EQcoin Bible

Table of contents

1. Terms

1. EQcoin is the original commodity of EQcoin ecosystem. EQcoin is a cryptocurrency，hereinafter referred to as "**EQC**".

2. Type represents the type of lock，hereinafter referred to as "**T**".

3. Operation is defined in Section 2.7.1 below，hereinafter referred to as "**OP**".

2. About EQcoin

2.1 What's EQcoin?

EQcoin is the first Passport oriented decentralized finance ecosystem of the people, by the people, for the people. EQcoin is open source, decentralized, permissionless, distributed and public shared digital ledger. Passport and EQC are the original commodities of EQcoin ecosystem. Passport and EQC are issued and circulated according to the EQcoin consensus mechanism via the EQcoin ecosystem based on the decentralized finance, everyone can participate in the issuance and circulation of Passport and EQC via crowdsourcing(private property is sacrosanct). The evolution of EQcoin is based on crowdsourcing, everyone can improve and perfect EQcoin via EQcoin Improvement Proposal.

2.2 What's Passport?

Passport is the original commodity of EQcoin ecosystem. Passport has a status, an ID, an EQcoin balance, a nonce, a LockMate and a **state root**[1]

[1] The state root used to store the state objects' relevant state root of the relevant smart contracts deployed in the current Passport.

that can send transactions on EQcoin network. The minimum balance value of Passport at the current stage shall not be lower than 51 EQC, and the EQcoin community will decide whether to increase or decrease the minimum balance value of Passport according to the EQcoin Improvement Proposal as needed in the future. Passport ID is a natural number. Passport ID starts from zero and increases one by one according to the order of Passport issuance. Using the status state object, Passport can add or delete Passport relevant state objects created by the EQcoin Improvement Proposal to add or delete its specific functions. Passport can be user controlled and used to deploy multiple smart contracts. Passport owners can provide issue/sell Passport services and smart contract deployment services for everyone and decide how much EQC to charge for issuing/selling Passport and deploying smart contract. Just like Bitcoin Address and Ethereum Account, Passport is anonymous and do not contain information about the owner.

The singularity block is the first block of EQcoin, the No.0 to No.1001 Passports will be issued in this block. Due to "without time at this time" so singularity block without timestamp.

2.3 What's EQC?

EQC is the original commodity of EQcoin ecosystem. EQC is a cryptocurrency. EQC needs to be paid in order to use EQcoin

decentralized financial services.

2.4 What's Lock?

The Passport owner uses Lock to lock the Passport. Lock has a lock type and the lock relevant state objects. New locks can be created through EQcoin Improvement Proposal to extend the functionality of the lock.

Lock consists of two lock types at the current stage:

2.4.1 T0 lock

T0 lock’ s lock type is 0 and use secp256r1(NIST P-256) elliptic curve to lock relevant Passport. T0 lock has a lock type 0, a SHA3-256 public key hash of secp256r1(NIST P-256) elliptic curve and a CRC32C cyclic redundancy checksum.

2.4.2 T1 lock

T1 lock’ s lock type is 1 which is pay to script hash. T1 lock has a lock type 1, a status, a SHA3-256 hash of the relevant redundant lock pairs and a CRC32C cyclic redundancy checksum.

The T1 lock supports the following functions:

1. User is allowed to create a redundant lock pair, which contains N (1<=N<=4) T0 locks from different devices provided by the user. User can select a lock to unlock from the redundant lock pair. Thus, if a single

device is damaged, the locks in the redundant devices are still available for use.

2. Single user is allowed to create N(1<=N<=8) lock pairs, and select the M(1<=M<=N) locks in the N lock pairs to unlock.

3. N(1<=N<=8) users are allowed to provide one lock pair per user and must use the N locks in the N lock pairs to unlock.

2.5 What's LockMate?

LockMate has a status, a lock, a publickey that can lock the Passport and store lock relevant state objects. Because the corresponding public key is stored in LockMate when the lock is unlocked for the first time, it can resist preimage attacks.

2.6 Passport and EQC total supply

The total supply of Passport at current stage is 8,388,607. The total supply of Passport may be increased in the future according to the EQcoin Improvement Proposal, and the EQcoin community will determine the total and maximum supply of Passport as needed.

The total supply of EQC is a constant 210,000,000,000 and the decimal is 8. The first block, the Singularity block, will issue 21,000,000 EQCs, and then will issue 21,000,000 EQCs every year.

2.7 What’s Transaction

Transaction is essentially a signed set of instructions from one Passport. Transaction is used to affect a state change on the EQcoin blockchain, such as transfer of funds, change the lock of Passport or execute a function within a smart contract.

Transaction has a status, a Passport ID, a nonce, one or more TxOut arrays and a signature. Using the status state object, Transaction can add or delete Transaction TxOuts created by the EQcoin Improvement Proposal to add or delete its specific functions.

2.7.1 What’s Operation

Operation is essentially a set of instructions from one Passport. Operation is used to affect a state change on the EQcoin blockchain, such as change Passport’s lock or deploy a smart contract. Each OperationTxOut contains one or more operation.

Operation has an OP ID and one or more OP state objects. New operations can be created through EQcoin Improvement Proposal to extend the functionality of the operation.

Operation consists of one operation type at the current stage:

1. ChangeLockOP

   ChangeLockOP is used to change relevant Passport’s lock. ChangeLockOP has an OP ID of 0 and a lock which is the new lock for

the current Passport.

2. ReservedNonceOP

ReservedNonceOP is used to reserve some nonces for future transactions, so that these reserved nonces can be used to execute some offchain transactions (such as EQC lightning network transactions), and these reserved nonces can be used to execute transactions update the relevant global state on the EQC network when needed.

ReservedNonceOP has an OP ID of 1 and a reserved nonce quantity(Values range from 1 to 256), which is the number of nonces reserved.

When the ReservedNonceOP is executed, the following operations will be performed:

1. The nonce of the current Passport will increase the number of reserved nonces.

2. The reserved nonce flag will be marked in the corresponding Passport's status state object (if necessary), and the value of the total number of reserved nonce state object will be increased according to the total number of reserved nonces, and the corresponding reserved nonces' value will be added to the reserved nonce ZeroOneDynamicMerklePatriciaTrie.

Transaction consists of four TxOut types at the current stage:

1. ZionTxOut

ZionTxOut is used to issue passports. A maximum of 129 ZionTxOuts can be included in the ZionTxOut array.

2. OperationTxOut

OperationTxOut is used to execute operation, for example ChangeLockOP. A maximum of 65 OperationTxOuts can be included in the OperationTxOut array.

3. TransferTxOut

TransferTxOut is used to transfer EQC. A maximum of 257 TransferTxOuts can be included in the TransferTxOut array.

4. SmartContractTxOut

SmartContractTxOut is used to execute smart contract function. A maximum of 5 SmartContractTxOuts can be included in the SmartContractTxOut array.

2.8 Transaction use case

2.8.1 Issue Passport

1. Adam issues passport and transfers 101 EQCs for Eve (Lock: 0bb...bb).

Before Adam sends the transaction:

Adam's Passport
Status: 0 ID: 0

Nonce: 0 Balance: 2100000000000000	
LockMate	Lock: 0aa...aa Publickey: null

Transaction sent by Adam to issue Passport:

Transaction	
Status[2]: 0000000[1][3]	
Passport ID: 0	
Nonce: 0	
ZionTxOut	Status[4]: 0000000[5][0][6]
	Lock: bb...bb[7] Value: 10100000000
Signature: xx...xx	

The size of the transaction is 105 bytes.

After Adam sends the transaction:

Adam's Passport

---

[2] The type of the Status state object is EQCBits.

[3] Indicates whether transaction includes ZionTxOut, 0: excludes, 1: includes.

[4] The type of the Status state object is EQCBits.

[5] This state object includes a series of consecutive bits. When ZionTxOut includes only one sub-ZionTxOut uses it to record the lock type part of the current sub-ZionTxOut' s lock, and when ZionTxOut includes multiple sub-ZionTxOuts uses it to record the number of sub-ZionTxOuts. The current record value is the lock type part 0000000(0) of the sub-ZionTxOut' s lock.

[6] Indicates whether ZionTxOut includes multiple sub-ZionTxOuts, 0: one, 1: multiple.

[7] When ZionTxOut includes only one sub-ZionTxOut uses it to record the hash part of the lock, and when ZionTxOut includes multiple sub-ZionTxOuts uses it to record the full lock. The current record value is the public key hash part bb...bb of sub-ZionTxOut' s T0 lock.

Status: 0 ID: 0 Nonce: 1 Balance: 2099989800090000	
LockMate	Lock: 0aa...aa Publickey: xx...xx

Eve's Passport	
Status: 0 ID: 1 Nonce: 0 Balance: 10100000000	
LockMate	Lock: 0bb...bb Publickey: null

3. Adam issues passports and transfers 101 EQCs for Moses (Lock: 0cc...cc) and Noah (Lock: 0dd...dd) and charge the service fee of 1 EQC per person. Therefore, after deducting the service fee, the transfer amount is 100 EQC.

Before Adam sends the transaction:

Adam's Passport
Status: 0 ID: 0

Nonce: 1 Balance: 2099989800090000	
LockMate	Lock: 0aa...aa Publickey: xx...xx

Transaction sent by Adam to issue Passports:

Transaction	
Status: 00000001	
Passport ID: 0	
Nonce: 1	
ZionTxOut	Status: 0000000[8]1[9]
	Lock: 0cc...cc Value: 10000000000
	Lock: 0dd...dd Value: 10000000000
Signature: xx...xx	

The size of the transaction is 144 bytes.

After Adam sends the transaction:

Adam's Passport
Status: 0 ID: 0

[8] Indicates ZionTxOut includes multiple sub-ZionTxOuts.

[9] Record the current number of sub-ZionTxOuts is 0000000(2).

Nonce: 2 Balance: 2099969800080000	
LockMate	Lock: 0aa...aa Publickey: xx...xx

Moses' Passport	
Status: 0 ID: 2 Nonce: 0 Balance: 10000000000	
LockMate	Lock: 0cc...cc Publickey: null

Noah's Passport	
Status: 0 ID: 3 Nonce: 0 Balance: 10000000000	
LockMate	Lock: 0dd...dd Publickey: null

2.8.2 Transfer

1. Adam transfers 101 EQCs to Moses.

Before Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 2 Balance: 2099969800080000	
LockMate	Lock: 0aa...aa Publickey: xx...xx

Transaction sent by Adam to transfer:

Transaction	
Status: 0000[10]1[11]000	
Passport ID: 0	
Nonce: 2	
TransferTxOut[12]	Passport ID: 2 Value[13]: 10100000000

---

[10] When transaction includes TransferTxOut indicates whether TransferTxOut includes multiple sub-TransferTxOuts, 0: one, 1: multiple, otherwise indicates whether transaction includes SmartContractTxOut, 0: excludes, 1: includes.

[11] Indicates whether transaction includes TransferTxOut, 0: excludes, 1: includes.

[12] EQcoin uses EQCHelix to store the transfer value and relevant Passport ID's bytes' length in TransferTxOut. On the underlying storage, Value is stored first, followed by Passport ID.

[13] The lowest 5 bits of the binary digits of Value are reserved as identifier bits to store the number of bytes occupied by Value and Passport ID respectively, among which the upper 3 bits are used

Signature: xx...xx

The size of the transaction is 72 bytes.

After Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 3 Balance: 2099959700070000	
LockMate	Lock: 0aa...aa Publickey: xx...xx

Moses' Passport	
Status: 0 ID: 2 Nonce: 0 Balance: 20100000000	
LockMate	Lock: 0cc...cc Publickey: null

---

to store the number of bytes occupied by Value and the lower 2 bits are used to store the number of bytes occupied by Passport ID. In the TransferTxOut, Value is stored first and then Passport ID is stored. Therefore, if the value of the transfer amount entered in TransferTxOut is not divisible by 32, some adjustments need to be made to make it divisible by 32 so that the lowest 5 bits of its binary digits are reserved as identifier bits. It is recommended to adjust it in the following ways: 1. Use the result of value-(value%32) as the transfer amount. 2. Use the result of value+(32-(value%32)) as the transfer amount.

2. Adam transfers 101 EQCs to Moses and Noah.

Before Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 3 Balance: 2099959700070000	
LockMate	Lock: 0aa...aa Publickey: xx...xx

Transaction sent by Adam to transfer:

Transaction	
Status: 0001[14]1000	
Passport ID: 0	
Nonce: 3	
TransferTxOut	Array length: 00000000[15]
	Passport ID: 2 Value: 10100000000
	Passport ID: 3 Value: 10100000000
Signature: xx...xx	

[14] Indicates TransferTxOut includes multiple sub-TransferTxOuts.

[15] Record the current number of sub-TransferTxOuts is 00000000(2).

The size of the transaction is 78 bytes.

After Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 4 Balance: 2099939500060000	
LockMate	Lock: 0aa...aa Publickey: xx...xx

Moses' Passport	
Status: 0 ID: 2 Nonce: 0 Balance: 30200000000	
LockMate	Lock: 0cc...cc Publickey: null

Noah's Passport
Status: 0 ID: 3

Nonce: 0 Balance: 20100000000	
LockMate	Lock: 0dd...dd Publickey: null

2.8.3 Change lock

1. Adam changes his Passport’ s lock to 0bb...bb.

Before Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 4 Balance: 2099939500060000	
LockMate	Lock: 0aa...aa Publickey: xx...xx

Transaction sent by Adam to change lock:

Transaction
Status: 000000$1^{16}$0
Passport ID: 0
Nonce: 4

[16] Indicates whether transaction includes OPTxOut, 0: excludes, 1: includes.

OPTxOut	Status[17]: 0000000[18]0[19] Lock: 0bb...bb[20]
Signature: xx...xx	

The size of the transaction is 101 bytes.

After Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 5 Balance: 2099939500050000	
LockMate	Lock: 0bb...bb Publickey: null

2.8.4 Execute smart contract

1. Adam executes the Buy function (ID: 4) of the EQswap smart contract (**ID**[21]: 0x**6a87**[22]**82**[23]) and uses 0.00000051 EQC to buy 201 Bethard tokens

---

[17] The type of the Status state object is EQCBits.

[18] This state object includes a series of consecutive bits. When OPTxOut includes only one sub-OPTxOut uses it to record the OP ID part of the sub-OPTxOut, and when OPTxOut includes multiple sub-OPTxOuts uses it to record the number of OPTxOuts. The current record value is the OP ID part 0000000(0) of the ChangeLockOP.

[19] Indicates whether OPTxOut includes multiple sub-OPTxOuts, 0: one, 1: multiple.

[20] When OPTxOut includes only one sub-OPTxOut uses it to record the OP body part of the OP, and when OPTxOut includes multiple sub-OPTxOuts uses it to record the full OP. The current record value is the lock part 0bb...bb of ChangeLockOP.

[21] The smart contract ID consists of two adjacent state objects. The first state object is PassportID, which is the ID of the bound Passport, and the second state object is SmartContractNonce, which is the smart contract nonce of the bound Passport. The type of the PassportID and

from Bethard.

Before Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 5 Balance: 2099939500050000	
LockMate	Lock: 0bb...bb Publickey: null

Transaction sent by Adam to execute smart contract:

Transaction	
Status: 000[24]1[25]0000	
Passport ID: 0	
Nonce: 5	
SmartContractTxOut	Status: 00100[26]01[27]0[28]

SmartContractNonce is EQCBits. The smart contract ID is presented as a hexadecimal string.

[22] PassportID which value is 1002.

[23] SmartContractNonce which value 2.

[24] When transaction includes SmartContractTxOut indicates whether SmartContractTxOut includes multiple sub-SmartContractTxOuts, 0: one, 1: multiple, otherwise reserved for indicates other states of the transaction.

[25] Indicates whether transaction includes SmartContractTxOut, 0: excludes, 1: includes.

[26] When the current smart contract function is called once uses it to record the function ID, and when the current smart contract function is called multiple times uses it to record the number of calls. The current record value is the current smart contract function ID 00100(4) which is Buy function.

[27] Record the bytes of the Passport ID in the smart contract ID. The current record value is the size of the byte stream corresponding to Passport ID 1002, which is 01(2) bytes.

	Smart contract ID: 0x6a8782 Function ID: 4[29] Value[30]: 51
Signature: xx...xx	

The size of the transaction is 72 bytes.

After Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 6 Balance: 2099939500039949	
Bethard token: 20100000000	
LockMate	Lock: 0bb...bb Publickey: xx...xx

2. Adam executes the Buy function (ID: 4) of the EQswap smart contract (ID: 0x6a8782) and uses 0.00000051 EQC to buy 201 Bethard tokens from Bethard, then executes the betting function (ID: 3) of the Bethard horse

---

[28] Indicates whether current smart contract function includes multiple calls, 0: one, 1: multiple.

[29] The value is saved in the Status state object identified by note 21.

[30] The lowest 3 bits of the binary digits of Value are reserved as identifier bits to store the number of bytes occupied by Value. Therefore, if the value of the transfer amount entered in SmartContractTxOut is not divisible by 8, some adjustments need to be made to make it divisible by 8 so that the lowest 3 bits of its binary digits are reserved as identifier bits. It is recommended to adjust it in the following ways: 1. Use the result of value-(value%8) as the transfer amount. 2. Use the result of value+(8-(value%8)) as the transfer amount.

racing smart contract (ID: 0x6a8783) and uses 201 EQCs to bet that No. 9 of the Royal Ascot's Her Majesty's Plate will win.

Before Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 6 Balance: 2099939500039949	
Bethard token: 20100000000	
LockMate	Lock: 0bb...bb Publickey: xx...xx

Transaction sent by Adam to execute smart contract:

Transaction	
Status: 001[31]10000	
Passport ID: 0	
Nonce: 6	
	Status: 000000[32]00[33]
SmartContractTxOut	Status: 00100010 Smart contract ID: 0x6a8782 Function ID: 4

[31] Indicates SmartContractTxOut includes multiple sub-SmartContractTxOuts.

[32] Reserved status flag bits.

[33] Record the number of sub-SmartContractTxOuts. The current record value is 00(2).

	Value: 51
	Status: 00011010 Smart contract ID: 0x6a8783 Function ID: 3 Value: 20100000000 Winner: 9
Signature: xx...xx	

The size of the transaction is 83 bytes.

After Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 7 Balance: 2099919400029898	
Bethard token: 40200000000	
LockMate	Lock: 0bb...bb Publickey: xx...xx

3. Adam executes the Transfer function (ID: 1) of the Bethard token contract (ID: 0x6a8781) and transfer 100 Bethard tokens to Eve, Moses and Noah.

Before Adam sends the transaction:

Adam's Passport

Status: 0 ID: 0 Nonce: 7 Balance: 2099919400029898	
Bethard token：40200000000	
LockMate	Lock: 0bb...bb Publickey: xx...xx

Transaction sent by Adam to execute smart contract：

Transaction	
Status: 00100000	
Passport ID: 0	
Nonce: 5	
SmartContractTxOut	Status: 00001[34]011[35] Smart contract ID: 0x6a8781 Function ID: 1 Passport ID: 1 Value: 100 Passport ID: 2 Value: 100 Passport ID: 3

[34] The current record value is the number of current smart contract function calls: 00001(3).

[35] Indicates current smart contract function includes multiple calls.

	Value: 100
Signature: xx...xx	

The size of the transaction is 77 bytes.

After Adam sends the transaction:

Adam's Passport	
Status: 0 ID: 0 Nonce: 8 Balance: 2099919400019898	
Bethard token: 10200000000	
LockMate	Lock: 0bb...bb Publickey: xx...xx

Eve's Passport	
Status: 0 ID: 1 Nonce: 0 Balance: 10100000000	
Bethard token: 10000000000	
LockMate	Lock: 0bb...bb

	Publickey: null

Moses' Passport	
Status: 0 ID: 2 Nonce: 0 Balance: 30200000000	
Bethard token : 10000000000	
LockMate	Lock: 0cc...cc Publickey: null

Noah's Passport	
Status: 0 ID: 3 Nonce: 0 Balance: 20100000000	
Bethard token : 10000000000	
LockMate	Lock: 0dd...dd Publickey: null

2.8.5 Complex transaction

Adam issues passport and transfers 51 EQC for Amon （Lock: 0ee...ee, transfers 101 EQCs to Moses, executes the Buy function (ID: 4) of the EQswap smart contract (ID: 0x6a8782) and uses 0.00000051 EQC to buy 201 Bethard tokens from Bethard and changes his Passport’ s lock to 0ff...ff and set the power price to 11 to execute transactions at a faster accounting rate.

Before Adam sends the transaction：

Adam's Passport	
Status: 0 ID: 0 Nonce: 8 Balance: 2099919400019898	
Bethard token：10200000000	
LockMate	Lock: 0bb...bb Publickey: xx...xx

Complex Transaction sent by Adam：

Transaction
Status: 001011[36]11
Passport ID: 0

[36] Indicates whether transaction specifies a custom PowerPrice, 0: default, 1: custom.

Nonce: 8	
ZionTxOut	Status: 00000000 Lock: ee...ee Value: 5100000000
OPTxOut	Status: 00000000 Lock: 0ff...ff
PowerPrice	Value: 11
TransferTxOut	Passport ID: 2 Value: 10100000000
SmartContractTxOut	Status: 00100010
	Smart contract ID: 0x6a8782 Function ID：4 Value: 51
Signature: xx...xx	

The size of the transaction is 151 bytes.

After Adam sends the transaction：

Adam's Passport
Status: 0 ID: 0 Nonce: 9 Balance: 2099904200008847
Bethard token：30300000000

LockMate	Lock: 0ff...ff Publickey: null

Moses' Passport	
Status: 0 ID: 2 Nonce: 0 Balance: 40300000000	
Bethard token: 10000000000	
LockMate	Lock: 0cc...cc Publickey: null

Amon's Passport	
Status: 0 ID: 4 Nonce: 0 Balance: 5100000000	
LockMate	Lock: 0ee...ee Publickey: null

2.9 About MerklePatriciaTrie

2.9.1 What's ZeroOneMerklePatriciaTrie and ZeroOneDynamicMerklePatriciaTrie?

ZeroOneMerklePatriciaTrie is used to store the Global State of the IDKey storage object(for example Passport、Transaction 、active Smart Contract relevant state objects) in each block of EQcoin. The IDKey state object has a unique ID, which is a natural number encoded consecutively from zero. In the ZeroOneMerklePatriciaTrie, it is bit by bit addressed from high bit to low bit according to the binary value of the ID of the relevant IDKey state object. ZeroOneMerklePatriciaTrie includes two types of keys, ZeroKey(0) and OneKey(1)， they are consist of only one bit(0 or 1).

Note：Due to the ZeroKey and OneKey contain only one character, there is no need to store it, and it can be obtained directly according to the corresponding status bit of its parent node.

ZeroOneDynamicMerklePatriciaTrie is used to store the Global State of the IDKey state objects(for example active and inactive Smart Contract relevant state objects) in each block of EQcoin. In the ZeroOneDynamicMerklePatriciaTrie, it is bit by bit addressed from high bit to low bit according to the binary value of the Hash of the relevant state object. ZeroOneDynamicMerklePatriciaTrie includes two types of

keys, ZeroDynamicKey(0xxx) and OneDynamicKey(1xxx) , they are consecutive binary sequences consisting of one or more bits starting with 0 and 1.

Note：When the ZeroDynamicKey and OneDynamicKey contain only one character, there is no need to store it, and it can be obtained directly according to the corresponding status bit of its parent node. When the ZeroDynamicKey and OneDynamicKey contain multiple characters, there is no need to store its first character because it can be obtained directly according to the corresponding status bit of its parent node.

2.9.1.1 What’s BinaryNode

BinaryNode is the key node that constitutes the ZeroOneMerklePatriciaTrie or ZeroOneDynamicMerklePatriciaTrie dictionary tree. BinaryNode has a status, a key, a ZeroNode, a OneNode and a value. ZeroOneMerklePatriciaTrie includes only two BinaryNodes, ZeroNode and OneNode. BinaryNode's underlying storage implementation includes a HashKey(Hash of BinaryNode's binary raw data, used to support state object verification based on light client protocol) and a StorageKey(UpdateNonce(A natural number starting from 0 and increments by 1 with each modification of the BinaryNode) of BinaryNode, used to access state objects from StateDB).

2.9.1.2 What’ s BinaryNode Status

BinaryNode Status is used to identify the composition of the state objects included in the BinaryNode. The type of the BinaryNode Status state object is EQCBits.

The default order of state objects that BinaryNode includes is: ZeroNode, OneNode, and Value.

BinaryNode Status consists of two status types at the current stage(in the underlying storage, they are compositely stored together):

1. HashStatus, the default universal identifier bit of the BinaryNode which participate in the calculation of the BinaryNode Hash.

00000$0^{37}0^{38}0^{39}$

2. StorageStatus, includes HashStatus identifier bit and storage relvant identifier bit of the BinaryNode which does not participate in the calculation of the BinaryNode Hash but it is used to get BinaryNode from StateDB.

2.1 When BinaryNode includes two state objects(ZeroNode&Value or OneNode&Value).

$000^{40}0^{41}000^{42}$

Note: The state object has the smallest StorageKey hereinafter referred to as “A”(when there are multiple equal value minimums, the one with the lowest default order is taken), another state object hereinafter referred to as “B”. If A’ s StorageKey equals B’ s StorageKey, the

---

[37] Indicates whether node includes OneNode, 0: excludes, 1: includes.

[38] Indicates whether node includes ZeroNode, 0: excludes, 1: includes.

[39] Indicates whether node includes Value, 0: excludes, 1: includes.

[40] Identifies whether the two state objects’ StorageKey are equal, 0: no, 1: yes.

[41] Identifies which node state object’ StorageKey is the smallest in the default order, 0: left, 1: right.

[42] These 3 identifier bits are the same as in HashStatus.

underlying data is A's StorageKey . If A’ s StorageKey is not equal to B’ s StorageKey, the underlying data is A's StorageKey and (B's StorageKey - A's StorageKey)(this saves more storage space than directly stores the two state objects’ StorageKey). For example, if B's StorageKey is 100,001 and the A's StorageKey is 100000, the underlying stored data is 100,000 and 1(this saves a lot of storage space than direct storage 100,000 and 100,001). When need to restore the B's StorageKey, can obtain its value through 100000+1.

2.2 When BinaryNode includes three state objects(ZeroNode, OneNode and Value).

0[43]0[44]0[45]00[46]000[47]

Note: The state object has the smallest StorageKey hereinafter referred to as “A”(when there are multiple equal minimum values, the one with the lowest default order is taken), the state object after A in the default order hereinafter referred to as “B”(If A is Value, the order is calculated from the beginning, so B is ZeroNode) , the state object after B in the default order hereinafter referred to as “C”(If B is Value, the order is calculated from the beginning, so C is ZeroNode) . The one with the smaller StorageKey in B and C hereinafter referred to as “D”(when the StorageKey of B and C are equal, the one with the lowest default order is taken)and the The one with the larger StorageKey in B and C hereinafter referred to as “E” (when the StorageKey of B and C are equal, the one with the highest default order is taken).

---

[43] Identifies whether E’ s StorageKey is equal to D’ s StorageKey, 0: no, 1: yes.

[44] Identifies whether D’ s StorageKey is equal to A’ s StorageKey, 0: no, 1: yes.

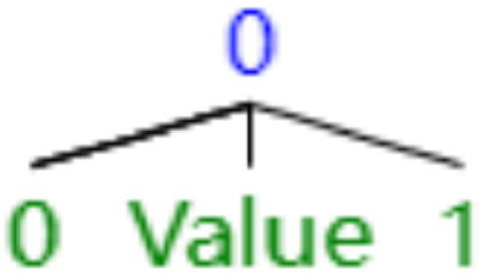
[45] Indicates B’ s and C’ s StorageKey who is bigger, 0: B<=C, 1: B>C.

[46] Indicates which state object has the smallest UpdateNonce, 0: ZeroNode, 1: OneNode, 2: Value.

[47] These 3 identifier bits are the same as in HashStatus.

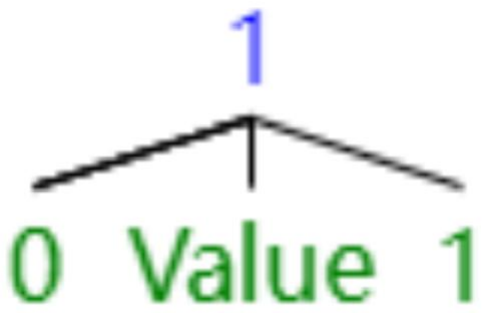
2.9.1.3 What’ s ZeroNode

As shown in the figure below, the key of ZeroNode is 0.



2.9.1.4 What’ s OneNode

As shown in the figure below, the key of OneNode is 1.



2.9.1.5 What’ s RootNode

RootNode is the root of ZeroOneMerklePatriciaTrie which has not Key and Value but has ZeroNode and OneNode. RootNode’ s StorageKey is equal to its HashKey.

2.9.2 HexMerklePatriciaTrie

HexMerkleDynamicPatriciaTrie is used to store the Global State of the HashKey state object(for example Smart Contract relevant state objects) in each block of EQcoin. ~~In the HexMerklePatriciaTrie, it is bit by bit addressed from high bit to low bit according to the binary value of the Hash of the relevant state object~~. HexMerklePatriciaTrie includes 16 keys, DynamicKey0(0xxx), DynamicKey1(1xxx) , DynamicKey2(2xxx), DynamicKey3(3xxx), DynamicKey4(4xxx), DynamicKey5(5xxx), DynamicKey6(6xxx), DynamicKey7(7xxx), DynamicKey8(8xxx), DynamicKey9(9xxx), DynamicKeyA(Axxx), DynamicKeyB(Bxxx), DynamicKeyC(Cxxx), DynamicKeyD(Dxxx), DynamicKeyE(Exxx), DynamicKeyF(Fxxx), they are continuous hexadecimal string keywords starting from 0 to F respectively.

2.9.2.1 What’s BranchNode

BranchNode is the key node that constitutes the HexMerkleDynamicPatriciaTrie dictionary tree. BranchNode has a status, a key, a BranchNode0, a BranchNode1, a BranchNode2, a BranchNode3, a BranchNode4, a BranchNode5, a BranchNode6, a BranchNode7, a BranchNode8, a BranchNode9, a BranchNodeA, a BranchNodeB, a BranchNodeC, a BranchNodeD, a BranchNodeE, a BranchNodeF, and a Leaf. HexMerkleDynamicPatriciaTrie includes 16 BranchNodes,

BranchNode0 , BranchNode1 , BranchNode2 , BranchNode3 , BranchNode4 , BranchNode5 , BranchNode6 , BranchNode7 , BranchNode8 , BranchNode9 , BranchNodeA , BranchNodeB , BranchNodeC , BranchNodeD , BranchNodeE and BranchNodeF. BranchNode's underlying storage implementation includes a HashKey(Hash of BranchNode's binary raw data, used to support state object verification based on light client protocol) and a StorageKey(UpdateNonce(A natural number starting from 0 and increments by 1 with each modification of the BranchNode) of BranchNode, used to access state objects from StateDB).

2.9.1.2 What’s BranchNode Status

BranchNode Status is used to identify the composition of the state objects included in the BranchNode. The type of the BranchNode Status state object is EQCBits.

The default order of state objects that BranchNode includes is:
BranchNode0，BranchNode1，BranchNode2，BranchNode3，
BranchNode4，BranchNode5，BranchNode6，BranchNode7，
BranchNode8，BranchNode9，BranchNodeA，BranchNodeB，
BranchNodeC，BranchNodeD，BranchNodeE, BranchNodeF, and Value.

BranchNode Status consists of two status types at the current stage(in the underlying storage, they are compositely stored together):

1. HashStatus, the default universal identifier bit of the BranchNode which participate in the calculation of the BranchNode Hash.

0[48]**0**[49]**0**[50]**0**[51]**0**[52]**0**[53]**0**[54]**0**[55]**0**[56]**0**[57]**0**[58]**0**[59]**0**[60]**0**[61]**0**[62]**0**[63]**0**[64]**0**[65]

2. StorageStatus, includes HashStatus identifier bit and storage relvant identifier bit of the BranchNode which does not participate in the calculation of the BranchNode Hash but it is used to get BranchNode from StateDB.

0[66]**0**[67]**0xxx0**[68]**0000xxx0000**[69]0000000000000000

---

[48] Indicates whether BranchNode includes BranchNodeF, 0: excludes, 1: includes.

[49] Indicates whether BranchNode includes BranchNodeE, 0: excludes, 1: includes.

[50] Indicates whether BranchNode includes BranchNodeD, 0: excludes, 1: includes.

[51] Indicates whether BranchNode includes BranchNodeC, 0: excludes, 1: includes.

[52] Indicates whether BranchNode includes BranchNodeB, 0: excludes, 1: includes.

[53] Indicates whether BranchNode includes BranchNodeA, 0: excludes, 1: includes.

[54] Indicates whether BranchNode includes BranchNode9, 0: excludes, 1: includes.

[55] Indicates whether BranchNode includes BranchNode8, 0: excludes, 1: includes.

[56] Indicates whether BranchNode includes BranchNode7, 0: excludes, 1: includes.

[57] Indicates whether BranchNode includes BranchNode6, 0: excludes, 1: includes.

[58] Indicates whether BranchNode includes BranchNode5, 0: excludes, 1: includes.

[59] Indicates whether BranchNode includes BranchNode4, 0: excludes, 1: includes.

[60] Indicates whether BranchNode includes BranchNode3, 0: excludes, 1: includes.

[61] Indicates whether BranchNode includes BranchNode2, 0: excludes, 1: includes.

[62] Indicates whether BranchNode includes BranchNode1, 0: excludes, 1: includes.

[63] Indicates whether BranchNode includes BranchNode0, 0: excludes, 1: includes.

[64] Indicates whether BranchNode’ s key is one character or multiple characters, 0: one, 1: multiple. When the key contains only one character, there is no need to store it, and it can be obtained directly according to the corresponding status bit of its parent HashNode. When the key contains multiple characters, there is no need to store its first character because it can be obtained directly according to the corresponding status bit of its parent HashNode.

[65] Indicates whether BranchNode is a branch node or a leaf node, 0: branch, 1: leaf.

[66] If Value exists indicates the absolute value of the difference between Value’ s StorageKey and the StorageKey of the largest or smallest BranchNode which is smaller, 0: the smallest, 1: the largest.

[67] Identifies whether the value's StorageKey is larger or smaller, 0: smaller, 1: larger.

[68] The 4-bit identifier identifies the sequence number of each BranchNode included in the current node sorted from small to large(when the StorageKeys of two adjacent BranchNodes are equal, the one with the lowest default order is taken).

[69] The one-bit flag identifies whether each BranchNode(from the second BranchNode sorted in ascending order) is equal to the adjacent BranchNode that is smaller than it.

Note： If Value exists, the smaller absolute value of the difference between its StorageKey and the StorageKey of the largest or smallest BranchNode will be stored.

2.9.2.3 What’s LeafNode

LeafNode is the leaf node that constitutes the HexMerkleDynamicPatriciaTrie dictionary tree. LeafNode is used to store state objects. LeafNode has a status, a **StateObjectMate or StateObjectMateArray**[70] and its relevant governance state objects. LeafNode related governance state objects can be extended as needed through its status state object. A **HashKey collisionless identifier**[71] bit is included in the current status to identify whether the current LeafNode includes multiple state objects with the same HashKey.

2.9.2.3.1 What’s StateObjectMate

StateObjectMate is used to store state object and its relevant state objects. StateObjectMate has a status, a specific state object and its relevant state objects. StateObjectMate related governance state objects can be extended as needed through its status state object.

---

[70] When the current LeafNode contains only one state object, only one StateObjectMate object is included. When the current LeafNode includes more than two state objects, the current LeafNode includes a StateObjectMateArray (its array subscript 0 represents 2 array elements, array subscript 1 represents 3 array elements, and so on).

[71] HashKey collisionless identifier identifies whether the current LeafNode includes state objects that have collisions, 0: collisionless, 1: collision.

2.9.2.3.2 What’s StateObjectMateArray

StateObjectMateArray is used to simultaneously store multiple StateObjectMates, which contain state objects with the same HashKey. These state objects can be identified and distinguished by their UUID(Universally Unique Identifier)s, which are generated by specific algorithms based on the type, raw data, and associated unique identifiers of specific state objects.

2.9.2.3.3 The HashKey collisionless design of HexMerklePatriciaTrie

Before accessing a specific state object in the HexMerklePatriciaTrie, the global unique access lock bound to its HashKey must be obtained first, and the related state object can be read, written and deleted only after the access right of the access lock is obtained. After the access operation of the relevant state object is completed, its access lock needs to be released.

Read operation:

When performing a read operation, if the current HashKey does not exist, null is returned directly.

When performing a read operation, if the current LeafNode does not have a HashKey collision, it will directly return it including StateObjectMate, and then obtain the corresponding state object from

the StateObjectMate according to the UUID provided by the current read operation.

When performing a read operation, if the current LeafNode has a HashKey collision, the StateObjectMateArray included in it will be returned, and then obtains the corresponding state object from the StateObjectMateArray according to the UUID provided by the current read operation.

Write operation:

When performing a write operation, if the current HashKey does not exist, the current state object is directly stored in the corresponding LeafNode.

When performing a write operation, if the current HashKey exists, and if the current LeafNode does not have a HashKey collision, then compare whether the UUID of the state object contained in the StateObjectMate currently contained in it is consistent with the UUID of the state object to be stored? If the UUIDs are consistent, the corresponding storage is directly overwritten. Otherwise, if the UUIDs are inconsistent, this is a HashKey collision. In this case, the HashKey collisionless identifier of the current LeafNode will be marked as 1 and the StateObjectMateArray will be used to simultaneously store the two state objects.

When performing a write operation, if the current HashKey exists, and if

the current LeafNode has a HashKey collision, then compare the UUID of the state object stored in the current StateObjectMateArray one by one with the UUID of the state object to be stored. If the UUID of a state object stored in the current StateObjectMateArray is consistent with the UUID of the state object to be stored, the corresponding state object is directly overwritten and stored. If the UUIDs of all the state objects stored in the current StateObjectMateArray are inconsistent with the UUID of the state object to be stored, add a new StateObjectMate array element containing the state object currently to be stored in the StateObjectMateArray to store it.

Delete operation：

When performing a delete operation, if the current HashKey does not exist, do nothing.

When performing a delete operation, if the current HashKey exists, and if the current LeafNode does not have a HashKey collision, then compare whether the UUID of the state object contained in the StateObjectMate contained in it is consistent with the UUID provided by the current delete operation. If they are consistent, delete the current LeafNode, otherwise do nothing.

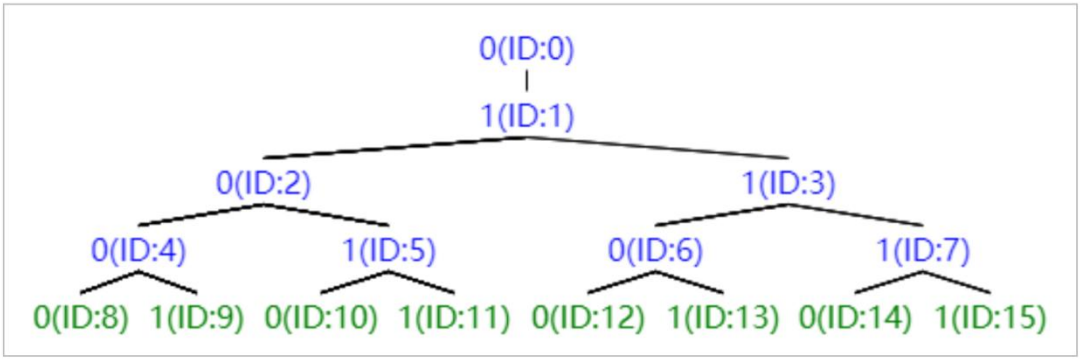
When performing a delete operation, if the current HashKey exists, and if the current LeafNode has a HashKey collision, then compare the UUID of

the state object stored in the current StateObjectMateArray one by one with the UUID of the state object to be deleted. If the UUID of a state object stored in the current StateObjectMateArray is consistent with the UUID of the state object to be deleted, the corresponding StateObjectMate is directly deleted(If the current StateObjectMateArray contains only one StateObjectMate after the delete operation, then mark the HashKey collisionless identifier of the current LeafNode as 0, and delete the current StateObjectMateArray then store the StateObjectMate it contains directly in the LeafNode), otherwise do nothing.

注：这里操作的对象应该统一是 StateObjectMate 而不是 StateObject，从而支持对 StateObject 的数据治理操作。

2.9.3 Passport/Transaction Global State chart

The location of the Passport/Transaction ID from 0 to 15 is depicted in the following figure.

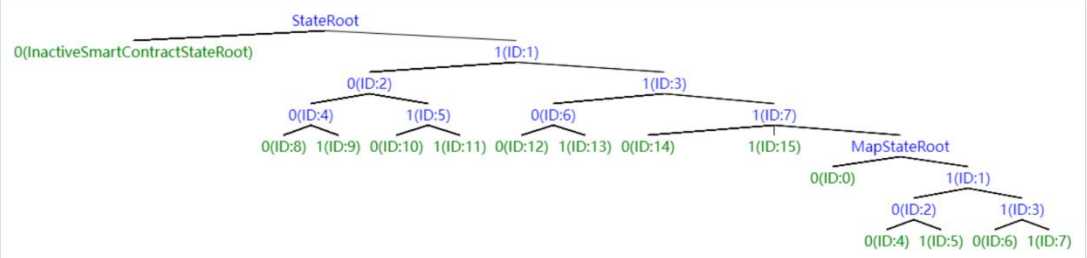


Note: The value of the node in the above figure is the value of the

relevant Passport/Transaction that has been omitted in this figure.

2.9.3 Smart Contract state object Global State chart

The location of the Smart Contract state object ID from 0 to 15 is depicted in the following figure.



2.10 EQcoin roadmap

Stage 1 - Inception

EQcoin mainnet online.

Stage 2 - Era

EQcoin supports smart contracts compatible with the Ethereum EVM and Lightning Network (LN).

Stage 3 - New dawn

EQcoin supports cross chain through the Interchain Communication Protocol.

Stage 4 - Nirvana

EQcoin moves from POW to POS.

2.11 EQcoin milestone

2018-01-01 EQcoin officially launched.

2018-04-10 GitHub Initial commit.

2019 Establish an EQcoin test network to achieve multiple miner nodes based on POW consensus mechanisms to mine, send transactions(issue Passport, transfer EQC and change lock), verify blocks, and compete the longest blockchain.

2020-02-10 Register the domain name of www.eqcoin.org.

2021-02-12 Create EQcoin organization in GitHub.

2021-04 Create EQcoin twitter.

At present, the overall design of the Inception phase of EQcoin has been completed. We have written thousands of pages of research and development technology documents and the code is about 80% complete and including a total of 33000+ lines. Our developer community currently has 13 members.

2.12 EQcoin GitHub

https://github.com/EQcoin

2.13 Our developer community

Currently we have 13 members. You can visit

https://github.com/orgs/EQcoin/people to learn more about our developer community.

2.14 Copyright

The copyright of all works released by Wandering Earth Corporation or jointly released by Wandering Earth Corporation with cooperative partners are owned by Wandering Earth Corporation and entitled to protection available from copyright law by country as well as international conventions.

Attribution — You must give appropriate credit, provide a link to the license.

Non Commercial — You may not use the material for commercial purposes.

No Derivatives — If you remix, transform, or build upon the material, you may not distribute the modified material.

Wandering Earth Corporation reserves any and all current and future rights, titles and interests in any and all intellectual property rights of Wandering Earth Corporation including but not limited to discoveries, ideas, marks, concepts, methods, formulas, processes, codes, software, inventions, compositions, techniques, information and data, whether or not protectable in trademark, copyrightable or patentable, and any trademarks, copyrights or patents based thereon.