VOOLA WALLET

TECHNICAL PAPER

More information on website: voila.io

INTRODUCTION

The flaws in the current financial foundations have led to a boost in the popularity of alternative systems. Services built using decentralized technologies offer faster and less costly transactions and better security as well.

The Voola project is created with the idea of helping people from all parts of the world to convert, transfer, and receive digital currencies speedily and securely without the involvement of a central authority.

The Voola project will have a native cryptocurrency (called VOOLA - VOOLA), secure blockchain (called VOOLA Secure - Voola), tokens (called Stable Tokens), a hybrid currency exchange, a Voola Pay wallet and a Voola prepaid credit card. The goal of the exchange will be to enable users to exchange Stable Tokens for FIAT currencies and vice versa.

The Voola Pay wallet will enable users to issue virtual prepaid credit cards. By allowing the NFC smartphone connectivity, it will be possible to make payments everywhere in the world.

Business cases

White

Personal Account

- PassportID
- Transactions on the open blockchain
- Create multi-currency wallets
- Unrestricted exchange of Cryptocurrency.
- ATM \ Crypto-ATM - unlimited fund withdrawal
- MultiSig wallet
- Cold wallet
- Investment & automated trading
- Business Account
- Create multi-currency wallets
- Issue stable coin
- Acquiring
- Exchange of the cryptocurrency & fiat Passport ID
- MultiSig wallet
- Cold wallet
- Salary projects on smart contracts. Deposits
- Credit products
- Automated business-trading

Black

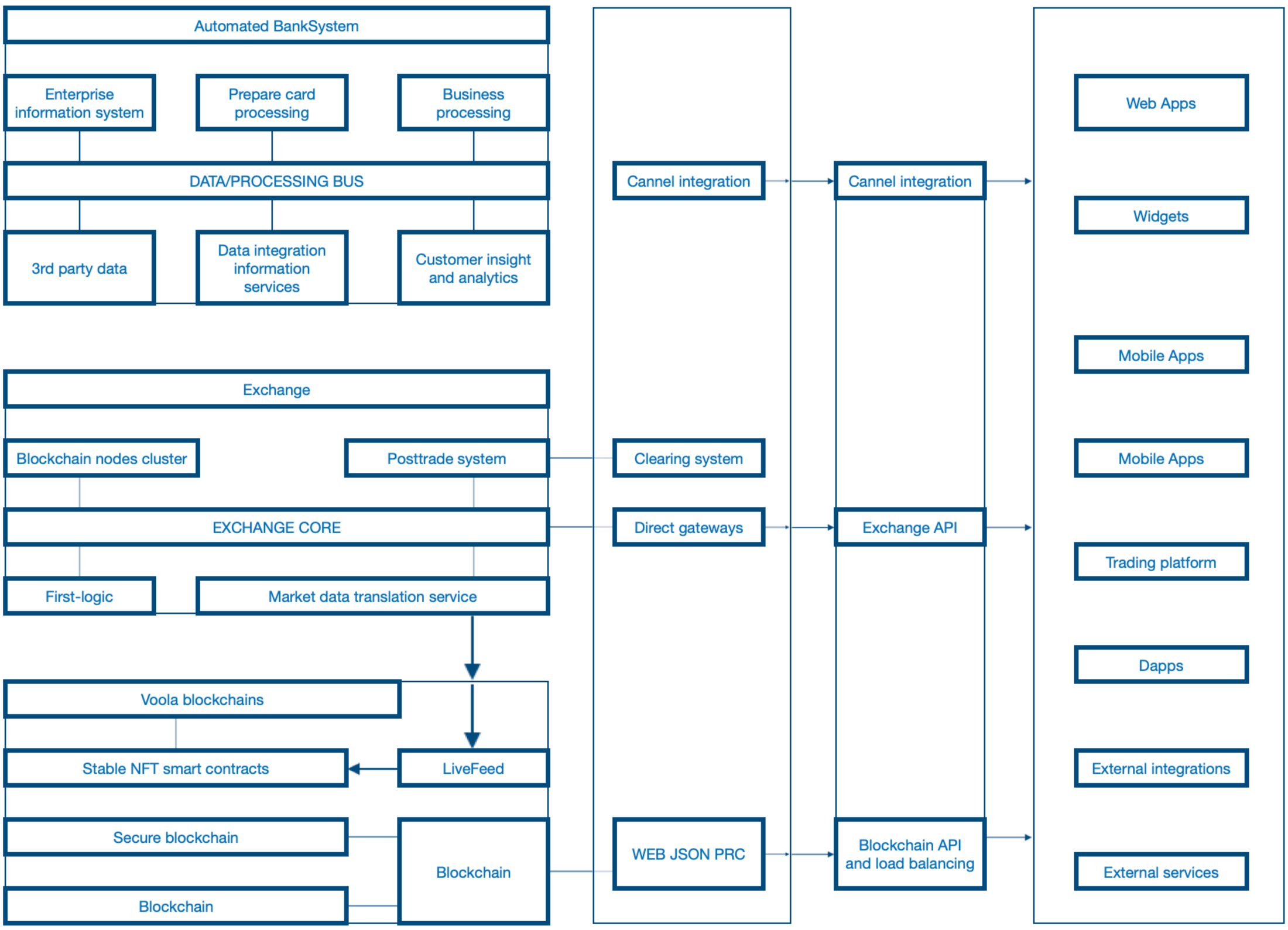
- Personal Account
- Anonymity
- Transactions on the Secure blockchain
- Create multi-currency wallets
- Connect an anonymous virtual and plastic card
- Unrestricted exchange of the Crypto-currency
- MultiSig wallet
- Cold wallet
- Investment & automated trading
- Business Account
- Acquiring
- Exchange of the cryptocurrency & fiat MultiSig wallet
- Cold wallet
- Deposits
- Automated trading

Why blockchain?

Trust has been a significant hindrance to personal dealing, transactions, and negotiation. Hence blockchain seems to be the solution since it guarantees a safe and secure deal yet in a decentralized ecosystem. It is understood that trust is a major element of business transactions when two parties engage in an agreement to swap value. And this trust is solving not only by financial tasks but social, resolving relationship with individuals. By adding this digital tangibility, the blockchain which is a trust- less technology could become the technology on which to build the tools to automate trust.

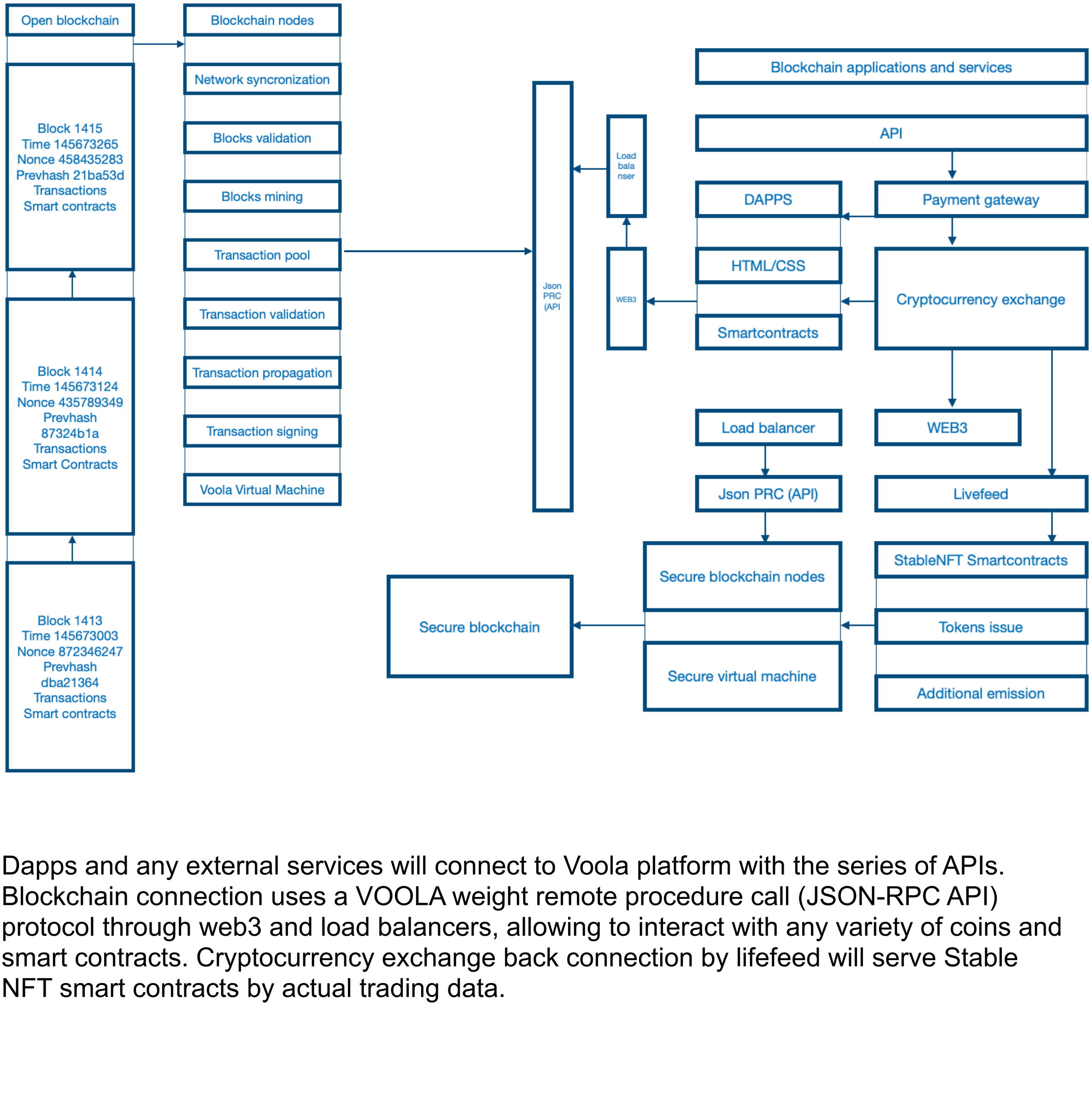
The shift in scale could be compared to the one caused by driverless cars. If there is no more need for a driver, there could be cars everywhere, flowing faster and more efficiently. The blockchain is what would enable these driverless transactions.

Main ecosystem



Own Blockchain planned structure

IT infrastructure



Dapps and any external services will connect to Voola platform with the series of APIs. Blockchain connection uses a VOOLA weight remote procedure call (JSON-RPC API) protocol through web3 and load balancers, allowing to interact with any variety of coins and smart contracts. Cryptocurrency exchange back connection by lifefeed will serve Stable NFT smart contracts by actual trading data.

Voola blockchain network

Blockchain (Ethereum fork)
Estimated Network speed: 15-25 TPS

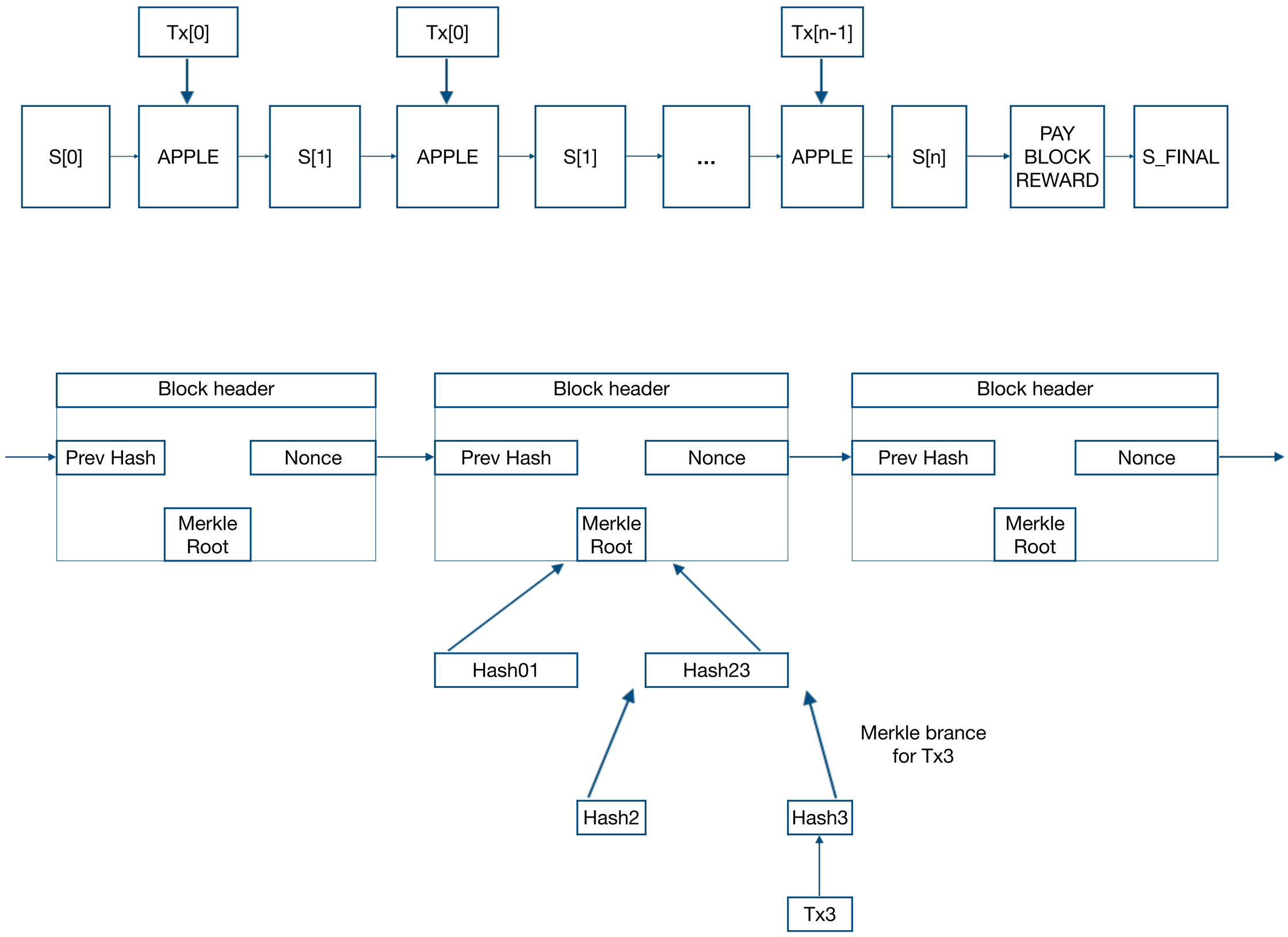
Private Blockchain
POA Ethereum fork Estimated Network speed: 250-500 TPS

Blockchain (Ethereum fork)
The purpose of our blockchain network is to develop an alternative protocol for building decentralized applications. It presents a set of solutions that will be very useful for a wide class of decentralized applications. The development solution will be suitable in situations where fast development time, safety for small and rarely used applications, and the ability of various applications to interact efficiently are priority. Voola network does this by creating the ultimate abstract foundational layer; a blockchain with a built-in Turing-complete programming language, letting anyone write smart contracts and decentralized applications. It will allow them to form their own arbitrary rules for ownership, transaction formats, and transition functions

VOOLA Secure blockchain network

The VOOLA Secure blockchain includes all advantages of the VOOLA blockchain, with the goal of providing secure in-chain services for the business. On the base of VOOLA Secure blockchain, we will launch Stable tokens smart contracts, KYC data storage, and a wide specter of business Dapps

Block architecture



The VOOLA blockchain is in many ways comparable to the Bitcoin blockchain, although it does have some enhancements. The main difference between VOOLA and Bitcoin concerning the blockchain de- sign is that, unlike Bitcoin (which only contains a copy of the transaction list), VOOLA blocks includes a copy of both the transaction list and the most recent state. Aside from that, two other values, the block number, and the difficulty are also stored in the blocks.

Block architecture

A Merkle tree in common sense is a way of hashing a large “chunk” of data concurrently which relies on dividing the chunks into containers, where each container contains only some chunks, then taking the hash of each container and repeating the same process, continuing to do so until the total number of hashes resting becomes only one: the root hash.

Every block header in VOOLA blockchain contains not just one Merkle tree, but three trees for three kinds of objects:

- Transactions
- Receipts (essentially, pieces of data showing the effect of each transaction)
- State

This allows for an extremely advanced VOOLA client protocol that allows VOOLA clients to inquire and get valid responses to various kinds of queries:

Code Execution and types of stored data

The code in smart contracts is written in a low-level, stack-based bytecode programming language, introduced as “VOOLA virtual machine code” or “LVM code.” The code consists of a sequence of bytes, where each byte represents an operation. In common, code execution is an endless loop that comprises of repeatedly carrying out the process at the current program counter (which begins at zero) and then incrementing the program counter by one, until the end of the code is reached or an error or STOP or RETURN instruction is identified. The operations have access to three types of space in which to store data:

The stack, a last-in-first-out container to which values can be pushed and popped - Memory, an infinitely expandable byte array

The contract’s long-term storage, a key/value store. Unlike stack and memory, which reset after computation ends, storage persists for the long term

The code can also access the value, sender, and data of the incoming message, as well as block head- er data, and the code can also return a byte array of data as an output.

The regular execution model of the LVM code is straightforward. While the VOOLA virtual machine is operating, its complete computational state can be defined by the tuple (block_state, transaction, mes- sage, code, memory, stack, pc, gas), where block_state is the global state holding all accounts and involves balances and storage. At the start of every cycle of execution, the current instruction is found by taking the pc-the byte of code (or 0 if pc >= len(code)), and each instruction has its meaning regarding how it affects the tuple. For example, ADD pops two items off the stack and pushes their sum, decreases gas by 1 and increases pc by 1, and SSTORE pops the top two items off the stack and injects the second item into the contract’s storage at the index specified by the first item. Although there are many ways to optimize VOOLA virtual machine execution via just-in-time compilation, easy implementation of VOOLA can be made in a few hundred lines of code.

Specifications

Network name: VOOLA
Programming language: Golang
Algo: Dagger Hashimoto / Ethash
Consensus algorithm: POW
Block reward: 0 (adjustable via hard fork)
Block time: 10 seconds
Network speed: 15-25 TPS
HTTP RPC server port: 8545
Websocket RPC server port: 8546
Network listening port: 30303
Network ID: 775
Chain ID: 775 (EIP 155 Replay Attack Protection compliant) Geth 1.8.14 fork including all last EIPs

Network name: VOOLA Secure Programming language: Golang Algo: Dagger Hashimoto / Ethash Consensus algorithm: POA

Block reward: 0
Block time: 5 seconds
Network speed: 250-500 TPS
Geth 1.8.14 fork including all last EIPs

POW Consensus

The specific proof-of-work algorithm that VOOLA uses are called ‘ethash’.

For each block of transactions, miners need to repeatedly and very fast calculate answers to a puzzle until one of them wins.

More particularly, the miners will run the block’s unique header metadata (including timestamp and software version) through a hash function (which will return a fixed-length, combined string of numbers and letters that looks random), only changing the ‘nonce value,’ which affects the resulting hash value.

If the miner discovers a hash that matches the current target, the miner will be granted coins the block across the network for each node to approve and add to their copy of the ledger. If miner B obtains the hash, miner A will stop work on the current block and start the process for the next block.

POA Consensus

By POA consensus algorithm, transactions and blocks are validated by approved accounts, known as validators. PoA consensus an optimized Proof of Stake model that leverages identity as the kind of stake rather than staking tokens. POA uses identity as the sole verification of the authority to validate, mean- ing that there is no requirement for use mining. POA security is centralized in the form of the authority node, so its suitable for business blockchain model.

Cryptocurrency exchange blockchain integration

Voola platform evolution will include own cryptocurrency exchange. We are planning to make extensive integration of cryptocurrency exchange with our blockchains, atomic Swap and VOOLAning Network implementations.

An Atomic Swap is an advanced feature in cryptocurrencies that allows for the exchange of one cryptocurrency for different cryptocurrency without the need for a trusted third party. An atomic Swap system can use a hash time-locked smart contract so that a party must deliver the currency to within a defined time, or else the transaction.

The use of VOOLAning Network is another feature to be used in exchange developmen. The payment channels permit participants to transfer funds to each other without having to perform all their transactions public on the blockchain.

Cryptocurrency exchange

Cryptocurrency Exchange is an online platform most common way to trade cryptocurrencies. They can be observed as an online marketplace for the entire cryptocurrency network.

Cryptocurrencies and blockchain are decentralized by nature, so this allows for the exchanges to also be decentralized. A decentralized cryptocurrency exchange (DEX) skips out the middleman by pro- ducing a highly intelligent “trustless environment.” Transactions are made within smart contracts and atomic swaps so that currency never passes through the hands of an escrow service.la.

The decentralized trading platform offers an alternative and more valuable service, by ensuring greater security and transparency. Its do not rely on third-party services to hold customer funds. Alternatively, peer-to-peer transactions are possible through an automated process.

Currently, the most extended version is hybrid: they retain some centralization to keep up transaction speed but store transactions on blockchain-based smart contracts.

The hybrid exchange is a semi-differentiated order-matching protocol. All incoming orders and trans- actions are encrypted, fixed by time and stored in a chain of blocks, and order coordination is made outside the network. The decentralized data on orders and transactions allows for transparent pricing and transaction reliability. The centralization of the order pool and their association allows achieving scalability without restrictions and locks.

Security of the Crypto Purchase Process

Our exchange will have an escrow system where the sellers' coins are held until the buyer sends the payment. This guarantees the seller's and the buyer's security throughout the purchase process. Without this system that exchange provides, it would be impossible for cryptocurrency trade to take place. That's because there would be no way for buyers and sellers to guarantee each other's transaction security.

Security will be provided at every level of the platform.

Our proof of work based blockchains having the high level of security, by using protected cryptographic keys. Only leaking of the private keys, as a human factor, can lead to funds lost.

The complete historicity and transparency of transactions on our blockchains provide a guaranteed lack of any malicious manipulation.

Complex monitoring system jointly with load balancing protects against any platform failure

Scalability

Scalability correlates with the ability of an exchange to handle the new influx of traders on their platform. Exchanges must grow as user bases expand, even if that growth rate is higher than expected.

A fully decentralized on-chain handling of exchange liveliness is limited in its scaling opportunities. With expanding scalability of blockchains, scalability of hybrid exchanges, in theory, is endless.

Order book

An order book is the table of orders that exchange uses to record the interest of buyers and sellers in a particular asset or token. Orders are executed when prices match, and the market price is determined. Transaction speed is directly related to the type of order book an exchange does. There is a notable speed difference between hosting interactions on the blockchain or off the blockchain.

The exchange is dependent on protocols regarding speed, prices and the variety of tokens they can offer. A protocol is a set of rules and guidelines for communicating data-in this case; it is about communicating purchasing and selling intentions

Liquidity

Like in equity trading, liquidity is a distinguishing feature of crypto markets. It refers to the extent to which a market allows assets to be bought and sold at stable prices. Lower liquidity tends to result in a more volatile market (especially when large orders are placed). But generally speaking, assets with less liquid- ity appreciate faster than more liquid assets due to the imposed limits on the interchangeability of the asset itself. Higher liquidity creates a less volatile market in the short term.

The main challenge for all exchanges is to provide sufficient liquidity for a cryptocurrency to reduce volatility.

Liquidity scenario

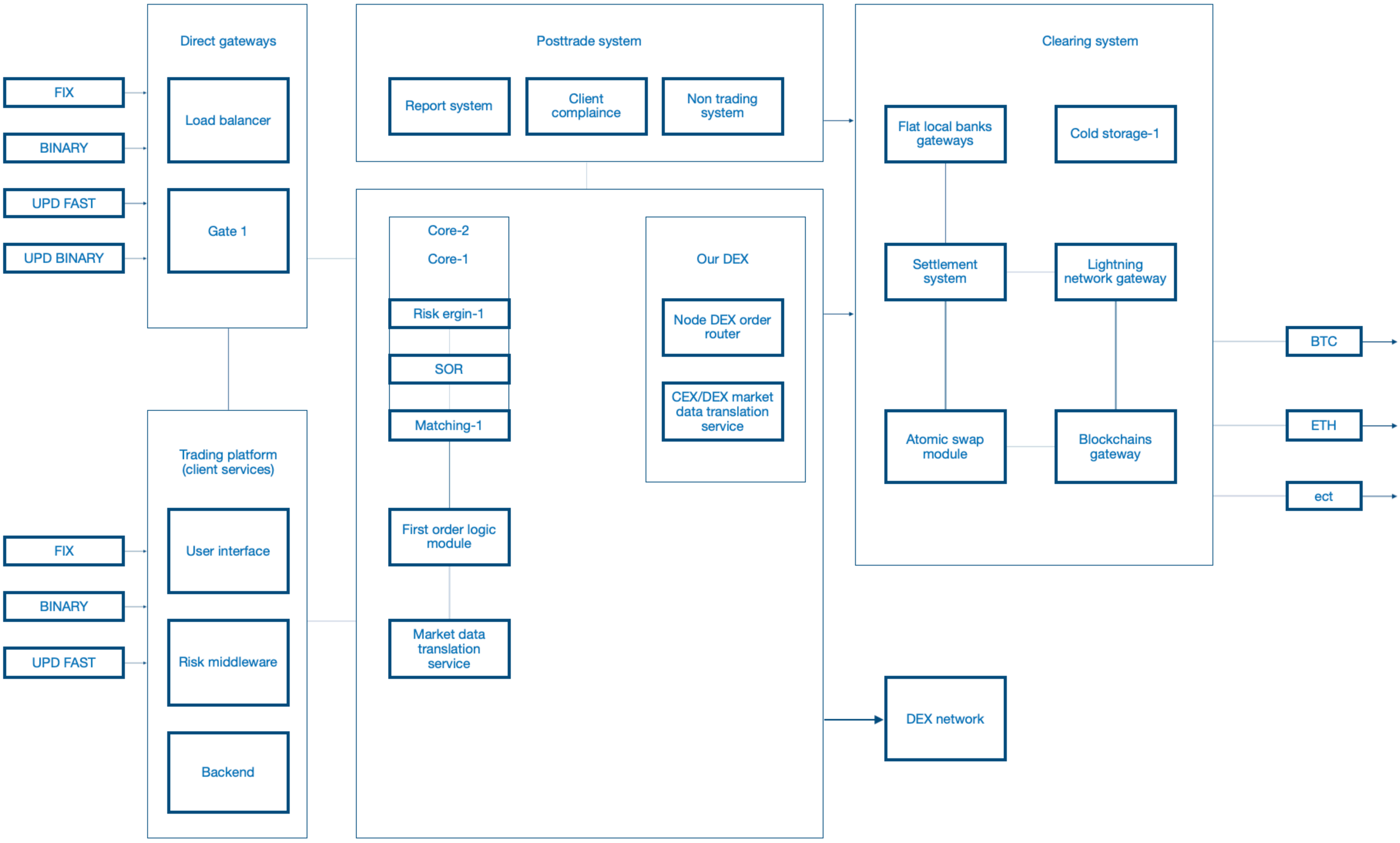
Wide ranges of businesses, from the small to a big one, will be able to issue cryptocurrency tokens on the VOOLA Secure blockchain. The goal of tokens issuance is to let businesses risk-free join the world of cryptocurrencies, earn money, and finally - to stabilize tokens price. Emission and additional emission of tokens will be available by smart contracts. Tokens burns, as a special contract function, will be also available. The decision to burn tokens will be made by the business itself.

The initial price of tokens will be about 70-80 cents of the final price. As soon as all tokens are distributed, the price is fixed at 1 dollar level and all investors (tokens buyers) will get its immediate interest. They can exchange tokens at 1:1 rate to USD, exchange for any available cryptocurrency. Also, it will be possible to buy some kinds of exclusive product, on sale only for tokens, get some private discounts (up to 30- 40%). All cryptocurrencies acquiring will be processed by Voola platform.

Liquidity reserve

To accelerate transactions, the exchange uses reserve wallets with exchange trading operations coins. These funds are used to maximize the speed of exchange transactions across all coins. Users initiate a trade transaction with the most favorable price. On the side of the exchange, all variations of trading operations are miscalculated to maximize the benefit of both the user and the exchange itself, using First-order logic module (Atomic logic). The exchange generates a reverse transaction in the exchange currency instantly, as soon as all conditions are met. As a result, a high transaction speed is achieved, the payout delay becomes minimal, and the exchange rate effiiency tends to the maximum.

Exchange architecture



Hybrid exchanges should be the golden middle that will combine the advantages of a centralized exchange, such as cooperation with large investors and the trust of many users with the benefits of a decentralized exchange, such as secure storage and the absence of subordination to a higher authority.

Migration from ERC20 token to own blockchain

In the case of Voola tokens is on the Ethereum blockchain as an ERC20 token and those various stakes in coins will need to be allocated to the new own blockchain.

The mainnet means Voola can now begin to allow individuals and businesses can now start to develop, host, and execute any decentralized apps and conduct transactions on the Voola platform.

Due to the same address space at Ethereum blockchain and VOOLA blockchain network, all holders of ERC20 tokens will get the equal quantity of the VOOLA blockchain coins right start of mainnet. So exchange rate will be 1:1. All coins will be pre-allocated via genesis block of the VOOLA blockchain.

{
“alloc”: {
“3282791d6fd713f1e94f4bfd565eaa78b3a0599d”: { “balance”:
“133700000000000000000”
}, “17961d633bcf20a7b029a7d94b7df4da2ec5427f”: {
“balance”: “2294270000000000000” },
“493a67fe23decc63b10dda75f3287695a81bd5ab”: {

DEX NETWORK

“balance”: “880000000000000000000” },
“01fb8ec12425a04f813e46c54c05748ca6b29aa9”: { “balance”:
“259800000000000000000”

Every time we will fire up VOOLA mainnet node, it will recreate this zero genesis block and all those initial transactions to those token holders.

So, if you invested in Voola in the ICO phase or while it was an ERC20 token, you will not need any ac- tions to get mainnet coins. You can access them using your Ethereum address private key or JSON-file.

KYC data storage

We are required to verify and identify their clients to comply with Anti-Money Laundering (AML) laws and regulations. This process called Know Your Customer (KYC). The special smart contract will be deployed at VOOLA Secure blockchain to store all KYC data. Its hash will store all file data. Internal audit and regulatory compliance will be used for the VOOLA Secure blockchain.

The process:

1. Whenever a new customer enters into the ecosystem, the ‘Trusted Party’ verifies the documents.
2. Once checked for veracity, its uploads this data onto the blockchain
3. Whenever any new data is needed to be appended, the ledger could enable encrypted updates to the ledger.
4. Other entities can access these updates in real time as and when required.
5. A Digital Identity - analogous to a digital passport - of the on-boarded customer can then be used for future operations.

StableNFT tokens for business

A StableNFT token is a ERC-721 token that keeps a stable value against a specific index like the price of one US Dollar. The VOOLA Secure blockchain will be used to issue StableNFT tokens, a fault-tolerant system with fast and reliable transactions.

These stable tokens can be used as a cryptocurrency aside, so you can buy and transfer money with it.

Custom clients tokens

We will enable individuals and companies to create their token as well. Using the tools provided by us, users will be able to create their tokens conveniently. These tokens will be accepted as usual currency, like USD, but will provide additional promo advantages and discounts. The terms of the issue will be negotiated individually with all clients. There is a lot of other smart contracts functions available for clients: additional tokens issuance, tokens burn, mass token distribution, etc. All clients smart contracts will be provided free of charge.

How secure is tokens ownership?

When you use a VOOLA Secure token, you trust the VOOLA Secure technology and yourself with the way that you store your private key.

The value is guaranteed by the robustness of the game theoretical financial mechanism that includes an ecosystem of traders, arbitrageurs, hedgers, index providers, laws enforcers, etc. You also usually trust the exchange that gives you access to these assets.

VOOLA Secure aims at leveraging blockchain technology to replicate market mechanisms on-chain, issuing StableNFT tokens backed by a game theoretical mechanism that runs in a trustless fashion

Payment machine for merchants

A Stable token is a crypto-token that keeps a stable value against a specific index like the price of one US Dollar. The VOOLA Secure blockchain will be used to issue stable tokens, a fault-tolerant system with fast and reliable transactions.

These stable tokens can be used as a cryptocurrency aside, so you can buy and transfer money with it.

Custom clients tokens

VOOLA will enable users to make direct payments for goods purchased at their favorites stores by simply using their Voola Pay mobile Wallet (IOS / Android). For this purpose, VOOLA will offer the option to provide merchants with NFC-enabled payment machines that will accept payments made with the Voola Pay mobile Wallets.

After creating their VOOLA account, merchants will be able to order the payment machine from the VOOLA website. Each machine will already have Voola Pay mobile Wallet integration, so, to use the machine, all the merchant will have to do is to start it.

Also, a unique app will be designed for small business to let them accept payments of Stable tokens through an IOS or an Android device.

How secure is tokens ownership?

When you use a VOOLA Secure token, you trust the VOOLA Secure technology and yourself with the way that you store your private key.

The value is guaranteed by the robustness of the game theoretical financial mechanism that includes an ecosystem of traders, arbitrageurs, hedgers, index providers, laws enforcers, etc. You also usually trust the exchange that gives you access to these assets.

VOOLA Secure aims at leveraging blockchain technology to replicate market mechanisms on-chain, issuing StableNFT tokens backed by a game theoretical mechanism that runs in a trustless fashion

Payment machine for merchants

VOOLA will enable users to make direct payments for goods purchased at their favorites stores by simply using their Voola Pay mobile Wallet (IOS / Android). For this purpose, VOOLA will offer the option to provide merchants with NFC-enabled payment machines that will accept payments made with the Voola Pay mobile Wallets.

After creating their VOOLA account, merchants will be able to order the payment machine from the VOOLA website. Each machine will already have Voola Pay mobile Wallet integration, so, to use the machine, all the merchant will have to do is to start it.

Also, a unique app will be designed for small business to let them accept payments of Stable tokens through an IOS or an Android device.

VOOLANET Pay Wallet

The VOOLA Pay Wallet is a digital wallet in which you can store all your tokens based on the VOOLA network. Each VOOLA Pay Wallet has a private key and public key. While the secret key should never be shared with anyone, the public key is the address that you should give when you want to receive funds. It is important to note that if you lose your secret key, you will not be able to recover it. So any funds will be stored by using a private key on a client side.

More than 150 cryptocurrencies and all platform tokens will be accessible via VOOLA Pay Wallet, for Fiat-related converting operations and trading. Users will be able to send and receive coins and any assets between each other. KYC will be required to pass initial transactions limits.

Users can create personal and business accounts on the wallet. The main difference is the business will use a multisignature keys to create an account. Multisignature will use flexible logic, configurable at the registration stage. It will include founder’s quantity, timelock features, withdrawals logic/limits, etc.

The VOOLA Pay Wallet app will be available on iOS, Android, Windows, Mac and Linux systems.

The VOOLA Pay Wallet can also be linked to your Voola card wallet address so that you can see your credit card balance directly from your VOOLA Pay Wallet.

Voola Card

To make cryptocurrencies and StableNFT tokens usable everywhere even in places where crypto-currencies are not accepted, we will offer a reloadable virtual prepaid credit card to all the user using our web and mobile wallets. Issued virtual card with enabled NFC smartphone connectivity will allow making payments everywhere in the world.

Customers services for our card users

Customer service is a significant added value that we want to provide to its users. So, we take pride in meeting the needs of our customers. Regardless of their location or time zone, we offer 24-hour customer support, and we are ready to go the extra mile just to put a smile on their face.

Technical issues of Blockchain Scalability

One common concern about VOOLA blockchain is the problem of scalability. Like Bitcoin, VOOLA blockchain suffers from the flaw that every transaction needs to be processed by every node in the network. With Bitcoin, the size of the current blockchain rests at about 15 GB, growing by about 1 MB per hour. If the Bitcoin network were to process Visa's 2000 transactions per second, it would increase by 1 MB per three seconds (1 GB per hour, 8 TB per year). VOOLA is likely to suffer a related growth pattern, worsened by the fact that there will be many applications on top of the VOOLA blockchain somewhat of just a currency as is the case with Bitcoin, but enhanced by the fact that VOOLA full nodes need to store just the state instead of the entire blockchain history.

Transaction costs, network speed

Bitcoin currently has high transaction costs after being touted as 'nearly free' for the first few years of its existence.

As of late 2016, it can only process about seven transactions per second, and each transaction costs about $0.20 and can only store 80 bytes of data.