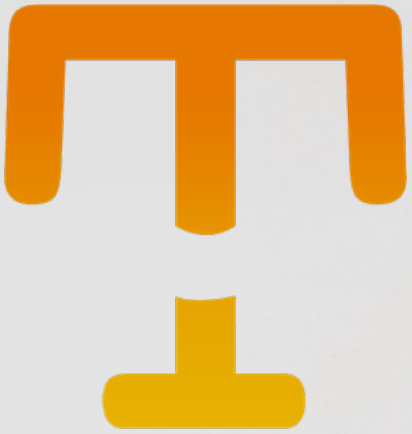

THEMIS

Public Chain for Digital Asset Escrow

Decentralized “PayPal”

Whitepaper

2018/03 v3

https://themis.network

1.Overview

Blockchain-based digital currencies are of radical importance in today's trading activities. As a result, a number of digital currency exchanges were founded and their usage is exploding. At the same time with the rise of a tokenized economy, more and more countries such as Japan, Germany, and Australia, are accepting cryptocurrency payments. There is huge potential that the market will continue to expand globally and accept the commercialization of digital currency.

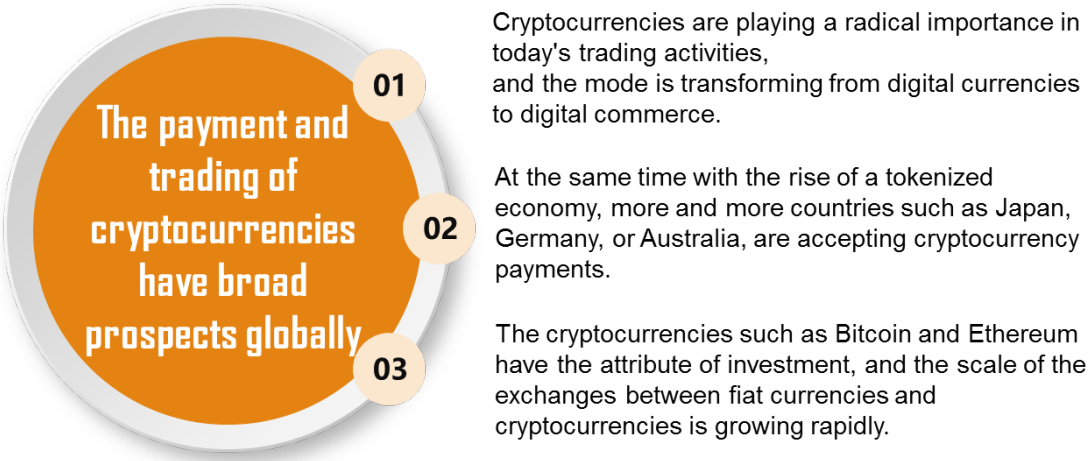

Figure1.1 Trend of cryptocurrencies

Currently, most digital currency exchanges and peer-to-peer transaction providers focus on ensuring the security of transactions but pay little attention to fairness. For example, HTLC (Hashed Time-lock Contract), a widely-used atomic exchange technology, is vulnerable to denial of service (DoS) attacks. Attackers may launch DoS attacks in the period of time-lock to make the counterparty unable to obtain a refund in a specific time.

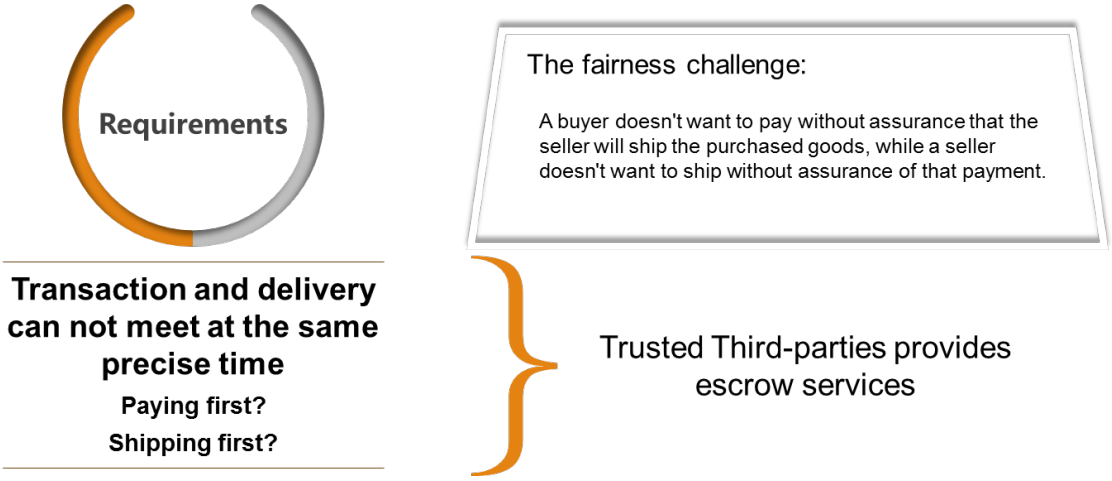

Figure1.2 Requirements Analysis

Meanwhile, during the process of trading between the digital currency and goods, buyers prefer paying to the seller after the goods are received, whereas the seller has an opposite preference in mind. This situation means the transaction and delivery are unable to take place at the same precise time, it can be difficult to achieve atomic exchange with the guaranteed fairness. A common solution is resorting to a trusted third-party to achieve fairness, however, this solution is not entirely satisfactory due to previous failures. There have been several Bitcoin exchanges and online markets (such as Mt.Gox, Coincheck) attacked by hackers. For decades, fair exchange protocols have been extensively studied. However, the recent emergence of blockchain takes fair exchange protocols to a renaissance.

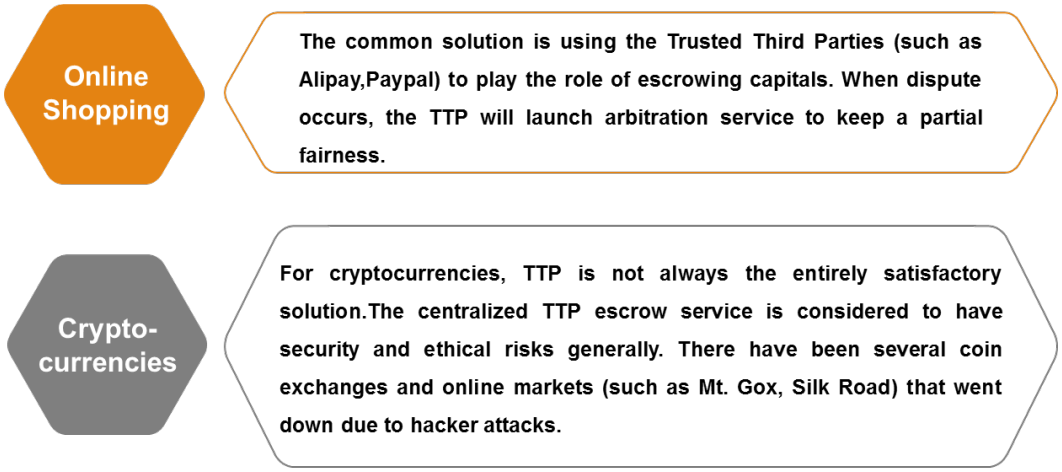

Figure 1.3 Trusted Third Parties

We developed Themis[1], a fair exchange system for digital currencies. Based on blockchain technology, Themis provides a decentralized digital currency escrow service to provide fair exchange services among digital currencies, digital assets, and physical goods. Themis leverages a novel group escrow protocol, along with threshold encryption, anonymous reputation mechanisms, non-interactive zero-knowledge proof, high performance digital signature algorithms, in order to provide atomic exchange with guaranteed fairness. Also, Themis is able to mitigate DoS attacks, and provide privacy for all peers.

[1] Themis is the most respected and trusted wife of Zeus's. As the goddess of law and justice, she is the creator and guardian of order.

2. Fair Exchange in Digital Commerce

Fairly exchanging digital content is an everyday problem. A fair exchange scenario commonly involves actors Alice and Bob. Alice has something that Bob wants, and Bob has something that Alice wants. A fair exchange protocol guarantees that at the end either one of them obtains what (s)he wants, or neither of them does. In digital commerce, it is a requirement to include fair exchange since one or both of the parties are using digital currencies as subject matter. For example, transactions between different digital currencies, or transactions between digital currencies and physical goods.

2.1 Transactions Between Different Digital Currencies

Traditionally, transactions between digital currencies are executed on cryptocurrency exchanges. Exchanges achieve this by creating internal accounts, which are also called IOU (I Owe You) accounts. In this mode, it's easy to achieve high transaction speed, however with the following issues; security, lack of liquidity, time lag of transactions. Regarding the transaction time lag, transaction results aren't submitted on the blockchain in a timely manner, and result in not being recorded immediately.

The model of decentralised exchanges was built to address the inherent issues of centralised exchanges. Most of decentralized exchanges are based on the Multi-Signature Scheme or Hashed Time-lock Contract (HTLC) to ensure atomic transactions. However, Multi-Signature Schemes depends on the Trusted Third Party(TTP)

which are vulnerable to collision attacks and DoS attacks. For the HTLC scheme, attackers may launch DoS attacks which could result in users being unable to make refunds in a given moment.

2.2 Transactions Between Digital Currency and Physical Goods

Current centralized coin exchanges and decentralized coin exchanges are focusing on transactions between digital currencies, but paying little attention to satisfy the requirements of fair exchanges between digital currencies and physical goods.

During the transaction between digital currencies and physical goods, it's hard to achieve transaction and delivery at the same time, thus the fairness of atomic exchanges face a challenge: a buyer doesn't want to pay without assurance that the seller will ship the purchased goods, while a seller doesn't want to ship without assurance of that payment. Traditionally, a trusted third party is required for hosting transaction funds and arbitration, and during the period between transaction and delivery, the third-party needs to host buyers' transaction funds to satisfy fairness. One common solution of third-party payment is using the 2-of-3 multi-signature. In this scheme, each buyer, seller and third-party holds a private key. A buyer sends his money to a multi-signature address, so only the party that has 2 private keys of these 3 can unlock the address and get the money. If things go well, the buyer will send his private key to seller, and seller will get the money. If any dispute arises, the third-party will mediate, resolve the dispute, and send his key to the winning party to finish the payment (or refund). There are two advantages of this escrow protocol. Firstly, if there is no dispute, buyers and sellers can close the transaction without the consent of the third party. Secondly, the third-party cannot take the hosted funds because the third-party only has his own key, the hosted funds can only be taken with at least 2 keys of the 3 parties. But this

protocol faces two critical problems. Firstly, collusion attacks. The hosting party can easily contact the specific buyer or seller for collusion unless the escrow protocol is meticulously designed. Secondly, DoS attacks. Even though the third-parties can't take the hosted funds, they can also refuse arbitrating disputes, and lock the hosted funds.

2.3 Design Objectives of Themis

Themis is a decentralized system which provides third-party escrow services and dispute resolution services to bring fairness to exchanges in which one or both parties are using digital currencies as subject matter. Technically, Themis should satisfy following requirements.

Figure2.1 Objectives of Themis

Fairness: After exchange, either both seller and buyer can obtain all the goods (digital currencies, digital assets, physical goods) they want, or they can obtain nothing (All-or-nothing);

Security: None of the parities can transfer the digital funds during the period of exchange;

Passivity: If no dispute arises, there is no need for the third-party to take part;

Correctness: Ensure transactions and settlement of disputes are executed by the protocol agreed in advance;

Dependability: Mitigate single point failure and DoS attacks;

Privacy: In case of no disputes, the third-party can't be aware of if the transaction completes, and only related parties can be aware of if disputes arise.

3.Architecture of Themis

3.1 Themis Blockchain

The Themis blockchain (aka. Themischain) is designed to provide a third-party escrow service (like the role that Alipay plays in online shopping). Themischain issues a token named Global Escrow Token (GET). Themischain motivates the blockchain peers by using an incentive mechanism which takes both deposit and reputation into consideration. Peers who take active part in escrow and arbitration will obtain a reward. When people use escrow services and arbitration services provided by Themischain peers, they pay GETs to the peers. And, if Themischain peers participate in arbitration, they earn GETs as well. Themis makes peer-to-peer fair exchange happen not only among digital currencies but also between digital assets and physical assets by escrow contract and arbitration contract.

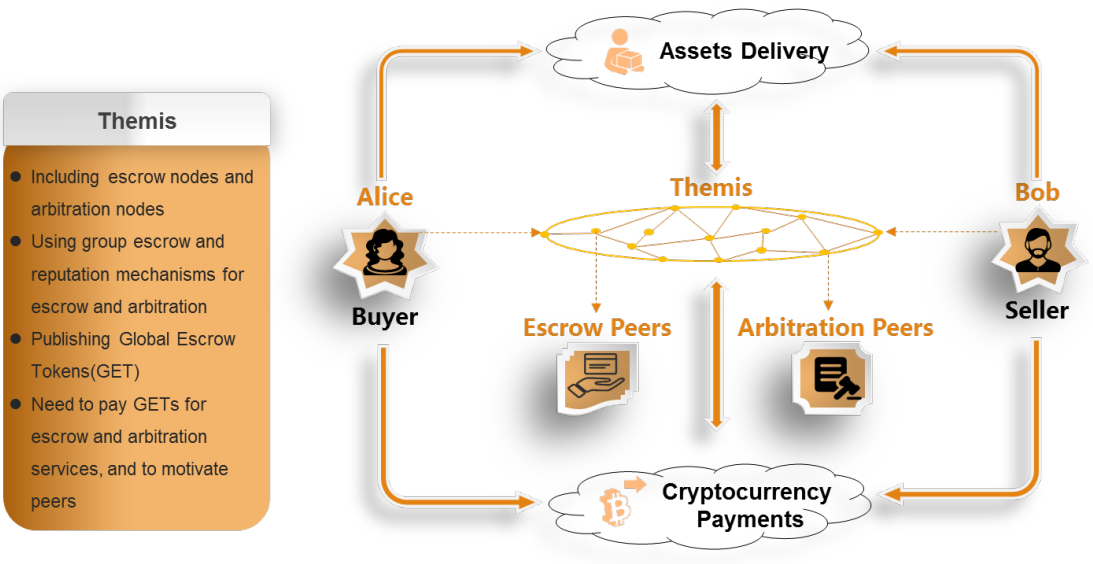

Figure3.1 Architecture of Themis

DPoSR Consensus. We improve the current DPoS (Delegated Proof-of-Stake) algorithm, and present a new consensus algorithm namely DPoSR (Deposit based Proof of Stake and Reputation). In DPoSR, we consider two key factors: the reputation of dispute settling peers; and deposit of peers. If a peer wants to act as a delegate, he must pay a deposit in advance, and the probability of being a delegate depends on its deposit and reputation.

Deposit Mechanism. If one peer wants to be a delegate, he or she must pay some deposit in advance. If this peer acts maliciously, the deposit will be confiscated by Themischain. A delegate will get rewarded for keeping the system running, that means he or she can share the transaction fee with other delegates. This forms a positive incentive to the peer, encourages it to behave well to keep the system running securely. As the blocks are signed by delegates in turn, if one delegate misses the signature by being offline, it will face the risk of being replaced by others. This encourages delegates to ensure they have enough online time for profits.

Escrow Peer Motivation Mechanism. If escrow peers provide the secret shares generated by Shamir-secret sharing protocol correctly, they will get reward according to the deposit they paid; Or if they are offline or lost the secret shares, they won't get any reward. If they provide manipulated or wrong information of secret shares, they will lose their rights as escrow peers. Thus, this mechanism will motivate peers providing correct secret shares, keeping online and storing their shares securely.

Reputation Management Mechanism. On one hand, peers in Themischain participate in dispute resolution, and give some arbitration suggestions. On the other hand, they give anonymous comments to the solutions other users gave for disputes continuously. Here on, we will create a practical anonymous

reputation mechanism, and it can update the value of reputation among users rapidly and privately. The reputation system will collect each user's feedback of arbitration suggestion correctly, and update the reputation value rapidly. And the value affects the possibility of being a delegate, that means if you have a higher level of reputation value, you are more likely to become a delegate.

Common peers motivation mechanism. Only the peers that have enough equities in Themis can have the opportunity to be the escrow peers, and the other peers are named common peers. Common peers can't participate in the process of escrow, however, they can transfer their equities to the trusted escrow peers, and the trusted peers will verify the fee they will earn from transaction, and pay back to the common peers by quota. If the escrow peers got punished, the common peers related to them will bear the loss too. This mechanism ensures that all the owners of equities on the Themis chain have the opportunity to receive rewards, and that motivates common peers entrust their equities to trusted escrow peers, and this way, we can improve the stability and security of Themis.

3.2 Group Escrow Service Protocol

In the protocol, Alice and Bob generate a 2-of-2 shared threshold address as their escrow account address, Alice has her private key x_A, Bob has his private key x_B, and according to the Thresh-Key-Gen protocol, both parties learn $y_A = g^{x_A}$ and $y_B = g^{x_B}$ and the shared public key is: $y = g^{x_A + x_B}$。Only if Alice or Bob has both x_A and x_B, he can unlock the public account.

Alice and Bob send escrow request on blockchain, and then they we accept response from several（odd）mediators. Then Alice

and Bob interact with mediators, and create a Shamir-secret sharing P_i of x_A and x_B. If there are $n = 2t + 1$ mediators, $t + 1$ secret shares of mediators is sufficient to recover the secret of x_A and x_B.

Using each mediator's public key, Alice and Bob encrypt x_A or x_B, and send the generated $c_i = E_{M_i}(P_i)$ to that mediator and gives all of these ciphertexts $\{c_1, c_2, \ldots, c_n\}$ to the other party.

During above procedures, in order to prevent fraud behavior, we use Feldman VSS[2] scheme as well as zero-knowledge proof to ensure the truth of the shares Alice sent to Bob, that means these shares are truly generated by Shamir-secret sharing protocol：when Alice gives Bob the ciphertext $c_i = E_{M_i}(P_i)$, Alice additionally includes a Feldman VSS value $w_i = g^{P_i}$ as well as a zero-knowledge proof of consistency between these two values。Thus, Bob then can verify that w_i is indeed a Shamir secret-share of x_A, and same to Alice.

Now, Alice or Bob can transfer his digital currencies to the hosted address, and if there is dispute, buyer will send his key to seller, and seller can get the hosted fund with these two keys.

And if disputes occur, mediators will activate the arbitration service. The winning party will transfer all the secret shares he received from the other party to each mediator, and if more than half of all the mediators work, we can recover the losing party's key, and send it to the winning party. And then the winning party will have two keys to unlock the fund in hosted address.

[2] Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: 28th Annual Symposium on Foundations of Computer Science, 1987, pp. 427-438.

3.3 Disputes Settlement

If a disputes occurs，both Alice and Bob refuse to send their private key to each other, and each party can apply for dispute settlement on Themis. When disputes occur, according to the settlement rules agreed in advance, Themis will launch the process of arbitration. If arbitration is launched, participants need to pay for arbitration fee, and in order to reduce the cost of fair exchange to the lowest, this process only be launched when disputes appear. Generally, we classify the settlements in two classes: first one is to generate the arbitration result automatically by Smart Contract; the second one is arbitrators vote for the arbitration result. In the first way, the Smart Contract will call Oracle Services automatically to obtain external inputs, and run a Smart Contract code to generate the arbitration result. In the second way, we introduce a crowdsourced arbitration service based on reputation score.

Crowdsourced Arbitration. The crowdsourced arbitration service of Themis is based on reputation score. We help both sellers and buyers to choose reliable arbitrators by grading anonymous arbitrators, and arbitrators can get rewards from blockchain. Meanwhile, Themis uses an opening censorship to assess arbitrators' reputation. The judgement of arbitrators will be submitted to Distributed Ledger for audit after being anonymously processed. In Themis, we list the information of dispute settlements including contract subjects, cases, judgements, reason for judgements by blockchain distributed ledger technology, and other users can rate the arbitrators' judgements. Then the arbitrators can get reputation scores according to their judgement behavior. Any behavior of abusing power of arbitration will be reflected in reputation scores, and users with lower scores will have lower possibility of being arbitrator.

Reputation Management Mechanism. The reputation system of Themis will provide other users' feedbacks of arbitration results reliably, rather than surrender personal information of users or rating details, and ensure reputation scores can't be changed maliciously. Currently, common reputation systems normally rely on feedback from other users to assess the quality of information, and motivate positive behaviors by updating reputation scores via algorithm. However, this data will link reputation scores to users' long-term identities. This identity linkage enables user tracking and appears at odds with the anonymity principle. We will create a practical anonymous reputation system which can update reputation scores amongst a huge crowd of users rapidly, and whilst retaining privacy. That means the reputation scheme of Themis doesn't need to link reputation scores to users' long-term identities.

Oracle Services. Oracle is a necessary mechanism when discussing and auditing the materials of transactions. The essence of Oracle is the information publishing of the real events in the real world. The data and materials required in arbitration must be determined by Oracle. These Oracle Services offer a series of AP. Themis determines the arbitration result and the following procedures by calling Oracle API. Oracle could be centralized(as Reality Keys), and it also could be decentralized (as Oracle Chain).

3.4 Strategy of Election

Election of Depositary. In the DPoSR consensus mechanism, If one node wants to have the right to be the depositary, he must pay some deposit in advance on Themis. If this node has malicious behavior, the deposit will be confiscated by Themis system. Nodes can vote for some other node as its depositary, and the Themis system will select the nodes with more votes by computing the

shares of these nodes have in the whole system as depositaries. These nodes will take charge of generating blocks by the turn agreed in advance.

Selection of Mediators. According to the escrow requests users sent, Themis system will use consistent hashing algorithm to select an odd number of nodes (2f + 1) as mediators.

Selection of Arbitrators. Themis system will use the weighted random algorithm according to the reputation scores of nodes to compute an odd number (2f + 1) of nodes as arbitrators.

3.5 Security Design

Our scheme might face three kinds of attacking threats. One is the DoS attack, that means a third-party denies settling any disputes and makes hosted funds locked. Another is the collusion attack from mediators and arbitrators, if the arbitrator tells both Alice and Bob they win the arbitration, and then both parties will send their secret shares to the mediators, and the mediators can recover 2 private keys to get the hosted funds. The last threat is the collusion attack of DPoS, there is a threat of DPoS itself that it might be attacked by partners. To avoid the first kind of attack, Themis uses the theory of incentives to increase the opportunity cost of DoS attack and it can lead mediators to be honest and civilized by the motivation of market, and makes the system complete escrow and arbitration objectively.

The motivation mechanism of Themis means to encourage mediators providing more effective services, and all the mediators with good behaviors will increase their reputation scores risen, as well as recovery Themis(GET) token. Otherwise, the mediators with bad behaviors will not only lose their reputation scores, but also the deposit they lodge to the system. This mechanism increases the

cost of bad behavior greatly, and mediators won't break the ecosystem for benefits, and in this way, Themis can avoid most attacks from malicious mediators.

We classified mediators into 3 groups, trusted committee mediators, certificated agency mediators and common mediators. The trusted committee mediators are reliable no-downtime mediators maintained by trusted organizations, and these mediators can guarantee the arbitration be executed even after DoS attacks. And the certificated agency mediators need to transfer deposit to Themis system in advance, and if they behaved maliciously, the deposit will be confiscated, in this way, we can avoid them from behaving maliciously. To avoid the second kind of attack, we upgrade 2-of-2 shared address to 3-of-3 shared address, and the third key x_C will be kept by both Alice and Bob but never disclosed to the third-party. Therefore, even though the mediators might launch attacks, they will only obtain x_A and x_B, and they still can't take the hosted funds. For the third kind of attack, as the more users use Themis to host funds and arbitrate disputes, the more value Themis will have, and the the less economically viable it is for mediators to act maliciously., the whole system will be more and more secure, and then that will attract more and more users to Themis services. This can be a beneficial circle loop to make Themis nodes grow, and to make Themis more powerful.

3.6 Typical Workflow

Using the example Alice pays Bitcoin to Bob for a toy giraffe, the following is the process of fair exchanging via Themis.

Agreement before transaction:

Alice and Bob require a Bitcoin escrow address;

Alice and Bob apply an escrow request on Themis, including disputes settlement (Smart Contract), service charge, arbitration bonus and so on;

Themis runs escrow smart contract, and responds the list of mediators to Alice and Bob;

Alice and Bob send secret shares to each mediator separately;

Alice and Bob send secret shares to each other.

Funds hosting and goods delivery:

Alice transfer her Bitcoins to the escrow address, and then, neither Alice, Bob nor the third-party could take the funds;

Bob posts the toy to Alice; Alice receives the toy, and after checking, starts the confirmation of goods, and sends her private key to Bob;

When Bob gets Alice's key, he can transfer the Bitcoins from escrow address to his own address;

The smart contract on Themis calculates and distributes service charge to mediators.

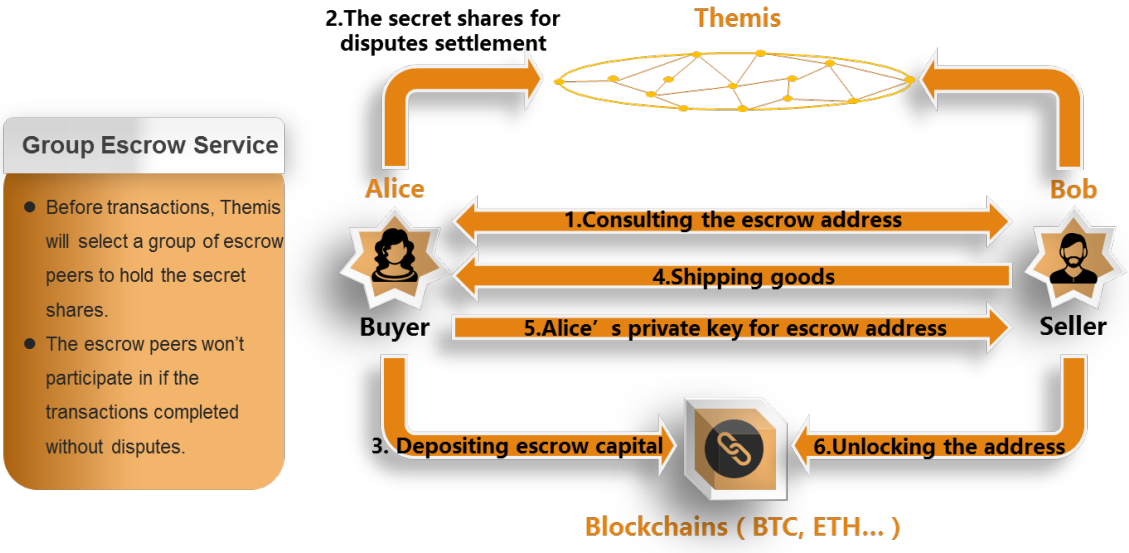

Figure 3.2 Funds hosting and goods delivery

Disputes Settlement:

Alice and Bob launch an arbitration request on Themis;

The arbitrators will determine arbitration result according to the agreement made prior to the transaction(Suppose Alice wins, Bob loses);

Alice sends the secret shares of Bob to mediators;

The mediators recover the key of Bob via shares and sends back to Alice;

Alice can transfer Bitcoins from escrow address to her own address by these two keys;

The smart contract on Themis calculates and distributes the bonus for arbitrators;

The smart contract on Themis calculates and distributes the service charge for mediators.

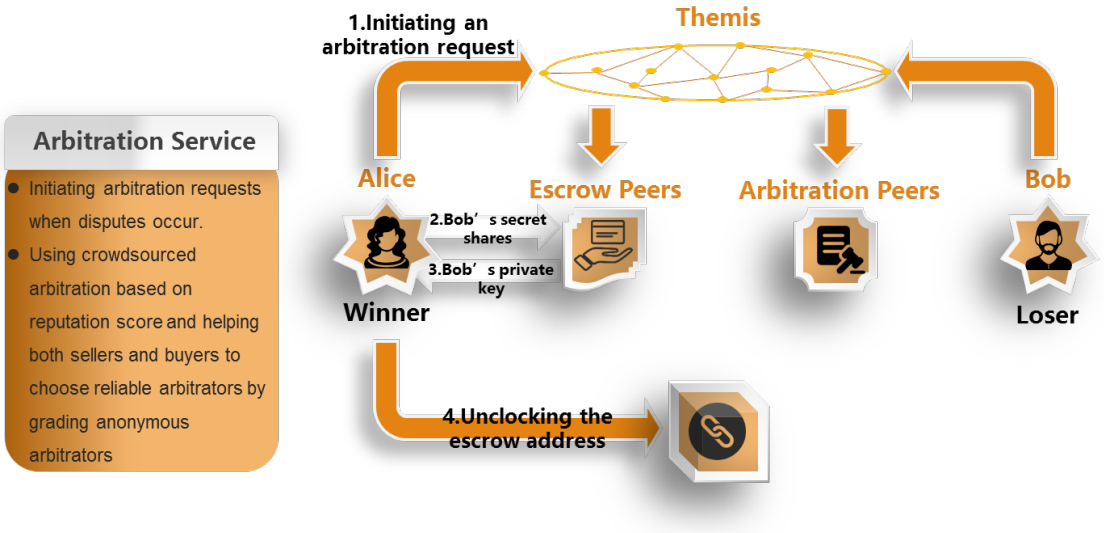

Figure 3.3 Disputes Settlement

3.7 Themis Wallet

Themis provides a hierarchical wallet based on a new generation of cryptography, named Themis Wallet, it can provide a kind of high-efficiency , low-storage-usage of private keys and address management service for users, and it can also achieve the interaction with Themis blockchains automatically, and make it easier for users to use Themis services.

In some typical use cases of Themis, users need to receive payments from other users frequently. For example, the e-shops using Themis to handle their digital currency transactions, they need to receive the payments from users of every transaction, and to ensure privacy, they need to generate addresses for each transaction, and they have to store and manage these addresses and related private keys. And as it's a linear dependence between the number of transactions and the number of addresses and keys, it will be quite a cost for wallet system to store and manage so many addresses and keys when the number of transactions is large.

Normally, when wallets generate new addresses, we need to save corresponding keys to key-storage area, and it could be a huge security risk for visiting the key-storage area. To avoid visiting this area frequently, current wallets usually generate a mass of keys each time, and save these keys into key-storage area each time in order to reduce the frequency of visit. For example, the Bitcoin Wallet, in the default setting, it can generate 100 keys and addresses each time, and users can use the way of storing keys in an offline storage (suck as flash disk, mobile HDD, or just print them on paper) to store them offline. And the addresses generated will be stored in the wallet client online. When the addresses are used up, the wallet will generate a mass of keys and addresses again, and

visit the offline storage to store keys. This method can reduce the frequency of visiting key-storage area in some degree, but it has no idea of reducing the cost of storage and management.

Themis wallet is a hierarchical wallet based on a new generation of cryptography, and it has following improvements：

1. API of Themis blockchain is supported, it can achieve the interaction with Themis blockchain automatically, and make it easier for users to use Themis services.

2. It can generate any number of addresses for users. And meanwhile, it only needs one space of key for offline storage. Users can use current offline storage schemes easily, such as paper-wallet (print keys on papers in the form of QR code)，or they can store the keys in hardware USB Key （the private keys of cryptographic currencies are usually standard Elliptic Curve keys, so we can store the keys of this scheme in every equipment that supports Elliptic Curve Digital Signature Algorithm）

3. There is no need for users to visit key-storage area during the payment. That means keys can be absolutely stored offline in this scheme.

4. The space of public key factor matrix for users is fixed, it won’t grow with the number of addresses.

5. It will be easier for users to manage their addresses. The addresses are generated by some payment information, and this information doesn’t need to be stored.

4.Key Technologies

4.1 Fair Exchange via Group Escrow

The problem of fair exchange is how two mutually distrusting parties can jointly exchange digital commodities such that both parties receive the other party's input or neither do. Indeed, fair exchange is a special case of fair two-party computation in which two parties wish to jointly perform a function over private inputs such that either both parties receive the output or neither does（All-or-nothing）.

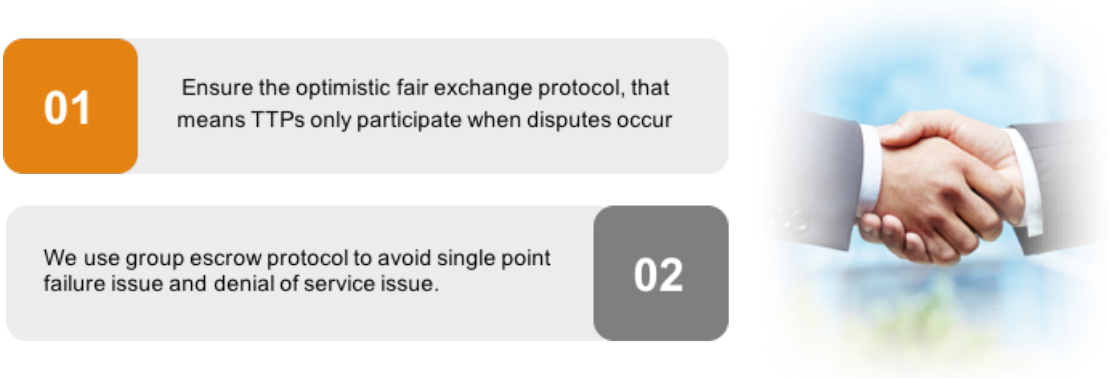

Figure 4.1 Fair Exchange via Group Escrow

Below is an informal description of fair exchange:

If there are two parties, A and B， each of them has an electron exchanging term i_X and its description d_X, in this situation, $X=A$ or $X=B$.

If there exists a verifiable function $f(*)$, which makes $d_X=f(i_X)$ protocol has 2 states, successful or failing， both A and B can verify his own state in the end.

Under the situation of asynchronous network, for the honest unit A (not able to judge if unit B is honest), only if he received the expected electron term i_B, then he would pay his electron term i_A; Conversly, same with the honest unit B. And here comes a trouble: Nobody wants to pay his electron term first, and that result in nobody could get expected electron term eventually. To overcome this situation, one effective solution is both parties send their electron terms to a trusted third-party(TTP), and the TTP can transit the terms and the TTP can arbitrate when disputes appear also.

Themis mainly solved two kinds of problems:

Firstly, during transactions, there are In-line TTP mode or On-line TTP mode, and both models need lots of TTPs, and leads the quality and security of TTPs being widely challenged. Hereby, Themis comes up with an optimistic fair exchange protocol, TTPs only participate when disputes appear;

Secondly, Themis comes up with a secure exchange protocol based on group escrow to avoid both the single point failure issue, and the denial of service issue.

4.2 Anonymous Reputation Mechanism based on Verifiable Shuffles and Linkable Ring Signatures

The current motivation mechanism of blockchain has two problems, on one hand is that it can't ensure anonymity, observers can easily find out the relation between identities and votes; on the other hand, this mechanism based on digital tokens can only increase the number of tokens of users, but it has no ideas about reducing the number of tokens of malicious users. Tokens'

cryptography mechanism restrict system from taking users' tokens, therefore, we can't reach the goal of punishing malicious behaviors. To solve this problem, the reputation mechanism of Themis based on verifiable shuffles and linkable ring signatures, and it can finish the calculation of reputation anonymously, without revealing users' identities, and it has the motivations of reward and punishment.

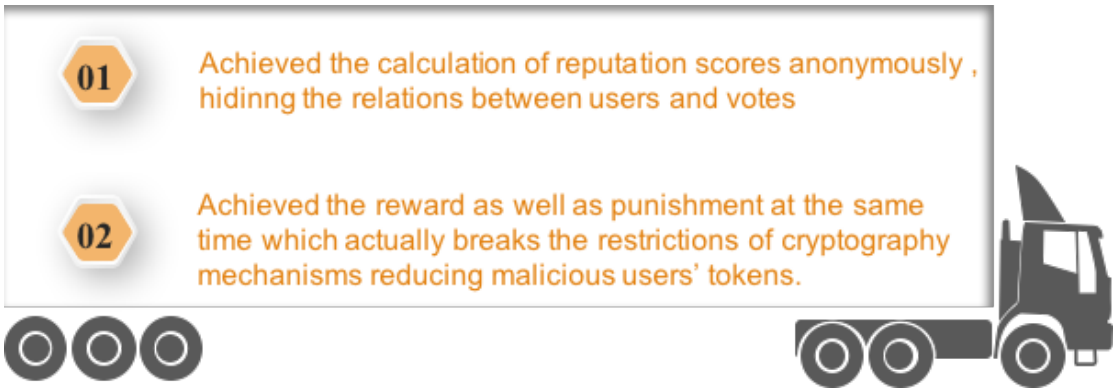

Figure4.2 Anonymous Reputation Mechanism based on Verifiable Shuffles and Linkable Ring Signatures

The reputation system of Themis operates in a series of message-and-feedback rounds. At the beginning of each round, the servers maintain a database containing all clients' long-term identities and their respective encrypted reputation scores. During each round, the servers successively run a scheduling protocol based on verifiable shuffles, which transforms the reputation list into an anonymously permuted list consisting of a one-time pseudonym for each client and an associated plaintext reputation score. Our scheduling protocol is decentralized: neither servers nor clients (other than the owner) can link one-time pseudonyms or reputations to long-term identities. Clients then post messages anonymously using these one-time pseudonyms. The servers can associate these messages with their corresponding reputation scores without learning clients' sensitive information. Each client may then provide

feedback (e.g., votes) on other clients' posted messages. Each vote is signed by a linkable ring signature, enabling the servers to verify that each client votes only once without revealing which client submitted each vote. This design enables the servers to tally positive and negative feedback without linking this feedback with long-term identities. Finally, the servers tally the feedback received for each one-time pseudonym, update the reputation score, and then perform a "reverse scheduling" to transform these one-time pseudonyms and their updated reputation scores back to the original long-term identities and their encrypted updated reputation scores.

4.3 Non-interactive Zero Knowledge Proof

Zero Knowledge Proof Systems are a cryptographic protocol between two parties (the prover and the verifier), and since its birth in 1983, this amazing theory has great influences on computer science and cryptology.

By executing Zero Knowledge Proof Protocol, when the assertion is true, prover is able to prove the validity of the assertion to verifier, and verifier can verify it quickly, but unable to learn any other information beyond the validity of the assertion. And when the assertion is false, even if the prover has unbounded computation power, he still not be able to fool the verifier accept a false assertion except with negligible probability. And when the assertion is like prover has some secret knowledge, the Zero Knowledge Proof system will specialize to the Zero Knowledge Proof of Knowledge (ZKPoK), that means the prover can prove to the verifier that he truly owns this secret knowledge, but he needn't to reveal any information about this secret knowledge. ZKPoK could be interactive or non-interactive according to if the prover need to interact with the verifier.

NIZKPoK minimized the round complexity (akin. communication cost), and thus is more applicable in the real world.

Themis uses the Zero Knowledge Proof Protocol to solve 3 problems: the first one is to ensure the secret shares offered to mediators by both parties of transactions in group escrow protocol is true; the second one is that, in verifiable shuffles protocol, all the observers and verifiers can use the Zero Knowledge Proof generated by shuffle servers to check if the shuffle servers executed random activities correctly; and the third one is that, in reputation system, clients will generate their Zero Knowledge Proof about reputation budget, and claim that 1) his actual reputation score is not lower than the expected value b, 2)he will use b as his reputation score to distribute messages.

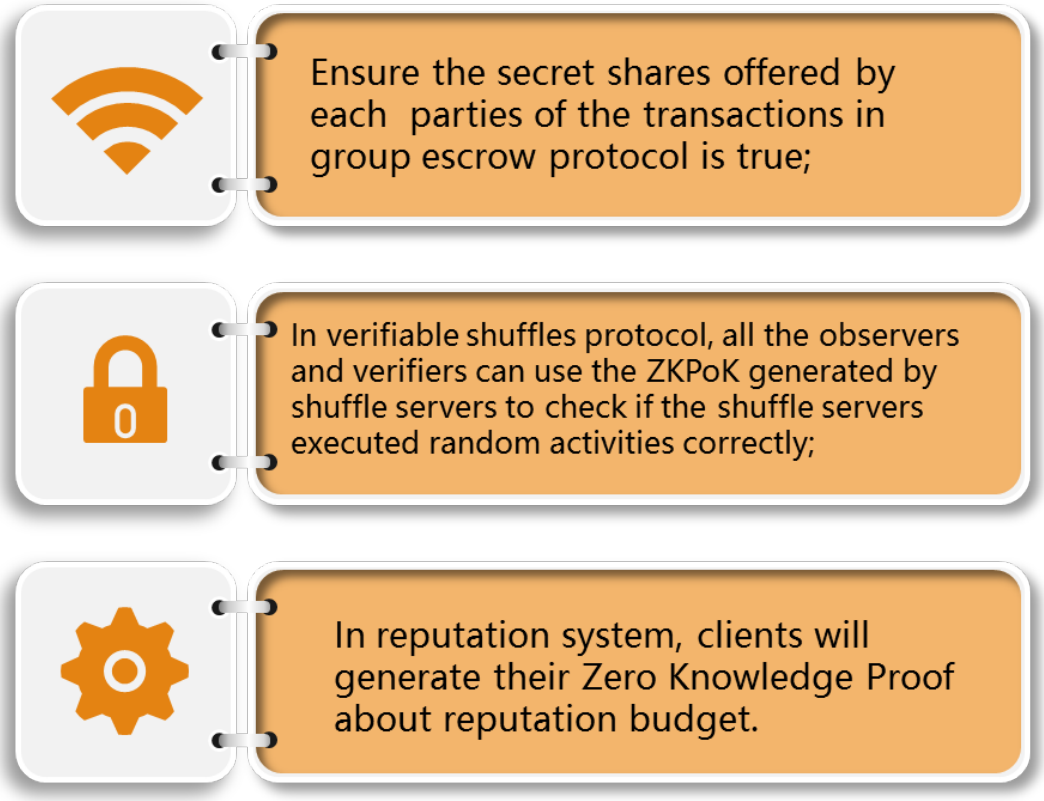

Figure 4.3 Non-interactive Zero Knowledge Proof

4.4 Digital Signature Algorithm with High-concurrency Verification Ability

For the transactions on public chains, the calculation ability of verification is the key factor of transaction processing speed. Currently, most blockchains employ the Elliptic Curve Digital Signature Algorithm using NIST's secp256k1 curve. This algorithm performs well at security, but the efficiency is poor, the mainstream CPUs can only calculate less than 10,000 times per second by this algorithm, so that there will be a significant delay when the number of transactions is large. Some allied chains and private chains usually try to avoid this challenge by involving trusted compute environment, but this method will involve a more complicated secure base, and it could be difficult to support the security requirement of public chains.

Themis solves this challenge by involving a new DSA algorithm with high-concurrency verification ability. Our system supports variety of digital signature schemes, and we can select a corresponding scheme according to the requirements of users and applications. With the situation needs one-time signature key, we will select the one-time signature algorithm based on hash algorithm to ensure high verification performance; in typical scenarios, upon ensuring 256bits security level, we will select specific elliptic curve and verification algorithms, and using the time-space tradeoff technology to improve the efficiency dramatically. We made a great improvement of the CPU and GPU vector instructions set in this algorithm, and take full advantage of every transistor's calculating ability. By optimization, we have improved the verification performance by 2 orders of magnitude in the typical calculation platform.

Figure4.4 New Generation of Cryptographic Algorithm for Blockchain

5.Scenarios

Themis is a fair exchange system based on blockchain technology, it provides escrow services for decentralized digital currencies, and solves the issues of fair exchange using digital currencies as a medium. Such as fair exchange among digital currencies, digital assets, and physical goods. There are many scenarios for Themis, such as peer-to-peer escrow payments, exchanges among digital currencies, supervising accounts and security escrow, multi-subject assets escrow and so on.

5.1 Peer-to-peer Escrow Payments

Themis can provide escrow payments of decentralized digital currencies for peer-to-peer online markets (such as OpenBazaar), to make it possible for both parties to exchange directly; Themis can connect to the payments system of e-commerce platforms, and generate corresponding escrow accounts via Themis original chains, then provide decentralized escrow service for digital currency transactions. During the transactions, buyers need to transfer digital currencies to the escrow account, and the sellers can only receive the money after the delivery is confirmed. This mechanism can solve the issue of payments not being able to effectively settle at the same time with deliveries.

In actual e-commerce activities, Themis will provide advance compensation for consumers. For example, 7 days after confirming receipt, 5% of seller's fund will be kept in platform account via smart contract as deposit; and if dispute occurs, Themis will take the advance compensation for buyer with the deposit, and then Themis

will contact seller about refund. This way we can improve buyers' satisfaction and sellers' reputation.

Figure5.1 Peer-to-peer Escrow Payments

5.2 Digital Currencies Exchange

Themis is a fair exchange system based on blockchain technology, it can satisfy the transactions between digital currency and physical goods as well as the transactions among digital currencies, and it can provide a fair guarantee for the transactions of all kinds of centralized or decentralized digital currencies.

Themis supports OTC transactions of digital currencies, and it can provide secure escrow service for cryptographic digital currencies based on blockchain, such as Bitcoin, Ethereum, and generate corresponding escrow accounts via Themis original chains to satisfy the requirement among digital currencies, and make it fair for the cross-chain transactions.

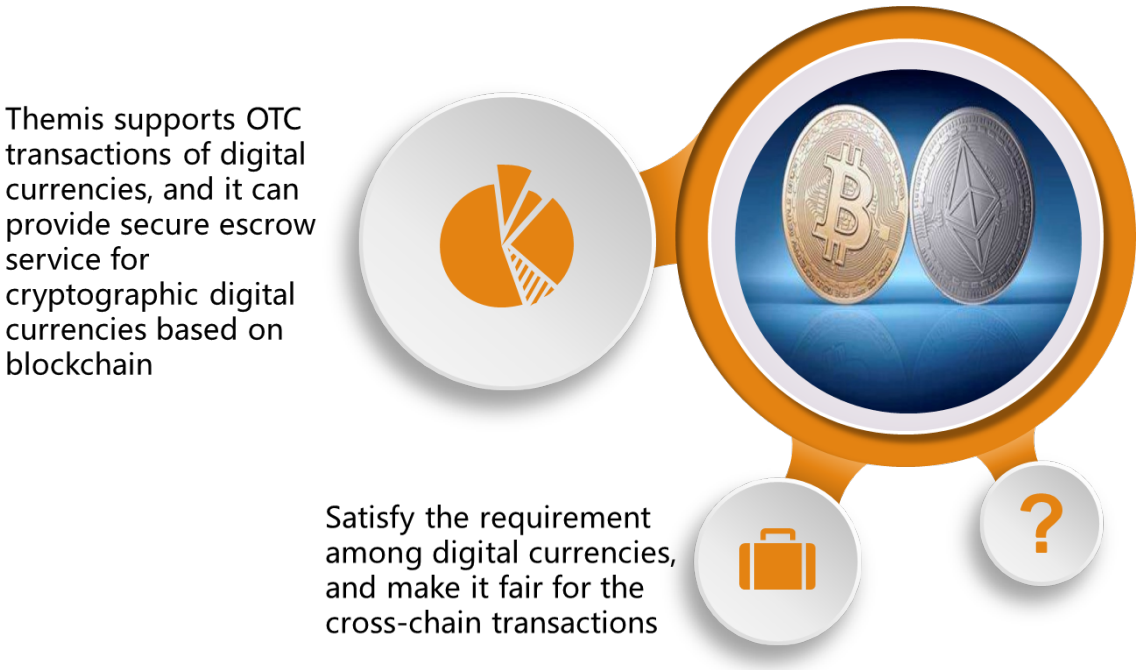

Figure5.2 Digital Currencies Exchange

5.3 Accounts Supervising and Security Escrow

Escrow service is an important method for the traditional financial industry to keep users' assets secure. For example, securities dealers need to set trust accounts with banks after opening accounts, peer-to-peer lenders need to open supervision accounts. However, for private equity funds, crowdfundings, and ICO investment funds, both the investees, investment proportion and return on investment are not transparent to the investors as they have no escrows or they just use a centralized third-party escrow mechanism.

As a group of smart contracts with scalacity, Themis can provide the API of distributed ledger and decentralized escrow service for digital currency supervision accounts, so Themis can solve the problems of funds security, project tracing, and rationalization distribution effectively. And as the digital financial market matures, there will be more and more products and

scenarios for digital currencies in the future. Such as lenders of digital currencies, futures of digital currencies, ETF funds of digital currencies, cross-chain transactions of digital currencies and so on, and all of these can be managed by Themis system to ensure security.

Figure5.3 Accounts Supervising and Security Escrow

5.4 Multi-agent Assets Escrow

In the transactions of SCF, real estate, and large equipment, as there are so many transaction agents, transaction links, and strong dependencies, it will be easy for problems of morality and credibility to occur.

Themis can host all the funds (deposits, initial payments, service charges, final payments) in multi-subject transactions on the original chains as the form of digital currency by creating smart contracts based on multi-subject duties and conditional instructions. And when the transaction comes to the corresponding link, the corresponding transaction subject will trigger the smart contract by inputs to achieve the fair exchange protocol. If any disputes arise, dealers can use the group escrow protocol and arbitration mechanism of Themis to launch an arbitration request. And every

member in the group escrow party will arbitrate, vote for the disputes, and form an arbitration result, the winning party will have the right to unlock the account.

6.Roadmap

- Jun,2017, started the design of fair exchange protocol based on group escrow mechanism.
- Dec,2017, finished the MVP (Minimum Viable Product) version.
- Mar,2018, internal test of decentralized escrow service, and test run of Themis OTC platform.
- Jun,2018, launch the Themischain test net.
- Oct,2018, launch the Themischain main net.