VeChain
Whitepaper 2.0

#Creating Valuable TXs

VeChain Foundation
2019.12

1. VeChain's Vision

VeChain believes that blockchain technology is one of the foundations for the next generation of information technology, alongside emerging technologies such as AR, VR, AI, IoT, 5G and more. With the technology's immutable and tamper-proof characteristics, blockchain, as an infrastructural technology, is uniquely positioned to enable unprecedented value and data-transfer among a wide set of users in a trust-less manner, boosting the efficiency and authenticity of information transfer itself.

VeChain's vision of lowering the barrier and enabling established business with blockchain technology to create value and solve real world economic problems has been clear to us from the very beginning.

To achieve and fully harness this technology that will enable mass public adoption, we have identified the three major phases of blockchain evolvement – Technical Consensus, Business Consensus, and Governance Consensus. These phases will be the foundation and strategy to enable the VeChainThor blockchain to be adopted as the world's premier choice of blockchain.

1.1 Technical Consensus

In this phase, technical developers are the major force to build up the initial infrastructure protocols based on imaginations and projections. The competition is about programming language, protocol, algorithm and technical developer community.

Applications in this early stage of blockchain adoption are coming from the more obvious use cases that leverage features and functionalities of the blockchain technology, such as ICOs, DAOs, and betting applications (or gaming with betting features), along with infrastructure applications as needed like explorers, wallets, exchanges (centralized or decentralized).

Very few applications for the traditional business world are created in this phase, much less affecting and improving business use cases and activities. Blockchain platforms that focus on use cases such as traceability, anti-counterfeiting, food safety, intellectual property management, product life-cycle management and all kinds of data provenance categories are rarely to be seen. Initial blockchain applications in this stage are primarily motivated by technology enthusiasts, and business applications are mostly in the Proof of Concept ("PoC") stages by enterprise technical and R&D divisions to better understand the technology.

VeChain, from its inception in 2015 and until now, has successfully moved past this crucial first phase of blockchain technology adoption, and is primed for the next phase to achieve Business Consensus.

1.2 Business Consensus

With Technical Consensus achieved, the initial benefits that were derived from the early experimentation and PoCs would start to positively influence behaviour from business executives and decision makers. Enterprises and businesses who made the judgment to

invest in early blockchain R&D in the Technical Consensus phase would gain a lead over competitors.

Business Consensus would be the second major phase in the blockchain evolvement, where we will see business owners and enterprises become the major force to drive blockchain technology development and adoption, based on business needs and demands. This phase is all about understanding business needs, blockchain technology adoption and integration, user friendly interfaces, agile system structure, and business developers community.

In this phase, blockchain applications are built to enable cross enterprise collaborations and new collaborative values would be generated, following the first business moves to blockchain. The first initialization of collaborative ecosystems gets started with common business goals and consent economic motivations among multiple business owners including big corporations, small enterprises and individuals. Blockchain infrastructure applications are introduced to fulfill natural business and enterprise demands, such as custodian services, payment services, Blockchain-as-a-Service ("BaaS"), and privacy protections along with technology evolvements.

We anticipate that large corporations with existing market dominant positions and ecosystem resources are able to exert influence over the adoption of blockchain technology, including but not limited to Internet giants such as Facebook, Amazon, Google, Alibaba and Tencent, but also traditional players such as Walmart, DNV GL, PwC and so on. Basically, they are able to move their own existing ecosystem to be running on reliable blockchain platforms and look for expansions and interconnections to others. Ecosystem-level applications such as DNV GL's Digital Low Carbon Emission Initiative gets to unite multiple different stakeholders including governments, enterprises and United Nations in pursuit of a common goal (in this case, reducing the carbon footprint and attaining more United Nations Sustainable Development Goals). At the late stage of the Business Consensus, the increased attention and adoption of blockchain technology in major enterprises and businesses would compel authorities and regulatory bodies to seriously look at the blockchain space. With more and more influential public corporations, entities, organizations, and large global scale of people involved in the development and adoption of blockchain platforms, we can expect governments and countries (especially small and progressive countries) that are aiming for progressive policy, economics and technology advancement to gain strategic advantages.

For VeChain, we are currently at a critical stage of the Business Consensus with the VeChainThor platform being adopted by major enterprises and assurance companies with the right reach, abilities and competences to achieve this consensus, along with reaching out to government partners such as China, Malta, Republic of San Marino, Cyprus and technology partners such as AWS, Deloitte and so on. At this moment, VeChain is moving forward towards the next stage of the current phase of our vision, Governance Consensus.

1.3 Governance Consensus

Regulation and legislation are naturally demanded by citizens regardless of country to protect the people and guide new technology to maximise societal and economic utility. We believe that the ultimate consensus in the blockchain space is the consensus among governments and legal authorities around the world.

In this phase, authorities along with or against big corporations and insightful technical players are the major forces to drive the regulatory development of Blockchain technology and applications. The recent development by the intergovernmental FATF (Financial Action Task Force) has proven that with effort, consensus among nations and financial regulators is possible, but it is still in a very early stage. The race for blockchain adoption in this stage is about merging regulatory requirements with advanced features of blockchain technology. We believe that the key to achieving the requirements of this race is working towards a comprehensive governance consensus for the blockchain protocol with balanced levels of centralization and decentralization.

At this point, more business activities are moving to ecosystems and new collaborative business models creating new values to the world. Besides the regulatory requirements like KYC and AML, more supportive applications are expected to be developed and adopted by governments and financial regulators, including the introduction of new crypto-assets such as stable coins, settlement coins, ecosystem utility tokens within an incentive system and so on.

With blockchain interest in the spotlight as a result of the push by nations and governments, the level and prevalence of global collaborations is reaching to a new maturity. Creativeness and innovations within blockchain ecosystems with a focus on enabling new business values are popping up everywhere. The existing Internet giants are facing their biggest challenges yet in terms of deciding on disrupting their existing offerings in favour of blockchain platforms, while traditional business owners that took the risk to run PoCs and trials in the previous phase of adoption are sitting solid and concrete by focusing on improving the essence of business through means of a mature blockchain platform – quality and scalability of products and services. New giants that focus on providing a reliable and proven blockchain ecosystem would be taking over the place by taking advantage of the technology and bringing together even more stakeholders onto the ecosystem, rallying partners with a common goal to solve business problems.

While blockchain adoption has reached the Governance Consensus stage, it also means that it is running concurrently with the previous phases, progressing forward in parallel with each other. To truly provide a mature and reliable blockchain platform and ecosystem, technology providers such as VeChain need to understand that achieving consensus is a result of mutual effort and understanding the different requirements of all phases mentioned above.

Even at the Governance Consensus stage where blockchain awareness reaches new heights, it will not be a surprise that there would still be a sceptical feeling towards blockchain technology by existing entrepreneurs and even traditional tech enthusiasts. When Amazon and Alibaba first started the E-Commerce business idea and campaign 20 years ago, nobody was confident or believed that E-Commerce is going to be the disruptive new way of doing business, as even the adoption and practice of going online and surfing the web was inconvenient at that time, where internet access was limited. Yet, both Amazon and Alibaba succeeded in their endeavours by focusing on two major factors. Firstly, they have been constantly educating the entire world, and setting up the right motivations in the consumer's mind by charging minimal fees and providing incentives to sellers to move their business online. Secondly, they have been focused on building up a powerful and reliable infrastructure and all necessary accessibility and ease-of-use services and tools such as one stop service for E-Commerce site, payment tool, logistics service, digital marketing campaigns, arbitration,

and shared customer services, to enable people to take advantage of their platform even without any E-Commerce technology and knowledge.

VeChain's positioning in the blockchain ecosystem is now an Enabler, which will enable everyone in the world to create valuable transactions as big or small parts of future collaborative ecosystems. By working together with our aligned partners and providing all of the necessary tools and services, VeChain's mission is to enable the blockchain community, business owners, enterprises, governments or any other individual to move their business activities to blockchain effortlessly, similar to opening an online store in Amazon or Alibaba with just a few clicks without technical knowledge required. VeChain will fulfill our mission and vision of achieving all phases of the consensus mentioned above by working relentlessly.

2. The VeChainThor Blockchain

VeChainThor is a public blockchain that is designed for mass adoption of blockchain technology by business users of all sizes. It is intended to serve as the foundation for a sustainable and scalable business blockchain ecosystem.

From a technical point of view, the VeChainThor blockchain is built upon existing proven blockchain innovations and novel technologies that are created for achieving mass adoption. These technologies include the Proof-of-Authority ("PoA") consensus algorithm, meta transaction features, protocols of transaction fee delegation, on-chain governance mechanism, built-in smart contracts as well as tools for developers.

2.1 PoA 1.0

The Proof-of-Authority consensus is a consensus algorithm that demands nodes to be authorized in order to participate in the blockchain consensus. Once authorized, nodes are given equal chances to publish new blocks and gain rewards. As a result, there is no need for nodes to spend vast amount of resources to compete with each other. In addition, richer nodes do not have more advantages than other nodes in the system.

PoA is also an efficient consensus algorithm in terms of network bandwidth usage. It takes little time to decide block producers and thus, allows more time for transmitting transaction data. The system can, therefore, have a high throughput, or TPS ("Transactions Per Second"), within the range allowed by the underlying network.

PoA uses a heaviest chain rule to determine the canonical chain, or in other words, the "trunk". When forming a new block, the round leader will add the number of active consensus nodes, observed locally, to `TotalScore` of the latest block on the trunk and store the result in the new block. Other nodes will have to agree on the value to accept the block. A node will be marked 'inactive' by other honest nodes after it misses generating a new block in the round when it is the leader. An inactive node will be considered "active" once it produces a new block again. More technical details of PoA consensus can be found here.

2.2 PoA 2.0

Despite all the above-mentioned advantages and the fact that the VeChainThor blockchain has been working securely and smoothly on this consensus since its launch, PoA still has its own limitations. For example, like Ethereum, it lacks, algorithm-wise, an effective means to deter a node from manipulating the system when given the right to add a new block, although PoA makes sure that any traced misbehavior can be used as evidence against the node later.

Moreover, PoA belongs to the family of the Nakamoto consensus and therefore, only provides probabilistic assurance to the safety of transactions, which might not be enough to maintain system consistency against the extremely asynchronous situation such as being subject to large-scale network partitioning.

Therefore, we have been working on the next-generation PoA that will address these issues and provide the needed security and stability to support the ever-growing on-chain business

activities on the VeChainThor blockchain. As the outcome of our work, the new PoA will deliver:

1. absolute finality (or safety guarantee) on blocks and transactions
2. significant reduction of the platform's risk of being temporarily disrupted, which will result in better stability of blockchain service
3. faster-converging probabilistic finality, which will result in faster transaction confirmation for applications

2.2.1 Solutions

We propose to introduce two new mechanisms into the existing PoA protocol.

Committee-Endorsing Mechanism

The committee-endorsing mechanism fundamentally changes the way a block is created. More specifically, besides the selected block producer, it demands other nodes to participate in the process of forming a new block.

In each round of consensus, some nodes will be randomly selected as committee members. Committee members need to validate the proposal sent from the block producer and formally endorse the proposal by signing it. The consensus algorithm will demand the block producer to combine sufficient legit endorsements into the new block to make it valid. Furthermore, the verifiable random function (“VRF”) will be used to make sure that the committee members are truly picked randomly from all the nodes. Note that VRF functions similarly to a cryptographic hash function except that it requires a private key as input.

As a result, to create multiple conflicting blocks, the block producer will now have to work with a certain number of committee members. Due to the use of VRF, it can do so only if

1. it colludes with a number of nodes
2. among those nodes there are, by chance, a sufficient number of them being selected as committee members

The above conditions will make it much harder for the block producer to do so to disrupt the blockchain system. In other words, the probability of a node manipulating its right to add a new block will be kept extremely low. An important implication is that we will be able to reach a satisfactory probabilistic finality (e.g., the probability of a transaction being reverted is smaller than 0.0000001) much faster than the current PoA.

Block Finality Mechanism

The block finality mechanism grants qualified blocks absolute safety guarantee. Once a block acquires its finality, the consensus will assure that it cannot be modified, replaced or removed from the public ledger even when the network encounters some extremely asynchronous situation such as being subject to large-scale network partitioning.

In theory, a block can be considered final if it is confirmed by the BFT consensus. We adopt the framework Yin, et al that implements the BFT consensus as a consecutive three-phase

process. In each phase, more than two-thirds of nodes have to agree on the block to be confirmed.

To apply the framework, we embed features that carry information of the finality process in blocks and consider endorsing a block as the way the committee member confirms such information. As a result, we can achieve one phase of the BFT consensus on a particular block once observing more than two-thirds of nodes having participated in the chain that descends from the block. We also introduce additional rules to assure system's consistency and liveness.

In this way, instead of asking more than two-thirds of all the nodes to respond simultaneously, our algorithm requires only the block producer and committee to respond in time. As a result, the service will be less likely to be delayed or temporarily halted.

Summary

The next-generation PoA will introduce

1. committee-endorsing mechanism that significantly lowers the possibility of a node manipulating his right to produce a new block and results in faster converging probabilistic finality

2. block-finality mechanism that grants absolute safety guarantee to blocks (as well as the included transactions) that qualify certain criteria

It can be seen that both probabilistic and absolute finality will be allowed to coexist by the consensus protocol, providing different levels of security guarantee for applications running on the blockchain platform. In general, the higher security is required, the less efficient the application will be, and vice versa. Consequently, enterprises will be able to select the correct security guarantee that best suits their needs to maximize application performance.

2.2.2 Implementation

The implementation, testing and integration of the new PoA consensus on the VeChainThor blockchain will go through multiple phases. We would expect a brand new testnet to be launched for the debugging and testing purposes. Moreover, the algorithm details of the new PoA consensus mechanism will be published in multiple VeChain Improvement Proposals (VIPs).

2.3 Meta Transaction Features (Enhanced Transaction Model)

The VeChainThor blockchain implements an enhanced transaction (TX) model to tackle some of the fundamental problems that hinder the adoption of blockchain technology.

2.3.1 TX Uniqueness

Every blockchain system has to find a way to uniquely identify each TX, or otherwise, it would be vulnerable to the TX replay attack. For a UTXO-based blockchain like Bitcoin, TXs are linked and can be uniquely identified and verified by the associated spending history.

However, such uniqueness no longer holds for an account-based blockchain. For such systems, we need to inject some extra information into TXs to make them uniquely identifiable.

The VeChainThor blockchain achieves its TX uniqueness as follows. First, it defines the TX Nonce as a 64-bit unsigned integer that is determined totally by the TX sender. Given a TX, it computes two hashes, the hash of the RLP encoded TX data without the signature and the hash of the previously computed hash concatenated by the sender's account address. The second hash which is 256-bit long, is used as `TXID` to uniquely identify the given TX. Note that the calculation of `TXID` does not require a private key to sign the TX.

Further reading of the TX uniqueness here.

2.3.2 Multi-Task Transaction (MTT)

The VeChainThor blockchain allows a single transaction to carry out multiple tasks. To do that, we introduce the `Clause` structure to represent a single task and allow multiple tasks defined in one transaction. A task is defined by fields `To`, `Value` and `Data`. A `Clause` array, named `Clauses`, is then introduced in the transaction model to accommodate multiple tasks.

The multi-task mechanism has two interesting characteristics:

- The execution of tasks in a single TX is atomic, meaning that either they are all executed successfully or rejected all together.
- Tasks in a single TX are processed one by one in the exact order they are put in `Clauses`.

The multi-task mechanism provides a secure and efficient way to handle, for instance, tasks such as fund distribution, token airdrops, mass product registration.

2.3.3 Forcible Transaction Dependency

The VeChainThor blockchain provides a safety mechanism that allows users to force a TX to depend on the success of another TX. It has been done with the help of field `DependsOn` in the TX model. If `DependsOn` has been assigned a valid `TXID`, the system will check the status of the referred TX. Only if the status says successful, then the current TX will be accepted for processing. Here by successful, we mean two things: 1) the referred TX has been included in the ledger; and 2) it has been executed without being reverted.

The second requirement is particularly important since seeing a TX included in the ledger does not guarantee that it has been successfully executed. A TX can be included, but with a status "Reverted" which means that the system does not actually do what the TX asks it to do. For the dependent TX, there is no limitation on who sends it or when it is sent or what it is about. It offers developers much required flexibility.

Further reading of the forcible transaction dependency here.

2.3.4 Transaction Lifecycle Control

The VeChainThor blockchain gives users control of the lifecycle of the TXs they send. In particular, users can tell the system when is the earliest time their TXs can be processed and how long a pending TX expires via fields via fields `BlockRef` and `Expiration` defined in the TX model.

`BlockRef` can be used to store the reference to a particular block whose next block is the earliest block the current transaction can be processed. `Expiration` stores a number that can be used, together with `BlockRef`, to specify when the transaction expires. Specifically, the sum of `Expiration` and the first four bytes of `BlockRef` infers the height the last block that the current TX can be packed into.

The transaction lifecycle control is particularly useful when the blockchain is running at high capacity, because it gives users and developers definite control over when the transaction is executed or abandoned, which is highly demanded by business applications.

2.4 TX Fee Delegation

TX fee delegation mechanism is a mechanism that allows ordinary people to be able to use decentralized applications (dApps) without having to purchase cryptocurrencies and directly paying the TX fee caused during their interactions with dApps. In this way, users, when using dApps, could have the same kind of experiences when they are using normal mobile or web-based apps nowadays, and this is crucial for the mass adoption of blockchain technology especially under this stage when the regulation on cryptocurrency is still not clear. The VeChainThor blockchain is the first public blockchain that successfully implemented the TX fee delegation mechanism.

There are currently two protocols running on the VeChainThor blockchain that enable such a mechanism: the *Multi-Party Payment* (MPP) protocol and the *Designated Gas Payer* protocol. The former exists as a built-in protocol from day one of the mainnet launch while the latter was proposed in VIP-191 and implemented on July 22 in the VeChainThor v1.1.2 release.

2.4.1 MPP

MPP allows an account on the VeChainThor blockchain to pay fees for TXs sent from some designated accounts.

As illustrated in the above figure, there are three types of accounts involved in the protocol:

- USER: account sending TXs

- PAYER: account receiving TXs from USER and paying the TX fee
- MASTER: account from which the TX fee is actually deducted from. MASTER can be either PAYER itself if it is a normal account or the account deploys PAYER if it is a contract account (i.e., a contract with code)

Users can use the built-in contract `Prototype` to set up the MPP relation between PAYER and USER. Once such a relation has been established on-chain, when executing a TX from USER to PAYER, the VeChainThor blockchain will attempt to deduct TX fee from one of the three accounts in an order of MASTER => PAYER => USER. Users owning multiple MASTER accounts can also set up a SPONSOR account such that all the TX fees are deducted from a single SPONSOR account rather than from individual MASTER accounts, easing the work of managing multiple on-chain accounts. Find more details about MPP here.

2.4.2 VIP-191 - Designated Gas Payer

It is clear that MPP was designed from the point of view of a dApp owner who controls multiple contract accounts running on chain. It is the sole responsibility of the owner to set up MPP and the protocol can only affect TXs sent to those contracts. Moreover, since MPP requires writing data on chain and therefore, causes certain overhead cost, it is more cost-effective to use the protocol for a relatively stable relationship between a user and the dApp, rather than some temporary arrangement.

VIP-191 is aimed to supplement MPP in order to provide more flexibility for TX free delegation on the VeChainThor blockchain. In particular, it allows a TX sender to seek for an arbitrary party, not necessarily the TX recipient, who is willing to pay for the TX. The protocol works quite simple. It requires both the TX sender and payer to put their digital signatures in the TX. The sender also needs to turn on the VIP-191 feature to inform the system that it is a VIP-191 enabled TX. Once the TX is accepted and executed, the fee will be deducted from the payer account.

Comparison

In comparison to MPP, VIP-191 gives control back to TX senders to activate the protocol. Moreover, it does not introduce any overhead cost. However, it does require the TX sender and payer to be both online to complete the TX while MPP does not. In terms of transparency, MPP is the better option since the payer will have to explicitly put his/her intention to fund TXs from a particular account on chain (via executing functions of contract `Prototype`).

Implementation

VIP-191 has been implemented in the Thor v1.1.2 release. There have been two major changes made to implement the protocol:

- Extending the TX model
- Adding extra logic for deciding the actual gas payer for a VIP-191 enabled TX

Field `Reserved` in the TX body structure has been re-defined to be of type `reserved` as shown below:

```
type reserved struct {
    Features Features
    Unused   []rlp.RawValue
}
```

Within the structure, we define field `Features` as a bitmap where each bit marks the status (1 for on and 0 for off) of a particular feature. For VIP-191, the least significant bit is used. Moreover, VIP-191 requires two valid signatures to be included in the TX. The TX sender's signature is concatenated by the payer's signature and assigned to field `Signature` as usual. Moreover, the protocol requires the payer to sign `TXID` which is a unique identifier of the TX.

The extra logic brought by VIP-191 is added in function `BuyGas` in the Go source file `THORDIR/runtime/resolved_tx.go`. When determining which account pays the fee, the system first checks whether there is a dedicated payer. If the answer is yes, it then tries to deduct the initial cost of the TX from the payer's balance. If the balance is too low, the system will return an error. Otherwise, it will mark the payer in the runtime context associated with the TX and pass on the context to the code that executes its clauses.

Further reading of VIP-191 Designated Gas Payer here.

2.5 On-chain governance mechanism (pure technical)

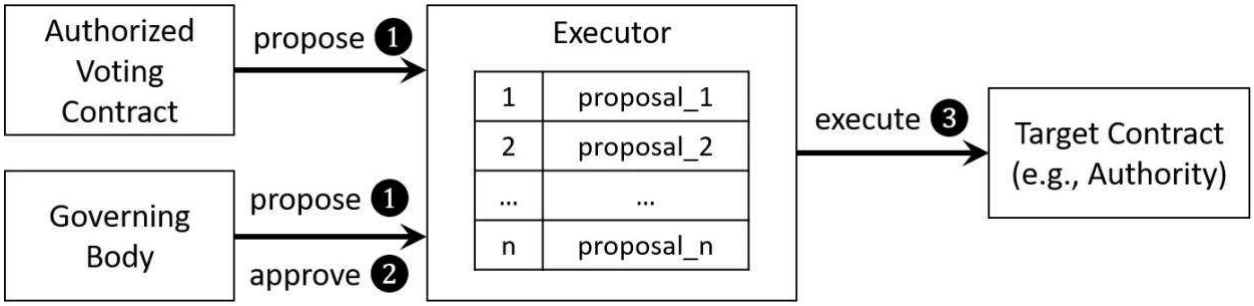
The VeChainThor blockchain's on-chain governance is about stakeholders or its governing body making decisions on some critical on-chain actions and executing those actions. (The governing body of the main-net is the Steering Committee of VeChain Foundation.) The actions can, for instance, be authorizing or revoking consensus validators (i.e., the Authority Masternodes), changing network parameters, such as the base gas price and block reward ratio, or any on-chain activity embodied by a smart contract deployed on the VeChainThor blockchain.

On-chain governance consists of three phases: decision making, authorization and execution:

- **Decision making** is the first phase where decisions on executing certain on-chain actions are made. Decisions are obtained through voting. Voting can be conducted either on chain via a voting contract or off chain within the governing body. The former provides maximal transparency and often involves all stakeholders, while the latter complements the former to offer efficiency and agility.
- **Authorization** is the second phase where a voted on-chain action is proposed to the governing body for final approval. Each proposal has to be approved by a majority of the members of the governing body. It is an extra security measure put in place to

safeguard on-chain governance against malicious activities (e.g., exploitation of voting-contract vulnerabilities).

- **Execution** is the final phase of on-chain governance. Once a proposal has been approved by the required majority, anyone can trigger the execution of the on-chain action defined in the proposal.



The VeChainThor blockchain provides a flexible framework for implementing the described on-chain governance, as illustrated in the above figure. At the center of the framework is contract `Executor` that is deployed both on the mainnet and testnet.

Contract `Executor` provides functions `propose` and `approve` to carry out the authorization phase. Only authorized voting contracts or members of the governing body can invoke function

```
propose(target_contract_address, encoded_data);
```

(marked by 1 in the above figure) to submit a proposal in `Executor`. The two function arguments define an on-chain action, i.e., invoking a specific function at a specific target contract address. A proposal is an instance of `struct proposal` stored in `Executor` and is created by function `propose`. Once a proposal is logged in `Executor`, members of the governing body are given a one-week time to authorize it. Each member can invoke function `approve` (marked by 2 in the above figure) to complete his/her authorization.

The *execution* phase is implemented simply by function `execute` of contract `Executor`. Once a proposal has been approved by the required majority (two thirds by default) of members of the governing body, Anyone can invoke function `execute` to trigger the execution of the on-chain action defined in the proposal using low-level call function:

```
target_contract_address.call(encoded_data);
```

It is often a safety practice that we code the target function of the target contract such that it can only be invoked by `Executor`. In this way, we are guaranteed that the action can only be executed after going through the process of on-chain governance. A good example of such a contract is the built-in contract `Authority` that manages Authority Masternodes.

Finally, a voting contract must be authorized before it can call function `propose` to submit proposals. Contract `Executor` provides functions `attachVotingContract` and `detachVotingContract` to manage the list of authorized voting contracts. Note that both functions have been coded such that they can only be invoked by `Executor` itself, meaning

that any change to the list has to be done through on-chain governance. It makes sure that voting contracts are managed securely and transparently.

Further reading of the on-chain governance here.

2.6 Built-in Smart Contracts

There are seven built-in smart contracts deployed on the VeChainThor blockchain. Their source code can be found in path `thor_root/builtin/gen`. They are called the built-in contracts not only because they are shipped together with the Thor source code, but because many of their methods are implemented natively in Go rather than in Solidity for the sake of efficiency. In fact, all functions whose names begin with `native` are such methods. Whenever these functions are called, the system will intercept the normal EVM procedure and run the native Go code instead.

Here we give some brief description of each of the built-in contracts.

1. Source code: `authority.sol`

   Deployed Address: `0x0000000000000000000000417574686f72697479`

   Contract `Authority` provides methods to deal with the Authority Masternodes (AMs). Users can use functions `get` to query the status of a particular AM and use `first` and `next` to iterate existing AMs. It also provides functions `add` and `revoke` to authorize and deauthorize an AM. These two functions can only be invoked by contract `Executor` via on-chain governance.

2. Source code: `energy.sol`

   Deployed Address: `0x0000000000000000000000000000456e65726779`

   Contract `Energy` defines the interface for operations on VTHO.

3. Source code: `executor.sol`

   Deployed Address: `0x0000000000000000000000004578656375746f72`

   Contract `Executor` provides methods to facilitate on-chain governance on the VeChainThor blockchain. We have provided an extensive discussion on it in the previous section.

4. Source code: `extension.sol`

   Deployed Address: `0x0000000000000000000000457874656e73696f6e`

   Contract `Extension` is implemented to allow contract code to query information of a previous block or be aware of the runtime information of the current TX. For the former purpose, it provides methods `blockID`, `blockTotalScore`, `blockTime` and `blockSigner` while for the latter purpose, it provides methods `totalSupply`,

`txProvedWork`, `txID`, `txBlockRef` and `txExpiration`. We can also invoke the natively implemented Blake2 hash function via method `blake2b256`.

5. Source code: `extension-v2.sol`

   Deployed Address: `0x0000000000000000000457874656e73696f6e5632`

   Contract `ExtensionV2` is an extension of contract `Extension`. It defines a new method to query the actual gas payer of the current TX.

6. Source code: `params.sol`

   Deployed Address: `0x0000000000000000000000000000506172616d73`

   Contract `Params` provides methods `get` and `set` to check and set the global network parameters. There are two such parameters: the reward ratio and base gas price that are indexed by keys (32 bytes) `0x0000000000000000000000000000000000000000726576172642d726174696f` and `0x0000000000000000000000000000000000626173652d6761732d70726963e65`

   in the system, respectively. The keys are required as the input to the above two functions and are used to locate the parameters in the blockchain state. Function `set` can only be invoked by contract `Executor` via on-chain governance.

7. Source code: `prototype.sol`

   Deployed Address: `0x0000000000000000000000050726f746f74797065`

   Contract Prototype is implemented to facilitate MPP and query information of a particular account. For the former purpose, it provides methods `master`, `setMaster`, `creditPlan`, `setCreditPlan`, `isUser`, `userCredit`, `addUser`, `removeUser`, `sponsor`, `unsponsor`, `isSponsor`, `selectSponsor` and `currentSponsor`. To query account information, it provides methods `balance`, `energy`, `hasCode` and `storageFor`.

2.7 Connex.js and Sync

As mentioned above, the VeChainThor blockchain has implemented many unique features to establish the foundation for a sustainable and scalable business blockchain ecosystem. To enable the 3rd party developers to fully leverage the aforementioned features, Connex API Standard is proposed to unify the communication between a client application and a running VeChainThor blockchain node.

2.7.1 Connex API Standard

Connex is not simply a client-side library but a set of well-designed APIs that allows re-implement across different environments by different vendors. As long as the implementation adheres to Connex Standard, the 3rd party developed dApps can be expected to run on those platforms without modification.

Currently, the Connex.js definition library released demonstrates the common behaviors according to the standard. Frontend applications running in browsers-alike environments can be a benefit with such interface regardless it is on mobile or desktop.

Connex exposes several crucial yet useful APIs to 3rd party developers to fully utilize the VeChainThor blockchain features such as MTT and ease the developer's life with up-to-date blockchain updates. Here are some examples.

Always Up-to-date Tip of Blockchain Status

Connex defines a `connex.thor.ticker()` object which is a `Promise`. Once the `ticker` ticks, the application can be sure a new block is included in the VeChainThor blockchain. This event trigger keeps dApps noticed whenever there are new changes and prevents the application from polling the blockchain mindlessly.

Multi-Task Transaction (MTT) support

Once the application depends on Connex as a low-level environment, the MTT feature is coming out of the box. Whenever a contract method is called, for example, `transfer()` method, a developer can chain-up several tasks by calling `transfer().asClause(…)` to box several operations into a single blockchain transaction.

Signing Service and Fee Delegation

As Connex definition does not include wallet implementation details, vendors can freely define the proper secure mechanism suitable for each environment according to devices (eg. Ledger, browser, or mobile apps). However, they all adhere to the same signing interface as `vendor.sign('tx')`.

`vendor.sign('tx')` is called right before the application sends out the transaction. The dApp calls `signingService.request(…clauses)` to ask the user to sign the blockchain transaction. To utilize the feature of VIP191 designated gas payer fee delegation, the vendor should further support `signingService.delegate(…)` to obtain another level of signature of a sponsor, thus the end-user can use the VeChainThor blockchain without too much hassle of paying for it with cryptocurrency.

Advanced User Identification

The Connex standard also includes a user identification API which allows the dApp to identify an account holder without a single online transaction to be performed. When the dApp triggers `vendor.sign('cert')` method, the user will be prompted and sign a self-identifying message. After the successful identification, the dApp can be sure this user holds the specific

account. This unique feature eliminates the friction to ask a user to sign an on-chain transaction which is costly and less time-efficient.

More details about the Connex API can be found here.

2.7.2 Sync and other clients

As the VeChainThor blockchain grows in the number of users and applications, the user interface on the front-end especially browser-like environment proves to be the easiest way for end-users to enjoy blockchain technology.

VeChain has released Sync, an open source browser-like client that internally implements the Connex standard for dApps to be run and debugged. Sync today has become a multi-platform full-fledged desktop client on Windows, Mac, and Linux.

Functionalities of Sync are so rich that it includes a wallet management section which enables a user to import/export wallets in the form of mnemonic words, key stores, private keys. An end-user can also connect a Ledger hardware wallet to Sync to sign transactions or self-proving certificates.

Apart from being a strong crypto wallet, Sync's internal Connex implementation supports dApps with various needs. As for today, many dApps such as token transfer, games, chatting rooms, decentralized exchanges all can be run in Sync just like any given web-based application.

Thanks to the Connex standard, other client-side software can all seamlessly run dApps developed. This is truly "develop once, run everywhere" and ease the burden for 3rd party developers to customize their applications accordingly.

2.8 VIPs

VeChain Improvement Proposals (VIPs) are ideas from developers and communities to improve the VeChainThor blockchain. As an open-source project, VeChain has a lively community that has proposed many features such as fee delegations, user identification.

There are four types of VIPs: core, application, interface, and information. The core type needs a consensus fork to take into effect; Application type will modify the standards and conventions; Interface type requires to modify the client API and message structures; the Information type does not require changes to the blockchain itself but rather provides information of guidelines.

Any VIP will go through several stages, known as the draft, accepted/deferred/withdraw or final. When a VIP is in the draft stage, it can be modified by the proposer or the reviewer; After the technology committee review and discussion of the development team, it will either be accepted or deferred. Once accepted it will be soon be implemented, however, if deferred it will be postponed for future implementation. Once implemented, the VIP then will go to the last stage of the life cycle - final.

3. Governance

3.1 Overview

Although decentralization is the well-known cornerstone of blockchain technology, in its pure form it has obvious defects leading to inefficiency and poor capacity to conduct fast iterations. We believe scalability issues relating to blockchain are not linked to technical problems but to consensus concerns of governance. Continuous updates and additions to the features and functions of blockchain are a natural product of the evolution of the technology, its use cases, and its applications.

A proper governance system, with transparency and operational efficiency, will enable continual and rapid innovation.

In order to achieve the main goal of operating a decentralized public blockchain with the capacity to scale and at the same time complying with regulators, governments and to meet the needs of large enterprises, the next step in VeChain's decentralization journey is to improve its governance model with the ability for continuous iterations alongside rapid progression in ecosystem development. To achieve this new governance consensus, we aim to identify the right stakeholders and determine how such stakeholder classes will be represented and how the authority to make decisions will be allocated.

It is important that such a governance model is both efficient and cost-effective, while resulting in consensus and decisions that balance the views of all stakeholders of the blockchain. The following Governance Principles and Charters are adopted by the VeChain Foundation to serve as a flexible framework to assist the Board of Steering Committee (referred to as, the "Board" or "SC") in the exercise of its responsibilities.

These Governance Principles reflect the Board's commitment to monitor the fairness and effectiveness of policy and decision making for the Foundation and should be interpreted in the context of all applicable laws, VeChain Foundation charter documents and other governing legal documents and are subject to modification from time to time by the Board.

3.2 Foundation Governance Structure

The VeChain Foundation is a nonprofit entity, committed to the development, governance and advancement of the VeChain ecosystem. The decentralized operating mechanism of the blockchain technology grants the Foundation a unique governance structure. The diagram below provides a stylized view of the Foundation's current governance structure.

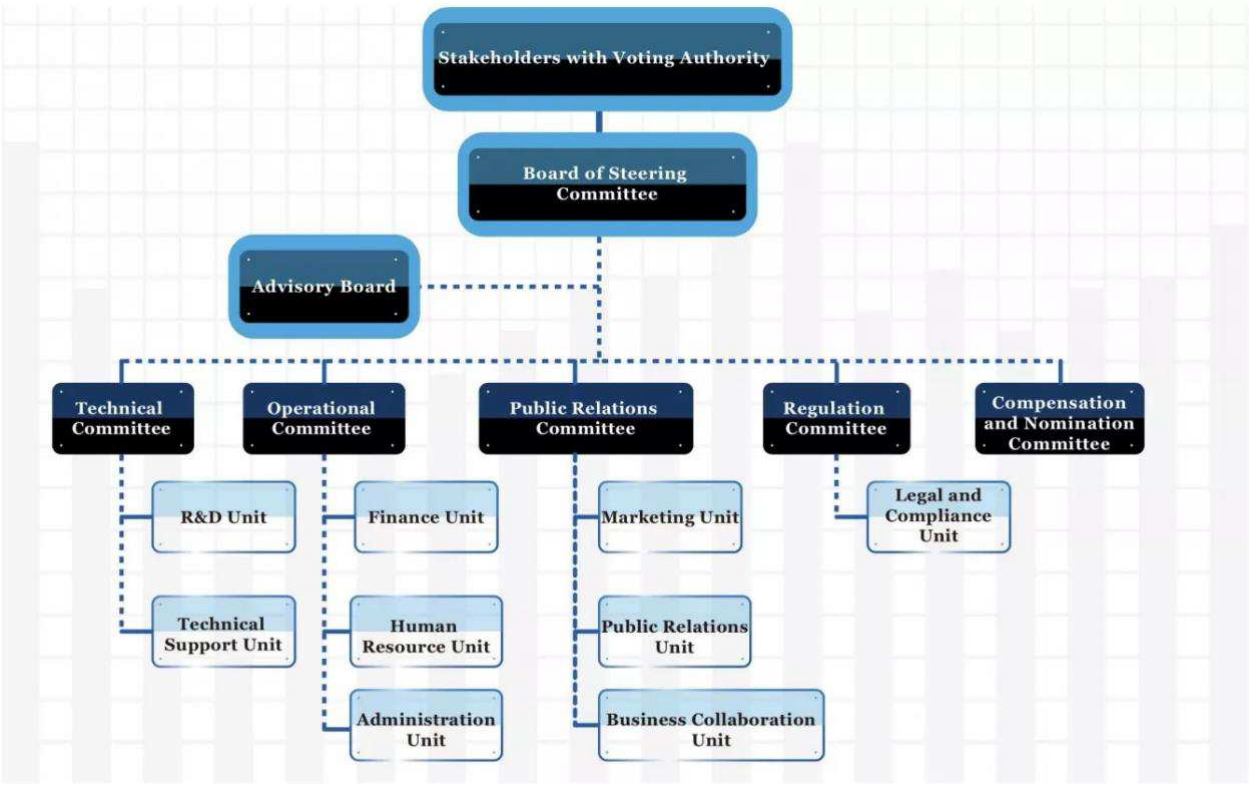


Figure3.2 Foundation Governance Structure

The Board of Steering Committee is the governing body of the VeChain Foundation. It is selected by Stakeholders with Voting Authority. The Steering Committee lays out the critical strategies and selects functional committee chairs to oversee the operational units of the Foundation. However, for fundamental subjects which could cause a significant impact on the Stakeholders, the all stakeholder voting is required. The fundamental subjects are as follows:

1. The election of the new Board of Steering Committee
2. Fundamental change to the consensus mechanism of the VeChainThor blockchain (updates or enhancements on the existing PoA consensus are not included)
3. Modification to the generation velocity of VTHO via holding VET
4. Other subjects that the Board of Steering Committee deem necessary for the all stakeholder voting

3.3 Stakeholders with Voting Authority

3.3.1 Stakeholders

In the VeChain ecosystem, stakeholders with voting authority is comprised of three categories i.e. Authority Masternodes, Economic X Nodes and Economic Nodes. Each category has different voting authority. The stakeholders can be individuals, corporations, government agencies, non-profit organizations and other institutions with a stake in the VeChain ecosystem, additionally Authority Masternode holders must go through Foundation's identity

verification and background check. The stakeholder voting mechanism ensures the inclusiveness of all designated stakeholders in the VeChainThor blockchain ecosystem.

Authority Masternodes

Authority Masternodes are network maintainers of the VeChainThor blockchain, and each of the node operator must hold at least 25,000,000 VETs at any given time. Currently, there are 101 active Authority Masternodes held by either corporations or individuals whose identities have been verified by the Foundation. Authority Masternodes are the only nodes that are authorized to pack blocks on the VeChainThor blockchain and they are rewarded by 30% of the transaction fee in each block.

Economic X Nodes

Economic X Nodes and Economic Nodes were created as the Foundation's initiative at the early stage of the ecosystem. Each node holder needs to stake a minimum amount of VETs and wait for the maturity period according to the node type and tier. The status of Economic X Node and Economic Node is tokenized according to VIP181 standard and managed via open source the VeChainThor Node smart contracts.

Economic X Node holders lie at the center of the VeChain community. The initiative was started on March 20, 2018 in a way that no new Economic X Node can be created, and Economic X Nodes can only upgrade their node tier. Therefore, the total number of Economic X Nodes will only decrease over time. Economic X Node holders are considered as long time supporters of the VeChain ecosystem. More information about Economic X Nodes can be found here.

There are four tiers of Economic X Nodes:

Node Tier	Minimum VET Holding	Maturity Period
Mjolnir X Node (MX)	15,600,000	90 Days
Thunder X Node (TX)	5,600,000	60 Days
Strength X Node (SX)	1,600,000	30 Days
VeThor X Node (VX)	600,000	No new VeThor X Node can be created

Economic Nodes

While the number of Economic X Nodes can no longer increase, any VET holder can apply to become an Economic Node at any time. Any VET address above the minimum holding requirement can apply via the VeChainThor Node smart contract and wait for the maturity period before the creation or upgrade is completed. More information about the Economic Nodes can be found here.

There are three tiers of Economic Nodes:

Node Tier	Minimum VET Holding	Maturity Period
Mjolnir Node (M)	15,000,000	30 Days
Thunder Node (T)	5,000,000	20 Days
Strength Node (S)	1,000,000	10 Days

3.3.2 Stakeholder category and the voting authority model

The following table summarizes different categories of stakeholders and their corresponding voting authority.

Category	Node Tier	Minimum VET Holding	Votes per Node (in-category)	Voting Authority
Authority Masternodes (AM) **KYC required*	N/A	25,000,000	1 AM vote	**40%**
Economic X Nodes (XN)	MX	15,600,000	26 XN votes	**40%**
	TX	5,600,000	10 XN votes	
	SX	1,600,000	3 XN votes	
	VX	600,000	1 XN vote	
Economic Nodes (EN)	M	15,000,000	15 EN votes	**20%**
	T	5,000,000	5 EN votes	
	S	1,000,000	1 EN vote	

All the above statuses are managed on the VeChainThor blockchain, stakeholders are responsible for keeping their status active in order to participate in the voting and have their vote authority calculated accordingly.

Active Authority Masternode holders (AM)

Each active AM holder staking a minimum of 25,000,000 VETs in the Authority Masternode collateral address has 1 vote. The total voting authority for all AM holders accounts for ω_{AM} = 40% of overall voting authority.

Economic X Node holders (XN)

Economic X Nodes are comprised of four tiers i.e. Mjolnir X Node (MX), Thunder X Node (TX), Strength X Node (SX), VeThor X Node (VX). The minimum VET holding of each active Economic X Node differs based on the node tiers. Each VX Node has 1 vote and the number of votes per node increases with the node tier.

- Mjolnir X Node: 26 votes
- Thunder X Node: 10 votes
- Strength X Node: 3 votes
- VeThor X Node: 1 vote

The total voting authority for all XN holders accounts for ω_{XN} = 40% of overall voting authority.

Economic Node holders (EN)

Economic Nodes are comprised of three tiers i.e. Mjolnir Node (M), Thunder Node (T), Strength Node (S). The minimum VET holding of each active Economic Node differs based on the node tiers. Each S Node has 1 vote and the number of votes per node increases with the node tier.

- Mjolnir Node: 15 votes
- Thunder Node: 5 votes
- Strength Node: 1 vote

The total voting authority for all EN holders accounts for ω_{EN} = 20% of overall voting authority.

Aggregation

The final voting result V can be computed as:

$$V = \omega_{AM}V_{AM}+\omega_{XN}V_{XN}+\omega_{EN}V_{EN}$$

where V_{AM}, V_{XN}, $and\ V_{EN}$ stand for the voting results for categories AM, XN, and EN. All the weights satisfy $\omega_{AM} + \omega_{XN} + \omega_{EN} = 1$ and their values can be adjusted by the Steering Committee when deemed appropriate. The vote of a single address can only be counted towards the category based its highest status. Through this equation an example result for EN may be split 15% “Yes” and 5% “No” in a Yes or No vote.

3.3.3 All Stakeholders Voting

Prior to an all stakeholder voting event, the Foundation will announce detailed rules such as voting day, voting period and minimum participation rate of each stakeholder category. Because all of the stakeholder statuses are managed on the VeChainThor blockchain, on the voting day, stakeholders with an active status in any of the three categories are eligible to cast their votes via the VeVote platform. Their votes will be counted towards the voting authority in the corresponding stakeholder category.

In addition, for any voting event to be considered as effective and not to be manipulated by a small percentage of stakeholders, the participant rate in each stakeholder category at the end of the voting period needs to be above a predefined threshold according to the voting announcement. If the participation rate does not meet the minimum requirement in one stakeholder category, the voting authority of that category will be allocated to the higher stakeholder category(ies) proportionally. If there are not enough Authority Masternode holders participating in the voting, its voting authority will be allocated to the Steering Committee. However, if none of the stakeholder categories meets the minimum participation requirement, a new voting event would be initiated. To ensure the efficiency of governance at the early stage of the platform, the Steering Committee reserves the right to make the decision among the Steering Committee members if the voting event fails twice in a row.

New Board of Steering Committee Election

According to the Foundation Governance Charter, the term for the Steering Committee is two years. Therefore the election of the new board of Steering Committee will happen every two years from the launch of the VeChainThor blockchain mainnet.

The nomination committee, with assistance from the administrative unit, will announce the detailed rules and timeline of the whole election process in advance. The existing members of the Steering Committee are by default considered as candidates for the new Board. The nomination committee will nominate candidates based on the size of the Steering Committee. In addition, the nomination committee will review and assess the applications received from public and add qualified applicants as candidates. In case that the number of qualified candidates exceeds twice the proposed number of the new board, a preliminary all stakeholder voting will be conducted to shrink the number of qualified candidates from public applications. Please see section 4.2.3 for more detailed rules.

A final shortlist will be announced by the nomination committee before the final election. The new Board of Steering Committee should be elected by all eligible stakeholders with voting authority two months before the term of the existing Board ends. The nominees will be ranked by number of votes and the membership will be granted to the candidates with the highest number of votes, based on predetermined Board size and composition rule. The results of the election will be announced by the nomination committee within 48 hours of ballot end time.

3.4 The Board of Steering Committee

The Steering Committee is the governing body of the VeChain Foundation. They define the important strategies and select functional committee chairs to oversee the operation of the Foundation. Designed for visibility, inclusiveness, transparency and efficiency, the Foundation will ensure the development, innovation, coordination and advancement of the VeChainThor blockchain ecosystem.

The Board believes that all committee members represent the balanced interests of the multiple stakeholders as a whole.

The Board represents the VeChainThor blockchain stakeholders' interest in long-term development of the technical infrastructure, business expansion, and VET value enhancement. The Board also recognizes the important role the Foundation plays in the blockchain

ecosystem and the importance of providing active governance, designed to ensure the safety and soundness of the operations within the VeChainThor blockchain. The Board is responsible for establishing the general oversight and framework, including the design of the operating rules of the blockchain, intended to achieve these goals.

The Board's principal functions are to:

1) Propose and organize all stakeholder voting events for fundamental issues of the VeChainThor blockchain

2) Review, approve, and monitor the Foundation's major strategic, technical, financial, and business activities

3) Review, modify and approve the governance principles of the Foundation

4) Review, approve and monitor the Foundation's annual budget, financial status including VET holdings, use of proceeds and its major transactions

5) Review, approve and monitor the procedure of nomination and election of the Steering Committee members, functional committee chairs and the General Secretary of the Foundation

6) Review, approve and monitor the operation model of VTHO (operating cost basis of the VeChainThor blockchain) and valuation model of VET

The Board is elected by the stakeholders with voting authority for their terms, and it is composed of representatives from the VeChain Foundation, Authority Masternode holders, developers, enterprise users, business partners as well as independent member(s). The Board meets at least once a quarter led by the General Secretary of the Steering Committee. For more details about composition, criteria, termination of the Steering Committee, please see the VeChain Foundation Governance Charter.

The current Steering Committee member profiles can be found on the VeChain Foundation Website.

3.5 Advisory Board

In addition to the Steering Committee, the Foundation seeks members from diverse professional backgrounds with a broad spectrum of expertise to serve on the Advisory Board which will provide industry insights and advice to assist the Steering Committee.

Members of the Advisory Board, in a predetermined order, serve as standby members for members of the Steering Committee in the case of termination or voluntary leave of any existing Board members during the current term. The current Advisory Board members can be found on the VeChain Foundation Website.

3.6 Functional Committees

The Board has established the following Committees: Technical, Operational, Public Relations, Regulation, Compensation and Nomination. Each of the committees should be chaired by one

of the Board of Steering Committee members or Advisory Board members and include key managers of the functional units as members. The Compensation and Nomination Committee should be chaired by an independent member of the Board of Steering Committee or a member from the Advisory Board. Committee assignments and the designation of Committee Chairs should be based on the members' knowledge, interests and areas of expertise.

The Board agenda shall include regular reports from the Chairs of each of its Committees on their proceedings and deliberations. The Committees shall bring to the Board for consideration those matters and decisions which the Committees judge to be of special significance.

For the introduction of functional committees, please see the VeChain Foundation Governance Charter.

3.7 Authority Masternode Management

3.7.1 What is an Authority Masternode?

The VeChainThor blockchain uses a Proof-of-Authority (PoA) consensus in which each transaction is validated by Authority Masternodes (AM), however, the VeChainThor blockchain node program is open source which means it does not require any permission to synchronize the full ledger of VeChainThor blockchain and initiate transactions on it. An AM is a network-connected server running the VeChainThor full node program which keeps a complete copy of the blockchain. Additionally, Authority Masternodes are the full nodes authorized via an on-chain whitelist to validate and produce blocks of the VeChainThor blockchain. The whitelist of Authority Masternodes is managed through the `Authority` built-in smart contract which requires multi-signature authorization of the VeChain Steering Committee members to make any modification.

All AM holders must do the following: a) be vetted to ensure that they have a legitimate identity, b) hold 25M VETs as collateral, and c) run and manage a server with a certain guaranteed level of performance and availability. More importantly, in addition to those minimum qualifications, AM holders are responsible for actively contributing to the VeChain ecosystem in their own fields.

As an incentive to AMs for maintaining the integrity of the blockchain, contributing to the VeChain ecosystem, and participating in the platform governance, the network rewards the AMs with VTHO tokens which is a native VIP180 token representing the transaction fees of the VeChainThor blockchain. In each block, 30% of the VTHOs consumed by transactions are paid out to the AM that produces the block. The other 70% of VTHOs are burned. On the VeChainThor blockchain, Authority Masternodes do not compete to produce blocks, rather the block producer is selected by a random algorithm. This helps solve one of the key concerns from enterprises to run a consensus node on a public blockchain regarding computing power / energy consumption: the PoA consensus consumes far less energy than Proof of Work. In addition, Authority Nodes are entitled to the highest weight per vote in the all stakeholders voting, based on the VeChain Governance Model. Collectively, AMs hold a total of 40% of the total voting authority.

The design of the PoA consensus and Authority Masternodes lies at the center of the VeChain Governance model. Unlike most public blockchains on the market, the VeChain AM holders are subject to strict Know Your Customer ("KYC") verification, and their reputation is part of the stake, in addition to the financial collateral. The VeChain Foundation conducts strict identity verification and hold AMs accountable for their activities and obligations to the ecosystem.

3.7.2 How are the AMs managed?

The Foundation seeks corporates and individuals that have aligned interests and are able to contribute to the growth of the VeChain ecosystem to apply to be AM holders, which may include but are not limited to the following roles:

- Enterprise users
- Blockchain development teams
- Business and technical development partners
- Community contributors
- Academic research partners

Corporates or individuals can apply to become an AM holder after going through the KYC process and obtaining a VeVID in the VeChain Portal. The VeChain Foundation operation team and its Steering Committee review the applications based on a set of selection criteria, and approved applicants are eligible to become Authority Masternode holders. The criteria covers both quantitative basic requirements and the ability to contribute to the ecosystem.

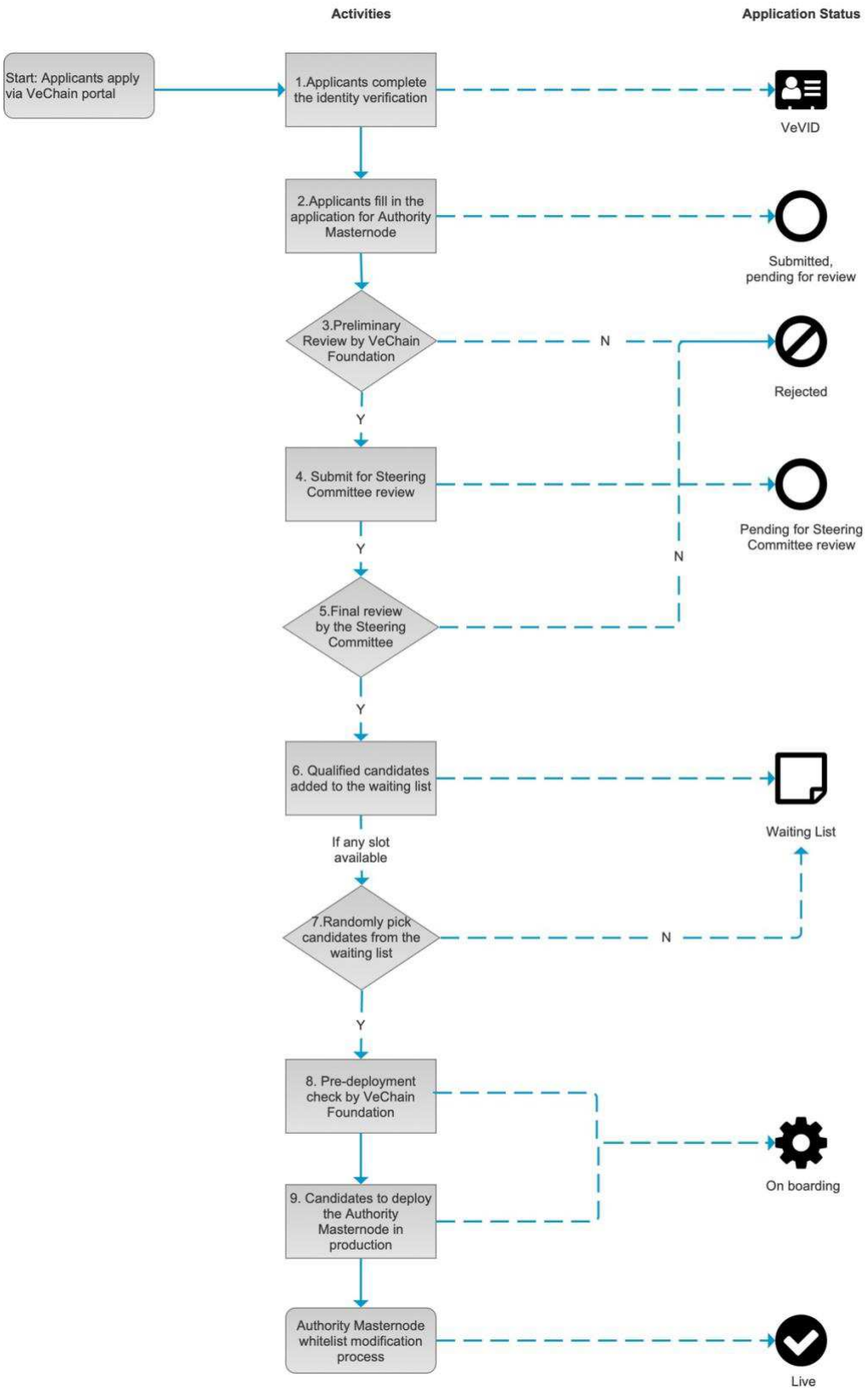


Figure 3.7.2 Authority Masternode Application Process

As the foundation of the VeChainThor blockchain, AM holders must maintain the security and availability of the Authority Masternode as well as contribute to the VeChain ecosystem. In order to measure the performance of AM holders, VeChain Foundation operation team

continuously monitors metrics relating to Authority Masternode Performance and VeChain Ecosystem Contribution. Failure to meet the requirements may result in the AM holder being disqualified.

For more details of the AMs management lifecycle, please refer to the Authority Masternode Handbook.

3.7.3 Authority Masternode Identity Disclosure

It has always been the VeChain Foundation's goal to provide the community with transparency. The Proof of Authority consensus relies on the public reputation of the node holders, on the other side, we all witnessed the fallout of Libra association where enterprises chose to withdraw as masternodes due to regulatory ambiguity. Though the VeChainThor blockchain was launched in June 2018, our AM holders especially enterprise holders shared the same perspective and some of them would prefer to keep their identities and activities on the blockchain from the public. However, the VeChain Foundation and its Steering Committee (who is elected by the stakeholders with voting authority, see section 3.2 for more information) apply strict identity verification and assessment during the onboarding process to ensure that legality of AM holders' identities and AM holders are able to make contributions to the VeChain ecosystem. For the stability of the VeChain ecosystem at its early stage, we understand that while AM holders are pioneers and innovators in their own fields to join a public blockchain network for a distributed business ecosystem, many of them want to spend more time to explore and gain more clarity from both technical and regulatory perspectives.

Therefore, during the trial phase of the VeChain Authority Masternode program, the Foundation has decided that it would be at the AM holder's discretion to disclose the status as an Authority Masternode holder to the public. New Authority Masternode applicants that are willing to disclose the status will be favored in the on boarding assessment. As the AM program matures, the VeChain Foundation aims to work closely with the AM holders to provide more transparency.

3.8 Financial Management

From a financial perspective, the VeChain Foundation's goal is to maintain a healthy financial status to support the advancement of VeChain blockchain technologies and the sustainable development of the VeChain ecosystem.

The VeChain Foundation set up a full-time financial management team to efficiently manage the finances and economic resources of the organisation. The team is responsible for financial planning, accounting, compliance and financial control to aid the management in better decision making. The financial management team periodically reports the financial status and planning to the Steering Committee.

3.8.1 Funding Sources

As a non-profit organization, the VeChain Foundation does not distribute profits or dividends to the founding team, controllers or shareholders in the Foundation. However, the Foundation will actively seek income to fund the sustainable development of the project. The income,

subtracted the operational expenditure, will all be allocated to the cause of ecosystem development. According to VeChain Foundation's operation model since inception, we have established several income streams to maintain a healthy financial status and support the long term development of the VeChain ecosystem.

- Asset management & investment

VeChain Foundation allocates about 10% of its capital to further invest in innovative projects on the VeChainThor blockchain that create value to the ecosystem. The Foundation injects a portion of the funds into the VeChain Ecosystem Fund which is a joint effort with reputable venture capitals in both blockchain and traditional sectors to further expand the development of the VeChain ecosystem. In addition, the Foundation hires professional third party service providers to manage its proceeds in fiat and cryptocurrencies such as BTC and ETH to mitigate the risk of market volatility and enjoy the appreciation of the unused assets.

The gain from the investment and asset management will be reused to fund the technology advancement and ecosystem development.

- Professional services

The VeChain Foundation, as the key enabler of the ecosystem, sometimes receive payment in fiat or digital assets for the services provided. For example, the project management team in the Foundation provides consulting or development services to traditional enterprises to ease the process of developing, building, maintaining and generally transforming their businesses by using the blockchain technologies provided by VeChain.

The Foundation experts also provide paid professional trainings to traditional enterprises, industrial associations, government agencies. As blockchain technology becomes more mainstream, the need to understand blockchain technology and use cases will significantly increase.

- Service / solution packages with VTHO support

From the long term perspective, as the VeChain economic model reaches its equilibrium, the VeChain Foundation will receive income for the VTHO generated from its VET reserve. The two token economic model of the VeChainThor blockchain is designed to detach the cost of using the blockchain with the market volatility. VET holders have equal rights to receive VTHO which can be used to conduct transfer and smart contract transactions on the VeChainThor blockchain.

Thanks to the economic model design, many developers and enterprise users in the VeChain ecosystem purchase VET on the open market to generate VTHO for their applications or directly purchase VTHO on the market. However, due to the ambiguity of the cryptocurrency regulations and standards, in the near future some of the enterprises will still opt to pay an intermediary or a third party on a lump sum or subscription basis, so that the third party can take care of the VTHO as part of their service or solution packages by utilizing the fee delegation feature of the VeChainThor blockchain.

3.8.2 Quarterly Financial Report

In the principle of transparency the VeChain Foundation publishes quarterly financial reports which cover the latest VET supply distribution (i.e. circulating supply vs non-circulating supply) and main expenditure in the areas of technical R&D, business development, compliance & legal and ecosystem development.

VeChain Foundation Quarterly Financial Executive Reports are available at the official blog.

3.8.3 Financial Policy & Compliance

The VeChain Foundation thrives to run a blockchain organization that is compliant with laws and regulations in relevant jurisdictions. To do this the financial management team keeps close contact with various regulators, advisors and auditors. The Foundation files financial audit reports and tax reports in Singapore based on the conversation with auditors, tax advisors and regulators. In addition, we work with big 4 accounting firms to define policies and procedures of accounting, reporting, taxing, and filing & disclosure, although we understood that there is still not clear financial reporting GAAP established for cryptocurrencies under any legislation.

Due to the decentralized nature of cryptocurrencies, the Foundation works closely with external advisors to optimize its internal controls and risk management processes. The financial management team applies a series of internal controls to securely manage its digital assets.

1. Segregation of duties - both technical and manual measures have been put in place to ensure that at least two authorized persons are needed to access digital asset wallets or move any funds, and internal control personnel must present during any operation relating to private keys

2. Wallet usage and amount limits - clearly define the usage of digital asset wallets and set corresponding limits on the amount that is allowed to be stored in each wallet

3. Continuous monitoring - the monitoring mechanism is built to supervise the use of digital assets. Any abnormal use of the assets will trigger an alarm so that an independent team will consider further investigation of such use. In addition, the reconciliation between accounting books and digital assets ledger is performed on periodical basis

4. Incident response plan - formal incident response plan has been established and approved by the Steering Committee. It defines various scenarios of emergency state based on the severity, and formalizes all critical elements such as the roles and responsibilities, handling procedures, communication plan, remediation and recovery, interactions with law enforcement, etc. In any unforeseeable scenario, it is up to the Steering Committee to call for emergency meetings and propose temporary solution in the best interest of all stakeholders, which should be agreed by Authority Masternodes or all stakeholders in extreme cases

The above digital asset management policies and procedures are reviewed and improved on a regular basis in consideration of digital asset management best practices. They will be approved by the Steering Committee.

4. Economic Model

4.1 Overview

Financial characteristics are inherent in every blockchain. A proper economic model is one of the fundamental elements in a blockchain ecosystem, and a key factor for its success.

After studying the economic models of most public blockchain networks, and several discussions with our business partners, especially corporations and enterprise business owners, we discovered the largest obstacle to adoption of massive applications on blockchain: the cost of using blockchain is directly linked to token valuation. While the token valuation usually goes up as the blockchain usage grows, the cost of using blockchain varies depending on whether a party wishes to conduct payment transactions or smart contract transactions. This does not even mention the speculation of investors and traders as a contributor to the value of a blockchain. No business owner would run applications or a business on blockchain, or anywhere, at an unpredictable and unstable cost.

This section describes the VeChainThor blockchain economic model that governs the VeThor Token (VTHO) generation from VeChain Tokens (VET), an estimation of market demand and supply of VTHO, and VTHO price modeling principles. In summary, VTHO is generated via holding VET with velocity v, which is established to allow any user with VET to make transactions at no extra cost if the user holds the tokens for long enough.

Based on the VTHO generation model, we can estimate the supply and demand of VTHO for each given day or a period of time. Because VET has a fixed total supply of 86,712,634,466, the supply of VTHO per day is calculated to be 37,459,858 at the current v. The demand of VTHO comes from smart contract execution and payment transactions. To stabilize the transaction cost in fiat and maintain the equilibrium of the demand and supply of VTHO, the Foundation closely monitors the market and estimates the demand VTHO based on the activities of applications running on the VeChainThor blockchain and token transmissions. When needed, the Foundation would decide to initiate the adjustment of economic model variables according to the governance model.

4.2 Design Philosophy

The principle of designing the model is to prevent transaction fees from being directly exposed to the volatility of the price of VET, making the VeChainThor blockchain more suitable for conducting business / financial activities for both individual and enterprise users.

In our design, there are two levels of blockchain usage. The lower level concerns blockchain-level operations such as token transfer and smart contract execution, while at the higher level developers and application owners conduct complex business and financial activities.

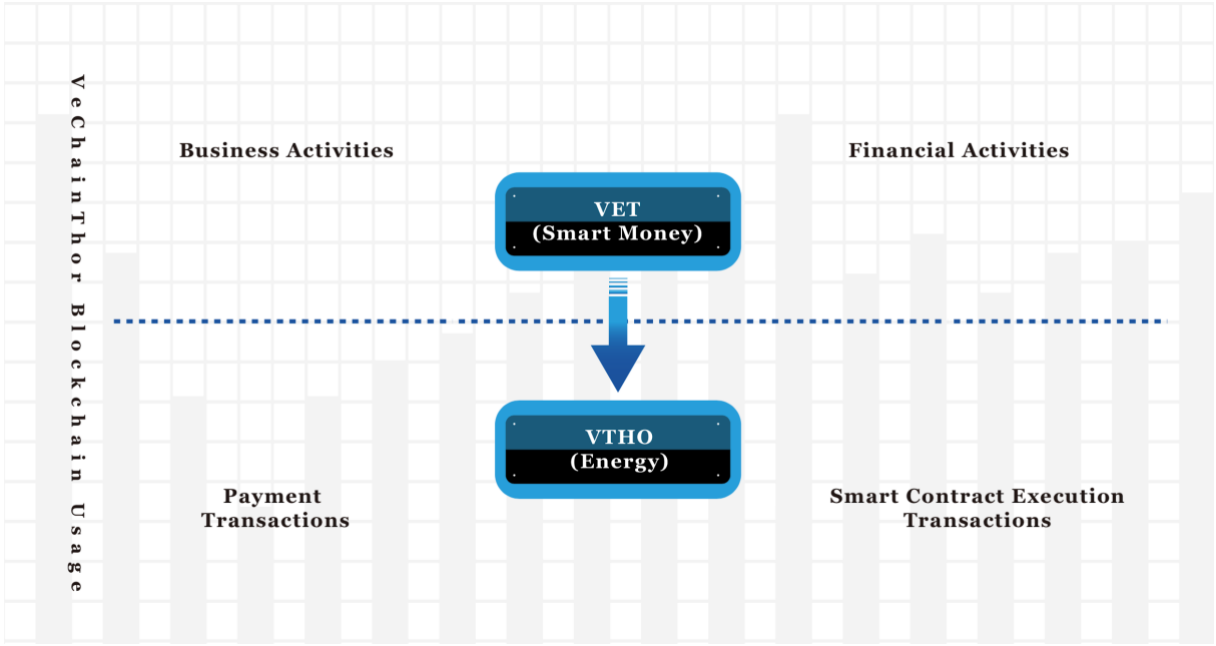


Figure 4.2 Two levels of VeChain blockchains

In our model, we designed a two-token system to facilitate activities at both levels, namely, VET and VTHO. The function of VET is to serve as a value-transfer medium, or in other words, smart money, to enable rapid value circulation within the ecosystem. On the other hand, VTHO represents the underlying cost of using the VeChainThor blockchain and will be consumed (or, in other words, burned) after certain blockchain operations are performed.

Since VET represents the right to use the VeChainThor blockchain, the model is designed in such a way that VTHO is generated automatically via holding VETs. In other words, whoever holds VET gets VTHO and are able to use the VeChainThor blockchain for free as long as the operations performed consume less than the VTHO generated. VTHO can be transferred and traded to allow users to acquire extra VTHO for performing a larger scale of operations such as running a blockchain application.

4.3 Model Settings

Let us first define some variables to be used to describe our model settings.

V: the amount of VET

E: the amount of VTHO

G: the amount of gas (in units of one thousand gas), where gas is the internal unit of the VeChainThor blockchain to price various blockchain operations. The name ‘gas’ is adopted from the Ethereum blockchain.

t: the amount of time used to accumulate VTHO from VET. Note that t is counted in number of blocks rather than conventional time units.

p: the gas price in VTHO

v: the generation speed of VTHO from VET

Mathematically, we can write our model as:

$$E = v * V * t \quad (1)$$

$$E = p * G \quad (2)$$

Equation 1 tells us that there would be v VTHO generated from 1 VET every time a block is generated. Equation 2 shows how VTHO is spent in the system. More specifically, when a transaction is put in a block, the system first calculates the amount of G required and then E using Equation 2, which means that there would be E VTHO spent. Note that p is set by the transaction initiator and can be different from transaction to transaction. A larger p would result in the transaction being processed with a higher priority at the cost of more VTHO consumed and vice versa.

We expect the use of the VeChainThor blockchain to be modest at the beginning, but will increase over time. We initialize the model parameters v and p such that the amount of VTHO generated from 1M VETs every day will be enough for conducting twenty VET payment transactions. According to our design, the VeChainThor blockchain generates one block every 10 seconds and each VET payment transaction requires 21,000 gas. The current setting for parameter v is 5 x 10^{-8} VTHO per VET per block. Therefore, for 10K VET there will be 4.32 VTHO generated every 6 × 60 × 24 = 8,640 blocks (24 hours).

Ideally, most of the VTHO generated would be spent to pay for transactions on the VeChainThor blockchain. In our model, we give users the flexibility to vary p when submitting transactions. Theoretically, one could set a very small p to allow transactions to consume near zero VTHO. If a large number of users followed such a practice, there would be a large stock of VTHO unspent, increasing the uncertainty of the stability of the VeChainThor blockchain.

In order to prevent p going below the minimum cost of running transactions, users can only choose p in the range of $[p_{COEF}, 2 \times p_{COEF}]$ where we currently set $p_{COEF} = 1$ VTHO/Kgas. We expect average p would be correlated with the number of applications running on the blockchain and active users who make transactions regularly. The minimum and maximum gas price in VTHO are designed to prevent people exclusively occupying blockchain resources and harming other transaction makers. All the transactions that have a gas price outside the range would not be executed as a penalty by the system.

4.4 Balance the Demand and Supply of VTHO

The design of the two-token model intends to maintain stable and predictable transaction cost (in fiat) of using the VeChainThor blockchain. Depending on the market participation of the VTHO market and the demand and supply of VTHO, the Foundation would adjust the minimum price of VTHO per gas, $p_{\_VTHO/GAS}$ (“GasPrice”) to achieve its goal. If there is a clear long term trend or the adjustment of minimum $p_{\_VTHO/GAS}$ does not effectively stabilize the transaction cost, the Foundation would propose to adjust VTHO generation velocity v. From a technical perspective the adjustment of GasPrice requires ⅔ of the signatures of Steering Committee Members as part of the on-chain governance mechanism, while the adjustment of VTHO generation velocity v will require an incompatible upgrade of the protocol (a.k.a

"hardfork upgrade") which requires all stakeholders voting according to the governance model.
The supply of the VTHO is based on the current velocity. When the supply, demand, hold, trading patterns are not set, there will be fluctuation and an equilibrium seeking process by the market players such as enterprises users, developers, and VET holders. The VTHO market might be in the premature status for a period of time before purchasing VTHO from the open market and using it for running applications becomes normal for most of the enterprise users. The VTHO price should not only be benchmarked with other blockchain platforms, but also the value added to business owners via the applications running on the VeChainThor blockchain.

The Foundation team does not intend to take action to directly affect the market until a definite conclusion is made by the close monitoring over all variables by the Foundation team and invited subject matter experts. The demand of VTHO for the next six months is estimated by a combination of econometric forecasting models with the adjustments by the inputs from the business development and application owners. The forecasting technique will be continuously tested against all the available data. Different models might be adopted to estimate the VTHO demand from the payment transactions and smart contract execution. The market participation ratio will be estimated using historical data.

If the Foundation team and subject matter experts deem it is necessary to interfere with the VTHO market, a proposal for GasPrice adjustment will be presented to the Steering Committee for approval. The process will be transparent to the community and disclosed on the VeVote platform. Only when there is a clear long term trend or the adjustment of GasPrice does not effectively stabilize the transaction cost, the Foundation would initiate an all stakeholders voting in order to adjust VTHO generation velocity v.

5. Use Cases

5.1 Overview

A new technology will only thrive and achieve mass adoption if it can add value to businesses and make the world a better place. We have seen so much discussions on the technical level about the blockchain technology, however, blockchain is one of infrastructure protocols which is, most of the time, invisible to ordinary people. Similar to the Internet, although it is being used everywhere and impacting people's daily lives, most people do not need to understand how the underlying protocols work such as TCP/IP. As the blockchain industry is moving from technical consensus to business consensus stage, questions asked by enterprises are tougher, more granular, more grounded, and more pragmatic.

The next focus of the development of blockchain technology towards mass adoption should be creating value to normal businesses, which is sustainable to motivate these businesses to continuously invest back and move the technology forward. According to Deloitte's 2019 Global Blockchain Survey, which polled 1,386 senior executives from established business all over the world, 53% (10% YOY growth) of respondents say that blockchain technology has become a critical priority for their organizations in 2019, and it is backed by the strong investment trend in new blockchain initiatives. Moreover, 83% (10% YOY growth) of the respondents see compelling use cases for blockchain.

Despite of the emerging awareness that the technology seems ready for prime time, the survey shows implementation, in-house capabilities and uncertain ROI ("Return on Investment") are among the top 5 barriers considered by enterprises to increasing adoption and scale in blockchain technology. VeChain's vision of lowering the barrier and enabling established business with blockchain technology to create value and solve real world economic problems has been clear to us from the very beginning.

VeChain started business engagement for blockchain use cases and implemented the first blockchain solution of anti-counterfeiting and traceability for luxury products in early 2016. Now there are dozens of live enterprise applications running on the VeChainThor blockchain used by established business in multiple industries across the world. In the past few years, based on the numerous projects we co-developed with consulting firms and the feedback from enterprises, we formed our own methodology to onboard enterprises that are mostly not blockchain savvy. VeChain ToolChain™ which is an one-stop data BaaS ("Blockchain-as-a-Service") platform running on the VeChainThor blockchain, can help businesses integrate their business and data with blockchain without frictions. Combined with the VeChainThor public blockchain, IoT ("Internet of Things"), industry expertise from business partners in the ecosystem, and potentially AI ("Artificial Intelligence"), a comprehensive solution is provided to significantly lower the barrier for enterprises to adopt blockchain technology and focus on exploring new business models and value chains, which is the most significant advantage of blockchain over existing systems according to the Deloitte's 2019 Global Blockchain Survey.

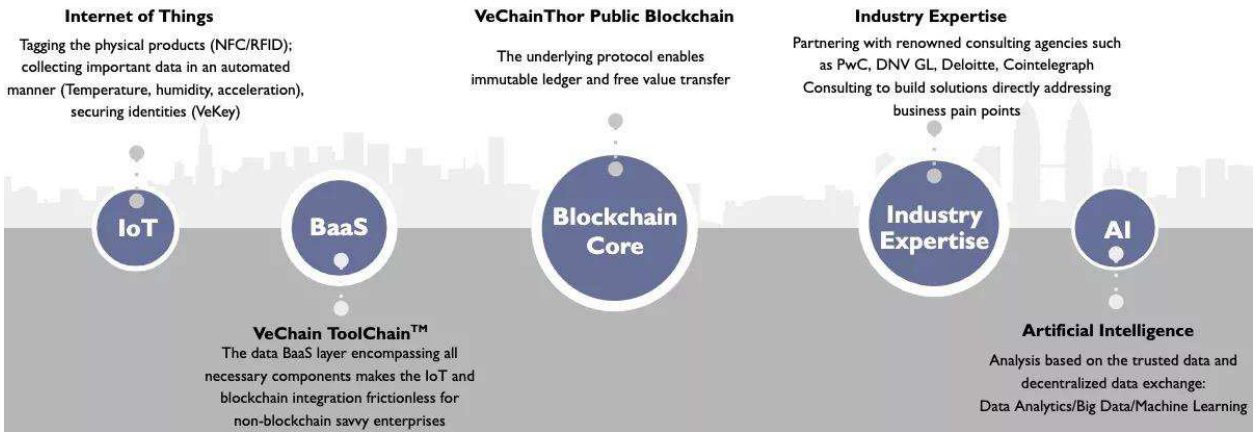


Figure 5.1.1 Enterprise solutions based on VeChain ToolChain™

Based on the hundreds of use cases we co-developed with consulting firms and enterprises, it is clear to us that the immutability, free value exchange enabled by the open blockchain infrastructure is the key to achieve the network effect and create new business models and value chains. However, in the enterprise blockchain space, most enterprises still have their eyes on private or permissioned blockchains, because most of the offerings on the public blockchain are seen as complicated and not business friendly. We feel that VeChain has the responsibility to demonstrate that it is feasible and practical to build enterprise solutions based on a public blockchain infrastructure which can bring benefits that are not possible on private or permissioned blockchains. To do that VeChain has been building all necessary technical components to facilitate the development of enterprise application through different stages of the value seeking process.

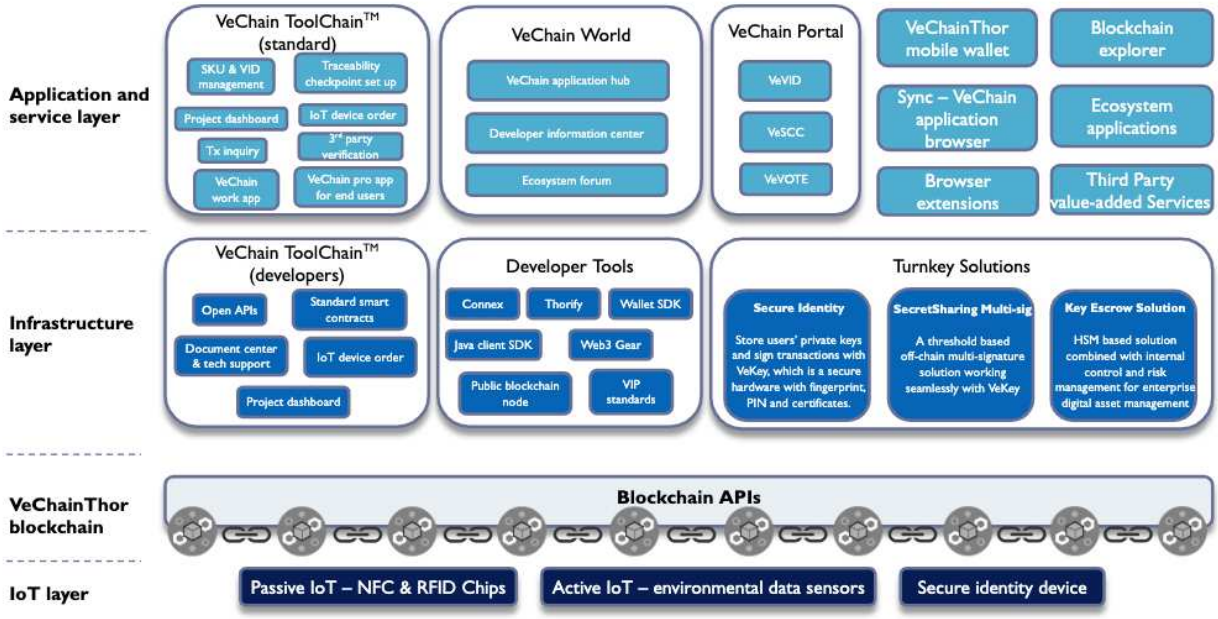


Figure 5.1.2 Enterprise solutions technology stack

The VeChain ecosystem is and will be formed by applications and new connections like dots and links. The role of the VeChainThor blockchain is to carry the value of more and more applications with business values. Among all the use cases and solutions that were developed and tested in the past few years, some have already been proven to be able to create

sustainable value for businesses and scale in real world environment. We want to share how they are addressing the business pain points and the process to unleash the power of blockchain to seek business value. We hope to inspire more businesses to adopt blockchain and push the technology forward.

Figure 5.1.3 Value seeking process for enterprise solutions

5.2 Provenance for food & beverage

Problem

The food sector is crippled with supply chain inefficiencies, frauds, and scandals. Most of the issues affecting the food industry stem from the inherent lack of trust and transparency within the supply chain. Our food system today fails to meet the transparency and assurance demanded by many consumers.

The World Health Organization (WHO) reports that almost one in 10 people in the world fall ill after eating contaminated food. Furthermore, foodborne diseases mainly affect the health of infants, young children, the elderly, and the sick. Costing the global food industry an estimated US $40 billion each year, food fraud continues to rise among consumers and the industry. In the food safety incidents, the sellers are bearing significant reputational risk because of the fragmented data and systems on the supply chain, making it difficult to establish the accountability.

Solution

VeChain's provenance solution for food & beverage allows participants on the supply chain to collaborate on a transparent and trusted data platform. By scanning the QR code on desired products, consumers can acquire detailed information secured by the blockchain, including the source and ingredients of the products, geographic location, logistics information, inspection report even temperature data, and the data is time stamped and cryptographically signed by the party who produce the data.

Figure 5.2 Provenance for food & beverage

VeChain provides the comprehensive solution that enables various parties to easily collect important data points related to the product. On the business side, users could choose to collect data and feed it to the VeChain data BaaS platform via the standard web portal, mobile applications or APIs depending on the business processes.

In addition, the solution supports the cold chain logistics in which the product temperature throughout the supply chain is recorded and available for verification. VeChain IoT sensors can collect environmental data such as temperature, humidity and acceleration and the sensor works seamlessly with the VeChain ToolChain™ platform to upload the data to the blockchain on a real time basis or through NFC interface at checkpoints. The sensors have been tested in real world scenarios for years, and it has industry leading specifications in storage, duration and transmission speed.

Value Proposition

- Enhanced the consumer confidence and brand reputation
- Improved transparency in the supply chain for better quality control and supplier management

- Reduced cost to acquire third party verification services for the product, such as My Story™
- Ability to collaborate with insurance companies to provide microinsurance on the product

Case Study

- In June 2019, Walmart China, together with VeChain and PwC, launched the Walmart China Blockchain Traceability Platform on the VeChain ToolChain™ platform. The first batch of 23 product lines have been tested and implemented using the VeChain ToolChain™. By scanning a QR Code, customers can acquire detailed information of the product. Participants in the supply chain will also share their portion of data, and promote the visibility and management efficiency of the whole chain by utilizing the decentralized and tamper-proof blockchain technology.
- ASI Group, in a tripartite collaboration with VeChain and DNV GL, initiated the first cross-continental logistics and trades solution powered by VeChain ToolChain™ for food & beverage industry named Foodgates. It is the first of its kind solution as it is powered by a public blockchain with verified and certified information of the full lifecycle of the products being tracked, such as from cow selection, slaughtering, packing, cross-continental shipping all the way to restaurants for beef products.

5.3 Anti-counterfeiting and digitization for high value products

Problem

As per the Global Brand Counterfeiting Report 2018, the amount of total counterfeiting globally has reached to 1.2 Trillion USD in 2017 and is bound to reach 1.82 Trillion USD by the year 2020. The rise of luxury resale has brought concern over the authenticity of pre-owned goods into sharper focus. The luxury resale market currently remains mostly unchecked with no real laws enforced. It is mainly the case in the peer-to-peer secondary luxury market where consumers buy items directly from online sellers. Luxury brands lost about $30.3 billion worth of sales to counterfeits online alone.

In addition, luxury and fashion brands are competing in the digital marketing spending to create a personalized experience for consumers. Many brands are spending billions of dollars in marketing, as consumers are growing more and more accustomed to buying clothes online, so much so that the share of e-commerce sales is set to grow from 20 percent today to 25 percent by 2020, according to a joint study by international marketplace Zalando and consultancy firm Boston Consulting Group (BCG).

Solution

VeChain's solution allows brands to digitize products on the blockchain by establishing the linkage between the physical product and unique blockchain identity using smart NFC tags. With the unique digital identity, the solution provides the traceability over the life-cycle of products from the manufacturing, logistics and supply chain, retail and wholesale, after service, and even consumer engagement on the blockchain. Each product has its own landing page

created by the brand with the product description, marketing and traceability information, which is a powerful tool for authentication, traceability, storytelling and digital marketing purposes. In addition, the ownership of the product on the blockchain is tied to the user's account and can be transferred on the B2C and C2C markets to provide consumers with a personalized experience.

Figure 5.3 Anti-counterfeiting and digitization for high value products

VeChain ToolChain™ provides a one-stop platform to seamlessly create product identity (VID), order NFC tags, add traceability information and transfer product ownership. NFC tags supplied by VeChain are available in different sizes, shape and materials specially designed for various types of products such as bags, wine, shoes, clothes, artworks. With the VeChain ToolChain™ API, brands are able to tokenize the product as VIP181 Non-fungible Token (NFT) using APIs without the need to develop smart contract. Brands can also embed the ownership transfer function of the tokenized product in their own application with VeChain's open source mobile wallet.

Value Proposition

- Enhanced experience to authenticate the product with users' mobile devices
- Improved transparency in the supply chain to avoid overproduction and cross channel sales
- New method of digital marketing with the multimedia product landing page
- A personalized experience with ownership transfer

- Avoid the loss due to counterfeit in returned products

Case Study

- In 2016, a LVMH portfolio Luxury Maison started to use VeChain's blockchain solution for a Limited Edition Collection. It has since integrated VeChain ToolChain™ for all leather products since F/W 2017 collection and intends to expand into ready-to-wear and shoes. With the immutable nature of blockchain & VeChain's proprietary encrypted smart chips, this solution enables the company to gain the control and efficient management over its fragmented supply chain and hundreds of distribution channels. This also enables the potential of derivative businesses such as ownership transfers, warranties, empowering the development of new verticals in luxury secondary markets such as re-financing and insurance.

- Reebonz, a leading online luxury marketplace and platform in Southeast Asia and the Asia Pacific region, integrated VeChain ToolChain™ APIs and built an application to establish the provenance and digital ownership of the products on its platform. Each product has a unique ID and is issued with a digital certificate on the VeChainThor blockchain. This digital certificate will bear a QR Code which contains information such as product details, transaction details and history, and provenance of ownership. In the instance a product is stolen, customers can revoke the certificate to ensure protection. Customers would also be able to take advantage of transacting on their own a C2C basis. The digital certificate can serve to verify authenticity and ownership transfer.

5.4 Digital vehicle passport

Problem

According to European Parliament, odometer tampering has seen the mileage rolled back on up to 50% of second-hand cars traded in the EU, with the price of vehicles fraudulently increasing by €2,000 - €5,000 on average. Car dealerships are not able to identify all cases of odometer fraud, many times passing down the problem to second hand buyers. This fraud costs an estimated €5.6- €9.6 billion a year to consumers, second-hand car dealers, leasing companies, insurers and manufacturers.

Solution

VeChain's digital vehicle passport solution began with addressing odometer fraud by storing and securing critical data on the VeChainThor blockchain across entire lifecycle of automobile. It is targeted to change the current data exchange model from peer to peer data exchange among car manufacturers, repair shops, insurance provider, technical experts, and even banks to share data with authorized access. The digital vehicle passport registered on the blockchain with digital ledger attached is created and maintained for each automobile by various authorized parties. The data feeds include data from the car computer, data from operation systems through APIs, and even directly user input.

In the end, the data of each automobile secured by the VeChainThor blockchain with clear accountability of each user and party will generate the new value of “data on blockchain” for automobile sales, financial support, insurance package, and trading in second hand markets. It is targeted to reduce the cost and improve efficiency greatly in terms of data and record validation.

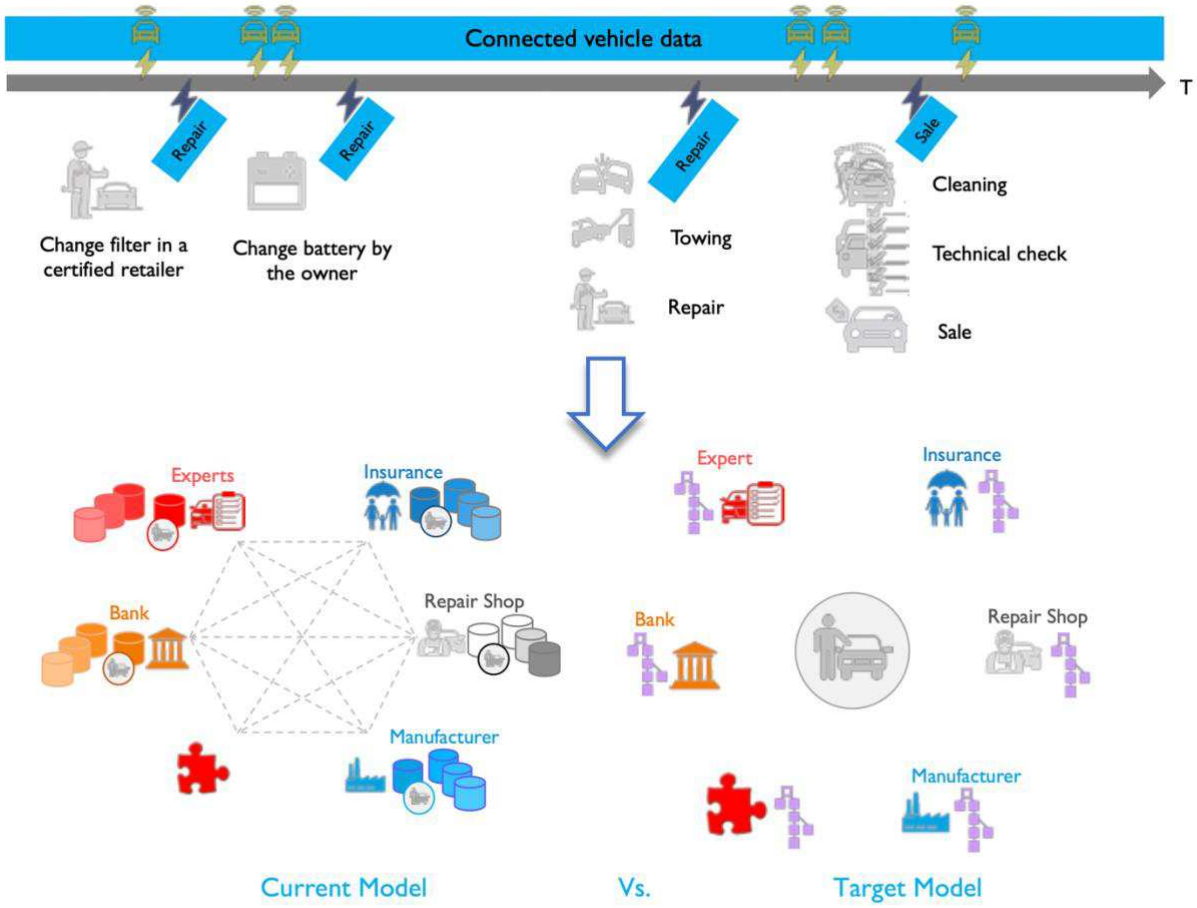


Figure 5.4 Digital vehicle passport

VeChain’s solution harnesses the blockchain to record vehicle ownership, usage and servicing histories. Each vehicle has a digital passport and verified mileage recorded on the blockchain. Information is uploaded to the maintenance book by related parties instead of the car owner, and it is time stamped and secured by the blockchain. Car owners control the read / write access rights to the digital passport. Data collected can be shared with potential buyers, insurance. When the vehicle is sold, it can be transferred to the new owners.

Value Proposition

- Reduced due diligence efforts by a potential buyer, an insurance company, a bank based on the trusted data in the digital passport
- Increase the value of second-hand vehicles and the ownership can be transferred
- Ability collaborate with insurance companies to provide user behaviour based insurance products

- Increase the awareness of new energy cars by incentivizing users for their behavior to contribute to environment protection
- Explore new business models relating to energy, part market, car sharing, autonomous driving with value of higher-level services, security, financial transactions, data collecting and computing enhanced by blockchain

Case Study

- BMW Group and VeChain developed a digital vehicle passport solution called VerifyCar with the mission to counter odometer fraud in the secondary market. Each vehicle is registered and assigned with a unique VeChain ID, together with existing IoT infrastructure embedded into the car, the car smartly tracks and records mileage on a per-trip basis using VeChain ToolChain™. This enables owners to prove they did not manipulate data with third parties. This use-case can be extended to track the entire health of individual cars by involving manufacturers, authorized repair shops, insurance companies, financial institutions to upload, share and verify data.
- BYD, the world's top electric vehicle maker, adopted VeChain's automobile lifecycle management solution which integrates mileage, electricity and gas consumption data with the VeChainThor blockchain. Such information is used to calculate the carbon emission reduction and reward the driver with carbon credits. This digital low carbon emission ecosystem rewards vehicle operators with carbon credits based on their vehicles' driving performance and carbon reduction. This solution provides the tools necessary to construct a blockchain-based ecosystem aimed at reducing the global carbon footprint. Each footprint captured will be recorded on the VeChainThor blockchain and made available to clients interested in participating in the initiative.

5.5 My Story™ - a blockchain-based digital assurance solution

Problem

Third party assurance service, an industry existed for hundreds of years, heavily relies on manpower. It is facing some common challenges:

- high risk for auditors and inspectors for the low margins earned
- limited coverage of certifiable business processes and products
- high labor cost, especially on renewal cost
- possibilities of errors due to inconsistent human behavior and limited sample size in limited time window
- subjective & inconsistent judgement, even corruption

According to DNV GL, a shifting paradigm is discovered to be driving new assurance needs including:

- Adoption of digital technologies combined with digital connectivity is impacting societies, enterprises and consumers
- The information content of product and service is growing to be more “embedded”
- Digitalization is exponentially increasing the number, kind and forms of transactions;
- Each transaction involves a large number of stakeholders, and the voice of consumers is getting more and more importance

Consumers are increasingly looking to the products they buy to confirm brands’ promises to be honest and responsible. Brands are struggling to share their efforts and investments, connecting actions to specific products, communicating the value behind certifications and labels, and not least finding engaging touchpoints on the product.

Solution

Following the global strategy of digital transformation, as one of key implementations of this 150 years company with global presence serving over 100,000 enterprise clients, DNV GL Business Assurance developed a blockchain based digital assurance solution on the VeChainThor blockchain – My Story™. MyStory™ helps brands bridge the trust gap between their efforts and consumers’ concerns.

Instead of sending experts physically to conduct data collection and inspection, the auditees just need to follow the pre-defined instructions with business process as-is to upload the data to MyStory™ platform and then call the specific smart contract for provenance to store the key data to the VeChainThor blockchain. By doing this, the new transactional and data driven model will replace the manpower basis model which leads to much lower and flexible cost structure to expand the current extremely selective market for assurance services. DNV GL started with three wineries in Italy and will go for more vertical markets with easy replication collaborating with national level associations.

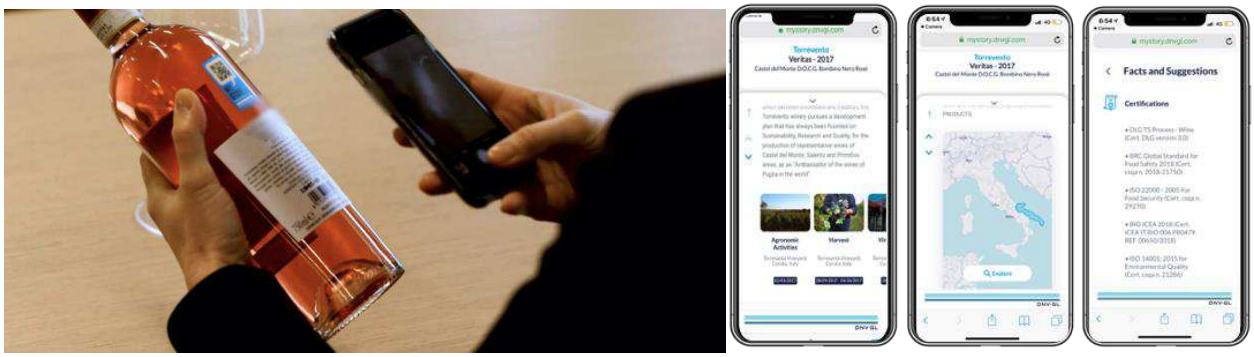


Figure 5.5 My Story™ - blockchain based digital assurance solution

And the integration with other technologies such as IoT, 5G and A.I. plays a critical role during this digital transformation. IoT sensors and machine controllers are responsible to collect the data from daily business activities to minimize the human intervene during the process. The implementing and expanding 5G network will make the data collection in more and more use cases run in a real-time and cost effective manner. A.I. is naturally demanded in the data analysis process to ensure the integrity and accuracy of digital certification issuing to minimize

inconsistency of human judgement and even corruptions. Especially the follow-up random inspection could be more efficient when more external data could be cross-checked and verified. The growing complexity of this kind of operations can be only handled by evolving A.I. in a continuous way.

In addition to the process, the result of digital assurance – digital certificates can be recorded and managed by the VeChainThor blockchain as well. With a unique identity for every certificate on the blockchain, the integrity of all of the critical data attached to every certificate can be ensured due to the real time provenance with accurate time-stamp. And new business collaboration involving such digital certification can be done online with customized smart contracts accorporating with other business operations represented by corresponding smart contracts. In April 2019, as the first step for global digitalization plan, Deloitte accomplished to migrate the existing certificates of DNV GL from Ethereum to the VeChainThor blockchain which created more than 1.7m smart contract transactions which outperformed most of the public blockchains on that day.

Going further, we can expect the auto-issuing of digital certificates by more sophisticated smart contracts with different ABIs (Application Binary Interfaces) based on the binary data input from different data collection points, data validation points and data re-validation points with external matrix of data for cross check. And NFT (Non-Fungible Token) will be implemented for each digital certificate for digital ownership and status management in a more transparent and timely manner.

In summary, blockchainization using VeChain's blockchain infrastructure is one of the most critical elements to the global digitalization of DNV GL along with integration of other technologies.

Value Proposition

- Reduced manpower cost by relying on the blockchain secured data
- Brand exposure of the assurance provider at the consumer level
- More efficient verification and cross check with more external data available
- Digitalization of verification process and results facilitate integration with other technologies

Case Study

- Three Italian wine makers, Ricci Curbastro, Ruffino and Torrevento, were the first to implement My Story™, a blockchain powered digital assurance solution. They are now ready to share the characteristics of their wines traced from the farming and wine making to packaging and distribution. Consumers have access to all the facts, using their smart device to scan the QR-code on the bottle. In the connected consumer dApp, they can instantly browse product facts, the wine's timeline and locations from grape to store for every bottle. The story shared with customers range from features related to how the wine was produced to recommendations as to how the wine is best consumed, all shared in an instantly accessible, consumer friendly way.

5.6 Digital low carbon emission ecosystem

Problem

Since the 1960s, environmental conversation has been widely discussed by the global society led by the United Nation and leading countries. Even though, various domestic and international organizations have raised numerous concerns and society has seen a resurgence of interest regarding global environmental problems including global warming, carbon emissions, pollution. The prevalence of methods for scientifically measuring individual participation and results lag far behind the expectations which consequently hinders efforts by key stakeholders and policy makers to incentivize the public to conserve and protect the environment. The whole world urges to find a better solution.

The issues of current carbon emission reduction progress include:

- Activities of carbon emission reduction are not quantifiable
- It's difficult to be sustainable and continuous
- The participants are not fully and really motivated with transparent and fair policy executions
- Individual participants are difficult to be involved
- It's difficult to be standardized and replicated
- Lack of effective certification and regulatory support

Solution

While many efforts have been made by enterprises and industrial experts on this topic, with the adoption of blockchain technology driven by pioneers with industry expertise these issues could be addressed.

VeChain and DNV GL initialized the low carbon emission ecosystem with a few pioneer companies. The roles in this ecosystem are as follows:

1) CER (Carbon Emission Reduction) generator – the platform digitalizes, qualifies and quantifies user behavior as individual CER contributors through IoTs and the others from different use cases such as driving electric vehicle, electric charging station use, carpooling, public transportation use, eco-friendly household appliance

2) CER validator – the experts such as DNV GL verify user behaviors based on collected data and issue the quantified proof. The validation process is executed by smart contracts for transparency and integrity

3) CER consumer – the sponsors such as enterprises and organizations who are willing to provide products, services or financial incentives to motivate individual CER contributors

4) Technical supporter – the technical provider who develops and launch the technical infrastructure and provides technical support to maintain this platform

5) Regulator – Authorities who can create the regulations to define the fair rules to monitor and motivate everyone in the system

In terms of system structure, there are the following levels:

1) Blockchain infrastructure level – the VeChainThor blockchain network with infrastructure services such as nodes, deployment tool and environment, explorer, wallet

2) Smart contract level – the smart contract gateway to host CER calculator smart contracts to fit different use cases along with common smart contracts such as CER library, provenance, token mint (VIP180 / 181) with ABIs (Application Binary Interfaces)

3) Data processor level – the data platform is responsible for data collection, data validation, data processing, data aggregation, data encryption, and data uploading with APIs

4) Front end application level – mobile apps, web portals, IoTs customized based on different scenarios

5) System function level – the common functionalities across the entire system such as user account, KYC management, contribution credits and index

The platform was initialized in June 2019 and the development directions include iterating the standardization of modules to fit replicable use cases and replicating the platforms in different cities, countries and regions. Eventually, it's a decentralized incentive system for positive individual behaviors. And SDGs (Sustainable Development Goals) defined by the United Nations can be implemented by the extended platform.

Value Proposition

- Individual users are incentivized to participate in environmentally friendly activities
- Non-Government Organizations and Green Groups can use this platform to organize online or offline events to attract more people to join and contribute to the cause of environment protection
- CER (Carbon Emission Reduction) generators can incentivize its user with carbon credits, enhance the user stickiness and receive CSR certificates
- CER sponsors can attract more user traffic and demonstrate corporate social responsibilities
- Government agencies can receive data of measurable user behavior of carbon emission reduction

Case Study

- BYD, the world's top electric car marker, is the first CER generator on boarded in the digital low carbon emission ecosystem. The mileage, electricity and gas consumption data on the latest BYD new energy vehicles is used to calculate the carbon emission reduction and reward the driver with carbon credits. This digital low carbon emission ecosystem rewards vehicle operators with carbon credits based on their vehicles' driving performance and carbon reduction. This solution provides the tools necessary to construct a blockchain-based ecosystem aimed at reducing the global carbon footprint. Each footprint captured will be recorded on the VeChainThor blockchain and made available to clients interested in participating in the initiative.

- A WeChat mini-app was launched in China as a platform for individual users to access the digital low carbon emission ecosystem. Users can receive carbon credits in the app from the activities that are integrated with the VeChain solution and spend credits in the app in exchange for goods or services. In addition, the platform is used to organize projects for poverty alleviation and charity program for schools donations.

- A Memorandum of Understanding has been signed between the Republic of San Marino Secretary of State for Industry, Trade, Business, Cooperation and Telecommunications, Republic of San Marino Innovation Institute S.p.A, DNV GL Business Assurance Group AS and VeChain Foundation Limited. VeChain and DNV GL, together with San Marino Innovation, will guide the Republic toward the adoption of blockchain technology, crypto-utility token infrastructure and utility token use cases, in order to define models capable of incentivizing sustainable behavior from its 33,562 citizens. It is part of San Marino's strategy to develop, promote, and deliver a full ecosystem of technological innovation to facilitate digital transformation.

5.7 Our vision on open finance

In 2019, the industry saw the boom of decentralized finance, aka De-Fi. First it was decentralized exchanges, players such as 0x and IDEX gained a lot of attention in the capital markets. Then we saw the rise of stable coins backed by cryptocurrencies such as Dai by MakerDao, and the creation of such settlement layer has birthed a wider decentralized finance ecosystem including lending, borrowing, staking, investing, etc. The future painted by De-Fi is extremely promising even to a layman's eye. A future where money becomes programmable, capital and financial products flow freely, and parties interact without a middleman with no counterparty risks. The global financial industry is worth around 15 Trillion dollars, more than 17% of the 88 Trillion-dollar global GDP, and most of the financial industry's value is derived from its elimination of cost of trust between parties. This cost of trust is also a cost which blockchain has a direct answer to.

One may then question how come De-Fi has not yet fulfilled what it promises to achieve, and most of the use cases of De-Fi now is still in the area of trading/speculation. The answer is: there are pre-conditions for the boom of De-Fi that has not yet been met, and a lot of these resources to set these pre-conditions are controlled by existing interest parties, so the transformation of the financial industry will likely take some time. For example, to build financial products such as insurance policies or loan contracts on top of the blockchain, one of the pre-

conditions is the existence of a trusted fiat backed stable coin that is connected to the blockchain and serves as the settlement layer for financial instruments. Libra attempts to build such settlement layer, even a project initiated by one of the largest internet companies in the world is facing significant amount of pushback by regulators and existing interest parties around the world, let alone a blockchain start-up. So currently most De-Fi projects we have seen are creating products built on top of cryptocurrencies, mainly Ethereum and Bitcoin, because these are outside the boundaries of mainstream finance.

While we do believe in the potential of cryptocurrencies, and it may eventually fulfill the decentralization dream that a lot of crypto believers believe in, however it is simply too small of a market when compared to the global finance market. We believe the full potential of the blockchain technology will only be realized if mainstream finance can adopt the technology. Therefore, we have a stronger belief in “open finance”, as opposed to De-Fi. VeChain aims to enable financial institutions and central banks through blockchain technology, transforming their current business practices to a more transparent, efficient, automated, and data driven form. There are three directions we will take to facilitate the creation of such ecosystem. 1. To establish a settlement layer consisting of different stable coins 2. Onboard enterprises and construct a data layer 3. Bring in financial institutions to create financial products using trusted enterprise data.

Settlement layer: The blockchain based settlement layer will enable financial products to be settled on-chain, allowing the utilization of smart-contracts, automated execution with transparent terms, thus significantly reducing cost and increasing transparency. For the past year and a half, we have advised governments around the world on their regulatory framework around cryptocurrency, and we have also been working with one of the most innovative governments in the world to design and launch a Euro-backed stable coin which is issued by the central bank of that country. This stable coin carries a lot of significance for both the blockchain industry and that country. Not only may it be the first state-backed Euro stable coin in the world, such legitimate/trusted settlement layer will serve as the soil to grow financial products with mass adoption potentials.

Data Layer: Through utilizing the data layer, financial instruments can be tailor made for each client based on the evaluation of their data, adjusting the terms of the financial product accordingly. Our strategy of building the data layer is to integrate blockchain solutions to more products and business processes, and eventually to tap into the end consumers through enterprises. We are proud to say that we have accomplished quite a lot in the past 3 years, and have become one of the leading players in the industry in terms of enterprise adoption and scaling valuable transaction. We currently offer more than 100 enterprise solutions covering over 16 industries and 36 sub-sectors using a combination of blockchain, IoT and AI technologies. These solutions are not just theoretical, they are solutions tested and discussed with over 700 enterprises and implemented for over 100+ fortune level enterprises.

Financial Institutions: As both the settlement layer and data layer are ready, the next step is to bring in financial institutions to build financial products. These may include loans, insurance products, supply chain finance, services and financial derivatives. We believe as more valuable data accumulates on-chain and user demand for better financial products, financial institutions will slowly adopt blockchain technology in their product design. The first wave of financial institutions has already utilized our technology in their products, and we are working with our business partners including financial service providers on many fronts. In the

existing use cases we are already exploring some financial products such as user-behavior based auto insurance, micro insurance on food cold chain logistics, and supply chain finance. On one hand, we found that with the business activities natively integrated on the blockchain such financial products can be provided at a lower cost and in a streamlined manner based on the on-chain data and activities. On the other hand, in order to unleash the full potential of such new business models comprehensive and commercial-grade settlement layer and data layer need to be put in place. It confirms our strategy to start with pushing the adoption in non-financial real world use cases and enable financial institutions and central banks to build the infrastructure and financial products using VeChain's blockchain technologies. VeChain helps to connect different companies in the ecosystem to reach a mutually beneficial partnership that also incentivizes the end consumers. Some may have concerns for data privacy issue, and this has been on our minds since day one. The easy solution is to obtain consent from the data owner before it is used by another party. On top of that, we are also working out privacy solutions such as multi-party computation (MPC) to further address this issue that many have concerns for. All of the above are cornerstones of the robust distributed business ecosystem that is envisioned by VeChain.

6. A Diverse Ecosystem

6.1 Overview

Although enterprises are critical for mass adoption, built on top of the VeChainThor public blockchain, the VeChain ecosystem is open for various types of participants to collaborate and the open platform could significantly help reduce the friction across organizations and industries. While most enterprises seek ways to integrate blockchain into or transform their existing business models and systems, many startups or community projects are building their business around blockchain from the start. Because they are usually more nimble, it puts them in a better position to apply disruptive thinking from the ground up to create new business models or value chains than established businesses.

As the enabler of the ecosystem, VeChain is committed to working with the ecosystem participants to solve real world economic problems and create value with the blockchain technology. VeChain connects the resources, supports and opportunities to the right participants with the goal to create value for the ecosystem holistically.

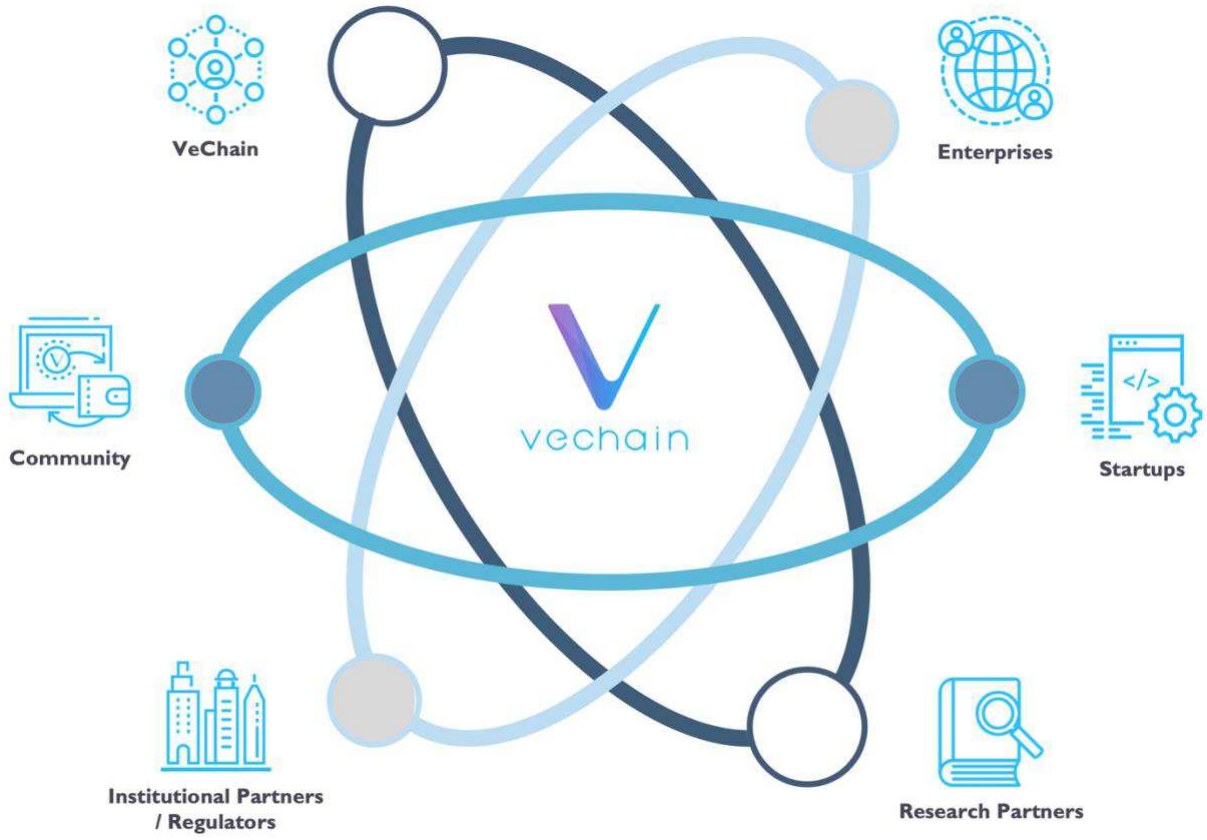


Figure 6.1 VeChain ecosystem builders

- **VeChain -** the enabler of the ecosystem, focusing on building the underlying technology, infrastructure utilities and services. VeChain holds a significant reserve to support the ecosystem growth

- **Enterprises** - small or large enterprises use the blockchain technology to enhance or transform their business models and build sustainable real world applications targeting the broader mass to solve industry pain points
- **Startups** - startups enhance the value proposition of their ventures by adding blockchain and / or token economy and attract more talents and capitals to the ecosystem. Identify and test viable solutions that larger organizations may then adopt on a wider scale, forming a symbiotic relationship that drives continued blockchain innovation
- **Community** - community developers or subject matter experts start their own projects or contribute in specialized areas, bring innovation and diversity to the ecosystem
- **Research partners -** following the real needs from ecosystem applications, VeChain works closely with research partners to improve the underlying technologies to support the ecosystem. VeChain set up the VeResearch program for the collaboration with academic research partners
- **Institutional partners / regulators -** venture capitals and incubation partners empower ecosystem builders with their capital, resources and expertise; Regulators provide well-defined and blockchain friendly legislation for projects to thrive

6.2 How do we support the builders

In the public blockchain space, VeChain has unparalleled track record in helping established businesses build blockchain solutions that are used as part of the daily business and add sustainable value.

Similar to a public cloud platform, enterprises and startups who may or may not have blockchain expertise or development capabilities will tend to choose the blockchain platform with comprehensive tools, services and supports.

Figure 6.2 The needs of ecosystem builders

Enterprises

- The VeChain ToolChain™ data BaaS platform is a powerful tool for enterprise to quickly adopt blockchain technology for the existing business without investing in the in house blockchain development capability

- With technology infrastructure, business acumen and a strong business partner network, VeChain is well positioned to be a trusted technology partner of enterprises' digital transformation journey to create new business models and value chain
- The VeChainThor public blockchain, development tools, turnkey solutions, as well as comprehensive technical support, makes it the most feasible public blockchain platform for enterprises to develop applications on

Startups

- VeChain developed a wide range of open source tools, BaaS and turnkey solutions to help startups integrate and develop blockchain without the need to start everything from scratch. In addition to the technical documentation, startups can get direct access to the VeChain tech team
- Startups will have the opportunity to work with our incubation partners to find the right business model and be prepared for investment. Since blockchain and crypto is a new space, we can help you explore and avoid pitfalls in areas such as legal, accounting and compliance
- As the startup scales the business, VeChain can bring business opportunities by facilitating collaboration between ecosystem builders and partners. Startups will also have the opportunity to raise public awareness and exposure of the business with our global community, media and events

Community

- VeChain helps entrepreneurs in the community turn ideas into projects with funding support and advisory services
- Developers can get technical support, join our developer channels or claim the bounty programs
- VeChain matchmakes community projects with contributors that share the same vision
- VeChain provides latest updates about the ecosystem and arranges events to engage with the community

Join the VeChain ecosystem and learn more information at vechain.org/builders