STABILA
PUBLIC CHAIN

WHITE PAPER

Decentralize the Financial System

1. INTRODUCTION
2. TERMINOLOGY
3. ARCHITECTURE
4. CONSENSUS
5. ACCOUNT
6. TRANSACTION
7. BANDWIDTH
8. FEE
9. STABILA VIRTUAL MACHINE
10. SMART CONTRACTS
11. GOVERNANCE
12. STABILA CHAIN SETTINGS

Building decentralized finance.

STABILA PUBLIC CHAIN

1. INTRODUCTION

STABILA is a project committed to financial system decentralization. STABILA Protocol provides a public blockchain service with high throughput, flexibility, and reliability. All of the Decentralized Applications (DApps) in the STABILA space are licensed to counter fraud and minimize risk for its users.

"Digital transformation lets the world reimagine itself – and Moneta is happy to be among the changemakers by enabling customer-centric services and lasting relationships.“

www.stabilascan.org

2 TERMINOLOGY

Address/Wallet

On the STABILA network, a key pair consists of a private key and a public key that produces an address or wallet carrying account credentials. Generally, the public key is used for session key encryption, identity authentication, and encrypts the data that can be decrypted using a private key.

ABI

Application binary interface (ABI) is a link in-between 2 binary programme components, one of which is usually a library or an operating system trait and the other as a user-run programme.

API

An application programming interface (API) is primarily utilized in the creation of user clients. Token issuing systems can also be built by developers with API support.

Asset

Asset is just the same as token in STABILA's network, which is usually referred to as SRC-10 token.

Bandwidth Points (BP)

STABILA network transactions require BP(Bandwidth) as fuel to keep the network running smoothly. Each account receives 500 free BP each day, with more BP available by surrendering (Contract of Deposit) STB for BP. Transfers of STB and SRC-10 tokens are both standard transactions that cost BP. Both BP and UCR are used in smart contract deployment and execution transactions.

2 TERMINOLOGY

Block

The digital records of transactions are stored in blocks. It includes

- ❑ *Height*
- ❑ *The size of block*
- ❑ *Block Header*
- ❑ *The transacted assets*
- ❑ *Transaction contents*

Block Reward

The incentives for block generation are paid to a sub-account (address/wallet). Governors and executives can claim their awards directly using the API or on stabilascan.org or in wallet client.

Block Header

A block header is a section of a larger block. The hash of the preceding block, the Merkle root, timestamp, version, and executive address are all included in the STABILA block headers.

Cold Wallet

The private key is kept fully unconnected from any network in a cold wallet, which is also referred to as an offline wallet. To maintain the security of the STB private key, cold wallets are often located on "cold" machines (such as, PCs or mobile phones that are not connected to the web.

2 TERMINOLOGY

DApp

A decentralized application is one that runs without the need for a centrally trusted third party. An application that allows end users and/or resources to interact/agree/communicate directly without the necessity of a mediator.

gRPC

(Remote Procedure Calls) is a Google-developed open source remote procedure call (RPC) framework. It supports authentication:

- *Flow management and bidirectional streaming*
- *Bindings that are blocking or nonblocking, as well as cancellation and timeouts.*
- *The transport protocol is HTTP/2, and the interface description language is Protocol Buffers.*

For a variety of languages, it builds cross-platform client and server bindings. The most common use cases include linking services in a microservices architecture, connecting smart phones, and connecting browser clients to backend services.

Hot Wallet

A hot wallet, also known as an online wallet, is subject to security weaknesses or hostile party interception since it allows a user's private key to be utilized online.

JDK

The Java Development Kit (JDK) is a software development kit for Java applications. The Java application environment (JVM+Java class library) and Java tools are at the heart of Stabila development.

2 TERMINOLOGY

RPC

In distributed computing, a remote procedure call (RPC) is when a computer program causes a procedure (subroutine) to execute in a different address space (commonly on another computer on a shared network), which is coded as if it were a normal (local) procedure call, without the programmer explicitly coding the details for the remote interaction.

Scalability

Scalability is a feature of the STABILA Protocol. It is the capability of a system, network, or process to handle a growing amount of work or its potential to be enlarged to accommodate that growth.

UNIT

UNIT is the smallest unit of STB. 1 STB = 1,000,000 UNIT.

Throughput

High throughput is a feature of STABILA Mainnet. It is measured in Transactions Per Second (TPS), namely the maximum transaction capacity in one second.

Timestamp

The approximate time of block production is recorded as Unix timestamp, which is the number of milliseconds that have elapsed since 00:00:00 01 Jan 1970 UTC.

SRC-10

A standard of crypto token on STABILA platform. Certain rules and interfaces are required to follow when holding an initial coin offering on STABILA blockchain.

STB

STB stands for Stabila, which is the official cryptocurrency of STABILA.

2 TERMINOLOGY

LevelDB

The fundamental purpose of LevelDB's adoption was to address the needs of quick Read/Write and rapid development.

Merkle Root

In a blockchain network, a Merkle root is the sum of all transaction hashes contained in a block.

RPC

A remote procedure call (RPC) is a term used in distributed computing to describe when a computer programme causes a routine (recursion) to operate in a different address space (usually on another machine on a shared network) without the programmer explicitly coding the details of the remote connection.

3 ARCHITECTURE

STABILA has a 3-layer architecture.

1. *Storage*
2. *Core*
3. *Application*

The STABILA protocol is based on Google Protobuf, which allows multi-language extension by default.

STABILA Virtual Machine (SVM)

The SVM is a Turing complete virtual machine that is lightweight. The SVM is fully integrated into the current environment.

Decentralized Exchange (DEX)

Decentralized exchange features are built-in to the STABILA network. Multiple trading pairings make up a decentralized exchange. A trade-off Market between SRC-10 tokens, or amidst a SRC-10 token and STB, is referred to as a trading pair (notation "Exchange"). A trading pair between any tokens can be created by any account.

The STABILA blockchain code is written in Java and was initially a fork of TRON TVM.

4 CONSENSUS

Delegated Proof of Stake (DPoS)

Many new networks suggested the Proof of Stake (PoS) consensus technique. Token holders in PoS networks lock their token holdings in order for them to transform into block validators. The validators propose and vote on the following block in turn. The difficulty with traditional PoS is that validator power is proportional to the number of tokens that have been locked up. As a result, parties with huge quantities of the network's basic currency hold excessive power over the network ecosystem.

The STABILA consensus process employs a novel Delegated Proof of Stake approach in which the network's blocks are created by 21 Governors (Gs). STB account members who CD their accounts have the opportunity to vote for a selection of Executives, with the top 21 Executives designated the Governors.

Every three seconds, the STABILA protocol network creates a new block.

5 ACCOUNT

In the STABILA network, there are three sorts of accounts.

1. Standard transactions are handled using regular accounts.

2. SRC-10 tokens are stored in token accounts.

3. Contract accounts are basically smart accounts that are established by ordinary accounts and can also be activated by them.

Account Creation

A STABILA account can be created in one of three ways:

1. Use the API to create a new account.

2. Move STB to a different address.

3. Send any SRC-10 tokens to a new address.

Private Key and Address generation

An address (public key) and a private key can be used to create an offline key pair. The user address generation algorithm begins with the creation of a key pair, followed by the extraction of the public key (64-byte byte array representing x, y coordinates) [1].

Extract the final 20 bytes of the hashed public key using the SHA3-256 function (the SHA3 protocol used is KECCAK-256). The initial address length should be 21 bytes, and 3F should be appended to the start of the byte array.

Use the SHA3-256 algorithm to hash the address twice and use the first four bytes as a verification code. You may acquire the address in base58check format by attaching the authentication code to the end of the initial address and encoding it with base58.

The first character of an encoded Stabila Mainnet address is S, and it is 34 bytes long.

6 TRANSACTION

Signing

STABILA uses a typical ECDSA cryptographic method with an SECP256K1 selection curve for transaction signature [2].

The public key is a point on the elliptic curve, while the private key is a random number.

To get a public key, first generate a random integer as a private key, and then multiply the private key by the base point of the elliptic curve to get the public key.

When a transaction takes place, the unprocessed data is transformed into byte format first. The unprocessed data is subsequently hashed using the SHA-256 algorithm. The output of the SHA256 hash is then signed using the private key associated with the contract address. The transaction is then updated with the signature result[3].

7 BANDWIDTH

Bandwidth Model

Smart contract activities consume both UCR (units of conventional resources) and BP(bandwidth points), whereas ordinary transactions just consume bandwidth points.

There are two different sorts of bandwidth credits

Users may earn bandwidth credits by generating Contracts of Deposits (CD) with STB, and there are also 500 free bandwidth points accessible every day. When an STB transaction is broadcast, it is transferred and stored across the network as a byte array.

The amount of transaction bytes multiplied by the total bandwidth points rate equals the number of bandwidth points required by one transaction.

***Example**:*

When a transaction's byte array length is 200, the transaction requires 200 bandwidth credits.

If the target account is formed as a consequence of an STB or token transfer, only the bandwidth points used to construct the account will be removed; No more bandwidth credits will be used.

The network will utilize the bandwidth points that the transaction initiator acquired via CDeing. The network consumes the transaction initiator's STB if this amount is inadequate. The network spends the bandwidth points earned by the transaction initiator for CDeing STB in normal STB transfer scenarios from one STB account to another. If it isn't sufficient, it will exhaust the 500 free daily bandwidth credits. If that is still not enough, then the network consumes the STB of the transaction initiator.

The value is computed by multiplying the transaction's number of bytes by 40 UNIT. As a result, for most STB owners who may or may not choose to CD their STB to participate in Governors voting, the first stage is automatically omitted (because STB balance CDed = 0) and the transaction is powered by the 500 daily free bandwidth[4].

7 BANDWIDTH

For SRC-10 token transactions, the network first checks if the issued token asset's total free bandwidth points are adequate. The bandwidth points earned through CDing STB are consumed if this is not done. If there are still insufficient bandwidth points, the transaction initiator's STB is used.

8 FEE

Fee

Most transactions on the STABILA network are free, although bandwidth use and transactions are subject to costs owing to system constraints and fairness.

1. Transactions with normal bandwidth costs bandwidth points.

2. Smart contracts are not only expensive in terms of UCR, but they also require bandwidth points in order for the transaction to be broadcasted and verified.

3. There is no charge for any query transaction. It costs neither UCR nor bandwidth.

The STABILA network also creates a set of pre-determined fees for the following transactions:

1. For constructing an executive node, you'll need 1000 STB

2. Issuing a SRC-10 token, you'll need 1000 STB

3. Create a new account: 1385 UNIT

4. Establishing a trading pair: 14 STB

Transaction Confirmation

A transaction is included in a future block once it has been broadcasted to the network.

The transaction is verified and respectively solidified when STABILA network mines 18 more blocks (including its own block). On the blockchain, each block takes 3 seconds to mine. A transaction is verified in less than 60 seconds.

9 STABILA VIRTUAL MACHINE

STABILA Virtual Machine (SVM)

SVM stands for STABILA Virtual Machine, which is a fully virtualized machine. Its mission is to create an efficient, convenient, reliable, secure, and scalable blockchain service. SVM was initially a fork of TRON TVM. SVM works in tandem with the current Solidity smart contract development environment.

DPoS consensus [5] is also supported by SVM. The notion of UCR is used in SVM. On SVM, transaction and smart contract operations are free, and no STB is used.

The compiler converts the Solidity smart contract into bytecode that the SVM can read and execute. The SVM then processes data using opcode, which is comparable to stack-based finite state machine logic.

10 SMART CONTRACTS

Compatibility

SVM is compatible with EVM and, in the future, with more standard virtual machines. However, because of the potentially fraudulent nature of smart contracts, a licensing mechanism is being recommended before any user can implement one.

Smart Contracts Licensing

Smart contracts are ineffective and will remain so for the foreseeable future. They lack asset backup proofing mechanisms and are unable to communicate with the outside world. The suggested licensing model allows only real-world smart contracts that are asset-backed by the underlying logic and organizational structure [6]. In the event that the smart contract owner is unable to keep up with his smart contract, a third party will assume responsibility, ensuring that clients on the STABILA network are safeguarded.

Units of Conventional Resources(UCR) Model

A lot of factors influence the maximal UCR limitation for implementing and operating a smart contract, including:

- *1 STB = 30,000,000,000 (Total UCR Limit) / Dynamic UCR from CDeing (Total UCR Weight)*
- *The daily account UCR limit from CDeing STB is the remaining daily account UCR limit.*
- *The remaining useable STB in the account is determined as UCR Limit - UCR Used.*
- *The fee limit in the STB is specified in the smart contract deploy/trigger call.*

Smart contract functionality will be activated in February 2022.

11 GOVERNANCE

Governors

Every account in the STABILA network is eligible to apply and become an Executive (denoted as E). Executives are voted for by the general public. The top 21 executives with the highest votes will be elected as Governors, having the power and responsibility to create blocks. Every 6 hours, the votes are counted, and the Gs are updated appropriately. There is a fee to becoming an Executive in order to avoid malicious assaults. The applicant's account will be charged 1000 STB when they apply. Such an account can then participate in the G election if it is successful.

Election

The quantity of STABILA Power (SP) required to vote is determined by the voter's CDed assets (STB). The following formula is used to compute SP: To acquire bandwidth, 1 SP = 1 STB CDed

Every STABILA network account has the ability to vote for their own Gs. Users will lose all SP if they don't have any CDed assets following the release (UNCD, accessible in 3 days). As a result, until STB is CDed again to vote, all votes for the current and future voting rounds become worthless.

Executive Reward

Often referred as Executive Reward, the topmost 79 Executives will split 78 STB as earned once per round (6 hours). The prize will be divided according on the vote percentage each Executive earns.

Total E reward per round = 10,972 Unit/block × 20 blocks/min × 60 mins/hr × 6 hrs/round .

A total of 28,834 STB will be given out every year to the 79 Gs.

11 GOVERNANCE

Block Incentive

The top 21 Executives (Gs) that are elected every round (6 hours) will divide around 1,596 STB as mined, also known as Governor Reward. The prize will be distributed evenly among the 21 Gs.

Total reward per round = 221,714 Unit/block x 20 block/min x 60 mins/hr x 6 hrs/round .

A total of 2,330,657 STB will be awarded annually to the 21 Gs. It should be noted that every two years the reward for mining Stabila is halved.

12 STABILA CHAIN SETTINGS

Circulating Supply *The number of STB coins that are publicly available and circulating in the market.*	**20,000,000**
Total Supply *Total supply refers to the number of STB that currently exists and are either in circulation or locked for miners.*	**30,000,000**
Max Supply *The maximum supply refers to the maximum number of STB coins that will be ever created.*	**30,000,000**
Block producing speed *Seconds per 1 block produced.*	**3**
Miners/Governors *Block producing nodes.*	**21**
Consensus *67% of 21 governors to achieve consensus on producing next block.*	**15**
1 STB = () Units *UNIT is the smallest unit of STB*	**1,000,000**

THANK YOU

“What we have is a maturation of the crypto market, and we get investors and traders more comfortable understanding the fundamentals around what they’re buying,”

Daniel Varzari, CEO

“Blockchain is a new technological paradigm of our time. It will fundamentally change the principles of work of the whole financial world.”

Igor Scvortov, CFO

“One day in our near future, everything will be tokenized and connected using the blockchain.”

Anastasia Kovaleva, VP Asia

STABILA

MONETA HOLDINGS LLC

ST VINCENT AND THE GRENADINES

First Floor
First St. Vincent Bank Ltd Building
James Street
Kingstown

BLOCKCHAIN TECHNOLOGY

Building decentralized finance.

info@moneta.holdings

info@stabilascan.org

SOURCES

1. EL Makhtoum, H. and Y. Bentaleb, Comparative Study of Keccak and Blake2 Hash Functions, in Networking, Intelligent Systems and Security. 2022, Springer. p. 343-350.

2. Pote, S., V. Sule, and B. Lande. Arithmetic of Koblitz Curve Secp256k1 Used in Bitcoin Cryptocurrency Based on One Variable Polynomial Division. in 2nd International Conference on Advances in Science & Technology (ICAST). 2019.

3. Sakkari, D.S. and M.M. Ulla, Design and Implementation of Elliptic Curve Digital Signature Using Bit Coin Curves Secp256K1 and Secp384R1 for Base10 and Base16 Using Java, in Innovation in Electrical Power Engineering, Communication, and Computing Technology. 2022, Springer. p. 323-337.

4. Mayer, H., ECDSA security in bitcoin and ethereum: a research survey. CoinFaabrik, June, 2016. ***28****(126): p. 50.*

5. Xu, G., Y. Liu, and P.W. Khan, Improvement of the DPoS consensus mechanism in Blockchain based on vague sets. IEEE Transactions on Industrial Informatics, 2019. ***16****(6): p. 4252-4259.*

6. Bodó, B., D. Gervais, and J.P. Quintais, Blockchain and smart contracts: the missing link in copyright licensing? International Journal of Law and Information Technology, 2018. ***26****(4): p. 311-336.*