WHITE PAPER

V.1.0

Introduction

Waves X is a new advanced cryptocurrency that will be created as a result of a hard fork of Waves - a token underlying a popular platform for ICO fundraising and issuing digital assets. Waves X is characterized by high transaction speeds, increased levels of decentralization, and extensive community involvement. It also offers a higher profitability for block validators due to the the implementation of a hybrid Proof-of-Stake/Proof-of-Work consensus protocol.

The Waves platform became a trailblazer in the field of token issuance and ICOs thanks to its simplicity and affordability. However, in its present state Waves confronts a number of serious challenges that cannot be solved without a major change to the system. In the first section of this White Paper, we introduce the advantages of the “old” Waves that are worthy of admiration and that will be preserved in Waves X, as well as provide a detailed description of its major flaws. Among these are excessive decentralization, lack of financial incentives, and limited smart contract functionality.

In the second part of the White Paper, we present our solution to the issues facing the Waves Platform. They include improved smart contract features (such as support for all major programming languages), off-chain order matching for the decentralized exchange, community voting procedures, a solution for offloading unused smart contracts from the network, and introducing tools for launching security token offerings.

Finally, we provide details on the hard fork itself, including its key element - a large-scale airdrop that will distribute free WVSX coins to all WAVES holders. An extensive roadmap (development plan) of the project is also provided.

1. Waves: current issues, challenges, and flaws

The founding team of Waves X has chosen to carry out a hard fork of Waves, as opposed to other possible cryptocurrencies, for a number of reasons. First, we believe that the concept of Waves has great merits and offers advantages not found with other digital currencies. These advantages are described in the first part of this section.

Second, we are convinced that the reality of the Waves platform differs greatly from its proclaimed goals and ideals: it is far less decentralized than what its management would have the audience believe, wrought with security vulnerabilities, and limited in its functionality. The hard fork proposed by Waves X aims to solve these problems and to offer the crypto community a much improved and streamlined version of Waves: one that is really decentralized, democratic, fast, profitable, and suitable for deploying blockchain projects of any complexity.

1.1. The Waves platform: advantages

1) Speed. After the last major update, Waves has delivered on its promises to guarantee a capacity of up to 1000 tpx per second. This does put it far above Bitcoin (less than 10 tps) and Ethereum (25 tps). This speed is enough for all the current applications of Waves, though it should be noted that it is still far from the fastest distributed ledger on the market. Interestingly, in October 2018 Waves set a record for the highest number of transactions processed on a single day (6.1 million, as opposed to the previous record of 5.4 million set by EOS).

2) Affordability. The Waves platform does not use gas (like Ethereum); instead, transaction fees are flat. Therefore, users do not need to pay extra for their transactions to be executed – even at peak load times. The fees are among the lowest on the market: a standard transaction costs 0.001 WAVES ($0.004 at the current price).
3) Simplicity. Waves is the justifiably popular for the ease with which one can launch a new token and conduct an ICO. Even users with no knowledge of coding can create a token and raise funds. There is a trade-off, however: the range of features is very limited.

1.2. Challenges and flaws

The Waves platform definitely offers advantages that are not found on other blockchain platforms, such as speed, flat fees, and ease of use. These are the qualities that the development team of Waves X admires and will carry into the new network after the hard fork. However, it is impossible to deny that the Waves model, concept, and execution also contain a number of very serious flaws: from incorrect claims of decentralization to security vulnerabilities.

1) Leased Proof-of-Stake (LpoS)

The Waves Platform employs an innovative modification of the standard Proof-of-Stake consensus algorithm known as Leased Proof-of-Stake. In the standard PoS, users “stake” their coins in order to be selected as validators for transactions, meaning that they purchase coins not to transact with them but rather to hold them in their wallet. Once a certain amount of time has passed (usually 30 days), coins become eligible for selection, which is akin to a raffles game. For each block, one coin is chosen “randomly” (in fact, usually the process is pseudorandom, creating potential security issues), and the owner of the coin becomes the validator for the current block and collects transaction fees for it. If the selected user’s computer is turned off, then a new coin is selected. Even though repeated selection can slow down the validation process, this concept is based on the assumption that users who want to earn fees in a PoS system and invest money to get enough coins will keep their devices running in order not to miss their chance. In most PoS networks, once a coin has “won”, it is excluded from the lottery for a certain period (normally for a month). However, the rest of the coins belonging to the same user, naturally , can still be selected. Therefore, the more coins one stakes, the higher the chance that one of them will be chosen for each new block.

The Leased Proof-of-Stake model is different in that average users cannot stake their coins themselves, unless they have enough to run a full node. This costs 1000 waves, which, at the current price of around $4 per wave, equals $4000. This is definitely too much for most users to stake; however, one can still use their waves to try and earn rewards by “leasing” them to a full-node user for a fee of 0.002 WAVES. The contract does not have a set duration and can be revoked at any time. Another alternatives is to join a mining pool, such as WavesGo. In both cases, the maximum profit that one can earn is circa 5% a year.

Leased Proof-of-Stake presents a problem, since it essentially creates two classes of users: those who cannot afford to buy enough WAVES to earn their own mining revenue and those who have enough resources to run a full node or a pool. This creates a source of centralization and single points of failure. What is worse, the whole original idea of Proof-of-Stake as a way to democratize mining loses its meaning: an average user with a simple device and a limited number of coins cannot do their own mining, and the fee for leasing WAVES, while not high in absolute terms, is still twice higher than the standard transaction fee in the network.

2) Absence of 2FA/MFA

One of the most prominent security issues present in the WAVES Platform is the lack of two-factor authentication. With 2FA, a user requires more than just the desktop client to confirm a transaction: a special code is received through another device (usually a smartphone), so that the transaction is confirmed using two seeds: the main seed and the mobile seed. The more secure way and decentralized way to implement 2FA is to have a user store two seeds safely: the main seed for the computer and a secondary seed for the mobile device. A less secure but easier alternative for average users who are not very good at storing their seeds safely is a third-party service like Google Authenticator. However, in this case seeds themselves are stored in a centralized remote database, which can make them an object of a hack.

While both 2FA options described above have their flaws, the key issue is that Waves yet has to implement any of them. As long as there is no two-factor authentication included in the Waves client, any malicious individual who gains physical or remote access to the computer of a WAVES holder (but not their phone) can easily gain possession of all the coins.

3) Centralization on Waves DEX

The Waves Decentralized Exchange is definitely a commendable enterprise, but it has serious flaws. Most importantly, the exchange is nor really decentralized at all: while actual asset transfers are decentralized, order matching is done through the central server. This goes against the concept of decentralized economy and creates a serious single point of failure. The server that carries out the matching can easily become the target of a DDoS attack. Since the size of the order book is not limited, it would be enough to flood it with orders set for the maximum allowed live time (1 month). This security vulnerability was stressed in the results of a recent audit.[1] The centralized order matching

[1] https://steemit.com/bitshares/@eosfan/wavesplatform-waves-security-audit-confirms-some-of-centralization-security-concerns-summary

pursues the goal of making exchanges faster, but the risk is serious: indeed, very soon after its launched the platform was hacked, resulting in the theft of $6 million.

The centralized structure of the Waves DEX also makes it possible for the system to front-run orders, making large profits. Essentially what happens is that when the exchange operators see that a large buy order has been placed, they place their own buy order and push it to the front of the queue (since the order of execution is determined by the exchange), making the purchase while the price is still low. Then they let the larger third-party order go through, which increases the price; next, the exchange sells what it had just bought – but at a higher price. Front-running orders is a very common practice for centralized exchanges and brokers; it is also a form of market manipulation and therefore dishonest.

4) Centralized governance and censorship

The Waves Platform is under full control of its founding team. Since there is no mining – all of the 100 million WAVES were pre-minted and are already in circulation – the founder's share of coins will not be reduced unless they decide to sell some of the WAVES they hold. There is little involvement of the community in the decision-making, and the management has the power to decide which coins and ICOs will remain on the platform. This was amply illustrated by the delisting of a coin whose name was considered offensive. While it is true that racism, hatred, and discrimination should not be promoted via coin issuance, the decision was supposed to be made by the Waves community by means of a vote. This voting principle is stated in the Waves White Paper, yet it was not employed.

5) Security issues due to LPoS

As noted above, only a certain proportion of users (those with over 1000 WAVES staked in the network) can run full nodes to validate transactions and collect fees. The rest of Waves users can only lease their coins to full nodes or public mining pools. Understandably, the number of full nodes constitutes just a small proportion of all the nodes in the system – and what is worse, they are all known. As the pool of users with over 1000 WAVES staked cannot be kept secret, and the mechanism for choosing the coin whose owner will validate each new block is only pseudorandom, full nodes are much more prone to hacker attacks than when the number of potential validators is really high.

6) Delisting from other exchanges and limited availability

WAVES themselves suffer from a limited circulation: they are not present on major exchanges and are generally traded only on the Waves DEX itself. The situation was exacerbated in late 2017, when WAVES and all tokens issued on the Waves platform were delisted from the well-known Cryptopia exchange. The delisting happened after Waves introduced a major update that was not marked as mandatory: over 70% of nodes chose not to update their nodes. This caused a hard fork and, as a result, instability, issues with audit, and financial losses for exchanges.

Not only the reputation of the Waves Platform itself, but also that of the ICOs listed on it suffered as a result. It is a sad truth that tokens issued on Waves are often considered “second-class” and are not readily accepted by outside exchanges. The very ease with which a new token can be issued on Waves to some serves as a sign that its founders were reluctant to invest a real effort. As a result, many worthy and potentially disruptive projects that conduct their ICOs on Waves never reach their full target audiences.

7) Smart contracts and RIDE

For most of its existence, the Waves Platform did not offer smart contracts – it was seen as a reasonable price to pay for the simplicity of issuing new tokens. However, in September 2018 the platform finally launched what it calls limited-functionality smart contracts – or, rather, smart assets and smart accounts. They are Turing-incomplete, meaning that in its present state the Waves smart contract system can be used to run some types of programs and perform some predefined types of calculations – but not all of them. By contrast, Ethereum Virtual Machine is said to be Turing-complete, because theoretically it can be used to run any program, given infinite resources (gas) and time. (Incidentally, Vitalik Buterin himself admitted that since there are economical limitations to gas usage, in practice EVM is running as a Turing-incomplete machine.)

In simple words, the smart contracts introduced by Waves are very limited in their scope and are aimed at non-coders and users with a limited programming experience. However, Waves smart contracts use a new programming language called RIDE, which was created specifically for the purpose. This means that anyone who wants to code a smart contract on Waves will have to learn a new language from scratch.

8) Limited motivation for validators

Since there is no real mining as such in the Waves system (all coins were pre-mined), block validators only get transaction fees for their computational work. With the majority of fees set at just 0.001 WAVES ($0.004 or 0.4 cent at the current price), reward amounts cannot be compared to those earned by miners in PoW systems. And even though the resources needed to run full nodes are very small (any computer can do validation on Waves), it remains an open question if fees alone are enough motivation for users to keep their WAVES staked in the network.

2. The Waves X solution: features and possibilities

At the heart of the Waves X ecosystem is WVSX - a new cryptocurrency that inherits all the best features of WAVES and enhances them with a wide set of cutting-edge solutions and advanced technologies. WVSX is designed to be used as a means of payment for real-life purchases and applications, as a trading asset, and as a way to earn mining revenue. It Waves X is much more than a coin

Thanks to streamlining the original Waves protocol, Waves X will ensure average speeds above 1000 tps, with a potential to rise over 10 000 tps on the decentralized exchange once off-chain order matching is introduced (see below). Even in peak load periods (for instance, during a popular ICO) the system will not stall.

This section introduces some particular applications of Waves X for various purposes, including launching new digital assets, developing distributed applications, and trading.

2.1. ICO and crowdfunding

Waves X will take the advantages provided by the old Waves to blockchain project founders to a new level. A true decentralized economy requires that all visionary creators, innovators, and authors of promising ideas be able to launch their projects without excessive expense. However, the actual situation on the ICO market is from this ideal: conducting an ICO in most cases costs so much money that the majority of teams cannot afford it without prior funding from an angel investor or venture capitalist. The problem is particularly acute on Ethereum.

On Waves X, issuing a new token will be be even more affordable than on the old Waves; and the smart contract functionality, with its database of templates (see below) will provide founders with a ready toolbox for building a functional MVP. The newly-issued token can be listed on the internal decentralized exchange right after the ICO for a nominal flat fee. What’s more, founders will be able to find backers for their project right on the platform. In order to ensure that only the best projects obtain funding, the community will be able to vote on all ICOs, evaluate and audit their smart contracts, hold Q&A sessions with founders, etc. A set of KYC/AML options will be available through a partnership with an external provider.

In the initial development and deployment period, Waves X will be open to all utility tokens (their utility character will be determined by the community together with the platform management). After that, a major update will introduce security token functionality, opening Waves X to projects whose tokens represent digital shares or cryptographic securities. In the present regulatory climate, security tokens will gain more and more popularity in the next two years. We expect digital securities to take part at least 30% of the market by late 2020. In the meantime, Waves X will not only introduce a wider range of KYC controls and whitelisting features, but also obtain all the necessary licenses.

2.2. Low flat fees

Waves X will continue the policy of the Waves platform regarding fees, promoting even cheaper transactions (in part, thanks to off-chain order matching – see below). Each individual transaction will cost 0.001 WVSX, with the fee for deploying a smart contract or issuing a new token set at 10 WVSX to prevent users from issuing spam tokens that have no potential for adoption.

Waves X will not charge any rental storage fee on smart contract owners, as long as a contract is active (that is, the associated dApp or campaign has users who conduct transactions). The issue of unused smart contracts that remain in the network as dead weight (very common in the Ethereum blockchain, for example) will be solved by using community voting. Smart contract owners will have a choice between their unused contract being placed in a state of hibernation (with attached regular fees, which will need to paid in full to restore the contract to an active state) or remove the contract from the blockchain using one of two options (at least one of which must be designed into each smart contract on the Waves X network from the start): a selfdestruct function or a delegatecall/callcode function referenced to another contract.

2.3. Decentralized exchange and off-chain order matching

The Waves X decentralized exchange will offer all the necessary tools for successful trading: a wide range of assets (including all the tokens listed on Waves X, as well as ETH, ERC20, BTC, etc.), high-speed P2P exchanges, atomic swaps, and – in the near future- trading in derivatives and margin lending.

The major difference between the Waves X exchange and the majority of its competitors lies in the implementation of off-chain order matching. Waves X users will be able to broadcast their orders to the whole network without recording them on the blockchain, which will decrease latency and transaction fees. Other users will be able to fill broadcasted orders. Matching will be conducted off-chain by a special category of users (relay nodes), who will not have a right to conduct actual transactions. By contrast, elements in the network that make exchange transactions go through will not have access to the matching process. This will allow to decentralize the trading process, keeping it fast and affordable. Such forms of abuse as front-running orders will be impossible with Waves X. Hacking the exchange will be almost impossible, just like with any proper decentralized exchange. These features will make Waves X a new standard in crypto trading.

2.4. Hybrid PoS-PoW consensus protocol

Waves X will implement an innovative combination of Proof-of-Stake and Proof-of-Work consensus mechanisms to ensure that the network is decentralized, secure, and efficient at the same time. Traditionally, only one of these two consensus algorithms was used in each blockchain network, which resulted in different problems. With Proof-of-Work, the main concerns are three. First, there is the waste of resources: mining rigs already consume more electricity than most smaller countries in the world, essentially spending the energy to find solutions to cryptographic puzzles. Since only the miner who finds the correct solution first wins a large block reward, thousands of miners race to solve the same puzzle every time a new block is created. The system (pioneered by Bitcoin) is built in such a way as to make the answer difficult to find but very easy to check. The difficulty grows over time, making mining less and less efficient.

Out of this diminishing efficiency comes the second issue, known in game theory as “the tragedy of the commons”. In it, each of a multitude of rational individuals (miners) seeks to maximize their own gain and fail to cooperate, even though cooperation would have been more beneficial for the group at large. In PoW mining, each miner will choose to confirm transactions that carry a higher transaction fee, potentially leading to many transactions getting delayed or not getting confirmed at all as the difficulty and computational effort needed to solve them grows. This can have negative consequences for the whole system of crypto payments.

Finally, PoW networks are prone to so-called 51% attacks: a hacker needs to compromise 51% of all nodes to carry out double spending or another malicious act. While this is almost impossible with larger networks, taking over 51% of nodes in a young, small project is absolutely realistic (Bitcoin Gold is a good example).

On the other hand, Proof-of-Stake is not without its issues, either. First, such a network is subject to another economic/game theory problem, known as “nothing at stake”. In it, once users stake their coins, they can generally just leave their machines running and receive transaction fees from PoS “mining”. If the network forks, it will be in the validator’s interest to continue building on both resulting chains, maximizing resulting fees. The validator loses nothing by confirming transactions on both forked chains (of course, this assumption applies to networks without security deposits which can be lost due to such behaviour). However, multiplication of chains leaves the network much more vulnerable to attacks.

The problem of nodes’ malicious behaviour in PoS networks also remains partially unsolved. It is expected that the very fact of staking one’s coins will prevent a node from breaking the rules, since that would jeopardize one’s stake and position as a block validator. However, this principle disregards the so-called Byzantine General Problem: single malicious nodes can transmit wrong or confusing messages to others, so that even honest nodes end up confirming “bad” transactions.

It should also be noted that many users are not motivated enough to join PoS networks, since the rewards they offer are simply too low. Even though the divide between PoW block rewards and PoS transaction fee revenue is narrowing down due to the falling efficiency of PoW mining, the 5% that a PoS can get on average seems to low to some.

The hybrid protocol introduced by Waves X will help resolve these issues and use the best of both worlds. In Waves X, all odd-numbered blocks will be validated using PoW, while even-numbered blocks will be confirmed using PoS. A voting mechanism will be used when a node is found to act against the rules. Nothing prevents the same user from both running a PoW mining node and acting as a PoS validator. At first, while the Waves X network goes through a period of active growth, PoW-mined blocks will ensure the necessary profit to users interested in “proper” mining (while the difficulty remains moderate), and the parallel presence of PoS will help prevent attacks. Indeed, a hacker would need to take over control over both 51% of PoW nodes AND 51% of PoS nodes to carry out a double-spend, which makes attacking Waves X much less attractive economically.

Later, when mining blocks using PoW becomes more difficult, lower but stable revenues from PoS will provide a safety cushion. Both users who already own powerful equipment and those who operate only a simple device like a Raspberry Pi computer will be included. For staked coins, there will be no maturity roll-back: even when a validator is selected to confirm a block, their coins retain their accumulated maturity. We do realize that it will give a certain advantage to those who stake more, but it will also provide more motivation to keep one's stake in place. This way, the production of new Waves X coins as a result of PoW mining and their increased staking will be balanced, preventing inflation.

2.5. Smart contracts

Waves X aims to be a user-friendly platform for launching new projects, which will satisfy both the needs of self-funded founders and large teams that include professional coders. Smart contracts are an essential element of such a system: indeed, while one can issue a token and raise funds without a smart contract, one definitely cannot build a functioning application without one.

The fact that smart contracts were absent from the Waves Platform for two years has led to the appearance of dozens of useless, low-quality tokens that nobody needed. By introducing fully functional smart contracts very soon after the platform launch and pairing it with a community voting mechanism, we can ensure that only worthy projects will issue tokens and build dApps on Waves X.

Unlike the original Waves platform, Waves X will be language-neutral, meaning that it will b e possible to compile new smart contract in any Turing-complete programming language, including JavaScript, Solidity, C++, Simplicity, Python, Vyper, and RIDE. It will also be possible to migrate an existing dApp into the Waves X platform quickly and easily.

New functions will be added constantly, starting from a large introductory package that will include ready blocks and templates. In this, the Waves X development team is inspired by the successful model of WordPress – the website-building platform. On WordPress, users can get free access to a large number of pre-compiled blocks, widgets, and add-ons, with even more advanced functionalities available for a fee as premium packages. In general, the better one can code, the fewer premium add-ons one needs, since most design elements can be implemented by either writing code or using visual pre-made widgets.

Waves X will use a similar model: a constantly growing database of templates to be used in smart contracts and dApps, with elements like token vesting, atomic swaps, multisig wallets, escrow (centralized and multisig), in-built exchange features, fiat gateways, and even advanced implementations like Lightning Network. New templates can be added by community members, to be voted up or down by all Waves X users. Those users who run PoW or PoS mining nodes will have votes with more weight (depending on the number of Waves X coins staked in case of PoS).

3. Waves X - Implementation

3.1. Network snapshot and coin distribution: key facts and figures

Snapshot date and time: January 17, 2019 21:00 GMT
The snapshot will establish how much ether is held by each WAVES blockchain user in their personal wallets. These figures will be used to distribute free WVSX coins after the hard fork.

Distribution ratio WAVES/WVSX: 1:5
Every user holding WAVES in their personal wallet at the moment of the snapshot will receive 5 WVSX for each WAVES they hold. WVSX will be distributed via an airdrop. Note: only personal wallets (Waves Lite, Waves for iOS and Android) are eligible for the airdrop; exchange wallets cannot participate.

Initial emission: 500 000 000 WVSX

Mining: yes
Consensus protocol: Hybrid PoW-PoS

Bounty program: yes (Twitter, Facebook, YouTube, blogs/articles)
Affiliate program: yes

3.2. Roadmap - project milestones

Q3-4 2018 Development of the Waves hard fork concept; building a development team and attracting advisors.
Jan 17, 2019 Snapshot of the WAVES network & distribution of WVSX coins

Q1 2019 Implementation of the basic ICO features (creating a new token, starting a fundraising campaign, KYC/AML, community voting on projects, wallet integration); launching of the first version of the desktop client including 2FA; launch of the decentralized exchange; listing first ICOs; submitting WVSX to several major digital exchanges; security audit of the Waves X smart contract; start of PoW and PoS mining; adding new members to the team; a large-scale bounty campaign and airdrops; launch of the affiliate program.

Q2 2019 Adding basic smart contract functionality (atomic swaps, vesting programs, multisig wallets, escrow, refunds); work on the off-chain matching solution for the decentralized exchange; attracting new advisors; integration with fiat payment gateways; adding first assets to the decentralized exchange; completion of first ICOs on the platform; roadshow; development of native iOS/Android apps.

Q3 2019 Major new smart contract features; implementing a tool for migrating dApps from other platforms; testing of the off-chain order matching solution; hiring advisors from the fields of decentralized exchanges and smart contract development; development of a smart contract hibernation feature using community voting; work on crypto derivatives trading tools; launch of native iOS/Android apps; introduction of a smart contract template library.

Q4 2019 Integration of derivatives trading and of the off-chain order matching tool; new technological partnerships, including in the field of second-layer payment protocols; introduction of smart contract hibernation