VESTCHAIN

WHITE PAPER

Description of the Project

hello@vestchain.io

Notice

We are issuing the note for your careful attention. We are asking you to read the Note Section with all the carefulness. Please pay attention that the information containing in the current White Paper does not present any kind of financial, fiscal or legal guidance. Before taking a decision to participate in any kind of activity in connection therewith, you should consult your own fiscal or legal agent. Nor the VestChain Team members, its developers nor the VEST vendors are responsible for any kind of loss that may become as a result of your activity in connection with the current White Paper or any other document or information placed on the VestChain website, as well as that placed on the other resources.

The current White Paper is of a general nature; it does not present any kind of offer or agreement and does not presuppose any contractual relations. There is no warranty as for absolute accuracy and completeness of the given information. As there is data obtained from external sources the VestChain Team has no responsibility for its accuracy and completeness as well. Moreover, taking into consideration that the circumstances under which the White Paper was drafted may change, VestChain does not bear responsibility for not updating or correcting the information with the connection to the possible changes.

The current White Paper does not present any offer by the VestChain Team and should not be considered as a promise or a statement by the Foundation as for its further operation. Any deal between you and the Distributor is to be made under specially agreed conditions.

The VestChain Team does not bear responsibility for any kind of loss which may arise from the use of the current White Paper. Potential buyers should assess all the possible risks with all the carefulness. The current White Paper is of a general informational character only and is not legally obligatory.

The current White paper does not oblige anybody to conclude any contract or agreement on buying the tokens, as well as no payment is not to be made on the basis of the current document. A deal on purchasing the VEST Tokens is to be closed only with a separate set of terms and condition. Such a contract is to be presented to each potential buyer by the VestChain managers. Given there is some contradiction or ambiguity as for the Terms and Conditions and the present White Paper, the Term and Conditions stated in the official contract are to overrule.

No official authority has considered or authorized the information contained in the present White Paper. No such actions are going to be done.

The present White Paper only presents the VestChain Network's aims and how the Team is going to achieve them. The Team may come to a conclusion that there is a need to make some amendments or to replace the current version. The VestChain Team nor bear responsibility for updating the present White Paper neither pledges to supply any further information beyond that given in the current White Paper.

The present White Paper is not to be distributed or copied without consent statement from the part of the VestChain Network Team.

Content

1. Abstract

Information has always been an integral part of the human's society; it has been a booster of any human's activity since the ancient times. Those various ways of information exchange people have found actually made us humans one day. The advent of the Internet may be by right called a peak of the development in the direction of the information exchange. We are lucky to become eyewitnesses that it was just the first stage of the revolution in information. As you are reading this, we guess you understand what has already started as the second one. The blockchain is the rocket that slammed into the digital dimension and captured a big segment on the financial market. Despite now industries are only discovering what are those inexhaustible opportunities that blockchain may offer, they all realize it is going to predetermine development of many spheres of our life if not all of them in the nearest future. The feature that makes blockchain outstanding is that it was invented connecting two most important spheres responsible for the evolution as a whole, i.e. finances and new technologies. One may argue that blockchain is not the pioneer from that point of view, as there are enough information technologies that from the first sight seemed to be world-changing, but all of them lacked one important thing – they were not born with the focus on the finances.

Blockchain nascence goes hand in hand with the cryptocurrency. The word "blockchain" first was found exactly in the cryptocurrency code. Still one has to understand that it is two separate things. Did Satoshi Nakamoto understand that he was a founding father of something truly great? Nobody knows, but his peer-to-peer electronic cash system laid a foundation for the bigger steps in the direction of the further financial and informational revolution, that is for sure. A series of cryptocurrencies, like Litecoin and many other Alternative Coins, continued going with the idea, but the one that made a considerable step forward was Ethereum. We work exactly on its base. Smart Contract developed by Ethereum presents a phenomenal means for launching various blockchain applications.

In a broad sense, finance is the management f anything related to money. Thus, in the present new financial environment, there are two main concepts: cryptocurrency and crypto assets, i.e. bitcoin and smart contract. Blockchain registers all the transactions within a ledger. Smart contracts in their turn stipulate all the necessary terms and conditions. Both enjoy the absence of authority and inalterability of the blockchain to provide successful and complete value exchange. In spite of all those advantages the blockchain presents, there are still some obstacles for users of the smart contracts to overcome. Among them:

- Need for the unified supra-system. The bitcoin system generates the data itself; that provides the necessary level of data genuineness and authenticity. As for smart contracts, they use the outside data. We cannot say its genuineness and authenticity are under a big question, but that can be a great disincentive.
- Growing need for the compliance inside of the chain. Incompliance remains a stumbling block within the smart contract blockchain system.
- Substantial transactions demanding greater backing. It makes sense that there is competition directed in the same way. As for the operating, it results in extra expenditures of resources as well as in greater complexities when it comes to transactions browsing and reconstructing.

VESTCHAIN is a decentralized accessible blockchain and cryptocurrency infrastructure; it is absolutely open source content management system. VestChain is promoting a smart contract platform, the main goal of which is to provide the most progressive properties no other platform is able to offer right now.
The main feature of it is that it is the only one developed out of a scientific doctrine and a methodology putting research in the first place.

A huge international team of highly-qualified engineers and scientists makes the core of the VestChain development process. We laid the following features into the operation of our platform:

- The unique ecosystem with numerous chains that makes use of EVM, where POS or POP relies on an instrument with numerous segment blockchains or shards, which is capable to complete transactions in a more effective way.
- The process of a smart contract encasing that gets much easier with the knowledge graph in its core. The sufficient W3C Smart Data is made extremely brainy; that makes possible to resolve any problems connected with the intelligence issues.
- The VestChain Smart Data aims at creating relevant data capable of separating that information which is necessary from all the other. It is to become an essential part of the unified supra-system. A number of Smart Contracts will be able to utilize the Smart Data features the same is for other demands between the chains within the VestChain Platform. Smart data may become a bridge between artificial intelligence and blockchain; moreover, it may promote the alliance of the big data with blockchain.
- The structure of the chains which is represented as a stem facilitates the value exchange.
- VEST Tokens meet the ERC20 standard, so they can be easily utilized to be applied by the VestChain Platform.

All the factors together prove that VESTCHAIN is the unique blockchain platform that has full capacity to tackle the challenges inherent to the existing blockchains.

2. Smart Contract Status Quo

Blockchain supporting smart contracts is a bit different from that supporting digital currency. If the aim of the latter one is just to document the digital currency flows then the blockchain supporting smart contract is to apply the contractual arrangements agreed under real-life conditions directly to a smart contract.

When managers launch a smart contract in frames of blockchain no party may change the existing principles. A smart contract becomes assigned to the stipulated conditions and is implemented in an automatic mode in accordance with them with no party being able to interfere with the process.

It is important to understand that blockchain supporting smart contracts with its development acquires additional advantages. It operates not only based on the principles agreed upon by the parties transforming them into the code. Blockchain applications start using more complex tools to register data recorded in core databases before that, in such a way data cannot be changed by anyone. With the system becoming more sophisticated the operations and transactions themselves may become more complex.

2.1 Smart Contract Support

The usual way of smart contract operation presupposes a language to write the program which is further set into the blockchain. After that blockchain implements the contract in a virtual machine and gives the desired results. Nowadays we have two ways to work on the issue. One way is to create a new language and to make it a base for a virtual machine. Another one is to use the existing language and virtual machine.

2.2 Current Issues

Here are the current issues connected with using blockchain supporting smart contracts:

- High volume transactions have not enough support. Current blockchain systems cannot conduct a large number of transactions per second. In comparison with widely spread social networks blockchain is several thousand times "slower". The transaction mechanism is not sufficient enough to conduct the desired number of transactions. High scale transactions need a special transaction system that is strong enough to conduct all of them and not to fall down. The operation starts with collecting all the DApp transactions together and putting them into one and the same block. Once the DApp block is given a full load processing the transactions it has already collected it may lack time to create another block for the incoming transactions, thus all the DApps have no time to respond. Such state of things may cause inappropriate work of the system as a whole.
- All the DApps work in frames of the same blockchain. All the data (including that on the DApp transactions) is distributed between all the blocks. Keeping operations on a separate DApp on a track demands monitoring all the chain that is less efficient.
- One-chain POW reducing calculation capability. Nowadays, POW mechanism is a widely spread tool exploited by most of the users of the smart contract public chains. When there is miners' fight for creating another block, calculation capability of all the miners is distributed between all the blocks. This causes a huge waste of the entire blockchain calculation capability. There is a possibility to change the POW quite easily, that may complicate the process of the transaction confirmation. Proof-of-stake does not waste calculation capability but at the same time, open POS systems do not crack the Sybil attack issue.

- The other side of the immutability of the blockchain supporting smart contracts. Codes of the smart contracts alongside with the other information are loaded into the blockchain and after that, they cannot be changed. It means if there is a need for modification even for the better work of the system it is impossible to change anything. The other issue here is that if one wants to get the original data of the smart contract to make a new one on its base it is going to take plenty of time.
- Need for a universal and highly effective Oracle method.While the cryptocurrency system is a closed loop, the smart contract system is more open as it needs an outside node to provide the blockchain net with the data – it functions as an Oracle.

2.3 Related work

Technology with numerous chains may productively split the single-chain technology initial structure into separate segments by means of reorganization. As a result, the structure of the entire block does not reflect the processing capability of one computer. Computing and storage capacity increases with the growth of the structures with numerous chains. A number of different structures have been created but none of them can provide sufficient support for the Ethereum Virtual Machine.

Developers create many different tools to enhance the performance of the entire system. A number of them are oriented to the improvement of the situation with transaction process and stochastic consensus. VestChain Network approaches to the solution of the problem in another way. The Team raises the level of the blockchain system performance drawing its attention to data processing and sharding enhancing. The approach employs a multi-chain structure; basing on it the Team creates a new consensus approach.

3. Technologies of the VestChain Network

There is a need to remedy the deficiency of the single-chain method that supports smart contracts. That is why the multi-chain approach is destined to enhance the DApp support. Multi-chain system presupposes the existence of the major chain alongside with the minor ones. Here we present the main properties of the Vest-Chain Network:

1. The VestChain network Growth. As we have already stated the network is made in such a way that there are one major chain and two minor ones. When there is a new DApp created (or a new smart contract is launched), a new side chain is being built simultaneously. There goes an appeal to launch a new smart contract. The major chain gets it and constructs a new block. At the same time, a new minor chain alongside with a new node will be constructed. This first node will carry the smart contract binary code. When there is a new appeal for launching a new smart contract the VestChain Network will process this appeal and construct a new block. In such a way the minor chain (that is dealing with the smart contracts) will be expanding. Moreover, the minor chain has an upgrading ability for the smart contract. When the smart contract is moved up within the chain the binary chain of the last launched smart contract will be located in a newly constructed block.
2. The charges of the major chain and those of the minor ones. The major chain retains the information on the accounts and relocates the digital currency between among the accounts. The major chain is also engaged in interrelating with the outside public blockchain as well as in supporting relevant for the minor chain service. The aim of the minor chain is generally to record the data on a particular smart contract.

Main Technologies of the VestChain Network.

Smart Contract Activation with the help of the Non-inherent Tokens.

The VestChain Network is capable of conducting cross-chain operations. It provides a toolbox, with the help of which the smart contract can be activated using tokens non-inherent to the chain in frames of which this very smart contract works, but those from the other chain. At the current moment, the system may work with the Ethers and those Tokens under the ERC protocol.

The working principle is the following:

The Toolbox of the VestChain Network that operates in frames of other blockchains activates the smart contract of the VestChain Network with a certain quantity of tokens in this blockchain. Further, the smart data in frames of the Knowledge Graph will provide the information on the exchange rate between the VEST and non-inherent token.

As the VestChain uses Ethers primarily, we will explain how the calling process is conducted on the example of Ethers. The caller gives the VetsChain Network the name, parameters, and powers of the smart contract that is to be activated with the help of the Toolbox. The Vest Chain estimates how many Vest Tokens the certain contract takes, using the exchange rate it calculates the necessary number of Ethers and returns them to the caller. The caller adds the necessary quantity of the Ethers returned before that and imports the smart contract name, parameters and powers again. The caller will submit the request when the contract is “concluded and signed”. The VestChain Network receives the request, gets necessary quantity of the VEST Tokens, calls the relevant smart contract and gives back the result. The same procedure takes place if we are speaking about the tokens under the ERC20 protocol.

Moreover, taking into consideration that the VestChain Network supports the Ethereum Virtual Machine it also is capable of issuing the tokens that meet the ERC protocol. The VestChain Network enjoys access to a number of external blockchains.

Sharding Consensus.

The VestChain Network is capable of conducting operations at different segments. We may propose using various POS instruments with the aim to enhance general efficiency, storage capacities and opportunities to expand.
The VestChain Network implements the sharding consensus in two ways:

- Major chain and the minor ones constitute a hierarchy. The major chain supports minor chains and transactions between them. It is possible to construct a new minor chain to perform a specific task. All this helps to distribute tasks between all the chains and in such a way reduce the burden of the major chain.
- Transaction-level sharding is to be used for specific chains with a number of nodes. The VestChain Network launches the transaction-level sharding if there is a great number of nodes in one chain that correspondingly increases the number of the transactions conducted. The mechanism works in the following way (Identify the present moment as a beginning of a new era; First, all the nodes of all the chains will be grouped in accordance with the quantity of the VEST Tokens. Thus, some of the nodes will become a part of a bigger execution group; those nodes with a greater number of VEST Tokens will form a smaller governance structure. Execution groups will be separated in accordance with some other characteristics as well; Basic on specific principle, the system will submit the incoming transaction to the specific execution group. Such a factor as the type of users directing the request will also determine the group where this or that transaction will go. The transaction is verified within the sphere of the selected group. The consensus is obtained on the transaction level;

After some time passes the execution groups report to the governance group on the transactions verified. The governance group compiles the reports to come to a block-level consensus and to construct a new block as well as to present it to the entire system; A new epoch can be started only after all the nodes are synchronized in respect to the latest block.).

Moreover, the VestChain provides POS instrument to every chain:

From the very beginning, every chain is provided with the POS instrument automatically. Functioning as a consensus tool the POS instrument may save the time needed for processing transactions and in such a way help to construct new blocks faster. In general, it helps to save time for mining and to contribute to the overall system efficiency.

Smart Data and Knowledge Graph

A great volume of information should be obtained outside of the blockchain. If we are speaking about the Ethereum, we know that there is such an instrument as Oracle. It provides the smart contracts with all necessary external information. Unfortunately, the operation of Oracle is not standardized. Consequently, it is difficult to organize interaction between various blockchains.

Resource Description Framework (RDF) is a model for presenting the data, in particular, the metadata. RDF presents the data in such a way that it would make its automated processing possible; it is a markup language. Extensible Markup Language (XML) is a language that enables to encode information in such a way that is would be easily readable for both a human being and a machine.

An RDF file is made of multiple resource descriptions that in their turn are made of multiple statements. The statement is a triple composed of resources, attribute type, and value that determine the resource property. Resource description statement corresponds to the natural language statement. Within the natural language, resource turns out to be a subject, attribute type – a predicate and attribute value – an object (SPO). SPO has two patterns: entity-attribute-value and entity-relation-entity. These triples connect and together make a digraph, i.e. the Knowledge Graph.

Smart Data is formed with the VestChain Network creating basic RDF triples inside of the built-in blockchain information base. The aim of the VestChain Smart Data is to provide consistent data free of noise. The VestChain Smart Data is to become an integral part of the Oracle of the smart contracts. Smart Data may be used not only in the sphere of the smart contracts but to meet the other cross-chain requests. Smart Data works as a link between artificial intelligence and the blockchain. It promotes interrelation between the external big data and the blockchain. Useless to say that it may go beyond its primary functions and to make a good contribution to the operation of the Network as a whole.

EVM Support

Ethereum Virtual Machine is the core of the Ethereumblockchain. It backs the Solidity language. EVM runs the business logic and administers all the commands, at the same time, fighting malware. It makes accurate calculations under the smart contracts using the Turing-complete Solidity language.

EVM together with Solidity created a remote procedure call (RPC) with an access through HTTP. Moreover, the framework of Node JS and Truffle back EVM+Solidity perfectly well. In frames of app programming, it makes great sense.

Taking into consideration all the above-stated reasons, the VestChain Network is pleased with using the EVM in hand with the Solidity language both in major and minor chains. All the advantages of this combination let users construct new Dapps and transfer the existed ones.

4. Advantages of the VestChain Network

- The VestChain Network has become a pioneer in using Smart Data that in its turn makes the base of the knowledge graph. The Team's priority is to continue using and developing the existing tools and instruments as well as to invent and design new products. The advantages that the VestChain team already has may become a useful aid on its way to the further development.
- Every DApp gets its own chain; that grants easy transaction browsing and re-storing.
- Greater backing for the substantial transactions.
- New consensus mechanism that saves power.
- Ability to improve the functions of the smart contracts.
- Errors that may occur in any chain affects only the chain itself but not the operation of the entire system.
- Expandability that presupposes that constructing a new chain is nothing difficult with the help of a new consensus mechanism.

5. Modes of the VestChain Network Application

A number of advantageous developments made by the VestChain Team provided many ways of using the Network's features; the following are among them:

- Allocated artificial intelligence and big data transference.
- Transactions with digital assets.
- Gaming.
- Notary System.
- Monitoring (for example, a possibility to register every word said in frames of certain dialogue).
- Liaison system with the elements connected on every level.

6. Plan of Development

VEST Token

VEST is the original VestChain Token that is secured cryptographically. It makes the core of the VestChain Network ecosystem. VEST is the Token that is created on the base f the Ethereum blockchain and that meets the ERC20 standard. VEST is the token to be used for exchange in frames of the VestChain Network.

The aim of the VEST Token is to provide transparent, safe and convenient means for the Network users to conduct transactions between each other. VEST Tokens serves as a kind of "energy" to launch all the possible functions within the VestChain Network. At the same time, it represents the economic stimulus that is intended to attract participants. VEST is an indispensable element of the VestChain ecosystem.

The VestChain Foundation presents a non-profit organization. Its prior aim is to develop the VestChain Network. To achieve the aim the Foundation establishes certain bodies with the Board of Directors as a head of the Foundation. Among the Departments are to be the following: Executive Department, Department of DApp Governance, Department of Code Monitoring, Department of Public Relations.

Use of the system technologies.

There are two main ways of how the VestChain network system may be used:

- Blockchains and smart contracts. The first step is the formation of the VestChain Network itself that will take some amount of the resources. Then it is expected that there will be a number of applications to become the participants of the network, as a consequence there will be a growing demand for the VEST Tokens.
- Services and instruments provided by the Network. Being the creator of the VestChain Network the Foundation has the primary access to all the technologies, instruments and features of the Network. Basing on the Network the Foundation will provide advantageous products. A number of the corresponding development projects are in their way right now.

7. Possible Risks

You understand and accept that there are various risks related to the operations with VEST Tokens. The worst thing that may happen is losing all the VEST Tokens or a part of them; about the other ones we can note the following things:

- Ambiguous Laws and Requirements and Enforcement Measures. Speaking about the Vest status, we should say that its status is not quite certain in most of the jurisdictions.

The spread of cryptocurrency made the governments of many countries address the issue of regulating activity somehow connected to it. No one now may predict when or in which way the governments will regulate anything connected to the cryptocurrency operations or blockchain platforms. Newly introduced regulations may affect the network operation. In case of such a situation, the VestChain managers will consult competent bodies and take their decision.

- Information Release. It is important to say that the VestChain Team's priority is constant development. It means that the Network's concept, instruments, approaches or other things may be in a process of amendment and improvement. The present White Paper contains the most updated information about the Network, yet still, it cannot contain 100% of the information. We ask you to understand and accept the fact that the VestChain Team is not responsible for informing the users about each detail amended or updated. Thus, absolute information disclosure is not possible and does not make sense.
- Competition. Decentralized platforms and applications have become a new industry that is constantly developing. Every day new applications, platforms, and tools appear. It means that the industry becomes more competitive. Accordingly, it is possible that some other networks or platform use the similar to the VestChain's approaches. The situation on the industry market may require the VestChain Network to compete. Competence may result both in losses and in profit.
- Brain Drain. The VestChain Team is all about machines and technologies but people present an integral part of the VestChain Network. The success rests in hands of those talented men and women making the core of the Network. Any kind of brain drain may negatively affect the potential development of the Network.

- Development Failure. There is always the risk of deviation from the plan for various reasons going beyond the Team's responsibilities and abilities.
- Security Vulnerability. Unfortunately, the VestChain Network like any other network or platform may become an object to hacker attack. The VestChain Team understands that perfectly well and pays great attention to the security issues but at the same time asks you to recognize that no one is safe from this danger.

8. Roadmap

1Q, 2018

Verification Code 0.1

Middleware Layer

Public API disclosure

2Q, 2018

Virtual Machine Beta

Functional Language Beta

4Q, 2018

Single Node Test Net

Smart Contracts SDK

1Q, 2019

Wallet 0.1

VestChain API Service

3Q, 2019

Multinode Test Net

Smart Contract 0.1

4Q, 2019

VestChain Core Alpha Version

SmartWallet Alpha Version

1Q, 2020

SmartWallet 2.0

VestChain Core 2.0

Main Net Launch

2Q, 2020

Global Platform Expansion

System Model Expansion

VestChain Council Establishment

9. Contacts

Follow and contact us on social media: