

# EQcoin Bible

# Table of contents

1. Terms .....	4
2. About EQcoin .....	4
2.1 What's EQcoin? .....	4
2.2 What's Passport? .....	5
2.3 What' s EQC? .....	6
2.4 What's Lock? .....	6
2.4.1 T0 lock .....	6
2.4.2 T1 lock .....	6
2.5 What's LockMate? .....	7
2.6 Passport and EQC total supply .....	7
2.7 What' s Transaction .....	8
2.7.1 What' s Operation .....	8
2.8 Transaction use case .....	10
2.8.1 Issue Passport .....	10
2.8.2 Transfer .....	14
2.8.3 Change lock .....	18
2.8.4 Execute smart contract .....	19
2.8.5 Complex transaction .....	23
2.9 EQcoin roadmap .....	28
2.10 EQcoin milestone .....	28
2.11 EQcoin GitHub .....	29

2.12 Our developer community .....	29
2.13 Copyright.....	30

# 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 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  $N$  ( $1 \leq N \leq 4$ ) 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  $N$  ( $1 \leq N \leq 8$ ) lock pairs, and select the  $M$  ( $1 \leq M \leq N$ ) locks in the  $N$  lock pairs to unlock.
3.  $N$  ( $1 \leq N \leq 8$ ) 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.

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: 21000000000000000	
LockMate	Lock: 0aa...aa Publickey: null

Transaction sent by Adam to issue Passport:

Transaction	
<u>Status</u> <sup>1</sup> : 0000000 <u>1</u> <sup>2</sup>	
Passport ID: 0	
Nonce: 0	
ZionTxOut	<u>Status</u> <sup>3</sup> : <u>0000000</u> <sup>4</sup> <u>0</u> <sup>5</sup>

<sup>1</sup> The type of the Status state object is [EQCBits](#).

<sup>2</sup> Indicates whether transaction includes ZionTxOut, 0: excludes, 1: includes.

<sup>3</sup> The type of the Status state object is [EQCBits](#).

<sup>4</sup> 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.

<sup>5</sup> Indicates whether ZionTxOut includes multiple sub-ZionTxOuts, 0: one, 1: multiple.

	Lock: <u>bb...bb</u> <sup>6</sup> Value: 10100000000
Signature: xx...xx	

**The size of the transaction is 105 bytes.**

After Adam sends the transaction:

Adam's Passport	
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

---

<sup>6</sup> 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.

2. 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: <u>0000000</u> <sup>7</sup> <u>1</u> <sup>8</sup>
	Lock: 0cc...cc
	Value: 10000000000

---

<sup>7</sup> Indicates ZionTxOut includes multiple sub-ZionTxOuts.

<sup>8</sup> Record the current number of sub-ZionTxOuts is 0000000(2).

	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  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: Odd...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: 000 <u>0</u> <sup>9</sup> <u>1</u> <sup>10</sup> 000

---

<sup>9</sup> Indicates whether TransferTxOut includes multiple sub-TransferTxOuts, 0: one, 1: multiple.

<sup>10</sup> Indicates whether transaction includes TransferTxOut, 0: excludes, 1: includes.

Passport ID: 0	
Nonce: 2	
TransferTxOut <sup>11</sup>	Passport ID: 2 Value: 10100000000
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

---

<sup>11</sup> 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.

LockMate	Lock: 0cc...cc Publickey: null
----------	-----------------------------------

3. 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: 000 <u>1</u> <sup>12</sup> 1000	
Passport ID: 0	
Nonce: 3	
TransferTxOut	Array length: <u>00000000</u> <sup>13</sup>
	Passport ID: 2 Value: 10100000000
	Passport ID: 3

<sup>12</sup> Indicates TransferTxOut includes multiple sub-TransferTxOuts.

<sup>13</sup> Record the current number of sub-TransferTxOuts is 00000000(2).



	Value: 10100000000
Signature: xx...xx	

**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: Odd...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 <sup>1</sup> <sub>14</sub> 0
Passport ID: 0

---

<sup>14</sup> Indicates whether transaction includes OPTxOut, 0: excludes, 1: includes.

Nonce: 4	
OPTxOut	<u>Status</u> <sup>15</sup> : <u>0000000</u> <sup>16</sup> <u>0</u> <sup>17</sup> Lock: <u>0bb...bb</u> <sup>18</sup>
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: 1002.2) and uses 0.00000051 EQC to buy 201 Bethard tokens from

---

<sup>15</sup> The type of the Status state object is [EQCBits](#).

<sup>16</sup> 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.

<sup>17</sup> Indicates whether OPTxOut includes multiple sub-OPTxOuts, 0: one, 1: multiple.

<sup>18</sup> 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.

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: 0 <sup>19</sup> 1 <sup>20</sup> 00000	
Passport ID: 0	
Nonce: 5	
SmartContractTxOut	Status: 00100 <sup>21</sup> 01 <sup>22</sup> 0 <sup>23</sup> Smart contract ID: 1002.2 Function ID: save in Status above

---

<sup>19</sup> Indicates whether SmartContractTxOut includes multiple sub-SmartContractTxOuts, 0: one, 1: multiple.

<sup>20</sup> Indicates whether transaction includes SmartContractTxOut, 0: excludes, 1: includes.

<sup>21</sup> 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 . The current record value is the current smart contract function ID 00100(4) which is Buy function.

<sup>22</sup> 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.

<sup>23</sup> Indicates whether current smart contract function includes multiple calls, 0: one, 1: multiple.

	Value: 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: 1002.2) and uses 0.00000051 EQC to buy 201 Bethard tokens from Bethard, then executes the betting function (ID: 3) of the Bethard horse racing smart contract (ID: 1002.3) 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: 0 <u>1</u> <sup>24</sup> 100000	
Passport ID: 0	
Nonce: 6	
	Status: <u>000000</u> <sup>25</sup> <u>00</u> <sup>26</sup>
SmartContractTxOut	Status: 00100010 Smart contract ID: 1002.2 Function ID: save in Status above Value: 51
	Status: 00011010 Smart contract ID: 1002.3 Function ID: save in Status above

<sup>24</sup> Indicates SmartContractTxOut includes multiple sub-SmartContractTxOuts.

<sup>25</sup> Reserved status flag bits.

<sup>26</sup> Record the number of sub-SmartContractTxOuts. The current record value is 00(2).

	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: 1002.1) 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: <u>00001</u> <sup>27</sup> 01 <u>1</u> <sup>28</sup> Smart contract ID: 1002.2 Function ID: 1 Passport ID: 1 Value: 100 Passport ID: 2 Value: 100 Passport ID: 3 Value: 100
Signature: xx...xx	

**The size of the transaction is 83 bytes.**

<sup>27</sup> 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 . The current record value is the current smart contract function ID 00100(4) which is Buy function.

<sup>28</sup> Indicates whether current smart contract function includes multiple calls, 0: one, 1: multiple.



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

## 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: 1002.2) 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: 7	
Balance: 2099919400029898	
Bethard token: 40200000000	
LockMate	Lock: 0bb...bb Publickey: xx...xx

Complex Transaction sent by Adam:

Transaction	
Status: 00101 <sup>29</sup> 1	
Passport ID: 0	
Nonce: 7	
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: 00000000
	Smart contract ID: 1002.1 Function ID: 4

---

<sup>29</sup> Indicates whether transaction specifies a custom PowerPrice, 0: default, 1: custom.

	Value: 51
Signature: xx...xx	

**The size of the transaction is 150 bytes.**

After Adam sends the transaction:

Adam's Passport	
Status: 0	
ID: 0	
Nonce: 8	
Balance: 2099904200018847	
Bethard token: 60300000000	
LockMate	Lock: 0ff...ff Publickey: null

Moses' Passport	
Status: 0	
ID: 2	
Nonce: 0	
Balance: 40300000000	
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 EQcoin roadmap

Stage 1 - Inception

EQcoin mainnet online.

Stage 2 - Era

EQcoin supports smart contracts compatible with the Ethereum EVM.

Stage 3 - New dawn

EQcoin supports cross chain through the Interchain Communication Protocol.

Stage 4 - Nirvana

EQcoin moves from POW to POS.

## 2.10 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](http://www.eqcoin.org).

2021-02-12 Create [EQcoin organization](#) in GitHub.

2021-04 Create [EQcoin twitter](#).

2021-04 Create [EQcoin facebook](#).

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.

## **2.11 EQcoin GitHub**

<https://github.com/EQcoin>

## **2.12 Our developer community**

Currently we have 13 members. You can visit

<https://github.com/orgs/EQcoin/people> to learn more about our

developer community.

## **2.13 Copyright**

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.

For any use of above stated content of copyright beyond the scope of

fair use or without prior written permission, Wandering Earth Corporation reserves all rights to take any legal action and pursue any right or remedy available under applicable law.