waves

www.wavesplatform.com

Whitepaper

Written and prepared by Sasha Ivanov

Abstract

WAVES is a decentralized blockchain platform focusing on custom blockchain tokens operations. National currencies transfer is maintained on the WAVES blockchain through compliant gateway operators. Decentralized token exchange facilitates fundraising, crowdfunding, and trading of financial instruments on the blockchain.

Lightweight clients provide an easy installation procedure and a flat learning curve for end users.

1. Introduction

Hypothesis:

> *"Every conceivable application of blockchain technology will be tried, but p2p digital cash will remain most used application"*
> *- Ryan X Charles.*
>
> *"The killer application of blockchain technology is the blockchain itself."*
> *Common wisdom.*

Since its inception, blockchain technology has been fraught with controversy over its most natural application – value transfer using the network token. Decentralized money is a ground-breaking development, but blockchain technology cannot be reduced to this alone. Being essentially a distributed database, the blockchain allows for various types of distributed ledger entries, the nature of which depends on their interpretation by the blockchain's users.

Introducing the blockchain as a foundation for digital cash attracted a great deal of attention to the technology, putting regulators and governments worldwide on high alert in the process. There is no doubtthat Bitcoinwillestablishitselfasavalidmonetarysystem.Butitisalsoobviousthatthere should not be too many blockchain tokens in use as money at the present time, since the low liquidity and high volatility this causes prevent the use of emerging blockchains as a secure store of value.

We propose to focus on other uses of blockchain tokens – those which are often overlooked in favor of the low-level opportunities which blockchain technology might provide, such as smart contracts. There is very strong untapped potential in a classical colored coins approach, and the WAVES platform is designed to realize this to its fullest extent.

Smart contracts, being a natural development of Bitcoin scripting, are inevitable and will be one of the cornerstones of blockchain technology. On the other hand, certain features are much easier to implement using other approaches. Custom tokens operations realized as an attachment to blockchain transactions are very flexible and can be used in a variety of applications, from national currencies transfer over the blockchain to decentralized trading. A focus on such operations might well complement the approach introduced by Ethereum. [1]

In the following sections we will describe the technical motivation for WAVES platform's features and illustrate them with use cases. We intend to determine the most "production-ready" aspects of current blockchain technology and apply them to the real-world problems.

2.
Custom blockchain tokens and their usage

2.1
Technical motivation

Blockchain assets and colored coins approaches emerged around 2013, when several protocols utilizing Bitcoin's blockchain were implemented. [4] [5] [6]
Besides this, there were several attempts to build custom blockchain tokens platform from scratch, of which the most notable is Nxt. [7]

We develop the approach which Nxt implemented, realizing custom tokens creation and transfer through attachments added to blockchain transactions. This approach has clear merits, such as the ability to implement new transaction types easily, but from practical point of view it is fraught with the problem of mandatory hard forks – when adding a new transaction type, network client software has to be updated, since old clients cannot support new transaction types.

WAVES approaches this problem by offering an extensible solution, in which new transaction types are introduced through plug-ins that are not included in the core software module, but are instead installed as an extension on top of it. Clients that do not have the relevant plug-in installed can still relay these custom transactions. This approach allows third-party developers to introduce new transaction types, and creates an Appstore-like ecosystem.

Only the most basic transaction types are supported at the core level, including:

- Custom token creation, deletion and transfer
- Decentralized token exchange, realized as a distributed order-matching engine, where Bid and
- Ask network transactions are matched against each other
- Anonymity features – anonymous order books are a must for an industry-grade trading platform

It should be noted that WAVES makes a crucial step ahead with decentralized blockchain trading by offering trading of one custom token against another (asset-to-asset trading).

This opens up a whole new range of opportunities, including trading against tokens tied to national currencies, thus replicating traditional trading infrastructures.

2.2
Use cases

2.2.1
National currencies on the blockchain

Although using the main network token for value transfer is quite natural, it nevertheless raises several issues. Use of low-liquidity and highly volatile tokens for value transfer has obvious drawbacks for merchants, and creates tension with regulatory bodies.

Still, fully decentralized money is viable, which is demonstrated by the slow but steady adoption of Bitcoin as a currency.

However, in order to provide sufficient liquidity and mitigate the volatility that prevents decentralized money usage as a store of value, the overall number of tokens used as currency should be limited (at least in the initial stages of the development of the technology). We strongly advocate using only Bitcoin as a currency for this reason.

Our approach to handling external value transfer tokens and currencies stems from the 'Multigateway' approach. [2]

In the case of Bitcoin there is a party (or multi-sig parties) that maintains an in-and-out exchange procedure for Bitcoin, swapping it for its corresponding network token. Thus we facilitate Bitcoin transfers using the WAVES blockchain.

This approach is obviously centralized, due to limitations inherent in Bitcoin itself. It is opposed to a "market peg" approach, which relies on providing a dynamic peg though certain market-making procedures. At first sight the market peg approach may seem to be an adequate way of mirroring financial assets on decentralised platform, but with further consideration hidden centralization invariably surfaces.

By explicitly introducing centralization into supporting blockchain national currencies and BTC we are able to open new horizons for existing financial institutions. Their role can be reduced to providing liquidity for their fiat assets and KYC/AML procedures. Maintaining payment infrastructure is fully outsourced to decentralized blockchains.

This approach to providing national currencies on the blockchain was pioneered with the CoinoUSD token on Nxt's blockchain. It is also similar to Ripple's gateways approach.

We believe that such a strategy can compete with the emerging permissioned blockchains approach and attract financial institutions willing to work on open blockchains.

2.2.2
Crowdfunding, decentralized financial instruments and beyond

We believe that blockchains are an effective means for managing most aspects of community-based projects, from financial to organizational elements. Blockchain technology, due to its innate latency, cannot support high-frequency trading. Most probably centralized solutions will always be preferable for high-volume transactions with milliseconds execution times. But for applications in which instant transactions are not required, blockchains provide a very natural environment – for example, for issuing crowdfunding tokens and managing financial flows within a community. This is an area in which using decentralized solutions is beneficial and centralization brings little to the table.

If we consider a Kickstarter-like model of pledging certain amounts of money in exchange for a product to be released in the future, we can see its obvious limitations. A project backer cannot exit her "investment" in the project by selling it another user. On the other hand such a use case is very natural using a blockchain-based system, where custom tokens can be swapped and transferred by design.

Issuing securities is highly regulated in most jurisdictions. Tokens can be associated with securities, especially if some projections about future token price are made or a token issuer promises to pay certain dividend. However, the blockchain is a regulation-agnostic instrument. If a legal entity wishing to utilize the blockchain for a securities issue is compliant with local laws and regulations then issuing securities on a blockchain is as legitimate as conducting a stock exchange listing.

Start-up fundraising, private investment placements and venture-stage investments seem to be the most appropriate areas for blockchain-powered financial instruments. On the other hand it can be used by a larger businesses for specific financial operations too, such as clearing and settlement, so long as these do not entail overly taxing speed requirements.

In most jurisdictions (notably excluding the US), blockchain-based fundraising that does not exceed a given limit can be carried out perfectly legally. Equity crowdfunding laws in the US allow fundraising with a simplified SEC registration procedure.

Strict US securities laws are intended to prevent fraud, and for this a strong centralized watchdog, such as US Securities and Exchange Commission, is needed. But the advance of decentralized technology can introduce some form of community and decentralized issuer vetting, which might eventually replace centralized regulators.

3.
Lightweight clients, two-tier architecture, Proof of stake and usability

3.1
Technical motivation

3.1.1
Two-tier architecture and lightweight clients

The classic Bitcoin approach is essentially a way to synchronize a distributed system through common transaction logs. It requires that each network node store the full copy of the transaction history. Obviously this does not scale well, since eventually not every node will be able to store the full history. There are different ways to mitigate this – a simplified payment verification procedure that allows storage of only that data essential for a given node; off-chain transactions; bidirectional payment tunnels; reducing blockchain bloat; working directly with the system state. [8] With the simplest approach, where all nodes are equal at Genesis block, centralization may emerge as low- capacity nodes have to rely on full, high-capacity nodes that can afford to store the full blockchain.

Effectively, a two-tier architecture emerges.

Does this make the system inherently centralized?
No, since a new node can always enter the network and become a full node if it has sufficient resources.

Of course, emerging centralization brings trust issues, since lightweight nodes have to trust the full nodes and can become a victim of a rogue full node. However, there are ways to mitigate this, such as polling several nodes, maintaining trusted nodes lists, and so on.

WAVES platform enforces an approach that might at first seem extreme to a classic cryptocurrency advocate. Lightweight nodes do not download the blockchain at all, instead relying on full nodes for payment verification and network interaction. The approach is based on the SuperNET lite client [3] that has successfully been run on the Nxt platform for over a year.

WAVES is built on the Scorex platform [8] which develops an approach based on using current network state as an alternative to full transaction history. A simplified payment verification procedure will be realized for the lightweight node, adding another security layer. System state can be downloaded by a lightweight node, and simplified payment verification procedures based on this.

3.1.2
Proof-of-Stake consensus and stake leasing

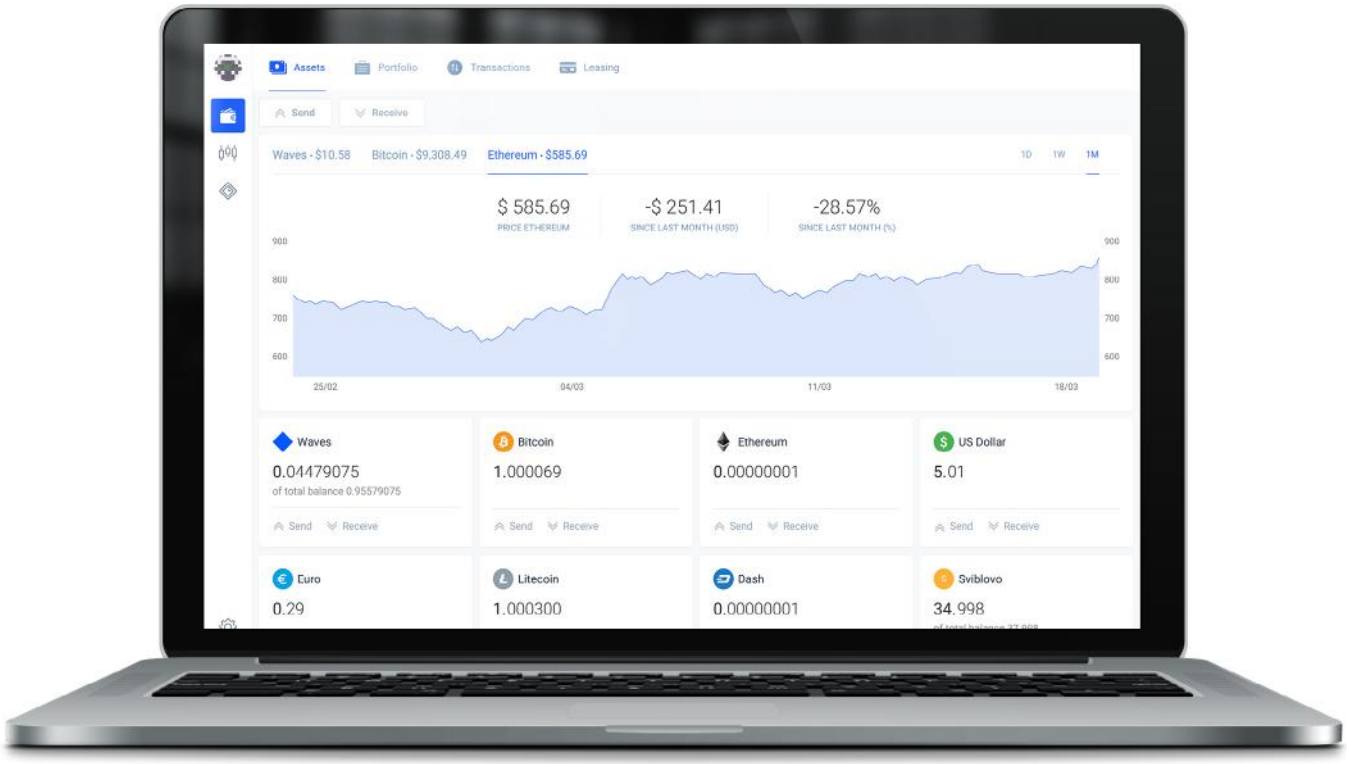
We have chosen the Proof-of-Stake protocol as a consensus algorithm for WAVES. This choice is based on its successful use in NXT, as well as on certain theoretical considerations. At the same time we propose an enhancement to the PoS protocol, which should provide for reduced transaction times and increased transaction throughput – Leased PoS (LPoS).

In a PoS system each node that holds a balance in the main network token has a chance (proportional to its balance) to produce a block. In the two-tier architecture it is logical to move payment processing onto the full nodes alone. At the same time, all nodes with non-zero balances still have to be eligible for staking rewards.

The theoretical issue of reduced security caused by fewer nodes staking can be addressed through explicit balance leasing from lightweight nodes to full nodes. By leasing their balance to a trusted full node a lightweight node actually increases its chance of collecting transaction fees, since it does not have to stay online, and the full node has an increased chance of producing a block due to its increased balance.

Account leasing is not equivalent to balance transfer; a lightweight node can still transfer its balance to another node and conduct other operations. By leasing out their balance, lightweight nodes effectively select which full nodes will carry out most of the network's payment processing. Reducing the number of nodes that can potentially produce blocks allows for faster confirmation times, lower latency, and a higher system throughput.

4.
Lightweight node realization and browser plugins



The wallet interface resembles traditional online banking/brokerage interfaces. Integrated national currencies allow for native value transfer denominated in fiat. Exchange of national currencies into and out of the blockchain is carried out by a trusted provider. Once a user has completed the national currency token purchase she can transfer it to another user or trade with it on a decentralized exchange.

Asset-to-asset trading makes it possible to provide a stock market-like trading interface, by allowing trading against USD, EUR, CNY, and so on. All in all, the platform interface is closer to traditional financial interfaces than to a normal cryptocurrency client. We find it important to provide an interface to which most users are already well accustomed, at the same time as empowering it with blockchain technology. Users can do things they were unable to do with traditional financial platforms, but the learning curve remains flat, which is a key to mass-market adoption.

5.
Additional key WAVES features

WAVES targets in the first place community-based development and projects. To that end decentralized voting and messaging are implemented. It will allow for a DAO-like experience in managing community projects, whilst remaining straightforward from a technical point of view.

WAVES will allow payment of network transaction fees in custom tokens (assets). Along with the transaction in question, an order to exchange the asset into the main network token is sent to the decentralized exchange, and the transaction can be included in the next block only after that order has been executed.

6.
Conclusion

WAVES platform is being built with mass adoption in mind from the start. In this general overview we have attempted to show the technical solutions that may be used to give the end-user previously unseen opportunities, and to pave the way for the rapid adoption of blockchain technology.

References

[1] https://github.com/ethereum/wiki/wiki/White-Paper
[2] http://multigateway.org/
[3] https://github.com/Tosch110/SuperNet-Lite
[4] https://github.com/CounterpartyXCP
[5] https://github.com/OpenAssets/open-assets-protocol
[6] https://github.com/OmniLayer/spec
[7] http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt
[8] http://arxiv.org/abs/1603.07926

www.wavesplatform.com