VeloxChain

CONNECTING URBAN MOBILITY ON BLOCKCHAIN

Veloxchain.io

Connecting Urban Mobility on Blockchain[1]

Version 1.8

Authors:
Smart Urban Technologies Pte. Ltd d.b.a VeloxChain

[1] The legal disclaimer at the end of the document.

1. Introduction

Ethereum[2] is a decentralized computing platform where users deploy smart contracts to perform computations. Nobody controls the Ethereum network and users completely control their own smart contracts - it is a trustless environment. This is a fantastic platform on which to build a decentralized ecosystem which uses smart contracts to process transactions.

One of the application areas for blockchain is Internet of Things (IoT). For example, BMW, General Motors, Ford and Renault[3] have launched their own blockchain research projects for the automotive industry, seeking to leverage IoT and blockchain technologies for a smart transport network.

VeloxChain is an open-source blockchain-based protocol and marketplace for shared mobility services. Our ambition is to democratise the sharing mobility market and accelerate the world's transition to an open and seamless mobility. We provide a one-stop solution for all participants in the ecosystem from developers, mobility providers and end-users, ultimately, benefiting from global network effects.

VeloxChain is empowered by several critical technologies:

1. Proof-of-stake Consensus with EVM-compatible smart contracts.
2. Enterprise Collaboration Solutions leveraging Zero-Knowledge Proof and cryptographic search algorithms.
3. Payment Channel and Revenue-sharing models.
4. Meta Transaction Relay Protocol
5. Vehicle asset tokenization developing from ERC721.
6. IoT in urban mobility industry

In the following sections we will explain our technologies in detail, beginning first with blockchain.

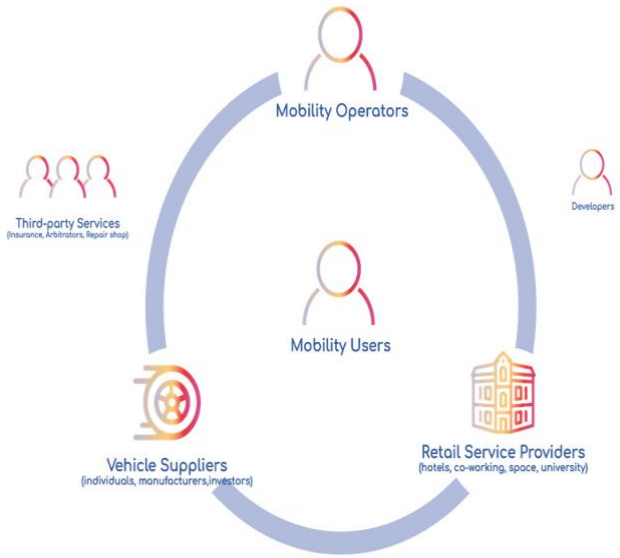
2.VeloxChain Core Products

2.1. VeloxChain Ecosystem

Shared mobility is gaining popularity around the globe. Mckinsey estimated that the combined market of shared mobility in China, Europe and U.S was nearly $54 billion in 2016, which could see 28 percent annual growth till 2030 (ref) in urban areas. Over hundreds of mobility solutions fiercely compete for market share. Incumbents like Uber, Didi, Ofo intensifies the competition, with smaller players and new entries face a huge gap in capital and technology to compete fairly with them. While users have greater choices to meet their mobility needs, it could be a daunting task to switch from one app to another to compare availability, resulting in fragmented user experience.

The global mobility market is too fragmented, centralised and unconnected, without a real network effect that benefits users from the expansion of the ecosystem. The centralised system creates a single point of failure, so users must be wary of their personal data privacy and deposit requirements. Proprietary software and data restrict integration with another system. Thus, it limits cooperation between mobility businesses, resulting in a fragmented user experience. We need a new decentralised collaborative business model for a healthier competition, for a more integrated, seamless travel experience and for stronger network effects that benefit the ecosystem.

VeloxChain project team is building a solution for these challenges. VeloxChain is an open, scalable blockchain-based protocol for sharing of urban mobility. Velox communicates the potential of decentralised collaboration. Our protocol enables mobility providers to offer vehicle sharing services while leveraging a global technology platform and a network of specialist



partnerships. Thus, it benefits those who use their services and produce network effects rapidly.

- For developers, creating decentralised apps for vehicle sharing has never been easier with our APIs, SDK and built-in modules of sharing-mobility services.
- For mobility providers, our decentralised collaborative network enables co-creation of vehicle sharing services that are seamless, smart and cost-effective. With Velox, anyone can offer shared mobility services by leveraging a global technology platform and a network of specialist partnerships. Moreover, our system could eliminate the need for third-party payment services, meaning faster and lower transaction fee. Revenue sharing is automated using smart contracts, ensure everyone gets a fair share of created value. While blockchain is about trust and transparency with immutable data that is open to the public. Our decentralised collaboration solution has also been designed to meet the needs of confidentiality and anonymity. All sensitive data can be encrypted using Zero-knowledge proof, giving our full control over who gets to see the content of them.
- For users, our open mobility marketplace allows unified access to a variety of shared mobility services, offering a seamless travel experience without the hassle of switching apps and multiple accounts created. Not only users' mobility needs are met, but our cryptographic incentive mechanism can also increase the demand and customer loyalty.

We believe that our cutting-edge technology and team competence could achieve broad adoption and network effects benefiting all participants. VeloxChain intends to start with bike sharing and micro-mobility like e-scooters, Segway; other types of vehicles will be supported at a later date.

Our core products include:

- **Velox Protocol (VeloxChain):** an open public blockchain layer with some of the core technologies such as EVM-compatible smart contracts, Proof of Stake consensus, distributed data storage and zero-knowledge proofs. **Velox Token** is a native token of the VeloxChain ecosystem, acting as a store of value and

medium of exchange. Users can also hold and stake (deposit) Velox tokens to receive block rewards.

- **VeloxDEV:** An all-in-one solution for developers, making it easy and hassle-free for deployment of decentralised apps for mobility services on our VeloxChain.
- **VeloxBIZ:** A open marketplace platform with bundle solutions for mobility providers, vehicle suppliers, retailer service providers and developers to discover partners, establish partnerships, collaborate and co-create services. It includes some essential functionalities: vehicle and user registration, fleet management, a merchant marketplace, payment processing, fraud detection, credit scoring and distribution of revenue splits.
- **VeloxGO**: a DApp to connect users and mobility providers, allowing them access to a variety of transport modes to meet their demand under one account. Velox ecosystem intends to start with bike sharing and micro-mobility like e-scooters, segways prior to venturing into the sharing of cars and other vehicles.
    - *VeloxGo 1.0 - multi-modal mobility marketplace*: A DApp for users to configure and order mobility services and below are some key functionalities:
        - User Registration
        - Integrated payment Fiat and Crypto Wallet
        - Services marketplace: users search, configure and order from a list of preferred mobility services built on VeloxChain, with immediate access and streamlined payment in one account.
        - Interactive Mapping for location search, directions, and mobility options
        - Ratings and Review

      Together with the open marketplace VeloxBiz, VeloxGo 1.0 allows any mobility providers to launch bike-sharing, scooter-sharing or Segway easily. Moreover, the mobility providers are able to customize VeloxGo 1.0 to build their own sharing-mobility DApp.
    - *VeloxGo 2.0 - Seamless Intermodal mobility marketplace:* When Velox ecosystem works well in the bike-sharing and micro-mobility like e-

scooter and segways, We engage other sharing-mobility modals like car-sharing and public transport. As a result, we will launch VeloxGo 2.0 which allow users to search, book and pay for integrated mobility options. VeloxGo 2.0 offers people a seamless travel experience with affordable, green, on-demand mobility without the hassle of switching apps and multiple accounts created. The payment process backed by VeloxChain will be highly transparent and settled automatically, no matter how many different mobility services or transport modes people use along the journey. VeloxGo 2.0 is also open source and thus mobility providers can customize VeloxGo 2.0 to build their own seamless intermodal mobility DApp.

2.2. Market Structure and Go-to-market Strategy

There are 3 components of ride-sharing value chain, regardless of which mobility device we are talking about. These are: device supply, fleet operations and retail service. We will locate partners in each segment and encourage them to link up using our VeloxChain technology. Literally anyone can start a fleet service by linking up with appropriate suppliers and retail outlets.

A good example might be a guided Segway service catering for tourists in the town of Florence Italy. With VeloxChain, the fleet operator has lower capex and lower operating expenditure than they would incur otherwise.

Our Go-to-Market strategy is subject to where our clients are (in point 9). However, the very first market we can gain dominance status is in Bike/Scooter Sharing. We do not position ourselves as a bike/scooter sharing company, we develop the infrastructure for such companies to migrate their platform from centralized system to a more open and secured decentralized one to enjoy a great deal of benefits of the blockchain technology. We will rapidly explore partnership opportunity with other car sharing companies and gradually tap into the ridesharing/ride-hailing market by collaborating with small players who can customize and optimize their service at local level. (We can learn how Grab defeats the mighty UBER in Asia by quick market adaption strategy). In other words, local players are armed with global technology to offer the greatest value to their end customers.

Specifically, we will launch the protocol by Mid 2019 with strategic partners dapps for bike-sharing and scooter-sharing. Marketing budget will be spent towards acquiring new B2B-1 partners who already have proven experiences in the industry. By Mid 2020, the product development can reach to the point of car-sharing integration readiness, we will start to acquire customers in this $8.7bil market. By 2022, we attempt to hold 10% market share of both Bike and Car sharing market. At that turning point, we will need to make a strategic decision on whether scale our business by tapping into the Ridesharing/ride-hailing market or strengthen our dominance status in the market we developed.

There are several aspects to consider whether we can keep up with the grow of the new market because we can expect other competitors may focus on this section from the beginning. Therefore, such decision will lead us to either dominate the shared mobility market by holding at least 33% market share or become a tiny player in the new field.

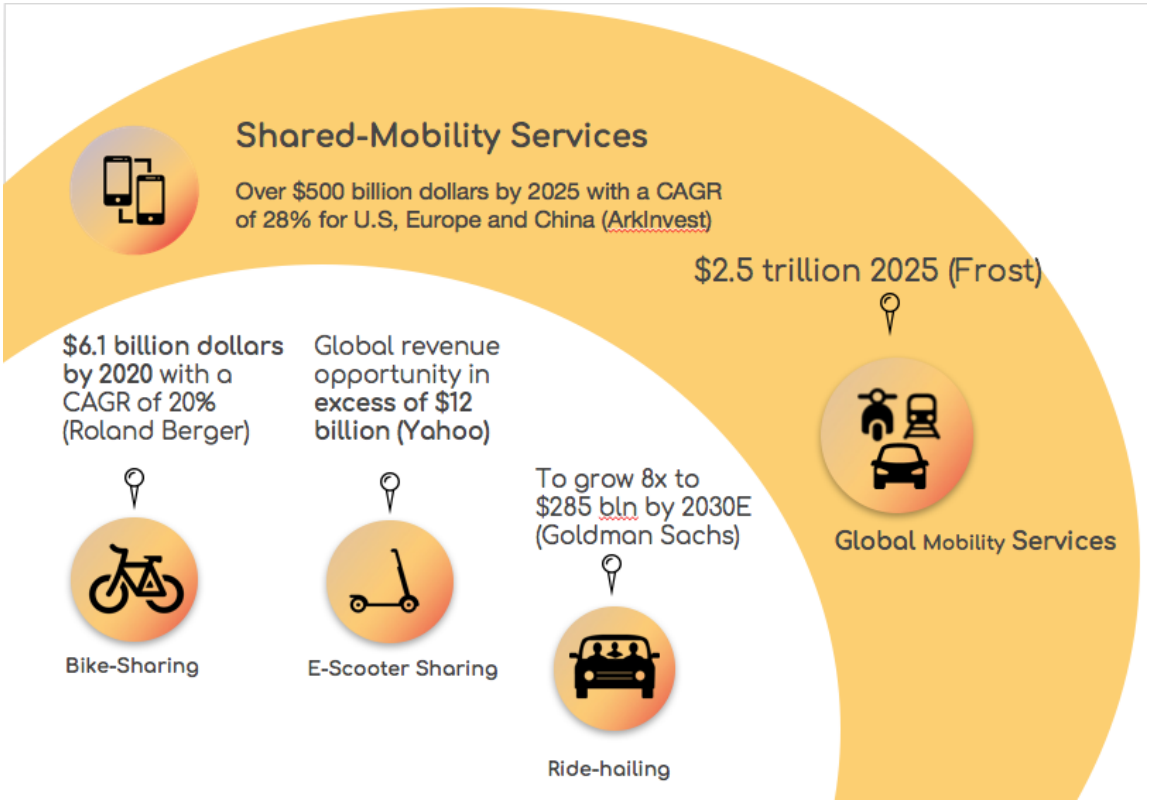


Figure 1 Global Shared-Mobility Market Structure (in U.S billion)

3. VeloxChain Technologies

Overall, there are five main layers in Velox Ecosystem:

- **Application Layer**: Besides VeloxGo and Velox Biz, there are significant numbers of sharing-mobility applications built on top Velox ecosystem such as bike-sharing, scooter-sharing, car-sharing. VeloxChain will provide SDK and firmware libraries to allow existing sharing-mobility application integrating easily.
- **Middle Layer**: there are SDKs and APIs allow third-party systems, IoT and smart vehicles to interact easily with the Velox Ecosystem.
- **Service Layer**: are distributed system hosted by Velox foundation or mobility providers. The service layers play as a “bridge” communication among applications and decentralised layer. In the bridge service layer, there are some core components:
    - Cache and indexing data module: allow the bridge server to sync data from decentralized layer and then index the data to provide faster search.
    - Order Queuing module: allow stakeholders to communicate with each other such as booking, accepting or cancelling a request. The queuing module can handle communication between users and vehicle providers, or among sharing-mobility service merchants
    - Meta Transaction Relay module: allow service layers to fuel gas of transactions or forward transactions to the decentralised layer.
    - Pricing and payment module: allow sharing-mobility service to use fiats or cryptocurrencies as payment methods.
- **Abstraction Layer**: are zero-knowledge of proof, keyword privacy-preserving search, payment channel smart contract- frameworks which enables seamless integration into the Velox Chain.
- **Decentralisation Layer**:

- Public blockchain protocol for the sharing-mobility industry: VeloxChain support with Ethereum Virtual Machine (EVM) smart contracts (solidity and viper), use Proof-of-Stake-voting consensus with over 1000 tx/s and 2 second block-time and have data privacy-preserving features, key management feature.
- Distributed storage layer: IFPS hosts to store public plain-text data while sensitive data are encrypted and stored in the distributed storage system.

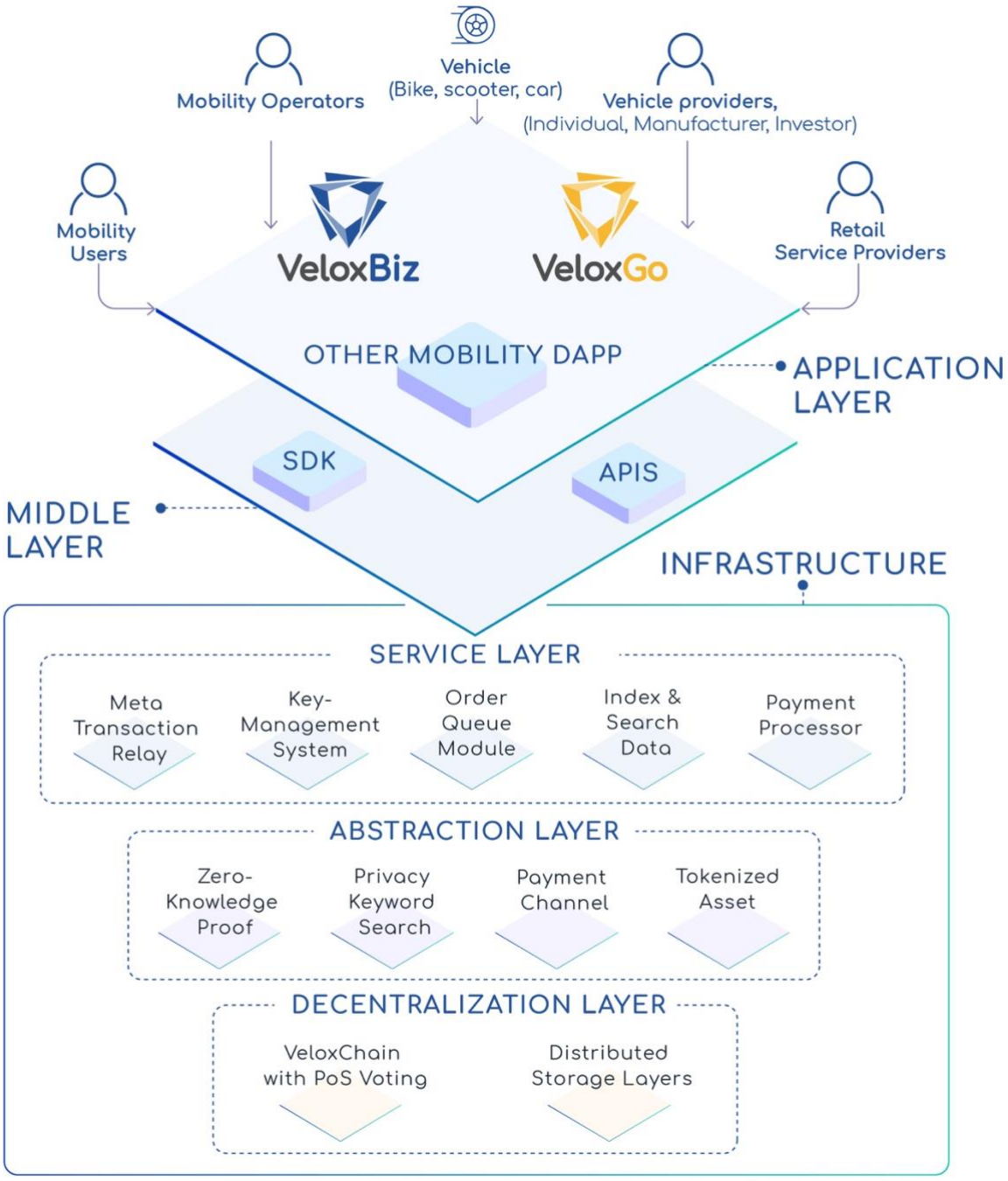


Figure 2. High-level Architecture of VeloxChain Ecosystem

Blockchain technology leads fuzzier APIs to allow more agile integration of new systems; however, public blockchain technology is still at the early stage and in order to meet rigorous end-user applications requirements such as low latencies, immediate transaction finality, high performance, excellent scalability and support multi-level of data privacy. At the time of writing, there is no existing blockchain solution to achieve planetary-scale with million transactions to serve almost

applications; Ethereum with less than 15 tx/s with 15 000 nodes[4] and delaying Ethereum's Casper (Proof of Stake) and Sharding until 2020[5], even Zilliqa blockchain with sharding solution only archives 2488 tx/s with 3600 nodes or EOS archives 3097 tx/s[6] with Delegated Proof-of-Stake and 21 block validators.

Therefore, we run Velox Protocol to decentralize and connect sharing-mobility applications as the public blockchain for a vertical industry. Velox Protocol supports with Ethereum Virtual Machine (EVM) smart contracts (solidity and viper), use Proof-of-Stake-voting consensus and have privacy-preserving collaboration features, key management feature, pricing models, fault-detection modules, incentive shared-mobility modules.

3.1. Proof-of-stake Blockchain with EVM-compatible smart-contracts

In our view, Ethereum has the largest community of developers of decentralized applications with various development tools. Therefore, VeloxChain provides the same functionalities as standard Ethereum which allow Ethereum developers build DApps on VeloxChain with low learning-curve and Ethereum DApps easily interact with VeloxChain; this means that:

- VeloxChain uses Elliptic Curve Digital Signature Algorithm ECDSA)[7] to generate public-private keys and authenticate the signature. ECDSA uses the algebraic structure of elliptic curves over finite fields ($y^2 = x^3 + ax + b$). Similar with Ethereum, VeloxChain use a Koblitz curve secp256k1[8]:$y^2 = x^3 + 7$ (where a =0 and b = 7), it looks like this:

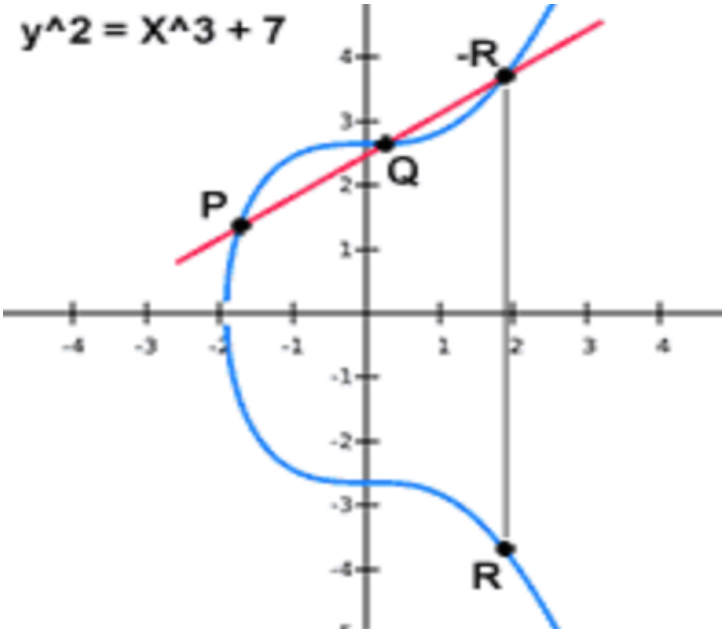


Figure 3. Koblitz curve secp256k1

- VeloxChain support for all EVM smart contracts (solidity and viper) and development tools, IDE, wallets and client software working with Ethereum chain.

It is widely accepted that a blockchain-based system is as secure and robust as its consensus model. The best consensus model will be one which best balances the following three following factors:

- Decentralization: Any node freely participates in processing transactions, and publishing a block without the use of a central authority or service.
- Security: The system has to prevent double- spends, keep data in sync. There are no conflicts when data get merged. All nodes see same data at the same time.

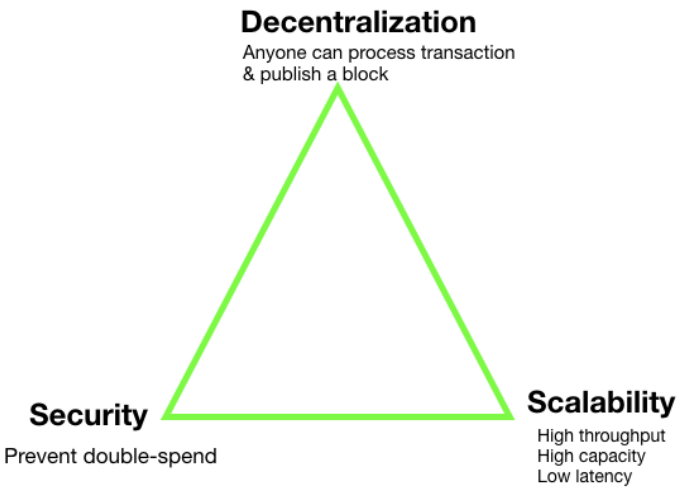


Figure 4. Three crucial factors of blockchain consensus algorithms

- Scalability: The system has to provide sufficient transaction throughput to serve enterprise-scale or even planet-scale needs, especially when the network size increases.

Following is a table listing different types of consensus algorithms, and highlighting the strengths of each.

	Types of Consensus				
Features	**PoW**	**PoS**[9]	**PoET**	**BFT * and variants**	**Federated BFT**
Blockchain Type	Permission-less	Both	Both	Permissioned	Permission-less
Blockchain	BitCoin, Ethereum	TomoChain, EOS, Omisego	Intel Ledger	Hyperledger Fabric	Ripple & Stellar
Transaction finality	Probabilistic	Probabilistic	Probabilistic	Immediate	Immediate
Transaction rate	Low	High	Medium	High	High
Scalability of peer network	High	High	High	Low	High
Trust model	Untrusted	Untrusted	Untrusted	Semi-trusted	Semi-trusted
Adversary Tolerance	<= 25%	Depends on specific algorithm used	Unknown	<= 33%	<=33%

* Note: BFT is Byzantine Fault Tolerance

Figure 5. A comparison of blockchain consensus mechanisms

Inspiring by TomoChain consensus[10], VeloxChain uses the PoS with on-chain governance philosophy of design which achieves the best balance of three factors above. With PoS, VeloxChain has a 2-second block time with over 1000 tx/s and provides a good security by leveraging the economic-game theory.

We believe that PoS with on-chain governance features provide more decentralized ecosystem and fairness distribution of value among stakeholders who takes responsibilities for development of the ecosystem. For example:

- **Masternodes** deposit Velox token to become a full-node to create, verify and validate a new block. Masternodes earn a significant portion of block reward and transaction fees.
- **Voters** are Velox token holders who participate in governing the chain by deposit token and voting someone becoming a masternode. As the result, the voters will also receive Velox tokens when their candidates become the masternodes and proceed transactions

Moreover, VeloxChain aims to connect sharing-mobility services and thus a small portion of block reward are distributed to the VeloxChain community wallet which will support sharing-mobility applications and incentivise users to use sharing-mobility service.

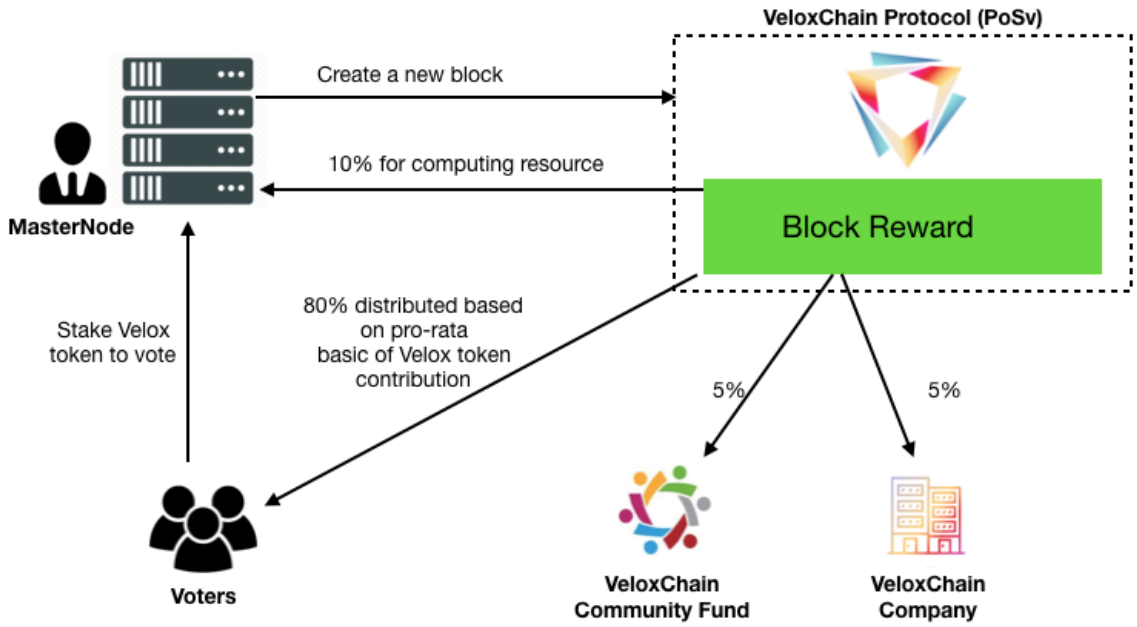


Figure 6. Token distribution among stakeholders in Veloxchain PoSv

Using Proof-of-Stake-voting, VeloxChain sacrifices some decentralization to achieve high transaction throughput. Sharding[11], however, is the most promising solutions to provide full-decentralized ecosystem. Sharding divides the chain into small groups (shards) for parallel transaction processing, to increase transaction throughput of the whole blockchain ecosystem. In addition, Plasma sidechains such as Loom network[12] with DPOS and interoperability blockchain projects like Cosmos[13] and Polkadot[14] are also potential solutions to improve decentralized features. VeloxChain actively embraces these promising scalability solutions.

3.2. Privacy-preserving Collaboration Solutions

Data on a blockchain is stored in a "distributed" ledger of records and is immutable. That is, once recorded, data cannot be changed retroactively without the alteration of all subsequent blocks and a collusion of the network majority. Immutability is a powerful feature of blockchain technology, but it comes with a compromise - all data is public. Although blockchain is an open and semi-anonymous system, someone can discover and trace the actors behind a transaction.

We believe that in the fleet services context, vehicle suppliers, fleet operators and retail service providers do not want disclosure of their commercial information. Merchants want privacy for things like supplier relationships and costs. Similarly, in the P2P context, riders and vehicle owners do not want to their data exposed without their permission.

Therefore, confidentiality for data is a fundamental requirement for the VeloxChain ecosystem. We design anonymous collaboration layers to hide the real identity and a cryptographic search engine modelled by smart contracts to manage and share sensitive data.

3.2.1. Anonymous Collaboration Layer with Zero Knowledge Proof

Anonymous Collaboration Layer allows merchant A and merchant B to prove their collaboration anonymously by the merchant A obtains a credential from the merchant B so that at some later point in time, the merchant A is able to construct a non-interactive proof of his credential to perform authenticated transactions. The VeloxChain masternodes accept the request only if the attached proof is valid. The

design of the component is inspired by the idea of Zerocoin[15] with Zero Knowledge Proof technique.

The following example describes how the anonymous collaboration layer works in practice. Let's suppose that there is a public bulletin board, one which is physical and everyone can access. There are two actors in the merchant market platform **VeloxBiz**: the bike-sharing fleet operator A collaborate with the scooter fleet operator B that the scooter-sharing fleet operator B provides his scooter asset to the bike-sharing fleet operator A and then the bike-sharing fleet operator A can provide multi-modal services (bike-sharing and scooter-sharing). In this scenario, the bike-sharing fleet operator A which plays the role of a data consumer and the scooter-sharing fleet operator B who plays the role of a data owner.

To produce a new credential for the bike-sharing fleet operator A, the scooter-sharing fleet operator firstly generates a pseudonym S for the party A and commits Susing a secure digital commitment scheme. The resulting commitment C can be opened using a random number r known by the party A. The party B pins C to the bulletin board, there is a set $S_C = (C_1, C_2, \ldots C_n)$ of commitments in the board. At a later point, the party A is able to prove possession of such credential by producing two statements in zero-knowledge:

- He knows a commitment $C \in S_C = (C_1, C_2, \ldots, C_n)$.
- He knows the opening r for the commitment.

The VeloxChain is used as a public bulletin board. Both the data owner and data consumer are able to access the public parts of the data stored on the blockchain. The public parts contain the commitments that we have described.

We now present a concrete construction using cryptographic accumulator proposed by Josh Benaloh[16], and later improved by Jan Camenisch[17]. The accumulator scheme comprises four algorithms:

- $AccumSetup(\lambda) \rightarrow params$. Generates two primes p, q, computes $N = pq$, sample $u \in QR_N$. Output (N, u) as the parameters.
- $Accumulate(C) \rightarrow A$.On a set of primes $C = \{c_1, \ldots, c_n\}$, outputs accumulator $A = u^{c_1 \cdots c_n} \bmod N$.

- $GenWitness(v, C) \rightarrow \omega$.Input a prime number $v \in C$, outputs a witnessK$\omega = Accumulate(C - v)$.
- $AccVerify(\omega, v, A) \rightarrow \{0,1\}$.Verifies $A = \omega^v \, mod \, N$The security of the scheme is based on the harness of Strong RSA and Discrete Logarithm assumptions.

The description of the anonymous authority layer consists of four algorithms:

1. $Setup(1^\lambda) \rightarrow params$. On the input parameter λ, run the algorithm $AccumSetup(1^\lambda)$to obtain (N, u). Generate primes p, q such that $p = 2^w q + 1$for $\omega \geq 1$.Let G be the subgroup of $Z_q{}^*$and select two random generator g, h such that $G = [g] = [h]$.
2. $GenCred(S, params) \rightarrow (c, skc)$. Given pseudonym $S \in Z_q{}^*$, select a random $r \in Z_q$ and compute $c \leftarrow g^S h^r$such that c prime and $c \in [A, B]$, where $2 < A$ and $B < A^2$. Set $skc = r$ and output (c, skc), submit $c$to the blockchain.
3. $ShowCred(params, S, c, skc, Sc) \rightarrow \pi_S$ Given data consumer pseudonym S, a credential c and its secret key skc, compute $A = Accumulate\,(params, S_c)$ and $\omega = GenWitness\,(params, c, S_c)$ and output the following proof of knowledge:

$$\Pi_s = ZKSoK\{\,(c, w, r, S) : AccVerify((N, u), A, c, \omega) = 1 \wedge c = g^S h^r\}$$

4. $VerifyCred(params, \pi, S_c)$. Given a proof Π_S, and the public set of credential S_C, first compute $A \rightarrow Accumulate\,(params, S_C)$, then verify that Π_S is the aforementioned proof of knowledge on c, S_c. if the proof verifies successfully, output 1, otherwise output 0.

The zero-knowledge proof which appears in step 3 of the scheme is a non-interactive proof that only requires one round of communication. Camenisch presents an interactive zero-knowledge proof of knowledge in which an accumulator contains a committed value. The construction of the non-interactive proof in step 3 leverages a Fiat-Shamir transform on the interactive proof. This is shown in the process flow diagram on the following page.

The $Setup$ algorithm is performed by the data owner to generate system parameters. Next, when the data consumer wishes to obtain a credential for data access, he sends a request to the data owner together with his pseudonym S. At this point, the data owner runs the $GenCred$ routine on this input S to generate a digital commitment and its secret key skc.

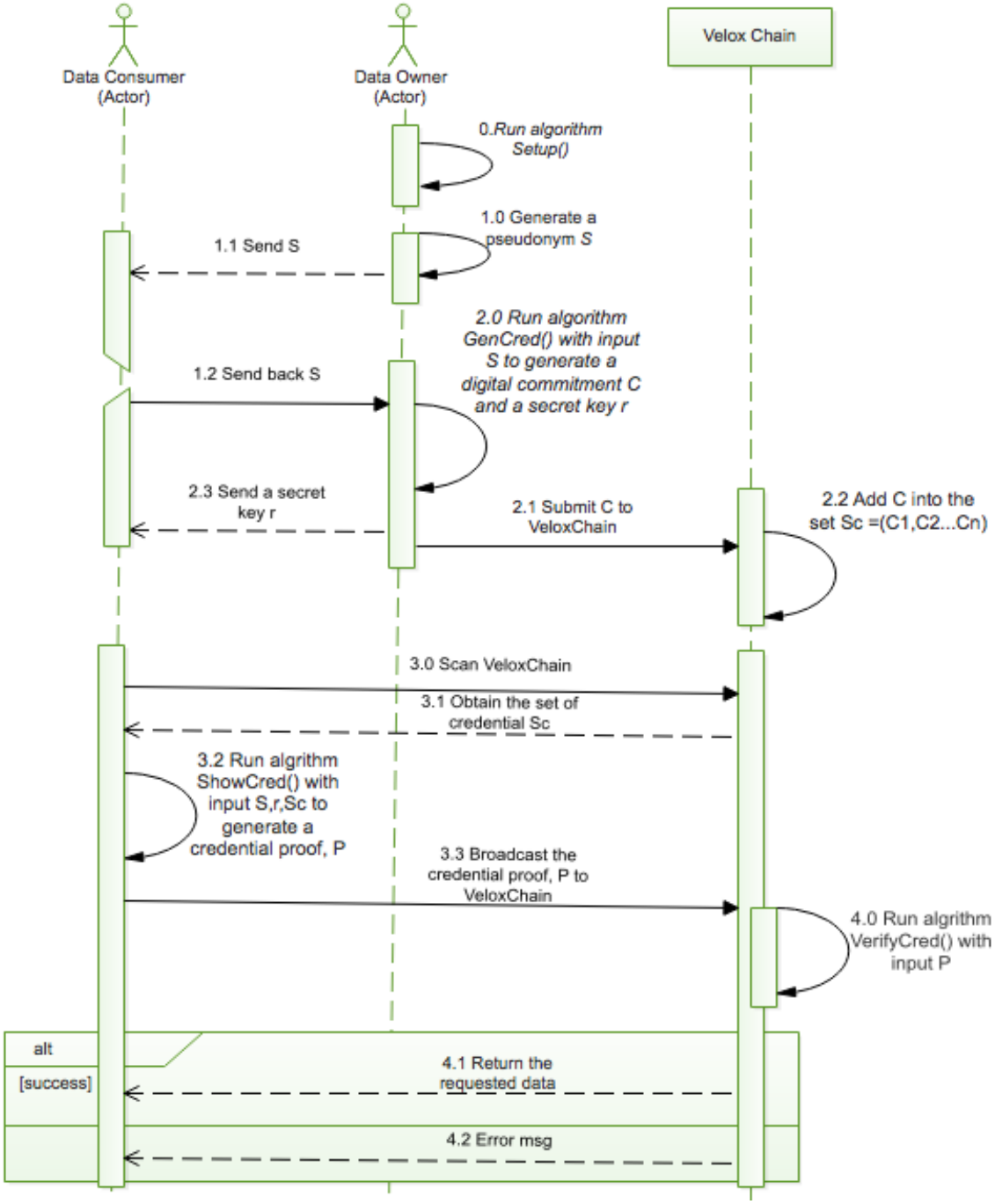


Figure 7. Sharing Data in the Anonymous Collaboration Layer

When the data consumer wishes to show his credential, he first scans through the VeloxChain to obtain the set S_c consisting of all credential issued by the data

owner. He then runs the $ShowCred$routine to generate a credential proof, and broadcasts it to all masternodes for verification. The masternodes also collect the set of credentials in the blockchain and validate the proof using the $VerifyCred$ algorithm. The credential certification is accepted if the last routine outputs 1.

The data consumer and the blockchain nodes are both required to compute $A = Accumulate\ (params, S_c)$ which requires a linear scan of the blockchain data. The complexity of the protocol increases linearly with the number of registered data consumers.

With this robust anonymous collaboration layer, the bike-sharing fleet operator A and the scooter-sharing fleet operator B can work together and exchange data with each other without exposing her/his identity address. It means that it is very difficult to trace the owner of collaboration transactions in VeloxChain but it is also easy to prove someone to participate in the collaboration.

3.2.2. Private Keyword Search Engine

In the Velox ecosystem, we provide the distributed data storage layer. IPFS[18] is used to store public and plain-text data while sensitive data are encrypted and stored in the distributed storage.

In order to support sharing-mobility DApps to easily develop and manage encrypted sensitive data, VeloxChain provides a built-in encrypted data search modelled by smart contracts. The crucial requirement of such a search must be fast return of results without exposing private data. Our solution is that the meta-data (i.e. the fingerprint) of the encrypted data are stored in the VeloxChain and only authorized clients are permitted to use it to conduct searches. The authorization process is done by the Anonymous Collaboration Layer presented in the section 3.2.1 An access key is computed using a hash function (i.e. The fingerprint of the data). The VeloxChain does not store the actual data content, however, it maintains the access key data so that data consumers are able to link real data to the distributed storage layer using blockchain.

We denote EKS as the encryption scheme that supports keyword search. The data owner appends a list of EKS ciphertext of each keyword to the access key and

stores it in the blockchain layer. A data D with keywords $W_1, W_2, \ldots, W_n$ is stored in the blockchain layer under the structure: $H(D)\,||EKS(W_1)\,||\ldots||EKS(W_n)$. An authorized data consumer is able to produce a certain trapdoor Γ_ω that enables a smart contract to test on each data entry whether one of the keywords associated with the access key (eg- the document) is equal to the word W. Given a trapdoor and EKSciphertext, the blockchain nodes can only test whether $W = W'$, and nothing else.

A typical keyword search cryptosystem consists of four general algorithms:

1. $KeyGen$:generates cryptosystem key.
2. $Trapdoor$: produces trapdoor T_W for a keyword W
3. $Encrypt$:produces a EKSciphertext for keyword W
4. $Test$: tests whether keyword in the trapdoor is matched to the EKS ciphertext.

In the VeloxChain ecosystem, an additional algorithm is required for the data owner to produce a secret search key for the data consumer. We denote that algorithm $KeyDerive$. Three algorithms $KeyGen, Encrypt$and $KeyDerive$ are performed by the data owner, while $Trapdoor$ is run by the data consumer to generate a trapdoor, and finally, the $Test$ algorithms is performed by smart contracts or the blockchain peers. We modify the protocol proposed by Raluca Ada Popa[19] to adapt to our environment.

We start the protocol description by reviewing a few concepts related to bilinear maps. We will use the following notation: $G_1$and $G_2$are two (multiplicative) cyclic groups of prime order $p, g_1$is a generator of G_1 and $g_2$is a generator of G_2. A bilinear map is a map $e: G_1 \times G_2 \rightarrow G_T$with the two following properties: $(1)\ Bilinear$: $\forall u \in G_1, v \in G_2$ and $a, b \in Z$,then $e(u^a, v^b) = e(u, v)^{ab}$, and $(2)\ Non-degenerate$: $e(g_1, g_2) \neq 1$.

We denote $H: \{0,1\}^* \rightarrow G_1$ and $H_2: G_T \times G_T \rightarrow \{0,1\}^*$ to be two random oracles, and g_1, g_2, g_T are respectively the generators of groups G_1, G_2, G_T. The private keyword search system consists of five algorithms as the follows:

1. $KeyGen: k \leftarrow Z_p$.

2. $KeyDerive(k,s)$: $k_s \leftarrow g^{\frac{k}{s}}$.
3. $Trapdoor(w,s)$: $T_w \leftarrow e(H(w)^s, k_s)$.
4. $Encrypted(k,w)$: $Random\ r \leftarrow G_T.Output$: $c = (r, H_2(r, e(H(w), g_w)^k)$.
5. $Test$: $Parse\ c = (r,h)$. Test whether $H_2(r,tk) = h$.

The data owner generates a secret key k for keyword encryption EKS, and derives keys for the data consumers. Each data consumer poses a secret $s \in Z_p$, which can be generated by a mapping from his pseudonym with the data owner. Using $k$and s, the data owner computes a search key k_s for the data consumer so that later he can use it for trapdoor construction.

The correctness of the protocol follows the two equations:

$tk = e(H(w)^s, g_2^{\frac{k}{s}}) = e(H(w), g_2)^k$, and $H_2(r,tk) = H_2(r, e(H(w), g_2)^k)$

The above scheme has data hiding and token hiding properties. Data hiding (privacy) requires that the semi-honest adversary is not able to distinguish between ciphertexts of two values not matched by some token. Token hiding (privacy) requires that the adversary cannot learn the keyword that one searches for. The complexity of the protocol increases linearly with the number of data sets stored in the VeloxChain ecosystem.

3.3. Payment Channel Technology and Revenue-Sharing models

The payment-channel[20] network allows us to transfer token near-instantly and with low-fees by using digitally signed and hash-locked[21] transfers. In the payment channel, users have to setup an on-chain deposit to open a payment channel smart contract, and then users can perform token transfers instantaneously, without limit, as long as the net sum of their transfers does not exceed the deposited tokens. Finally, users have to close the payment channel by calling functions $cooperativeClose\ (\ )or\ uncooperativeClose\ ()$ in the smart contract $TransferChannels.sol$ [22] which requires on-chain transactions. VeloxChain leverages multi-signature smart contracts and payment-channel technology to enable

automatically revenue-sharing models among stakeholders. To reduce the volatility of token price, merchants will use stable coins such as DAI or gold-backed cryptocurrency. Moreover, VeloxChain will also support payment processing module using fiat.

One of the unique features of VeloxChain is that multiple parties can collaborate to supply, operate and provide sharing-mobility services. These are described as fleet operations and the parties collaborating choose one or more of the following roles:

- Vehicle suppliers (bike, scooter, segways or car suppliers)
- Fleet Operators (rental shops, retailers or distributors)
- Service Providers (hotels, premium resorts, co-working spaces, local councils, police forces, universities).

In a centralized business, collaboration between vehicle suppliers, fleet operators, and service providers would be difficult because they would be required to store data centrally - resulting in reduced data privacy and increased data security risks.

Moreover, a membership business model - with fixed costs borne by the service provider - is not a fair way to share cost and revenue among suppliers, fleet operators, and service providers. For example, service providers such as hotels and resorts have a seasonal business cycle. They should not bear costs when ridership is low or face bike/scooter shortage when the ridership is high. A flexible revenue-sharing mechanism is required.

VeloxChain provides a neutral and fair revenue sharing model which, once agreed upon by the parties, will operate in an automated manner using smart contracts.

In the VeloxChain ecosystem, vehicles can perform actions such as: closing a payment-channel, transfer token to distribute revenue among stakeholders and record location, status, user profiles or other data into Velox Chain. In the future, VeloxChain will cooperate with IoT manufacturers to produce smart computers and smart locks which work with Velox ecosystem. These steps will ensure broad adoption of VeloxChain by vehicle manufacturers.

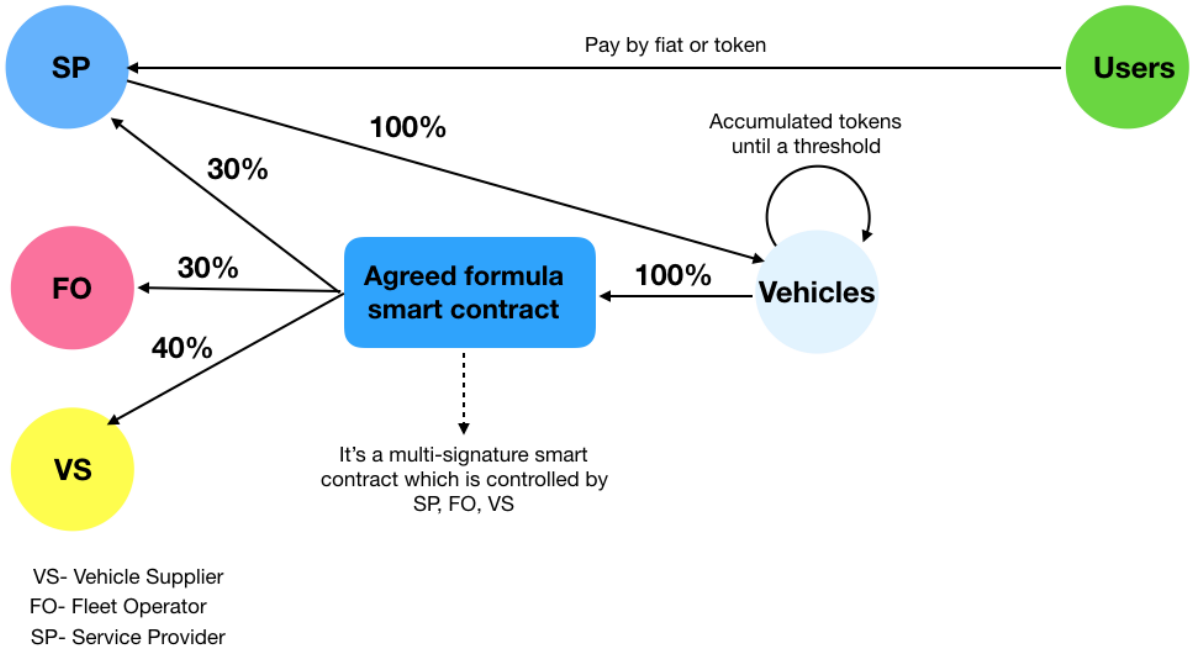


Figure 8. Revenue distributed by smart contracts

Following is a hypothetical usage scenario. There are 4 actors in this scenario: (a) bike supplier Volata Cycles, (b) fleet operator BCPS, (c) service provider Marina Hotel and (d) the Rider, who happens to be a hotel guest.

1. Volata, BCPS and Marina Hotel (the merchants) make an agreement regarding deposits, revenue split, maintenance terms and costs. For example, the merchants might agree a revenue split of Volata 40%, BCPS 30% and Marina Hotel 30%. They might also agree that, regardless of how much Marina Hotel charges their guests to use the bikes, the hotel will pay 8 cents per riding minute, to be shared according to the split.
2. These terms are recorded immutably with a multi-signature contract in which any change requires an endorsement of three parties.
3. Marina Hotel has to buy tokens to transact. Each morning, staff of the hotel deposit 1000 tokens to open a payment channel with each Volata bike. This is an on-chain transaction; however, it is not necessary to be a real-time transaction.
4. Marina Hotel staff use the Velox Fleet Services DApp to rent and unlock bikes and the Rider uses a VeloxGo DApp to record and share riding data. After each ride, the Marina Hotel account will automatically send a signed off-chain

transaction directly to the Volata bike (which has its own address on the blockchain).

5. At the end of each day, the bikes and Marina Hotel automatically sign and close the payment channel to settle their payments on-chain. This does not need to be a real-time transaction.
6. Whenever the balance on one of the Volata bikes reaches some pre-set threshold, the bike will automatically distribute revenue amongst the 3 merchants, according to the agreed split. The token is transferred by the smart contract created in step #2.

In the Velox ecosystem, vehicle suppliers, fleet operators, and service providers freely search and collaborate with each other trustlessly - without having to trust one another. All stakeholders rely on smart contracts. Service providers use the vehicle as an intermediary and the bike is only unlocked if it gets paid. In turn, the vehicle distributes revenue directly to all the merchants using multi-signature smart contracts.

3.4. Meta Transaction Relay Protocol

All on-chain transactions on blockchain are paid using transaction fees known as *gas*. Many people, however, have little-to-no knowledge about blockchain and hold no Velox token. Therefore, without meta transaction relay service, we can imagine the customers like Join use a scooter-sharing DApp from merchant B:

1. Join know about the scooter-sharing DApp through his friend and download it to try.
2. Join try to create an account and book a scooter from merchant B; but he realizes that he has no Velox token to perform on-chain transactions.
3. Join has to go to his favourite exchange, doing KYC and wait for few days to buy some Velox token. And then he is able to perform on-chain transactions.

Consequently, it is a terrible user experience to force all users to buy and then hold token to use sharing-mobility services on VeloxChain. Meta Transaction Relay

aims to solve this problem by allowing a third-party to fuel gas of transaction (fund) and then replay the transaction for the users.

How the meta transaction relay magic works in the practical example. Firstly, Join download the scooter-sharing DApp from merchant B. Although Join holds no token, he can sign the transaction and send this transaction to a relayer server which probably to hosted by the merchant B. This relayer server can pay the gas for this transaction and then forward it to Velox Chain through the *relayMetaTx*[22] protocol. As a result, Join does not require to hold token and the merchant B is able to pay his users on-chain transactions.

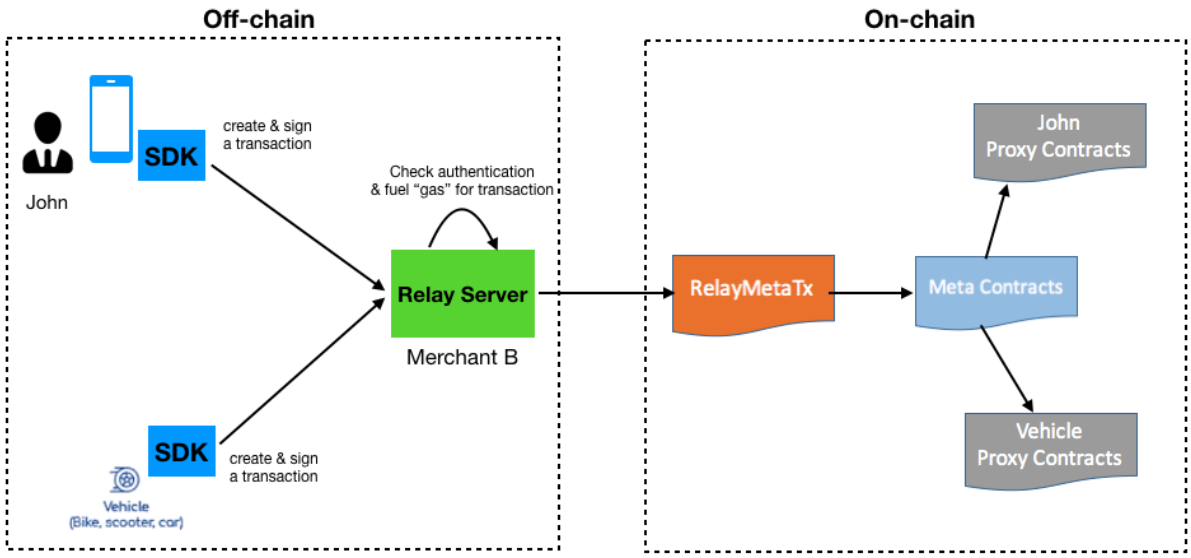


Figure 9. Meta Transaction Relay Service.

3.5. Vehicle Ownership and Tokenization from ERC721

VeloxChain has developed a Vehicle-Ownership protocol to share ownership information. Vehicle owners can prove their ownership and report the location of stolen the smart vehicle by referencing immutable records on the blockchain. When a smart vehicle is stolen, the police are able to see the latest position to respond instantly. Potentially, insurance companies could automate claim processing for such losses through a smart contract running on the blockchain.

We have often heard how the Ethereum ERC721 smart contract is non-fungible, meaning that tokens of the same class or contract can hold a different value. The

Cryptokittie[24] project is one interesting application. Cryptokitties are unique (and collectible) assets because each is tokenized with a different ERC721, having a different value.

For this reason, we developed the Vehicle-Ownership protocol[25] using ERC721 tokens from OpenZeppelin[26]. Each ERC721 represents a different vehicle, and the value of the Vehicle-Ownership token is based on the metadata of token including vehicle technical information, picture, owner's information, supplier, and manufacturer. Ownership is determined by an array of token *indexes* or *ids* that is mapped to owner address. The total supply of Bike-Ownership tokens is the length of array $allTokens$. The number of vehicles registered in the VeloxChain ecosystem is virtually unlimited, as the maximum number of any given type of ERC721 tokens, based on the unsigned integer storage type, is $2^{256} - 1$.

When a vehicle owner registers a new vehicle, the system will generate a random integer as a new token id and then call $addTokenTo$from the VehicleOwnershipProtocol.sol to issue a new Vehicle-Ownership token.

```
58
59    /**
60     * @dev Returns an URI for a given token ID
61     * @dev Throws if the token ID does not exist. May return an empty string.
62     * @param _tokenId uint256 ID of the token to query
63     */
64    function tokenURI(uint256 _tokenId) public view returns (string) {
65      require(exists(_tokenId));
66      return tokenURIs[_tokenId];
67    }
68
```

```
98
99    /**
100    * @dev Internal function to set the token URI for a given token
101    * @dev Reverts if the token ID does not exist
102    * @param _tokenId uint256 ID of the token to set its URI
103    * @param _uri string URI to assign
104    */
105   function _setTokenURI(uint256 _tokenId, string _uri) internal {
106     require(exists(_tokenId));
107     tokenURIs[_tokenId] = _uri;
108   }
109
```

Figure 10. Each Vehicle-Ownership token mapped to a URI

Each Vehicle-Ownership token holds metadata which is the URI of the vehicle information record, such as manufacturer, vehicle technical information, images storing in the distributed storage layer.
Whenever users create a new Vehicle-Ownership token, the matching engine scans through all tokens using our searching engine (described in section 2.2.1); and if the matching engine finds any Vehicle-Ownership token with the same metadata, the system suggests users merge or transfer their token between users.

Consider this simple example: Alice bought a Volata smart bicycle from Bob. This bike has a computer chip IMEI: VOLATA123456789. With the bike, Alice obtains a new Vehicle-Ownership token. But the matching engine detects that Alice's token has the same metadata (i.e.- IMEI code) as another vehicle-ownership token held by the bike manufacturer. The system notifies Alice and the manufacturer to merge these Vehicle-Ownership tokens. This could be accomplished by Alice burning the token received from Bob and the manufacturer sending Alice the token in its possession, by a multi-signature contract.

4. Smart Urban Mobility Technologies

4.1. Emerging Smart Mobility Trends

A bicycle is the most energy-efficient means of human transport ever invented, and the future is all about sustainability. Bikes solve multiple problems of urban mobility and sedentary life. With a rapidly increasing number of riders active in the bike-sharing market, bicycle manufacturers and tech giants are seeking to apply innovative Internet of Things (IoT) technologies to enable smart bikes which can navigate and provide a better and indeed safer user-experience.

Ofo and Huawei have worked together to build the NB-IoT-based[27] smart shared bike lock solutions

Figure 11. The remote Controller and lock system

providing lower power consumption, better coverage, and lower latency. Similarly, Mobike, AT&T, and Qualcomm[28] are currently collaborating on Mobile IoT smart bike sharing technology. Moreover, IoT-Smart bike technologies are being embraced as equipment add-ons by tech enthusiast riders. This is the case with the MAT Remote Controller and Lock system (pictured above), which won the HONOREE prize at CES 2018 Innovation Awards in the *Vehicle Intelligence and Self-Driving Technology category*.[29]

4.2. Volata Smart Bike Technologies

Volata Cycles is the first bicycle company to design hardware, develop software and take care of distribution and service and Volata is also the first catalyst partner of VeloxChain.

Volata provides the user with all the features that he or she needs when using a bike for commuting or recreational riding, with a focus on safety, and providing them significant rewards while riding. Information is provided using a dashboard with a built-in computer which is easily controlled via thumb joystick and shows smartphone notifications (such as calls, text messages) on its display. Of particular note, the rider is able to receive navigational cues.

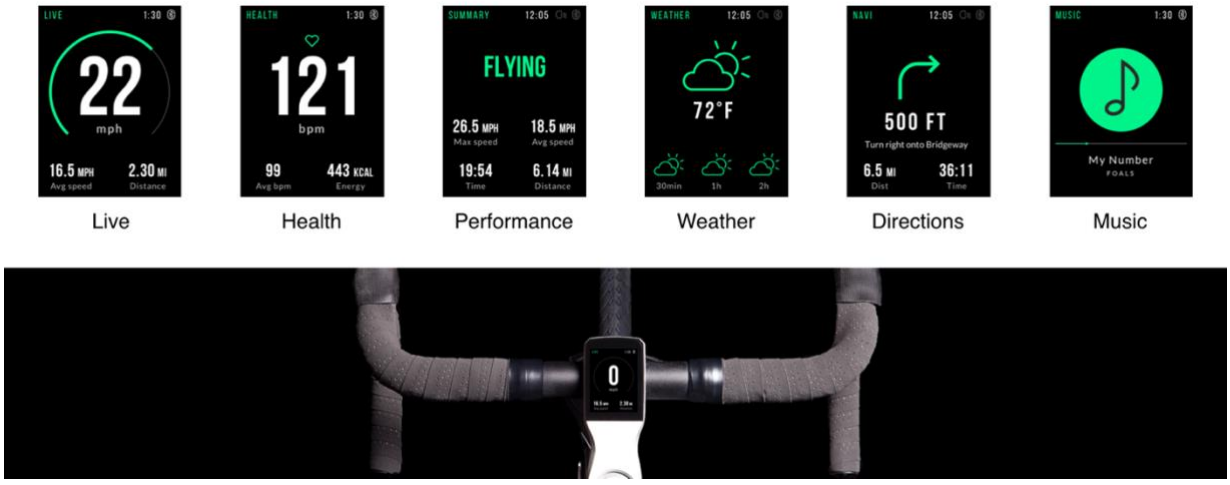


Figure 12. Built-in applications on Volata Smart Computer

Following are illustrations which show how the subsystems fit together.

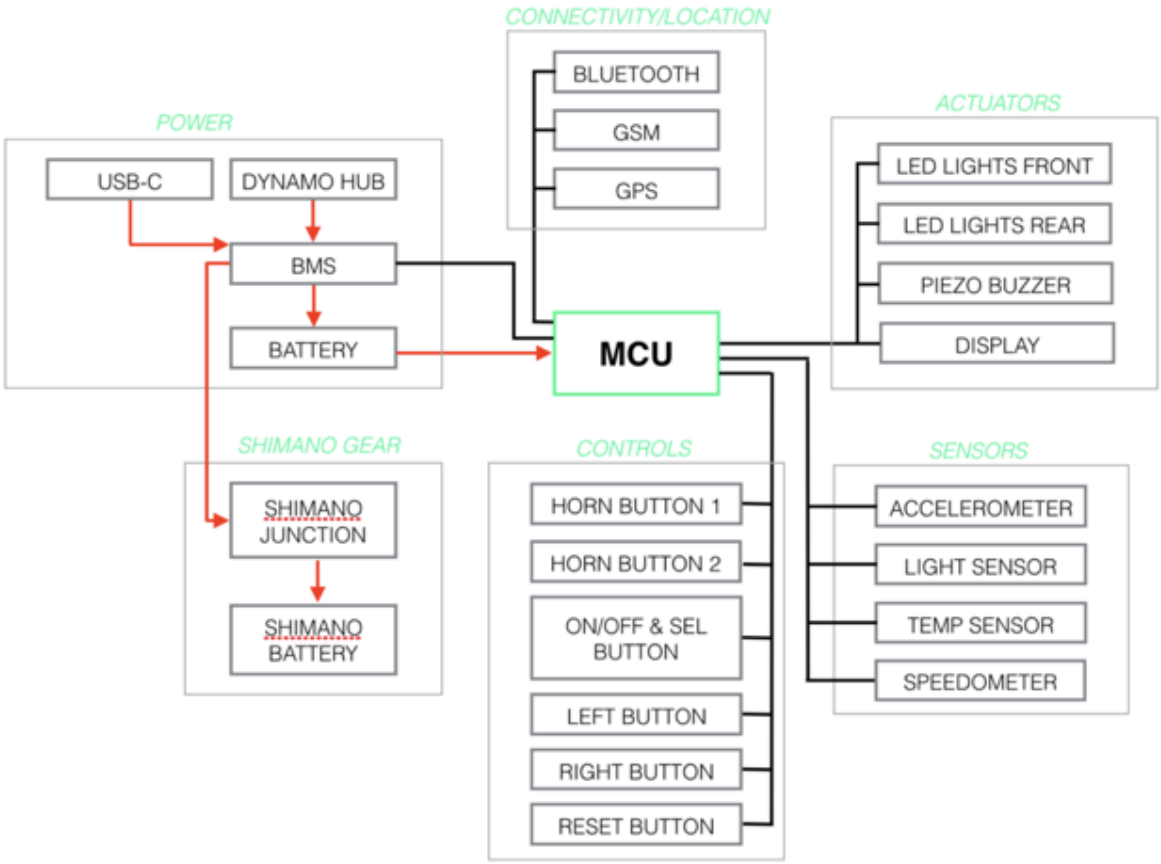


Figure 13. Overall Architecture design of Volata smart computer

The bicycle connects to the internet (via GSM) and to the rider's smartphone. Using an app, the rider can: obtain a riding data summary, record personal milestones, review a timeline of all trips, set a destination and receive navigational assistance. They can, if desired, use the app to share their performance with friends. Just like Tesla and BMW autos, a Volata bike can be located, monitored, and remotely locked or unlocked at any time from a smartphone. As part of the anti-theft system, users can receive notification if somebody tries to steal a bike, and can track the bike via GPS if it is missing.

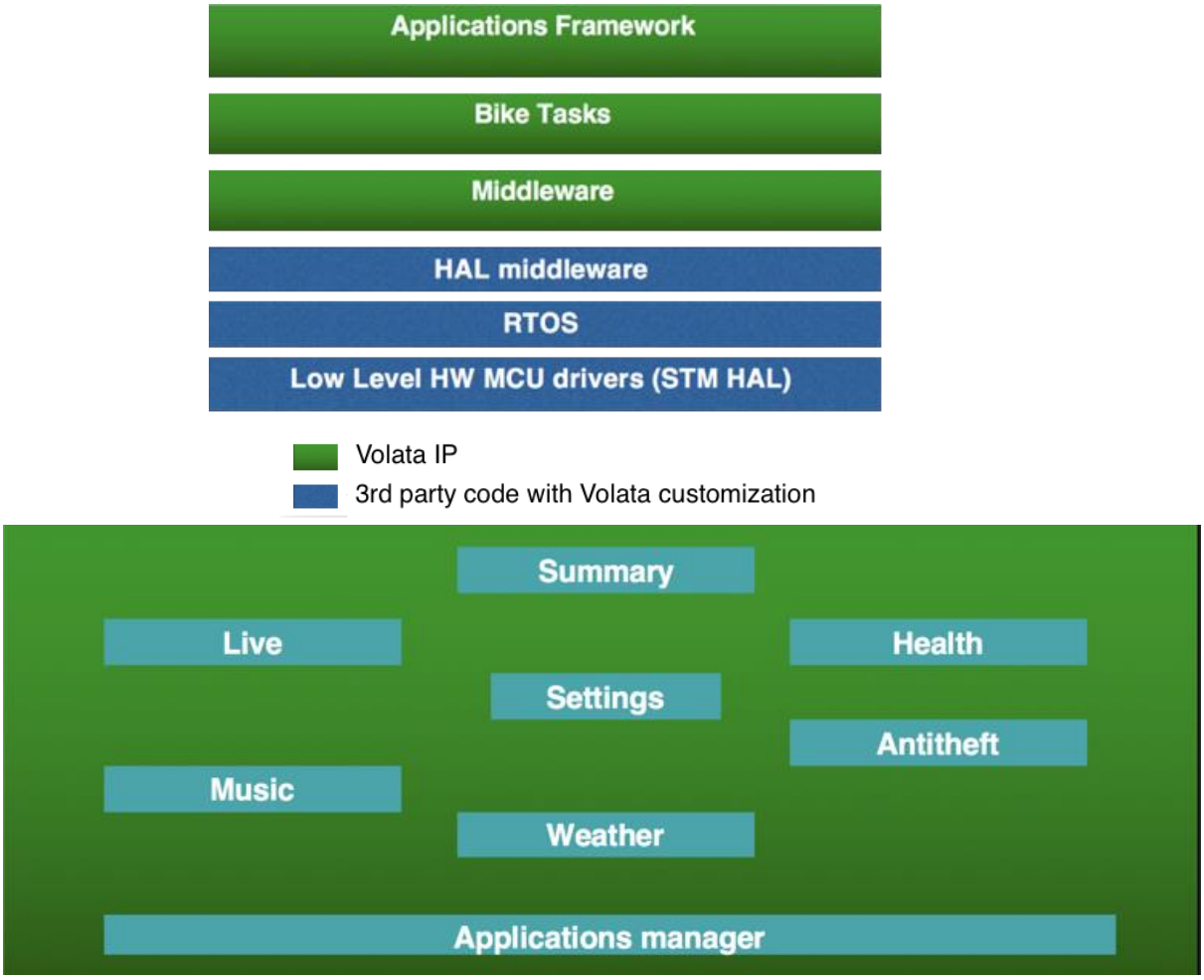


Figure 14. Software Components of Volata smart computer

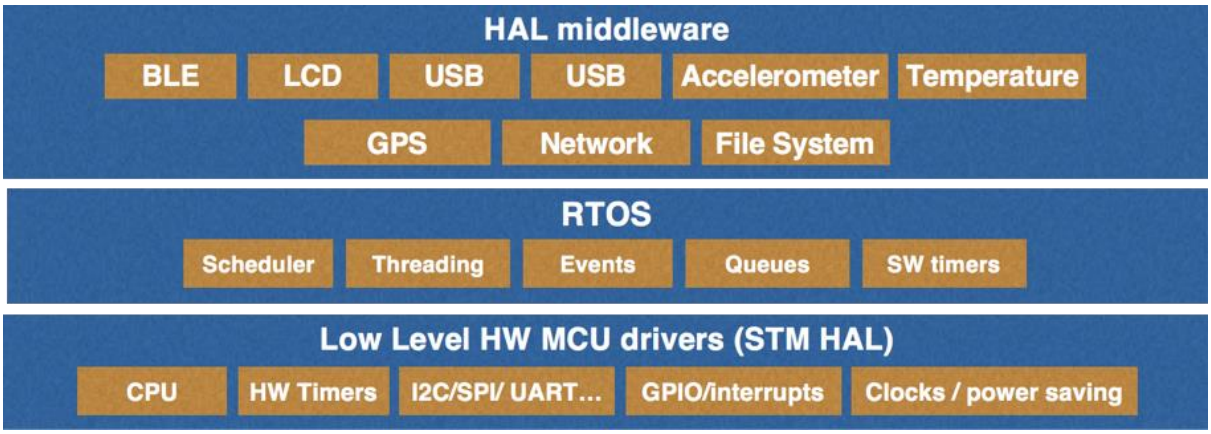


Figure 15. RTOS and Drivers

5. Velox Token Economy

VeloxChain is preparing to launch a token sale to fund development and marketing of the Velox platform, including both the underlying blockchain technology and the operation of a fleet of premium bicycles supplied by Volata Cycles. In a token sale,

a project offers to investors units of a new cryptocurrency (their token) in exchange for cryptocurrencies such as Bitcoin or Ethereum[30].

Our project's investment unit (symbol: VELOX) is a utility token[2] developed using the Ethereum ERC20 token standard. This token fulfills the following currency-related functions:

- As an accounting unit for service fees and micro-payments
- As a medium of exchange within the platform
- As a store of value for incentivising and rewarding platform contributors

Using VELOX tokens to make purchases on the platform entitles users to concessions at the discretion of the VeloxChain team, to encourage the use of tokens on the platform. Another primary use of the token is to incentivise individuals who make available their computing resources for the platform.

5.1. Velox Token Use Cases

Tokens are created by pre-mining prior to the token sale. They are then divided into allocations for sales (50%), reserves (35%), and block rewards for block validators (15%). The purpose of the block rewards is to incentivise participants who contribute computing resources to the platform.

Utility tokens provide users with two things: (a) future access to a blockchain-based service, and (b) a medium of exchange to pay for that service. Here is a list of uses for VELOX tokens:

[2] The VELOX token shall not and cannot be considered as shares or securities in any jurisdiction as they do not give any rights to dividends, interests, profits or to participate in the general meeting of the company. They will not be listed on any regulated stock exchange. The offering of BKC tokens on any trading platform is done in order to allow their use as utility tokens on the platform and are not for speculative purposes. Such offering does not change the legal nature of these tokens, which remain as a simple means for the use of the platform and not security.

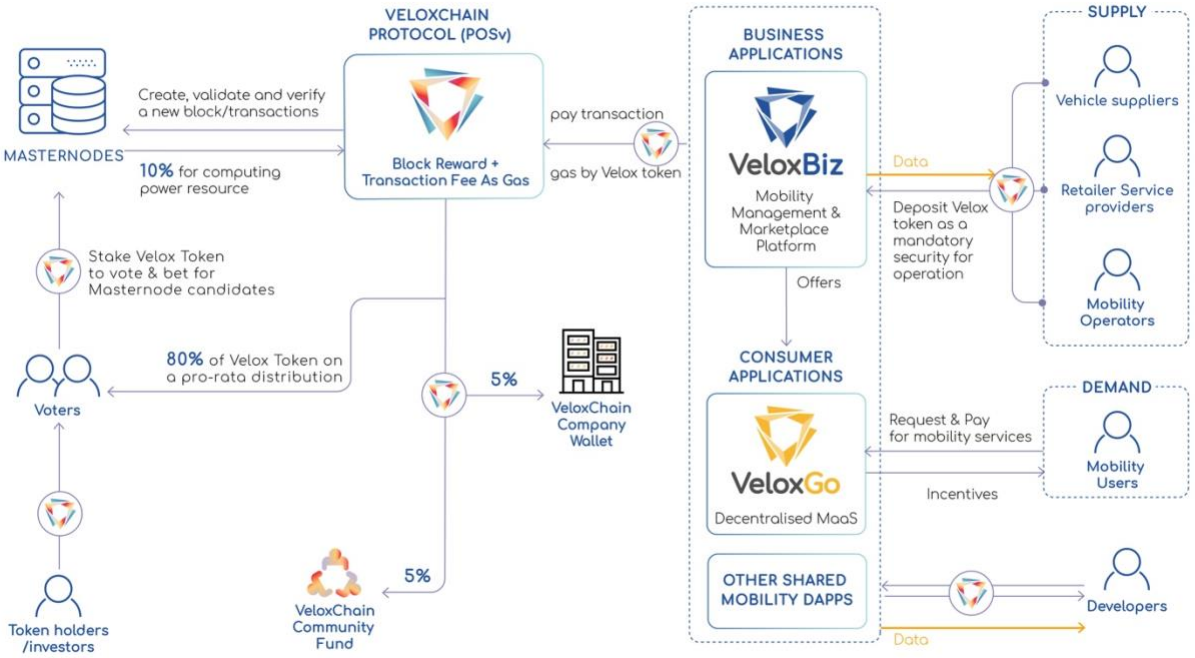


Figure 17. Velox Token Economy

- **Stake Velox token to govern VeloxChain**: With Proof-of-Stake consensus, coin holders can participate in governing the Velox Chain by staking VELOX token.
    - **As Masternode**: Instead of investing in high-computing and expensive computers as “miners” in Proof of Work chain, users can stake VELOX token during a certain period for example 100,000 VELOX tokens for 45 days to become masternode candidate. If voted by the Velox community, Masternode candidates will officially become Masternodes to create, validate and verify blocks of VeloxChain. In exchange, Masternode will be rewarded portion of Velox Tokens as block reward plus gas of transaction fee for their effort and computing resource.
    - **As Voter**: Velox token holders can participate in governing the Velox Chain by voting for Masternode candidates to be listed and became

Masternode in each block epoch. Velox token holders can vote for Masternode candidates by sending their Velox Tokens to Masternode candidate's addresses and being locked up for a certain period such as 3 days and each VELOX token is counted as one vote. In exchange, Voters will receive Velox Tokens as the portion of block reward basing on pro-rata.

- **Transaction gas**: sharing-mobility DApp services have to use VELOX token to pay gas of on-chain transactions.
- **Deposit Velox Token as a loyalty escrow:** VeloxChain merchants such as mobility providers (bike-sharing, scooter-sharing, car-sharing…), retailer service providers (hotels, co-working space…), vehicle suppliers have to deposit Velox Token as a loyalty escrow to collaborate in VeloxChain ecosystem. In the case, the merchant violates terms of collaboration smart contract and detected by the third-party such as sharing fake-data records, the merchant will be punished by lost his loyalty escrow amount to the third-party detector.
- **Cryptocurrency**: Tokens are circulated and used as payment in all DApps built on top of the VeloxChain. Here is a list of monetary policies we will use:
    - On the platform, transactions are not limited to the VELOX token. Customers will be able to use popular cryptocurrencies such as Ether and other Alt-coins. This helps to attract users to the platform.
    - Customers will be able to use stable coins, such as DAI or golden-backed crypto currencies, as an alternative to other cryptocurrencies. This is useful in the case that they plan to make a large purchase and want price stability, i.e.- to avoid the potential volatility of VELOX.

    - Customers who do make purchases on the platform using VELOX tokens will get a discount relative to those using other forms of payment. This is to reward loyalty and encourage the use of the VELOX token.
    - Credit payment processor will be integrated into the VeloxChain ecosystem to serve non-crypto customers to use fiat, however, it will have a transaction fee.
- **Community rewards**: VELOX Tokens are awarded to community contributors
    - Third-party developers to build the supporting tools or sharing-mobility DApps and report bugs by Velox bounty programs.
    - Third-party detectors to find frauds in merchants collaborations
- **Sharing-mobility service incentives**: VeloxChain community fund reward Velox Tokens to incentivise users to participate in the sharing-mobility economy through VeloxGo marketing campaign or merchants campaign.
    - Using green sharing transport services such as bike-sharing, scooter-sharing or e-vehicle sharing.
    - Sharing the personal vehicle assets to sharing-mobility service.
    - Using sharing-mobility services.

These policies are discretionary and do not violate any securities regulations. They are simply tools with which we encourage the use of the new VELOX token.

The following table details how, once the platform is fully operational, VELOX tokens will be used by stakeholders.

Stakeholders	Description	Benefits	Velox Token Use case
Masternode	Who run servers to create, verify and validate a new block	Earn the portion of block reward and gas of transaction. More productive than Proof-of-work chain.	Stake a large amount of Velox token to qualified and voted to become masternode
Crypto Investor	Buy and hold Velox Token	Earn portion of block reward and gas of transaction. Earn profit when Velox token's value increase.	Vote and bet their Velox token for masternode candidate to receive block reward. Either use their tokens to purchase services, or sell them to other customers of the service
New or small sharing-mobility service providers	Merchants want to launch a small set (0-300) of vehicles in the local area in multiple models, B2B (campus, resorts, tours, co-working space), B2C (end-users), P2P and so forth. Local business or vehicle owners want to monetize their idle assets.	Use VeloxBiz platform and VeloxGo 1.0 DApp to establish the business, build partnerships to launch and scale up services more easily, quickly and cost-effectively without heavily technology investment by inheriting VeloxChain network effect and open source software	Pay gas of on-chain transactions. Stake token as loyalty escrow to collaborate with other merchants.
Established sharing-mobility service providers	Merchants that already operate share-use vehicles sharing and in a growth stage.	Use VeloxBiz platform to search and establish partnerships to exchange data to monetize idle assets or optimize trip service. Incentivise user using the sharing-mobility services. Transparent their data and	Pay gas of on-chain transactions. Stake token as loyalty escrow to collaborate with other merchants. Reward token.

		transactions with others such as insurance service.	
Retail Service Providers	Resorts, hotels, co-working space, airlines, university campuses	Provide add-on service to increase customer satisfaction and generate extra income	Pay gas of on-chain transactions such as signing collaboration smart contracts. Stake token as loyalty escrow to collaborate with other merchants. Payment method.
Vehicle Suppliers	Vehicle manufacturers or local shop	Use VeloxBiz to source and establish valuable partnerships and increase revenue	Pay gas of on-chain transactions such as signing collaboration smart contracts. Stake token as loyalty escrow to collaborate with other merchants.
Third-party developers	Freelancer or software solution providers	Rich support blockchain ecosystem to build sharing-mobility DApps. Develop add-on tools for sharing-mobility services such as crash detection, remote status check and sell it as software-as-a-service. Connect with business clients for gig	Pay gas of on-chain transactions. As payment methods.
Sharing-mobility	Users participate in sharing-mobility	Using VeloxGo DApp as a unified access to a variety	Use Velox token with a discount to use sharing-

Users	services such as bike-sharing, scooter-sharing, ride-sharing	of shared mobility services, offering a seamless travel experience without the hassle of switching apps and multiple accounts created	mobility service on Velox Ecosystem.

5.2. Token Sale & Distribution

Following are some of the key features of the VELOX token sale, distribution and use of proceeds. There will only be one Token Generating Event and we plan to distribute 75% of the issued tokens to the public. This generous distribution will ensure long-term growth of VELOX platform, and will support the development of the ecosystem as a whole.

Token Sale - Key Facts

Component	Description
Token Symbol	VELOX
Issue Size	800,000,000 (Eight hundred million)
Schedule	To be confirmed (refer to website for updates)
Token Price	1 VELOX = 0.0375 USD (token price in Ether will be fixed 72 hours before start of the public sale)
Fundraising Target	USD 15m (hard cap)
Minimum Target	USD 5m (soft cap)

Distribution

Following is the token distribution plan. The team (including founders and seed investors) will get 15% with another 10% going to advisors and partners. That's 25% in total.

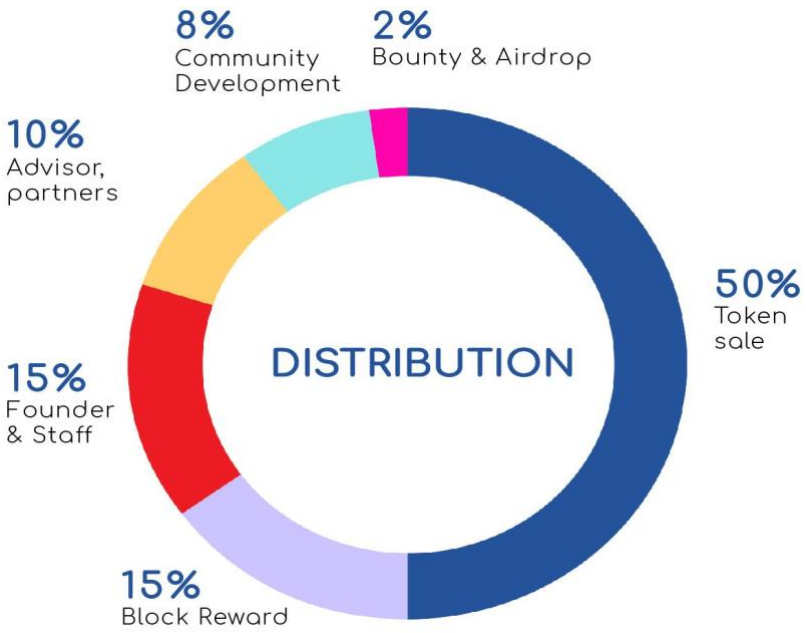


Figure 16. Velox Token Distribution.

The other 75% is distributed to the public. We will offer 50% of our tokens for purchase during the token sale. This includes presale bonuses. Then, 15% of the pre-mined tokens will be set aside as block rewards for those providing resources used by the platform and acting as validators. Another 8% will be retained as a reserve for community initiatives, business development, standards-promotion, education, and market expansion. Finally, 2% will be set aside for bounties and airdrops, to drive token adoption.

Ether received during the sale will be held in a multi-signature wallet. The vesting period for the team is 2 years, in equal quarterly installments, subject to a cliff of 6 months. This is to align incentives to our long-range plans.

Proceeds

The largest category of expense is 45% for Research and Development. Another 35% is for marketing, to recruit partners and expand the ecosystem. For operations, we budget 15% and the remaining 5% covers legal, tax, and accounting.

The figures given here are budgetary and subject to the discretion of the team. Development costs will increase to the extent we need to: (a) integrate with other technologies and (b) add new functionalities for payment processing.

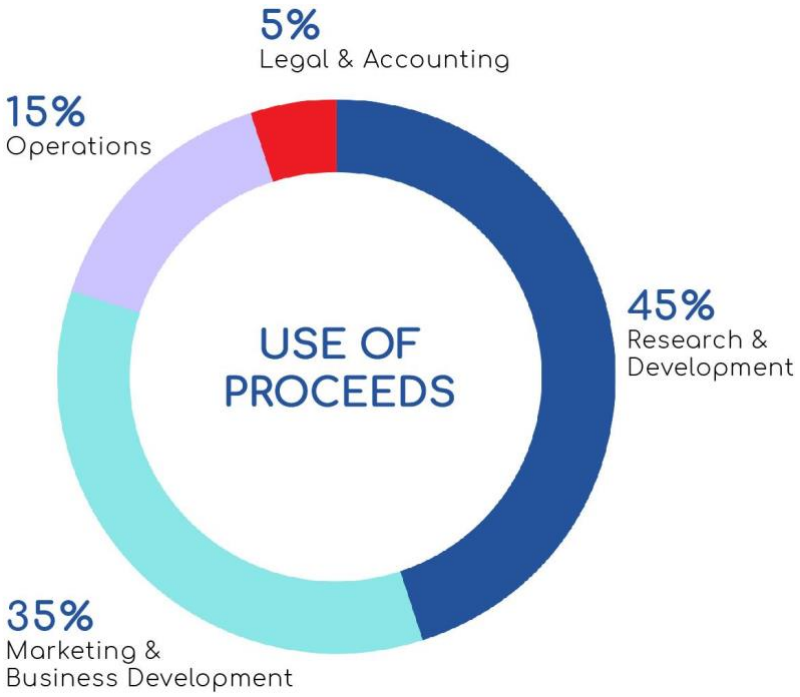


Figure 17. Velox Use of Proceeds

6. Roadmap

On the following page is the technical roadmap of the VeloxChain project. We aim to launch the main-net with some bike-sharing, scooter-sharing and segway services in Q2 2019 and open the platform in stages for other developers.

- **Q1- 2018: Concept Design**
  - Design the concept
  - Validate technical feasibility: zero-knowledge proof and full-homomorphic encryption models
  - Release Business & technical white papers
- **Q2-2018: Proof of concept on Ethereum Test-net**
  - Peer-to-peer sharing-mobility platform
  - Vehicle ownership (ERC721) protocol
  - Meta Transaction Relay protocol
  - Micro-payment channel smart contracts
  - IPFS p2p storage layer
- **Q3-2018: VeloxChain with PoA**

    - Launch VeloxChain with PoA , 2-second block time and 1000 tx/s
    - VeloxChain block explorer
    - VeloxGo: p2p sharing-mobility platform
    - Design VeloxBiz: the marketplace for sharing-mobility providers, vehicle suppliers
    - Update Business & technical white papers
- **Q4-2018: Pre-Launch Stage**
    - Implement Proof of Stake voting consensus.
    - VeloxBiz: marketplace for sharing-mobility providers.
    - VeloxGo Dapp for sharing personal vehicle service.
- **Q2-2019: Full Launch**
    - VeloxChain main-net with PoSv
    - VeloxBiz: fleet management system for service operators, network operators for bike-sharing, scooter-sharing and segway-sharing services.
    - Velox Dev tools and packages for sharing-mobility DApps.
    - Deploy secure multi-party computation protocol.
- **Q3-2019: Opening ecosystem**
    - Credit Rating models
    - Fraud-detection models
    - Sharing-mobility incentive models
    - APIs for third-party services such as hotel, co-working, insurance services.
- **Q1-2020: Interoperability ecosystem**
    - Cross-chain transfer data with Ethereum, TomoChain
    - Develop other privacy-preserving approaches - trusted execution environment
    - Develop sharding solution

- Integrate car-sharing or motorbike sharing services

7. Team

7.1. Corporate Structure

Smart Urban Technologies Pte Ltd as VeloxChain is incorporated in Singapore as a Private Limited profit-making corporation. We chose Singapore as the domicile for our token sale because it is a centre of excellence in blockchain development and one of the world's best jurisdictions for token sales.

7.2. Management Team

The founding team and key management are all serial entrepreneurs and veterans with diverse experience in the technology, internet, and blockchain industry.

Fabrizio Martini
Co-Founder, President & Chairman

Mr. Martini is an innovator, investor, serial entrepreneur with a passion for sustainable transportation. Over his career, he covered the positions of Director of R&D as well as Principal Investigator and Program Manager of several U.S. government-funded and successfully completed programs for the Department of Energy, Department of Defense, and NASA managing over $10M. He has contributed to the accomplishment of six world records related to energy storage technology, and was in charge of the commercialization of the first-of-its kind high temperature ultra-capacitor for oil and gas and geothermal applications. Mr. Martini, a Co-Found of Volata Cycles, is a strong believer in bicycles to be the most advanced and efficient means of transportation. He is author of 17 patents, including 3 from Volata Cycles.

Eric Bui
Cofounder & CTO

Eric holds a Bachelor's degree with Honours in Computer Science (Intelligent System & Entrepreneurship) from NTU,

Singapore. He was a founder and tech-advisor to AEvice Health, an asthma monitoring device and a winner of the SWITCH 2016 pitching competition. Eric has experience working on various blockchain technologies such Bitcoin, Ethereum, Hyperledger, Zero-Knowledge Proof, Homomorphic encryption and other cryptography. He is also a technical advisor for several blockchain start-ups and is one of the founders of the largest Vietnam Blockchain Developer Community. Most recently, Eric was the blockchain lead of Electrify.Asia, which completed a successful token sale raising the equivalent of USD 30m.

Mattia DeSantis

Head Of Engineering

De Santis holds a degree in mechanical engineering from Polytechnic of Milan, one of the top university in Italy. He is a master in bicycle technologies, and he has developed over 20 bicycles models from scratch over his career. De Santis combined in Volata Model 1 and Model 1c all his experience and knowledge to develop the smartest and most advanced bicycle on the market. De Santis deeply interested in both innovative and conventional manufacturing processes and has excellent handling and creativity to solve all type of design or functionality problem. He has over 10 year-experience in design and manufacturing of consumer products, FEM and CFD analysis, prototyping of mechanical systems and CNC machines programming.

Bill Claxton

Operations Director

Bill Claxton is a seasoned technology entrepreneur. He holds a certificate in Blockchain for Technical Executives and Analysts from B9Lab Academy in the UK and has spoken at various blockchain events. Bill has been active in the IT scene in Singapore for more than 20 years, was an early Bitcoin investor and most recently served as Operations Director of fintech start-up KYC Chain.

Tuan Nguyen
Blockchain Lead

Tony Tuan Nguyen has 10 -year experience in IT industry with various positions, including web developer, mobile developer, software architect, technical advisor, CTO and CEO. With his passion for cutting-edge technology, he masters in web application, mobile application, clouds computing and now blockchain. With his deep knowledge of healthcare industry and his experience in solutions development like ERP, CRM, Tony is consistently recognized as a trusted leading advisor for his vision, passion and commitment to his customer's missions.

Winnie Nguyen
Marketing Manager

Winnie has over 7 years of experience in multiple marketing facets, specialising in the hospitality and service industry in Asia. Originally from Vietnam, she moved to Australia after working as a Marketing Manager for major hospitality brands in Indochina. Being a challenge seeker who embraces the growth mindset, Winnie has accepted the challenge to help VeloxChain empower the sharing-mobility economy. She has a great interest and understanding about technology and the innovation behind it. Winnie is also a casual content writer about blockchain technology and how business embraces it, sharing her passion with the community.

7.3. Advisor Team

We have assembled a panel of world-class industry advisors who are passionate about the industry, the application of blockchain technology and the open source community. They not only help advise on Go-to-Market strategies but also evangelize our platform to help drive adoption among industry leaders.

Assoc Prof Ng Wee Keong
Technical Blockchain Advisor

Dr. William K. NG works in the areas of machine learning, privacy-preserving techniques, query-permissible encrypted databases, blockchain systems, and data security. He contributes to companies and industries as technology consultant on projects involving data analytics, artificial intelligence, data privacy and security, and blockchain. In recent years, he was General Chair of the 18th International Conference on Information and Communications Security (2016), Senior Program Committee Member of the 22nd to 17th Pacific-Asia Conference on Knowledge Discovery and Data Mining, General Chair of International Symposium on Cyber Security (CyberSec2013).

Lui Morais
Supply Chain Advisor

Luis Morais is a supply chain expert with an extensive international track record. He is currently a CEO and Founder of LM-Supply. Prior to that, he has worked for multinational companies such as Kraft Heinz, Thai Union Group (France) in several roles such as Director of Finance, supply chain, procurement, consultancy and technology, leading numerous multimillion euro projects with successful outcomes.

Sherwin Lee
Legal Advisor

Sherwin is a partner of TLB law firm in Singapore and holds a Masters in Law (Distinction) in International Banking and Finance from The University College London in 2008. Sherwin currently focuses on advising companies within the financial and emerging technologies space and particularly on the application of distributed ledger technologies (DLT), token generating events / ICOs / ITOs as well as set up and design of blockchain ecosystem players.

Dr Hector Gonzalez Jimenez
Marketing Advisor

Hector Gonzalez-Jimenez (PhD) is a global marketer and academic. He is an Associate Professor at the York

Management School, UK. A true global citizen, Hector has gained experiences in countries such as Spain, Germany, Japan, South Korea, USA and the UK. Over the last fifteen years his professional portfolio has grown in various roles in marketing, education and corporate strategy. During this time Hector has worked on projects for small to medium sized businesses as well as large international companies such as Pepsi or Ford. Hector is particularly interested in contributing to our understanding of global consumer perceptions and human-technology interactions.

Roberto Rossi

Finance and Operations Advisor

Roberto is an expert in the financial aspect of the bicycle worldwide sector. He currently serves the position of Finance and operations director at Crank Brothers Inc. - Selle Royal USA Inc. He previously worked for Maschio Gaspardo Spa and for Ferrari Spa. Roberto has a strong experience in budgeting and forecasting, especially for the bicycle sector where he has been working for the last 6 years of his career. He supports Volata in most of the financial related aspects.

Gaspare Licata

Management and Strategy Advisor

Gaspare is an experienced entrepreneur and leader with strong experience as CEO of CrankBrothers, manager of P&L at Selle Royal, Usa Sales Manager (Dell, Michael Page, Sell Royal Usa, crankbrothers), Marketing Manager (crankbrothers) Product and branding strategist (crankbrothers) Additional specialties: Negotiation, Human Resources Management, Branding, Marketing.

8. Conclusion

VeloxChain is an open-source blockchain-based protocol and marketplace for shared mobility services. Our ambition is to democratise the sharing mobility market and accelerate the world's transition to an open and seamless mobility. We provide a

one-stop solution for all participants in the ecosystem from developers, mobility providers and end-users, ultimately, benefiting from global network effects.

As the speed and scale of shared mobility continue to grow, the global market becomes fragmented and unconnected. Centralised system creates a single point of failure, so users must be wary of their personal data privacy and deposit requirements. Proprietary software and data restricts integration with another system. Thus, it limits cooperation between mobility businesses, resulting in fragmented user experience for users. We need new a decentralised collaborative business model for a healthier competition, for a more integrated, seamless travel experience and for stronger network effects that benefit the ecosystem.

VeloxChain's implementation will include five products to support this model:

- **Velox Protocol (VeloxChain):** an open public blockchain layer with some of the core technologies such as smart contract, Proof of Stake consensus, distributed data storage and zero-knowledge proofs to foster trust and transparency while ensuring privacy for sensitive data.
- **VeloxDEV:** An all-in-one solution for developers, making it easy and hassle-free for deployment of decentralised apps for mobility services on our VeloxChain
- **VeloxBIZ:** A platform promotes decentralised collaboration, which allows mobility providers and third-party partners to connect, collaborate and co-create vehicle sharing services that are seamless, smart and cost-effective. A bundle solutions will support some essential functionalities such as fleet management, merchant marketplace, analytics and reporting.
- **VeloxGO**: an open mobility marketplace to connect users and mobility providers, allowing them access to a variety of apps to meet their demand under one account.
- **Velox Token:** a native token of the VeloxChain ecosystem, acting as a store of value and medium of exchange. Users can also hold and stake (deposit) Velox tokens to receive block rewards.

9. Legal Disclaimer

Please read the following notice carefully before proceeding to read this Whitepaper document issued by Smart Urban Technologies Pte Ltd, a company incorporated and existing under the laws of the Singapore (hereinafter – "Distributor"). This notice applies to all persons who read this document. Please note this notice may be altered or updated. The Whitepaper does not constitute any relations between you (hereinafter – "you" or "Holder") and the Distributor.

Acquiring of the Velox tokens is available only after accepting the Terms of token sale (hereinafter – "T&C"). Acquisition of Velox cryptographic tokens does not present an exchange of cryptocurrencies for any form of ordinary shares of the Distributor and a Holder of Velox cryptographic tokens is not entitled to any guaranteed form of dividend. Holders of Velox tokens are only entitled to certain rights within the T&C. Velox tokens are not intended to constitute securities in any jurisdiction.

This Whitepaper does not constitute a prospectus or offer document of any sort, and is not intended to constitute an offer of securities or a solicitation for investments in securities in any jurisdiction. This Whitepaper is for information purposes only. The contents of this Whitepaper are not a financial promotion. Therefore, none of the contents of this Whitepaper serves as an invitation or inducement to engage in any sort of investment activity. Prospective acquirers of Velox tokens should carefully consider and evaluate all risks and uncertainties associated with the cryptocurrencies, Smart Urban Technologies Pte Ltd and their respective businesses and operations, the Velox tokens and the Velox Initial Coin Offering.

Familiarize yourself with all the information set out in this Whitepaper and the T&C prior to any purchase of Velox tokens. Ensure that you are aware of all of the would be risks prior to obtaining Velox. We recommend that you seek out independent financial advice before engaging in any sort of business endeavor.

10. Reference

[2] Ethereum https://en.wikipedia.org/wiki/Ethereum

[3] BMW, GM, Ford and Renault launch blockchain research https://techcrunch.com/2018/05/02/the-mobility-open-blockchain-initiative-bmw-gm-ford-renault/

[4] “Ethereum Next 12 Months” by Vitalik Buterin https://www.youtube.com/watch?v=jJt3yag96fU

[5] Ethereum’s Casper and Sharding Delay https://www.trustnodes.com/2018/07/08/ethereums-casper-sharding-delay-disappoints-can-2020-deadline-reached

[6] EOS smashes blockchain records with transaction speeds faster than visa. https://blokt.com/news/eos-smashes-blockchain-records-with-transaction-speeds-faster-than-visa

[7] Elliptic Curve Digital Signature Algorithm. https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

[8] SEC 2: Recommended Elliptic Curve Domain Parameters http://www.secg.org/sec2-v2.pdf

[9] Proof-of-stake https://en.wikipedia.org/wiki/Proof-of-stake

[10] TomoChain Whitepaper https://tomochain.com/docs/technical-whitepaper---1.0.pdf

[11] Sharding in Zilliqa blockchain https://docs.zilliqa.com/whitepaper.pdf

[12] Loom Network - highly scalable DPoS sidechains to Ethereum https://medium.com/loom-network/dappchains-scaling-ethereum-dapps-through-sidechains-f99e51fff447

[13] Cosmos – a decentralized network of independent parallel blockchains https://cosmos.network/docs/resources/whitepaper.html#introduction

[14] Polkadot: Vision for a heterogeneous multi-chain framework https://polkadot.network/PolkaDotPaper.pdf

[15] Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin http://zerocoin.org/media/pdf/ZerocoinOakland.pdf

[16] Josh Benaloh, Michael de Mare https://www.microsoft.com/en-us/research/wp-content/uploads/1993/01/owa.pdf

[17] Jan Camenisch, Anna Lysyanskaya http://cs.brown.edu/~anna/papers/camlys02.pdf

[18] IPFS – InternPlanetary File System https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

[19] Raluca Ada Popa and Nickolai Zeldovich https://people.csail.mit.edu/nickolai/papers/popa-multikey-eprint.pdf

[20] Payment Channel Technology in Raiden- https://raiden.network/101.html

[21] Hashlock - https://en.bitcoin.it/wiki/Hashlock

[22] Smart contract *RaidenMicroTransferChannels.sol* https://github.com/raiden-network/microraiden/blob/master/contracts/contracts/RaidenMicroTransferChannels.sol

[23] Velox Meta Transaction Relay https://github.com/VeloxChain/Velox_Meta_Transaction_Relay_Protocol

[24] Cryptokitties https://www.cryptokitties.co/

[25] Bike-Ownership protocol https://github.com/VeloxChain/VehicleOwnershipProtocol

[26] ERC721 standard OpenZeppelin https://github.com/OpenZeppelin/openzeppelin-solidity/blob/master/contracts/token/ERC721/ERC721Token.sol

[27] Smart Shared Bicycle Lock http://www.huawei.com/minisite/iot/en/smart-bike-sharing.html

[28] Mobike, AT&T and Qualcomm collaborate https://www.prnewswire.com/news-releases/mobike-att-and-qualcomm-collaborate-on-mobile-iot-smart-bike-share-technology-300516548.html

[29] MAT awarded at CES 2018 innovation awards http://www.esb.bike/mat-awarded-ces-2018-innovation-awards/

[30] ICOs, Token Sales & Compliance", Medium post byUnibright.io, April 2018, https://medium.com/@UnibrightIO/icos-token-sales-compliance-76992ab57028