where Smart Assets transactions are conducted, searched, and immutably logged to the blockchain ledger.

Each NEM node works with other nodes to build the **peer-to-peer blockchain network**. In sum, this network creates and supports the blockchain itself. The NEM node software verifies transactions, maintains a database, synchronizes with other nodes, and maintains stability and trustworthiness to create a network that is fast, secure, and scalable.

2.1. Tokens and standards

2.1.1. Assets

The base cryptocurrency of the public blockchain NEM is called XEM. A total of 8,999,999,999 XEMs were issued initially, and no additional issuing is envisaged in the future. The capacity of XEM is 6 digits after the decimal point. In the NEM Blockchain, the token is called a Mosaic [11].

To create Mosaic, one needs to create a namespace. In this Namespace, the owner can create any number of mosaics with unique names.

A Namespace can have up to 3 levels: one top-level namespace (required) and up to two sub-namespaces. The length of a namespace is limited to 16 bytes, or in other words, 16 single-byte alphanumeric characters. The length of the sub-namespace is limited to 64 bytes. The name of the mosaic is limited to 32 bytes. The validity of the root names of Namespace is limited to a year (365 * 1440 blocks). At the end of the term, one needs to pay in order to extend the validity period of the Namespace [13].

2.1.2. Consensus algorithm for Blockchain (PoI)

NEM’s consensus is built on a unique Proof of Importance algorithm, using a technique similar to Google’s PageRank to prevent a variety of attacks on the trustworthiness of blockchain transactions. It serves the same purpose as typical Proof of Work (PoW) mechanisms used by Bitcoin and others, but it is much more scalable and energy efficient. This allows nodes to run on almost any hardware while still providing an absolutely secure network that can scale without limit [12].

To confirm new blocks and to receive awards, NEM uses harvesting “competition” using PoI.

The right to harvest is possible if the following requirements are met:

- the number of crypto-tokens on the account;
- transactions activity by account;
- the time when account was online.

Delegated Harvesting means obtaining XEM [1] for participation in the formation of blocks. For this, the following is necessary:

- in order to run the basic NODE one needs a balance of 10.000 XEMs;

[1] XEM is the native currency of the NEM public blockchain. It is used to pay for transactions on this public blockchain in order to incentivize its network of public nodes that process and record transactions for businesses and users there.

● in order to run the SuperNODE, one needs a balance of 3,000,000 XEMs (SuperNODE can take part in voting and in the development of NEM Blockchain).

A NEM's block time is 1 minute; the limit of the number of transactions in the block, to date, is 120, which corresponds to a transaction flow of up to 2 transactions per second (tps) [10].

2.1.3. Checking the Integrity of Nodes (Eigentrust++)

Algorithm Eigentrust++ in conjunction with the POI algorithm ensures stable operation of the network and protects it from malicious Nodes. Nodes that are not trusted are rejected and ignored.

2.1.4. Web architecture

The NEM architecture is made as a web server application environment (web server & application server). The NEM API interface corresponds to the industry practice: JSON RESTful API.

Each node is a server that accounts can use for harvesting. Thus, each node includes a web server, a database, and the main application that provides the work of the NEM Blockchain technology.

3. Stellar

Stellar was founded in 2014 and operated by non-for-profit Stellar Development Foundation. The platform was designed by well-known blockchain experts Jed McCaleb and Joyce Kim for microfinance multi-currency transactions across borders. Coin XLM with total circulation 100 billion coins with 1 % yearly inflation is in TOP-10 of the world cryptocurrencies by market capitalization. Transaction fee is 100 stroops (0.00001 XLM) always deducted from the source account. To send a transaction to a new asset there is a need to establish a trustline, which means one trusts to the asset issuer; transaction fee for setting up the trustline is also 100 stroops.

Stellar Consensus Protocol consists of two sub-protocols: a nomination protocol and a ballot protocol. The nomination protocol produces candidate values for a slot. If run long enough, it eventually produces the same set of candidate values at every intact node, which means nodes can combine the candidate values in a deterministic way to produce a single composite value for the slot. There are two huge caveats, however. First, nodes have no way of knowing when the nomination protocol has reached the point of convergence. Second, even after convergence, ill-behaved nodes may be able to reset the nomination process a finite number of times. When nodes guess that the nomination protocol has converged, they execute the ballot protocol, which employs federated voting to commit and abort ballots associated with composite values. When intact nodes agree to commit a ballot, the value associated with the ballot will be externalized for the slot in question. When they agree to abort a ballot, the ballot's value becomes irrelevant. If a ballot gets stuck in a state where one or more intact nodes cannot commit or abort it, then nodes try again with a higher ballot; they associate the new ballot with the same value as the stuck one in case any node believes the stuck ballot was committed. Intuitively, safety results from ensuring that all stuck and committed ballots are associated with the same value. Liveness follows from the fact that a stuck ballot can be neutralized by moving to a higher ballot [7].

Stellar has a well developed guide [15] and SDK's [16] for Software Developers, including REST API, Java, JavaScript, Go, C#, Python, and Ruby. Two developer communities https://stellarcommunity.org and https://galactictalk.org/ provide comprehensive support for newbies.

Stellar has its own wallet called lightweight, as well as a third parties desktop, mobile and web; however, not all of them provide comprehensive support for customers. For example, Interstellar [6] for authorization of new wallets uses charging in Bitcoin rated by exchange, so you easily appear in a situation when your Bitcoins sent for confirmation purposes are "ignored" by the Interstellar system because of Bitcoin course change in the past ten minutes while block was formed in BTC network, and now it is not a required amount to complete authorization. We recommend to verify new accounts by sending 40 XLM purchased at exchanges or other sources instead of using Bitcoin. However, third-party wallets have huge functionality and security measures which are not present in Lightweight wallet.

There are 2,380 assets created by May 2018 on Stellar platform; they could be observed using Stellar Expert https://stellar.expert/explorer/public/asset

Most known projects are as follow:

● DRA https://www.diruna.org/ – new world currency;

● MOBI https://mobius.network – Universal Proof of Stake Oracle Protocol;

● REPO https://repocoin.io – Auto repossession, locating delinquent vehicles;

● SLT https://smartlands.io/ Asset Tokenization;

● RMT http://sureremit.co/ Global non-cash remittances;

● TERN https://ternio.io – Advertising.

The Token creation process is very easy; tokens could be created by using one of the available SDK’s or manually at Stellar Laboratory [17]. In details this process is described by Jed McCaleb, the founder of Stellar, in [8]. For creation of the token on Stellar platform we need 2 wallets: an issuer and a distributor. For this article, I created one lightweight wallet (Issuer), one Interstellar wallet (Distributor), and one StellarTerm wallet for customer. For the activation of the first two wallets ~40 XLM were sent from Kuna.io cryptocurrency exchange. The result for setting trust between Issuer and Distributor, creating KMACoin token (as part of research startup at cryptocurrencies field at Faculty of Informatics NaUKMA [1]), and setting a path for it is that 2.000.000 tokens are now distributed over Stellar network. Another possible way for issuing based tokens is Stellar Tokens https://poliha.github.io/stellar-tokens/

Stellar platform also has such useful instruments as a multi signature and Compliance server, which makes setup of payment gateways and currency exchanges simple and fast. Stellar Smart Contracts, which are sequences of transactions, support a lot of constraints like multisignature, time stamps, batching (several transactions in one), limitation of time when transaction could be executed, as well as combinations with protocol events [18].

Conclusion

To date, the leader in the field of blockchain technology and related tools is still not defined. Each blockchain-based project seeks to do something better in order to become a leader in this “race” and win. Very soon, the usual Internet will look very different, and meanwhile, key points in the history of technology unfold right before our eyes.

Having worked out our own platform comparison methodology, based on the process of developing a smart contract and token issuing, we have come to the conclusion that the key indicators for comparing blockchain-based platforms can be as follow: the date of launching, Programming Language, Availability of API access, Type of Consensus, Availability of SDK, Availability of TestNet, Network bandwidth, Invoice creation, etc.

Also, it is necessary to remember and pay attention to the maturity of the blockchain-based platform, since an important indicator is the availability of assembly tools and proper, regularly updated documentation.

Table. **Key characteristics of the investigated blockchain platforms**

Comparison criteria	**Ethereum**	**NEM**	**Stellar**
Launched	2015	2015	2014
Programming Language	Solidity[2], JavaScript JSONRPC API as Web3.js library	JavaScript/Typescript, Java	JavaScript, Java, C++, C#, Python, Go, Ruby
Open source	Yes	No	Yes
Availability of API access	Yes	Yes	Yes
Consensus	POW (Proof-of-Work)	POI (Proof-of-Importance)	FBA (Federated Byzantine Agreement)
Currency name	ETH	XEM	XLM
Availability of SDK	Yes	Yes	Yes (Java, JS, Go, C#, Python)
Availability of TestNet	Yes	Yes	Yes
Multi-signature accounts	No	Yes	Yes
The minimum (optimal) transaction cost	≈ 0.00001 ETH	0.05 XEM	0.00001 XLM
The minimum transaction speed (seconds)	15	30	5
Network bandwidth (per second)	30	120 – NEM 3000 – Catapult	1000
P2p transactions	Yes	Yes	Yes
Encrypted messaging	Yes	Yes	Yes
Invoice creation	Yes	Yes	Yes
ICO support	Yes	Yes	Yes
Airdrop support	Yes	No	Yes

[2] Solidity is high-level language for implementing smart-contracts in EVM.

All of the above platforms seek to dominate the Internet in the field of decentralized solutions. New projects, coins, and solutions appear every month, and many of them have the right to be considered the best in their field. Theoretically, any of them can surpass the projects discussed above. However, world recognition will take time. We can also take a direct part in the creation of a new branch in the historical tree of technology development.

To finalize the article, we should mention one more criterion of investigated Blockchain platforms which reflects one of the most important characteristics besides the technical features; it is the current level of capitalization and the period of keeping it.

The obvious conclusion is that the level of technical formation of the crypto world is incomparably higher than the level of usage of blockchain technology, crypto-currencies, and smart contracts in the real sector of the economy. The main and the most valuable feature which blockchain technology brought us is the very new level of trust and confidence which could not be compromised. Traditional and accustomed measurements of trust in the material world are fiat money or capitalization. The more customers or investors trust to the platform, the more money invested, the higher capitalization is. The same way we are measuring cryptocurrencies and Blockchain platforms: by using fiat money as a habitual general equivalent. So, our researched platforms are designed for the very new type of assets: smart contracts which work for the real economy, in other words for goods and services supply and quality confirmation. It does not mean that Ethereum is better than Stellar because it holds steadily the second position in the capitalization for more than a year with a large margin from the other crypto-assets; or Stellar is better than NEM because its capitalization is more than two times higher. In reality, new customers use mainly the mentioned criteria for choosing the platform. However, just considerations regarding choosing the platform for smart-contracts creation is not enough for a successful project. A much more important issue is to understand what aspects of one's business one wants to make with the most possible level of trust for one's customers using smart-contracts. Then it is necessary to just use the features of a blockchain platform to achieve it.

References

1. Глибовець М. М. Методологічні аспекти розробки платформи для залучення інвестицій в освіту на базі інструменту ICO (Initial Coin Offering) технології блокчейн – стартап НаУКМА «Knowledge Measurable Assets» / М. М. Глибовець, Є. І. Невмержицький, К. С. Гороховський, Є. Й. Грабов // Наукові записки НаУКМА. – 2017. – Т. 198 : Комп’ютерні науки. – С. 47–53.
2. Ethereum Yellow Paper [Electronic resource]. – Mode of access: https://ethereum.github.io/yellowpaper/paper.pdf. – Title from the screen.
3. Github issue #14359: Geth works incorrectly with large values of networkid [Electronic resource]. – Mode of access: https://github.com/ethereum/go-ethereum/issues/14359. – Title from the screen.
4. Github issue #16218: geth node is consistently behind the mainnet [Electronic resource]. – Mode of access: https://github.com/ethereum/go-ethereum/issues/16218#issuecomment-380023338. – Title from the screen.
5. Guide to Ethereum token issuance [Electronic resource]. – Mode of access: https://www.ethereum.org/token. – Title from the screen.
6. Interstellar wallet [Electronic resource]. – Mode of access: https://interstellar.exchange/ – Title from the screen.
7. Mazieres D. The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus [Electronic resource] / D. Mazieres. – 2016. – Mode of access: https://www.stellar.org/papers/stellar-consensus-protocol.pdf. – Title from the screen.
8. Mccaleb J. Tokens on Stellar [Electronic resource] / Jed Mccaleb. – Mode of access: https://www.stellar.org/blog/tokens-on-stellar/ – Title from the screen.
9. Mulders M. A comparison between ERC20, ERC223, and ERC777 token standard [Electronic resource] / Michiel Mulders. – Mode of access: https://www.cointelligence.com/content/comparison-erc20-erc223-new-ethereum-erc777-token-standard. – Title from the screen.
10. NEM official docs: Harvesting [Electronic resource]. – Mode of access: http://docs.nem.io/en/gen-info/faq/faq-harvesting. – Title from the screen.
11. NEM official docs: Namespaces and Mosaics [Electronic resource]. – Mode of access: http://docs.nem.io/en/gen-info/namespaces. – Title from the screen.
12. NEM official docs: Proof of Importance [Electronic resource]. – Mode of access: http://docs.nem.io/en/gen-info/what-is-poi. – Title from the screen.
13. NEM official docs: Transaction Components [Electronic resource]. – Mode of access: http://docs.nem.io/en/transaction-components. – Title from the screen.
14. Official site of the Ethereum project [Electronic resource]. – Mode of access: https://www.ethereum.org. – Title from the screen.
15. Stellar concepts [Electronic resource]. – Mode of access: https://www.stellar.org/developers/guides/concepts. – Title from the screen.
16. Stellar Github Repository [Electronic resource]. – Mode of access: https://github.com/stellar/ – Title from the screen.
17. Stellar Laboratory [Electronic resource]. – Mode of access: https://www.stellar.org/laboratory/ – Title from the screen.
18. Stellar Smart Contracts [Electronic resource]. – Mode of access: https://www.stellar.org/developers/guides/walkthroughs/stellar-smart-contracts.html. – Title from the screen.

Іванов О. С., Бабіченко Є. Є., Канунніков Г. А., Карпусь П. П., Фою-Хацкевич Л. В., Кравченко Р. С., Гороховський К. С., Невмержицький Є. І.

ТЕХНІЧНІ АСПЕКТИ ПОРІВНЯННЯ ПРОВІДНИХ БЛОКЧЕЙН-ПЛАТФОРМ ЗА КЛЮЧОВИМИ ХАРАКТЕРИСТИКАМИ

Блокчейн як технологія стрімко розвивається, знаходячи все нові і нові точки входу в повсякденне життя. Вона є одним з елементів технічної революції 4.0 та використовується у сфері постачання, ведення різних типів реєстрів, доступу до програмних продуктів, боротьби з DDOS-атаками, розподіленого зберігання даних, збору коштів для проектів, IoT та ін.

На сьогодні у світі вже існує безліч блокчейн-платформ. Вони мають один технологічний корінь, але різні застосування. Є багато передумов для того, що в майбутньому кількість нових децентралізованих додатків тільки зростатиме. Тому, на нашу думку, важливе значення має розробка методології визначення оптимальної блокчейн-платформи для розв’язання конкретної задачі. Як приклад розглянуто всесвітньовідомі платформи Ethereum, Nem та Stellar. Кожна з них дає змогу розробляти децентралізовані додатки, випускати токени та робити транзакції. При цьому ключові характеристики цих блокчейн-платформ не схожі одна на одну. Саме такі характеристики розглянуто в статті.

Мета: визначити ключові параметри, що характеризують блокчейн-платформи. Це дасть змогу представити, на перший погляд, складну блокчейн-технологію у вигляді простої і зрозумілої архітектури. Ґрунтуючись на цих параметрах і використовуючи експертизу авторів статті, ми зможемо розробити методологію, яка використовуватиметься для розв’язання задач вибору оптимальної блокчейн-платформи для розв’язання задачі розробки смарт-контракту та випуску токена.

Методи: аналіз складності використання блокчейн-платформ, реалізація видачі токенів, використання тестових та публічних мереж, реалізація транзакцій, аналіз діяльності команди розробників і спільноти, аналіз інтерфейсу користувача та інтерфейсу розробника.

Дискусія: розробивши методологію порівняння блокчейн-платформ для виявлення оптимальних характеристик, ми зможемо вивести процес розробки на новий рівень. Це дасть змогу швидко і максимально ефективно вирішувати поставлені завдання.

Результати: створення методології порівняння блокчейн-платформ.

Ключові слова: блокчейн, токен, консенсус, розумний контракт, криптовалюта, децентралізовані додатки, блокчейн-платформа.

Матеріал надійшов 30.05.2018