2020
TrustBase
TrustBase White Paper

Polkadot Parachain Based on Independent Smart Contract Language Subscript
# CONTENTS

1. Background 01

2. Subscript Language 04
   1. Native Design for WASM 04
   2. Subscript Language and Syntax 04
   3. Subscript Contract Library Functions 06
   4. Mature Compilation Framework 07
   5. Package Management Tools Familiar to Developers 07
   6. Debugger Support 08
   7. Subscript Workbench 08

3. TrustBase Parachain 10
   1. Project Introduction 10
   2. TrustBase Structure 11
   3. Virtual Machine Based on WASM 12
   4. TrustBase Smart Contract 13
   5. TrustBase Storage 14
   6. Cross-chain Operation with Polkadot 15
   7. Application Scenario 15
   8. Core Advantages 17
4. Governance Model 19
   1. Consensus Mechanism 19
   2. Role Setting 19
   3. Penalty Mechanism 21
   4. Role Election 21
5. DAO Autonomy 24
   1. National Assembly 24
   2. Council 25
   3. Technical Committee 26
   4. Voting Mechanism 26
   5. Noun Interpretation 27
6. Economic Model 30
   1. TBE Commercial Value 30
   2. Node Rights 31
   3. Gas Rate Setting and Standard 32
   4. TBE Issuance Plan 33
   5. TBE Destruction Mechanism 33
7. TrustBase Foundation 35
   1. The Composition System of Fund Committee Members 35
   2. Duties of the Fund Committee 36
8. Development Plan 38
9. Founding Team 41
10. Risk Warning and Disclaimer 43
Chapter 1

INDUSTRY BACKGROUND
1. Background

1.1 Web3.0 and Polkadot

Web3.0 is a new stage in the development of the Internet, and the emergence of Blockchain technology has given higher expectations to Web3.0. What Web3.0 empowered by Blockchain will realize is everyone’s control over all their personal values in the digital world, such as their data, identity, and assets. Finally, it will bring a truly transparent and credible Internet economic model to the world.

In order to realize the vision of Web3.0 and solve the current problem of ”data islands” in the Blockchain, Polkadot came into being. Polkadot is committed to creating a network protocol, similar to the Internet TCP/IP protocol, by defining and developing a set of fragmented multi–chain structures of parallel chains and relay chains. Let all the Blockchains connected to this architecture better complete the information interaction between each other, and finally realize the ”all chain interconnection”.

1.2 Substrate

Polkadot has revolutionized the Substrate development framework for Blockchain developers around the world. The Substrate framework modularizes the basic low–layer design of the Blockchain, allowing developers to call it with one click, saving the original complicated workload.

The Substrate framework gives the Polkadot Blockchain unprecedented features:

- **Scalability:**
  An isolated Blockchain can only handle limited traffic. Polkadot supports multiple Blockchains through a parachain mechanism, so that transactions can be processed efficiently and in parallel;

- **Specialization:**
  Each Polkadot parachain can be customized according to specific use cases or applications;

- **Interoperability:**
  Different Polkadot Blockchains and applications can share information and functions, thanks to the interoperability design of the project and the compatibility between chains;

- **Fork–free Upgrade:**
  Polkadot can be upgraded without time–consuming and split hard forks; new features can be added without the need to completely transform the network;
Although Polkadot is the golden track in the Web3.0 era, Substrate’s native smart contracts use a Rust-based ink! Language. The language has a large learning difficulty curve, and the ink! contract currently lacks tools to support the development of DApp. There are basically no tools or applications that are easy to use and can safely migrate existing EVM-based applications to the WASM-based Substrate Blockchain. The high threshold of Polkadot Blockchain development makes it difficult for a large group of traditional developers to enter.

To help traditional Web developers and Java engineers participate in the construction of the Polkadot ecosystem without barriers. TrustBase has independently developed Subscript, a lightweight WASM smart contract language. To meet the needs of traditional developers to break through industry barriers and develop Blockchain development business, and to promote the realization of the vision of Web3.0.
2. Subscript Language

The Subscript language follows the Typescript syntax and completes the encapsulation of the Substrate smart contract in Assemblyscript. So that traditional developers can quickly get started, one-click deployment of native smart contracts that can run on Polkadot.

※ 2.1 Native Design for WASM

Polkadot uses WASM as the byte format of Runtime on all chains, and WASM is also the main format of Polkadot smart contracts. WASM (Web Assembly) is a bytecode that can run in modern browsers. It is similar to assembly language and its binary format has high compactness, which can greatly reduce the size of object code files and improve the efficiency of network distribution of applications. The runtime efficiency of WASM bytecode can be close to that of native machine code, and it can be used as a compilation target for languages such as C++ and Rust.

Subscript is a native contract language designed for WASM as a whole, and provides access instructions to the bottom of WASM, which can support any smart contract development platform compatible with the Substrate architecture. Compared with Parity’s official Rust-based ink! language, it provides easier-to-use features:

- No need for Rust development foundation, Web developers can get started quickly;
- Good interoperability with JavaScript, easy to integrate with Dapp;
- Easy-to-use development environment support, you can run deployment and testing based on the existing js IDE.

※ 2.2 Subscript Language and Syntax

Subscript uses strict typing and language checking as a whole from API to syntax. At the same time, it provides a generic function to support the packaging of third-party libraries:

- Static Syntax Checking
  Unlike TypeScript, which is targeted at dynamic type runtime environments, Subscript has strict static syntax checking during compilation, avoiding the inability to effectively compile TypeScript’s dynamic features in advance. By assigning or inferring certain types, the compiler can produce predictable performance from the beginning of execution, while ensuring that the generated WASM target code is small;
● **Strict Type**

The basic types in Subscript are designed for the WASM standard, using WASM-specific integer and floating-point types. Allow developers to realize the ideal type of numerical value when dealing with numerical types;

● **Low-layer Access Support**

When the smart contract interacts with the environment outside the sandbox, the parameters that can be passed are limited to basic integer types. Subscript provides a complete syntax that can be used to define external interface types. Subscript also comes with instruction functions that can access the bottom layer of WASM, providing operations such as integer arithmetic, virtual machine stack access, and memory loading;

● **Paradigm Support**

Paradigm types can be defined to support code reuse. Subscript defines a series of reusable library functions through paradigms.

---

![Image 1 Subscript Language and Syntax Structure](image-url)

---

**TrustBase White-Paper**

05
2.3 Subscript Contract Library Functions

Subscript provides a wealth of library functions for developers to call. Library functions are divided into three parts: standard library, core library, and extended library:

- **Subscript Standard Library**
  (StandardLib) contains basic mathematical operations, array operations, string processing and memory access functions;

- **Subscript Core Library**
  (CoreLib) can be accessed directly in the contract code, and developers can access through functions:

  1) Contains basic cryptographic functions, Blake2b, Sha3, Sha256;

  2) Information on the chain (random number, block height, block time, etc.);

  3) Smart contract transfers, calling other contracts, calling modules on the chain (XCMP cross-chain messaging, pledge, governance, etc.).

- **Subscript Extension Library**
  (SupportLib) is a modular contract library function collection, including many commonly used contract templates. By extending the contract template in the library, developers can automatically integrate currently widely used contract functions, enhance the security of the contract, and avoid repeated development of basic functions:

  1) ERC20 Compatible Contract: provide token library functions compatible with ERC20 interface;

  2) ERC721 Compatible Contract: support the creation of non-homogeneous tokens;

  3) Permission control contract: Provide an account-based permission control function for the extended contract by using the contract base class;

  4) Agency Contract: realize the upgradeable function of the contract through the abstract contract interface;

  5) Governance Contracts: provide on-chain governance through voting;

  6) Multi-signature Contract: Multi-signature address contract that can support multiple account formats.
2.4 Mature Compilation Framework

Subscript uses the proven Binaryen compilation framework to compile smart contracts, focusing on reducing the volume of generated code during compilation. When dealing with WASM low-layer code, Subscript can provide faster execution speed than C++ and Rust.

Subscript adds language extensions to the Binaryen compilation framework, enabling it to directly support the mapping of object structures to contract state trees. Subscript’s state decorator has built-in state serialization and deserialization functions. After the developer adds the state decorator to the structure, the language can automatically serialize the structure into a string in the state tree, and the same is true for deserialization.

![Subscript Contract Compilation Diagram]

2.5 Package Management Tools Familiar to Developers

Subscript is integrated into the current Web development environment. There is no need to reset the development environment. Developers only need to use the familiar Npm tool to set up the entire smart contract compilation and deployment environment.

- To establish a development environment, you only need to execute a simple installation command: Npm Install;
- Compile smart contract code: Npm Run Build;
2.6 Debugger Support

Subscript uses the SourceMap mechanism to generate a mapping from compiled code to source code. SourceMap is a file about source code information, through SourceMap you can know the position and identifier of the compiled code in the source code. When debugging, the debugging tool can give the corresponding source code position at the breakpoint position, which will bring great convenience to the developer.

A smart contract virtual machine that can provide debugging support is under development. The virtual machine can provide WASM’s single-step execution function and display all stack information. After adding a breakpoint to the source code, the virtual machine can pause the current execution logic. Print out detailed stack information and memory data.

2.7 Subscript Workbench

Subscript Workbench is a browser-based smart contract integrated development environment (IDE). Subscript Workbench is similar to the Ethereum development environment Remix, and comes with the compilation tools needed for WASM smart contract development. DApp developers can synchronize the code in Github in Subscript Workbench, create smart contract projects, compile WASM, and publish to the test network.

After the development of the smart contract virtual machine is completed, Subscript Workbench can also provide online debugging functions for smart contracts similar to Remix. Developers can choose to add breakpoints to the browser source code to step through the compiled WASM code.
Chapter 3

RUSTBASE PARACHAIN
3. TrustBase Parachain

※ 3.1 Project Introduction

TrustBase is a Polkadot parachain based on the Substrate framework that independently develops the Subscript smart contract language and supports multiple tool plug-ins and smart contract applications. As an infrastructure project in the Polkadot ecosystem, TrustBase has been supported by the Web3 Foundation Grant.

TrustBase is committed to providing traditional developers with a more lightweight language that can easily deploy Polkadot native smart contracts. Assist developers to participate in the construction of Polkadot’s ecology without barriers, forming a powerful multi-dwelling ecosystem Polkadot — TrustBase Parachain — Smart Contract.

Image 3 TrustBase Architecture Diagram
3.2 TrustBase Structure

### 3.2.1 Sophisticated Underlying Architecture

In terms of function, TrustBase researched and realized the integrated security development and cross-chain deployment of smart contracts based on WASM. Provides a complete and easy-to-use development tool support. This is a new generation of lightweight developer tools.

The TrustBase parachain is developed based on the Substrate framework. Based on the WASM virtual machine and P2P network, TrustBase has built multiple runtime modules to process transactions on the chain. The runtime module of TrustBase is written in Rust language, compiled into WASM format and built into the client. Each runtime module of TrustBase can be independently upgraded online by redeploymeNT WASM code.

![Image 4 Schematic Diagram of the Underlying Architecture](image)

<table>
<thead>
<tr>
<th>DApp</th>
<th>Smart contract execution environment component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programmable Finance</td>
<td>Wasm virtual machine</td>
</tr>
<tr>
<td>Digital currency</td>
<td>Binaryen</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Account management component</th>
<th>Consensus algorithm component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority Management</td>
<td>NPOS</td>
</tr>
<tr>
<td>Account Management</td>
<td>Consensus Network</td>
</tr>
<tr>
<td>Security Verification</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>Digital Signature</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State management and data</th>
<th>Communication components of P2P network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource data</td>
<td>HTTP communication protocol</td>
</tr>
<tr>
<td>Block data validation</td>
<td>Data Encryption</td>
</tr>
<tr>
<td>Status Data</td>
<td>Data Synchronization</td>
</tr>
<tr>
<td>Transaction data hash</td>
<td></td>
</tr>
<tr>
<td>Transaction data hash</td>
<td></td>
</tr>
</tbody>
</table>
The TrustBase runtime includes the following functions:

1) **Account system**: The account system stores all user account information and balance data. TrustBase’s account status supports balance lock and penalty;

2) **Pledge**: The pledge module defines the pledge and delegation information of the validator. Handle the pledge, reward and profit distribution of all validators;

3) **On-chain Vault**: Part of the block rewards and penalties will be collected into the on-chain vault. The funds in the treasury distribute financial support for the TrustBase ecosystem through on-chain governance. Maintain the technology development of the TrustBase development community;

4) **Governance**: TrustBase token holders can use governance, initiate proposals, execute community on-chain voting, and participate in TrustBase community decision-making without access.

### 3.2.2 Isomorphic Parachain

Structurally, TrustBase is an isomorphic parachain of Polkadot. After connecting to Polkadot through a slot, it has the following characteristics:

- **Shared Cross-chain**
  TrustBase isomorphic parachain natively supports cross-chain protocols. Smart contract applications running on TrustBase can also share the interoperability of TrustBase and other parachains of Polkadot. For example, a DeFi contract deployed on TrustBase can use the aUSD stablecoin on the Acala parachain through XCMP cross-chain messages.

- **Fork-free Upgrade**
  TrustBase is based on the Substrate framework for runtime upgrades without forks.

- **Good interoperability**
  As a Polkadot parachain, TrustBase will share the interoperability of other Polkadot parachains. Achieve interoperability with other public chains such as Bitcoin and Ethereum through the Polkadot bridge structure.

### ※ 3.3 Virtual Machine Based on WASM

At the smart contract layer, TrustBase uses a high-performance virtual machine based on WASM (Web Assembly). WASM is a new generation code format that can be run directly in the browser. Compared with the EVM used by Ethereum, WASM can run at a speed close to the native speed while providing a more flexible contract interface.
3.4 TrustBase Smart Contract

The functions of smart contracts deployed on TrustBase are roughly the same as those of Ethereum or other EVM-compatible Blockchains. Any user with a TrustBase Token TBE can deploy a contract, and the contract can also call other smart contracts.

The Gas consumption during the execution of the smart contract is calculated by the TrustBase token TBE. Each transaction has a Gas cap, and any excess transaction fees will be refunded. If the message call exceeds the upper limit of Gas, the execution will be terminated and the running state will fall back to the initial environment. The contract will also be able to interact with other TrustBase modules through a set of predefined lists. In particular, you can call the accounts in the Identity and Council modules. In the future, TrustBase’s smart contract system will also support parallel transactions and state leasing functions.
3.5 TrustBase Storage

TrustBase uses MPT (Merkle Patricia Trie) to store and access the state of objects. MPT is a combination of Merkle tree and Patricia tree. It is an improved combination of Merkle tree and prefix tree. The key of a node is the path from the root node to the node. That is, when different keys have the same prefix, they share the path corresponding to the prefix.

TrustBase uses Base-16, each node has up to 16 child nodes,

A hash value is calculated for each node. The value in TrustBase is obtained by performing Blake2 operations on the node content, which is used to index the database and calculate the Merkle root. In other words, MPT uses two key types.

The first is the key corresponding to the Trie path, which is determined by the storage unit of the runtime module. The state of each storage unit is indexed or saved in the form of Trie nodes through key-value pairs. The value of this key-value pair is the result of SCALE encoding of the original data (such as numeric value, boolean) and is stored as part of the content of the MPT node.
3.6 Cross-chain Operation with Polkadot

The TrustBase smart contract platform natively supports the XCMP cross-chain protocol. TrustBase will bid through the Polkadot Parachain slot to access the Polkadot relay chain. Any smart contract application on the TrustBase platform can communicate with other Parachains of Polkadot through the XCMP protocol.

TrustBase uses a crowdfunding model to successfully bid for slots to become parachains. All smart contracts deployed on TrustBase can access other parachains in a Polkadot cross-chain manner. For example, a DeFi contract deployed on TrustBase can use the aUSD stablecoin on the Acala parachain through XCMP cross-chain messages, without having to build a parachain auction slot by yourself. Compared with building a parachain, developing smart contract applications on TrustBase saves the huge cost of bidding for Polkadot’s official slots, and only needs to use a small amount of TrustBase tokens to pay for Gas. Using the TrustBase platform to spend a small amount of platform currency can deploy complex smart contracts, while supporting interoperability with other parallel chains through the XCMP cross-chain protocol.

3.7 Application Scenario

3.7.1 Programming Tools

TrustBase has deployed a series of plug-ins based on Subscript language, such as browser-based IDE development environment, package management tools, contract library functions, etc. Assist developers to design their own products, such as new debuggers, project editors, multi-page windows, etc. TrustBase supports more developers to participate in the underlying construction and enrich the Polkadot ecology.
3.7.2 Native Smart Contract

TrustBase supports the deployment of WASM–based Polkadot native smart contracts. At the same time, it supports value interoperability with different Polkadot parachains. After the smart contract deployed based on the TrustBase parachain is issued a token, it can be freely exchanged through the value anchor of the TrustBase algorithm and the tokens on the Polkadot ecology.

3.7.3 DeFi

TrustBase supports the development and deployment of the DeFi ecosystem including but not limited to loans, DEX, derivatives, payments, assets, insurance and other types of products. Support the deployment of various stable currency protocols to meet the needs of users to maintain constant value during the transaction process. At the same time, it supports the ecological landing application of non–custodial wallet (NCW). In the DeFi ecosystem, the most missing part is the user–friendly non–custodial wallet (NCW). Building NCW on TrustBase can provide users with non–custodial encrypted asset storage, improve user experience and promote interoperability between DeFi protocols.

3.7.4 DAPP

TrustBase supports and is not limited to a variety of DAPP applications such as media, games, charity, airdrops, copyrights, wallets, music, and trading platforms. Ethereum is the public chain with the largest number of DAPPs, but the low TPS, network congestion, and high processing fees have become the biggest pain points of its current development, and it cannot meet the development of projects with high–frequency needs. TrustBase as a parachain of Polkadot, has features such as TPS hundreds of times higher than Ethereum, almost zero transaction costs, and a friendly smart contract development language. It will help developers around the world make DAPP better in the Polkadot ecosystem.

3.7.5 Oracle

TrustBase will support developers to deploy various oracles to establish a new transmission mechanism for off–chain data and on–chain data for the TrustBase and Polkadot ecosystems. The use of the oracle machine includes financial derivatives trading platforms, lending platforms, express tracking/IoT, stable coins, gambling games, insurance, prediction markets, etc. Provide core data sources such as transaction price information and volatility to the smart contract agreement to ensure the operation of the agreement.
3.7.6 DAO

TrustBase supports developers to deploy various decentralized autonomous organizations for the later prosperous economic ecology to realize the transformation of the basic functions of social institutions to automation. The DAO project developed on TrustBase will be completely open source, and anyone can audit its code. As the development continues and the overall platform improves, DAO will promote a paradigm shift in the concept of TrustBase economic organization.

3.8 Core Advantages

Through participating in the TrustBase parachain for full life cycle development and ecological deployment, it has the following core advantages:

1) Low Technical Participation Threshold
2) Smart Contract Applications are Simpler and More Reliable
3) WASM Execution Speed is High
4) Meet Diversified Customized Models
5) Sharing Cross-chain and Good Interoperability
6) Fork-free Upgrade
7) Low Deployment Cost
8) Low Gas Cost
4. Governance Model

The design purpose of the TrustBase governance model is to keep the security of the project and the collaboration of the participants consistent with the development direction of TrustBase through the value-added of the token. On the one hand, it ensures that participants obtain corresponding benefits by participating in the ecological development of TrustBase. On the other hand, participants can maintain the stability and security of the TrustBase network through the consistent design of economic goals. While pursuing their own interests, all participants also contribute to TrustBase’s ecological network.

※ 4.1 Consensus Mechanism

TrustBase uses a hybrid consensus algorithm to separate the final certainty from the block generation process. TrustBase uses the VRF algorithm to select the validator for block generation, and the block generation interval is set to 6 seconds. In the Slot time of each block, no one can infer the block validator in advance. When the random VRF algorithm cannot determine the block producer, the alternate algorithm will provide a block leader. When each validator in TrustBase collects the forked block, the best block is selected by the timestamp.

Use the GRANDPA algorithm to provide final certainty for the block and realize the proof of certainty. In the GRANDPA protocol, all validators of TrustBase vote for a sufficient number of chains with the highest number of votes through signature voting. The number of votes collected for each confirmation requires more than 2/3 of the validators.

TrustBase will adopt the POA (Proof-of-Authority) consensus mechanism in the CC1 testnet stage. Used to verify the running and calling environment of smart contracts, and governance is limited to a single Sudo (Super User Do) key. This key is held by the TrustBase Foundation and is used to issue commands and upgrades required to complete the startup process. During the development and upgrade period, as the number of validator nodes increased and began to join the TrustBase network. After ensuring a sufficient number of verification nodes, TrustBase Foundation will adjust the consensus mechanism to the POS (Proof of Stake) consensus mechanism during the CC2 testnet stage.

※ 4.2 Role Setting

TrustBase sets the following core roles according to the management needs of the participants and the community:

- Super Verification Node
  
  It has the function of generating blocks. It maintains the security of the TrustBase network by staking TBE, and is responsible for verifying, generating blocks, transmitting, storing, and collecting information transmitted. After the candidate validator participates in the election, if the total number of votes of the current node reaches the top 50, it will automatically become a super validator node, participate in the block generation, and get the income of each dividend cycle;
- **Ordinary Verification Node**
  Does not participate in block generation, only block data is synchronized. Responsible for the delivery, preservation, and collection of the information delivered. After the candidate verifier participates in the election, if the current total number of votes of the node is between 50 and 100 (including 100), it will automatically become an ordinary verification node and will not participate in block generation, but it can still get the income of each dividend cycle. At the same time, it is regarded as a candidate node for super verification node. If a super verification node is punished multiple times or dropped by Top50, the ordinary verification node will follow up and convert to a super verification node to produce blocks and obtain higher returns;

- **Nominator**
  The nominator is a user who holds a TBE to participate in the election of verification nodes. Users elect verification nodes in TrustBase by staking TBE. When the verification node is rewarded or punished, the nominator will also be rewarded or punished at the same time according to the voting ratio;

- **Law Enforcement Node**
  The law enforcement node is used in the role of Polkadot phisher and is also a super verification node of TrustBase. The main task is to monitor the nodes of the network in order to detect misbehaving verification nodes. The law enforcement nodes need to invest a small amount of TBE, but if they find node’s bad behaviors, they will get rich returns. The early–stage law enforcement nodes will be in charge by the TrustBase Foundation. Until the TrustBase community elects enough law enforcement nodes, all the work of the TrustBase Foundation law enforcement nodes will be handed over to the selected law enforcement nodes. Before the election of law enforcement nodes, the funds confiscated by all TrustBase Foundation law enforcement nodes will be deposited in the TrustBase treasury to encourage better development of the community.

![Role Relationship Diagram](image)
4.3 Penalty Mechanism

TrustBase has a penalty mechanism for malicious verification nodes. Once the law enforcement node finds that the verification node has violations (such as offline, destruction or malicious deletion of stored data, etc.), it will be punished. At the same time, his nominees will also receive corresponding punishments according to the voting ratio:

1) The amount of assets punished due to disconnection is the maximum penalty ratio in a cycle multiplied by the amount of deposit pledged by the verification node. The penalized assets will enter the treasury penalty account. If the appeal is not returned to the verification node within a certain period of time, the system will confiscate these assets by default. As a nominator, when the voting verification node is punished, the nominator is also punished according to the voting ratio;

2) If the verification node maliciously destroys or deletes the stored data, all mortgage deposits will be fined and the nominator will also be severely punished. The confiscated assets will be locked into the treasury penalty account. The severely punished nodes will enter the blacklist and be replaced by new candidate nodes;

3) For verification nodes that have been punished many times, the system will deduct all their rewards and collect them into the national treasury. Replaced by new candidate nodes according to corresponding rules.

4.4 Role Election

The verification node needs to pledge a certain amount of TBE to enter the election list. Whether it can become a validator node is determined by the number of pledges of the nominator and the number of pledges. The ranking is based on the number of mortgages and the number of pledges of the nominator (100 in total). Ranked 1–50 become super verification nodes. Ranked 50–100 become ordinary verification nodes.

In the first year, TrustBase will select 15 super nodes and 15 ordinary nodes according to the number of pledged DOTs during the parachain auction process. The top 8 contributions of the two will each become members of the TrustBase Heads of State Council and the Administrative Council, with a default term of six months. Becoming a super verification node or an ordinary verification node requires a certain threshold of TBE pledge, and is selected according to the final ranking of the token holders. In subsequent plans, the number of super verification nodes and ordinary verification nodes will be increased to 50 each.

The dividend cycle of the verification node is the unit block time of the TrustBase blockchain. The miner’s reward for unit production will be distributed to a certain super verification node that successfully produced the block in a certain proportion, a small amount will flow into the law enforcement node reward pool, and the remaining part will be
evenly distributed to all ordinary verification nodes. The verification node can determine the specific dividend ratio with the nominator within the specified interval.

The TBE pledged by the verification node and the nominator will not be forced to lock up. After a short unfreeze period, the nominator is free to withdraw or change the supporting validator. Ordinary verification nodes and super verification nodes also have a short unfreeze period, after which they can freely withdraw coins and untie them. However, if the verification node becomes a member of the parliament, it needs to initiate the corresponding parliamentary proposal, and then can withdraw after the vote is passed.

Becoming a law enforcement node requires the super verification node to pledge a certain amount of TBE, and the term of office is half a year by default. After the thawing period is over, if you want to release the pledge and withdraw, you also need to initiate a proposal and vote. Once the law enforcement node successfully punishes the malicious node, it will receive a certain percentage of the current law enforcement node reward pool as a punishment reward.
5. DAO Autonomy

In the construction of TrustBase community autonomy, the mainstay is TrustBase’s verification nodes and community volunteers. The members of the TrustBase Board of Trustees choose among all community members who are capable, strong, energetic, and responsible. Mainly responsible for the implementation of TrustBase DAO governance, proposals, voting and other community work. Therefore, the validator of TrustBase is also a candidate for the council. The members of the board of directors will be voted in the referendum (the referendum mechanism for board members also uses the time lock weight mechanism to avoid election bribery). Further participate in development decision-making and governance. Share the dividends of TrustBase ecological development together.

※ 5.1 National Assembly

The National Assembly is one of TrustBase’s three on-chain governance institutions. The members of the National Assembly are composed of all nominees on the TrustBase chain. The National Assembly’s participation in the governance process mainly includes three stages: the proposal stage, the voting stage and the vote counting stage.

1) Proposal Stage

There are two ways for participants to make proposals. Public proposals and opposition proposals to proposals already resolved by the TrustBase Council;

2) Voting Stage

First, the members of the TrustBase board of directors vote. Participants can choose to agree or disagree, and those who do not participate in voting are considered abstentions. The members of the board who have not participated in the voting multiple times will be replaced. If members of the National Assembly disagree with certain members of the decision-making level, they can re-election by launching an opposition proposal;

3) Counting Stage

In the counting stage, there are three ways to determine the voting result:

- When the voting rate is high, a majority pass method is adopted, that is a simple comparison of votes. If there are more votes in favor than against, the proposal is passed.

- Positive voter turnout bias, that is when the turnout rate is low, it must be passed by an absolute majority.

- Negative voter turnout bias, that is when the turnout rate is low, it must be rejected by an absolute majority.

At the same time, in order to encourage the National Assembly to actively participate in community building, the National Assembly will set voting reward weights when voting. The more members of the parliament participate in the referendum proposal, the corresponding
vote reward weight will increase. According to the participation rate of members of the National Assembly in the referendum, the weight of rewards for election and voting increases by 1% every month. Participants who vote for the proposal will receive voting rewards. When the number of participants reaches the minimum threshold, all members participating in the voting will be divided into voting rewards according to the voting reward weight. Voting rewards come from TrustBase’s on-chain vault.

※ 5.2 Council (Head of State Council and Administrative Council)

The council is the most important part of the three on-chain governance institutions, and consists of the "Head of State Council" and the "Administrative Council".

5.2.1 Heads of State Council

The Heads of State Council is composed of members of the super verification node. The heads of state assembly initially had 13 seats. These 13 seats were selected for the first time from the first batch of 50 super verification nodes. The number will be gradually increased to 26 through elections. Each member has a term of one year. The additional candidates for the Parliament of the Head of State come from the proposals of members of the National Assembly. The members of the Parliament of the Head of State are elected through voting by members of the National Assembly.

Any member of the National Assembly can vote in the Parliament of the Head of State. Users can select all legal candidates, and select the candidate with the most support through the voting counting algorithm of the time lock weight mechanism.

The Heads of State Council is mainly responsible for:

- Initiation of the board of directors’ proposal and voting for resolutions;
- Voting on the resolution of code upgrade;
- Initiation of system parameter adjustment proposals and voting for decisions;
- Initiation of proposals for changes in governance rules and voting on decisions;
- Voting on financial appropriations.

5.2.2 Administrative Council

The Administrative Council is composed of members of the ordinary verification node. The heads of state assembly initially had 13 seats. These 13 seats were selected for the first time from the first batch of 50 ordinary verification nodes. The number will be gradually increased to 26 through elections. Each member has a term of one year. The additional candidates for the Parliament of the Administrative Council come from the proposals of members of the National Assembly. The members of the Parliament of the Administrative Council are elected through voting by members of the National Assembly.
Any member of the National Assembly can vote in the Parliament of the Administrative Council. Users can select all legal candidates, and select the candidate with the most support through the voting counting algorithm of the time lock weight mechanism.

The Administrative Council is mainly responsible for:

- To vote on proposals initiated by the Heads of State Council;
- Initiate an opposition vote to the proposal that has been resolved by the Parliament of the Head of State;
- Voting on the system parameter adjustment proposal;
- Voting on proposals for changes in governance rules;

※ 5.3 Technical Committee

The members of the TrustBase Technical Committee are composed of members of the technology developer community. It mainly includes the TrustBase technology development team, members of the Polkadot ecological project cooperative development team and TrustBase technology development enthusiasts.

- The members of the technical committee passed the TrustBase council proposal and voted by majority. You can add or delete teams from the technical committee;
- The technical committee can formulate an emergency referendum together with the members of the Heads of State Council of the TrustBase Council to quickly vote and implement. These emergency referendums are only used in emergency situations;
- The Technical Committee is mainly responsible for initiating proposals for technical code upgrades and changes to important system parameters. Follow up and supervise the development and maintenance progress of the TrustBase ecosystem. Promote the development of technical committees and technology developer communities.

※ 5.4 Voting Mechanism

5.4.1 Time Lock Weight Mechanism

All voters are weighed according to the following two dimensions.

- TBE Number: the number of TBE token holders;
- Time: The length of time that TBE tokens remain pledged and locked after the referendum ends;
5.4.2 Adaptive Voter Bias

In the name of decentralization, TrustBase allows anyone to come up with new ideas, but this has certain volatility. One of the benefits of a centralized system is that no one can come up with new ideas. Adaptive quorum biasing allows TrustBase to avoid fluctuations while promoting effective change.

- A standard voting participation bias requires an overwhelming majority of voters to vote "aye" in support to pass a low voting participation referendum;
- An inverted voting participation bias requires an overwhelming majority of voters to vote "nay" to reject a referendum with low voting participation;

5.4.3 Council Priority Decision Mechanism

In order to improve the efficiency of development and community work, TrustBase will create a priority decision mechanism for the board of directors. The decision-making layer of the council is also elected by the community and has a rotation cycle. The characteristic of these decision-makers is that they have the right to determine and veto the proposal. If community users disagree with the results of certain proposals, they can re-election by initiating an opposition proposal during the period of delayed execution of the proposal.

5.5 Noun Interpretation

1) Time Lock–up Weight Mechanism

Time lock–up weight mechanism is an innovative mechanism that allows TBE holders to increase the voting weight of certain proposals. The function of this mechanism is to encourage long–term currency holders to contribute to the community through a weighted method and to raise the threshold of bribery. Under the time lock weight mechanism, all voters are weighed according to the two dimensions of the number of TBE tokens of TBE holders and the length of time the TBE tokens remain pledged and locked after the referendum. 5 different time periods will be allowed: 4 weeks, 8 weeks, 16 weeks, 32 weeks, 64 weeks. Each time before double the length of time increases the weight of voters. Voters can also choose not to lock the tokens at all, which will cause their voting weight to be reduced by a large percentage. Voters need to lock up their TBE tokens for at least four weeks. This design is to ensure that voters have the most basic economic investment to reduce ticket buying and election bribery.

2) Adaptive Voter Bias

One of the main refuted reasons for token voting is that no matter where this mechanism
is tried, the voting participation rate is always low. The original intention of TrustBase’s adaptive voter bias is to solve the problem that the number of voting results may not be 100%. This mechanism will change the situation where more than a majority is required to pass a referendum proposal based on the proportion of the number of voters participating. When a proposal in favor of TrustBase is voted by the board of directors with non-consensus opinions, this mechanism will gain value from the inverted voting bias. However, the referendum must be passed using the standard curve. This is done to mitigate malicious attacks and malicious proposals, and to ensure that a majority of Stake pledges can always control the core principle of the network.

3) Council Priority Decision-making Mechanism

The disadvantage of Polkadot’s council mechanism is that it is expected to have low governance participation. Council members have great rights, but there is no corresponding incentive mechanism. The token voting mechanism will have a lower voting participation rate for newly developed projects. Therefore, TrustBase created the “Council Priority Decision Mechanism” based on the Polkadot council mechanism. TrustBase needs to optimize the details of the council system, conduct quantitative analysis on small proposals and invalid proposals, and gradually adjust the corresponding parameters according to the size of the community. The advantage is that while maintaining the overall decentralization, it also alleviates the efficiency problem of the on-chain voting mechanism criticized by others. The grassroots does not have to spend time voting on small and invalid proposals for each proposal. If community members have objections to some members of the decision-making level, they can initiate a re-election by launching an opposition proposal during the period of delay in implementation of the proposal, which also acts as a check and balance on the decision-making level. The voting mechanism will be implemented in accordance with the ”Time Lock Weight Mechanism” and ”Adaptive Voter Vias”. 
6. Economic Model

6.1 TBE Commercial Value

TBE (TrustBase Token) is an ecological token issued by TrustBase based on the Substrate protocol. It will be used to encourage and maintain the healthy development of the ecology, and connect the participating roles of the TrustBase ecology to form a positive circulation. In addition, TBE will also be used to participate in Polkadot ecological mining, increase user income, and share ecological prosperity.

6.1.1 TBE Usage Scenarios

- **Staking**
  As the only target of TrustBase Staking mining rewards. Staking rewards account for 50% of the total TBE issuance and are distributed to the participants in the TrustBase ecosystem. The annual mining ratio is set at 2% of the total issuance. 3.8 TBEs will be awarded for unit block. The adjustment of the subsequent annual mining issuance requires the parliament to initiate a proposal to vote;

- **Node Election**
  As a measurement standard for elections, super verification nodes and ordinary verification nodes need to pledge a certain amount of TBE to participate in the election;

- **Nominator Verification**
  the only equity token for the nominator verification node Staking mining;

- **On-chain Governance**
  The only pass for on-chain governance, through which TBE can participate in the mortgage and voting of on-chain governance.

- **Proof of Weight**
  combined with the token holding time, as a holding (TBE) nominee, he has the weight to run for and elect members of the National Assembly;

- **DAPP Call**
  As the fuel of DAPP on the TrustBase chain, the Gas fee and handling fee for running the transaction called by DAPP will be allocated to super verification nodes and ordinary verification nodes;
• **Transaction Gas**
  As the transaction fee for transferring TBE between accounts, super verification nodes and ordinary verification nodes receive corresponding accounting rewards;

• **Block Rewards**
  Blockchain generation and confirmation of TrustBase network, super validator nodes will get corresponding block rewards;

• **DAO Autonomy**
  TrustBase will reward or fund the community and ecological contributors with a decentralized governance model;

• **DEX**
  The exchange medium of TrustBase DEX. For the token issued on TrustBase, TBE will be the exchange medium of these certificates in the DEX Dapp integrated in the TrustBase system;

• **Pledge**
  The collateral for DeFi and Dapp related applications, on-chain DeFi derivatives and the core collateral for asset cross-chain trusts, are the risk control measurement standards for DeFi financial derivatives and the main tool to improve trust credit.

※ 6.2 Node Rights

6.2.1 Super validator node rights

Super validator nodes enjoy the following rights:

1) Proportionately obtain the income of the whole network transfer fee;
2) Staking rights are pledged for mining, and miner fee dividends are obtained;
3) Become a member of the Heads of State Council and have the right to make proposals for governance on the chain;
4) Become a law enforcement node and obtain law enforcement benefits;
5) Obtain the white list of TrustBase issuing pass;
6) The network’s blockchain generation and confirmation will receive corresponding maintenance rewards;
6.2.2 Ordinary Verification Nodes Rights

Ordinary validator nodes enjoy the following rights:

1) Become a candidate for a super verification node;
2) Proportionately get the income of the whole network transfer fee;
3) Obtain the white list of TrustBase issuing pass;
4) Become a member of the Administrative Council and vote on proposals;
5) The network's blockchain generation and confirmation will receive corresponding

6.3 Gas Rate Setting and Standard

In order to prevent DDOS, users need to pay miner fees to send transactions on the chain. The initial handling fee for an ordinary transfer transaction set by TrustBase is only 0.001 TBE. With the gradual improvement of TrustBase's performance and throughput, the handling fee for each operation initiated by the user will gradually be ignored.

The system will deduct the corresponding gas fee according to the complexity of different operations. Users can also choose different acceleration multiples according to network congestion to achieve flexible control. Although users need to pay a handling fee, as long as users participate in voting or have appropriate assets, a large amount of mining revenue can be obtained in the early stages of network development. Enough to meet the transaction needs of non-high-frequency users on the chain.

When the super verification node is packaged, part of the handling fee will be collected into the node prize pool and returned to the voting users of the National Assembly. Therefore, voting users can still use the Blockchain "for free" in this closed-loop system, and most mining users will be profitable. Only certain high-frequency trading users need to pay additional fees. Networks like Ethereum tend to be too expensive for a single transaction due to low throughput. This situation will no longer exist in the TrustBase parachain.
6.4 TBE Issuing Plan

1) Total Issuance: 1 billion

2) Distribution:

- 50% Miner Incentives
- 20% Private Placement
- 15% Founding Team
- 10% DAO
- 5% Validator Node Pledge

6.5 TBE Destruction Mechanism

TrustBase will formulate a quarterly destruction plan for TBE through the destruction proposal initiated by the Heads of State Council. In order to further enhance the scarcity of TBE and reasonably control the circulation of tokens. Due to the importance of the proposals related to the destruction mechanism, all members of the National Assembly need to participate in the voting on the proposal of the destruction mechanism.
7. TrustBase Foundation

The TrustBase Foundation was created to cultivate and manage technologies and applications in the field of decentralized network software protocols. Especially those who use modern encryption methods to protect decentralized technologies and applications, which stabilize the interests of the TrustBase ecosystem.

TrustBase Foundation was initiated and established by the TrustBase startup team. It mainly consists of two teams with a total of 23 members. The research team is conducted by the internal research team in Berlin, Germany, in cooperation with industrial projects and academic research teams. The team is composed of PhDs and experts focusing on cryptography, security models and messaging protocols;

The other team is the Adoptions Team of the TrustBase Foundation, which is mainly responsible for communication and docking, community and growth (such as the Subscript Developer Community Program, TrustBase Verifier Community), and business cooperation (finding partners, establishing partnerships, etc.). They work closely with the technical education team and are also responsible for fund review and distribution.

※ 7.1 The Composition System of Fund Committee Members

The TrustBase’s on-chain vault is initially managed by the TrustBase startup team. With the development of the ecosystem, the startup team will vote for 9 members from the various councils of the TrustBase community to form a fund committee:

- 1 representative from the National Assembly
- 1 representative of community outstanding contributors
- 2 representatives from the Heads of State Council
- 2 representatives of the Administrative Council
- 2 representatives of Technical Committee
- 1 member from TrustBase original development team

In order to ensure operational efficiency and continuity, the TrustBase Fund Committee elects its own secretary-general and directors, and decides on its own personnel replacement (subject to the board of directors for record). Secondly, the TrustBase board of directors has the right to initiate a proposal for removal of one or some members of the Fund Committee, and with the consent of two-thirds of the board of directors, pass the proposal for removal. The TrustBase Fund Committee has multiple dynamic working groups, which are created for a specific task.
7.2 Duties of the Fund Committee

The TrustBase Fund Committee, under the supervision of the community and the board of directors (the Fund Committee is required to regularly release work reports and fund use reports to the community) performs the following duties:

1) Infrastructure deployment, operation, maintenance, network security, such as monitoring services, auditing, etc.;

2) Audit and control the funds of the TrustBase on-chain vault;

3) Provide advice or consultation on the development and planning of the TrustBase parachain project;

4) Cultivate, manage and support TrustBase community development (community promotion, advertising, cooperation, offline activities, etc.);

5) Provide direct technical support to TrustBase technical community developers;

6) Coordinate and organize ecological user groups or development teams, and provide on-chain vault support or technical support for special projects.
8. Development Plan

2020

04.2020
The project started and the Subscript contract language was developed:

Subscript Milestone1
1) Realize support for the runtime of Substrate contract;
2) Build the overall operating environment of smart contracts;
3) Implement the deployment and call functions of the contract.

Subscript Milestone2
1) Complete smart contract and Web3 application integration;
2) Support the automatic generation of contract status data;
3) Add support for smart contract basic templates.

Subscript Milestone3
1) Add support for cross-chain calls of smart contracts;
2) Realize the WASM smart contract sandbox simulation environment;
3) Build a complete IDE to support the testing and debugging of smart contracts.

09.2020
Web3 Foundation Grant Certification

11.2020
Start operations and brand work

12.2020
The validator node candidate criteria were released

2021

03.2021
Launched the CC2 version of TrustBase trial network, including the following functions:
1) The testnet uses the POS consensus operation of the GRANDPA mechanism;
2) The testnet supports the pledge and redemption operations of the validator, and supports the nominator’s entrusted operation;
3) The testnet supports the deployment and operation of smart contracts in WebAssembly format;
4) The testnet completes the distribution of the initial TrustBase token in the genesis block;
5) Provide TrustBase client operation services, provide block browser services for the test network;
6) Subscript language supports the creation of ERC20 format certificates on the testnet.

02.2021
Completion of the CC1 version of TrustBase testnet, including the following functions:
1) The testnet supports the POA consensus mechanism and the validator node is designated by the genesis block;
2) The testnet supports the running of WASM virtual machines, which can run smart contracts in WebAssembly format.
8. Development Plan

04.2021
Access to the Polkadot relaychain, participate in the parachain slot auction through DOT crowdfunding and provide cross-chain interoperability for contracts.

05.2021
Ecological expansion, TrustBase application scenario landing.

10.2021
Layer 2 will be expanded, adding Layer 2 network expansion to provide network throughput.

12.2021
A cross-chain bridge will be built, linking Ethereum, Bitcoin and other public chains.

01.2022
Network sharding, which provides network sharding of contract parachains. Realize real network expansion and Web3.0 application platform development support.
Chapter 9

FOUNDING TEAM
9. Founding Team

Paul Safranek  
TrustBase CEO

Graduated from New York University;  
Blockchain and smart contract expert;  
Senior Technical Advisor;  
Started technical work in the field of Bitcoin and Blockchain in 2011;  
Leading the technical development of multiple open source projects. EOS1.0 core developer.

Symon Ho  
TrustBase CTO

Full–stack Developer;  
Leading consensus R&D and engineering in multichain system;  
Over 10 years of experiences in Development and Management;  
Has plenty of experience in Software Architecture;  
Currently focused on Blockchain Development and Cross–chain Technologies.

Regina Yang  
TrustBase CMO

With many years of Internet marketing experience, she has provided brand marketing services and strategy support for Huawei, Intel, and other companies. More than 5 years of experience in Blockchain industry. Independent entrepreneurs. Community KOL.

Served as a brand consultant for many high–quality projects and exchange. Served as the head of user growth in a well–known exchange.

Developer Team

The core developer team is headquartered in Berlin, Germany, and is personally led by TrustBase CTO: Mr. Symon Ho. The team is composed of PhDs and experts in cryptography, security models and messaging protocols; they mainly focus on (provable) security Decentralized algorithms for security, cryptography, and privacy: consensus and optimization cryptoeconomics and game theory.

The other 15 members of the developer community come from three countries and regions: the United States, Germany, and China. Under the leadership of Symon Ho, they jointly participated in the construction and development of Subscript language optimization and TrustBase parachain.
Chapter 10

RISK WARNING AND DISCLAIMER
10. Risk Warning and Disclaimer

(1) License and Approval

Licenses and approvals are not guaranteed in all jurisdictions. TrustBase will operate in full compliance with applicable laws and regulations. The views expressed in this white paper represent TrustBase, and do not reflect the jurisdiction of any government quasi-government, authority or the official policy or position of the institution (including but not limited to any regulatory agency in any jurisdiction).

(2) Risk Warning

Any investment project has systemic and unsystematic potential risks. The content in this white paper only describes the resources controlled by the project, the actual development situation and the long-term vision. It is used to convey information and has no intention to provide any investment advice. This document does not constitute and is not understood to be any offer, request or recommendation for any trading behavior, and is not a contract or promise in any form. As a new investment model, digital asset investment still has various potential risks. TrustBase Token belongs to the category of digital assets, and price fluctuations are normal. Investors are required to carefully assess investment risks and have risk tolerance. Blockchain is in the early stage, and the supervision of Blockchain projects in various countries is currently undetermined. Does not rule out changes in project operation and management.

(3) Disclaimer

Once the investor participates in the investment, it means that he understands and accepts the risks of this project. Willing to bear the corresponding results. The TrustBase team is not responsible for any direct or indirect asset losses caused by participating in the TrustBase project. The capital market is unpredictable, investment is risky, and you need to be cautious when entering the market.

(4) Third-party Information

This white paper contains data and references obtained from third-party sources. The management believes that the data is accurate and reliable and accepts independent review, verification or analysis by any professional law. Regarding the auditing activities of accounting, engineering or financial consultants, this white paper cannot guarantee the accuracy of opinions, the reliability or completeness of data.