Yee: A Blockchain-Powered & Cloud-based Social Ecosystem

(Draft)

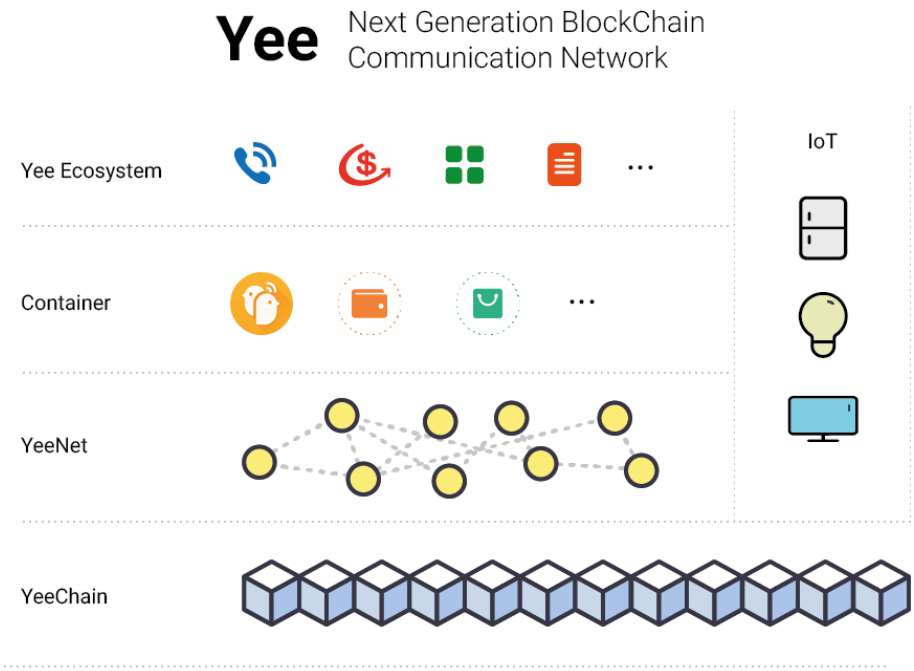
Yee Foundation English Version · January 2018

1 Project Overview

The current decentralization movement is ambitious and will provide great opportunities for new social and economic interactions. The rapid development of blockchain technology, initially used for cryptocurrencies, is expanding to various applications and is expected to revolutionize the Internet world. However, for industrial-scale application, current and recent blockchain architectures alone does not yet have a solid technical and ecological foundation to meet the demands of massive content delivery and fast transaction capability to provide the superior user experience. Now it is the time to build such an industrial-scale platform.
Having established a large-scale centralized cloud communication & social platform, Yee plans to smoothly migrate to a blockchain-based decentralized ecosystem while improving the user experience. We will build a new generation of blockchain architecture that provides the underlying platform for related DApps and evolving ecosystem.

The project is composed of four parts as follows:

- YeeChain: a blockchain supporting fast transaction and high-efficiency storage
- YeeNet: a cloud-based communication network based on YeeChain
- Launching typical applications: YeeCall, YeeWallet, Dapp, and YeeStore
- Yee ecosystem blueprint



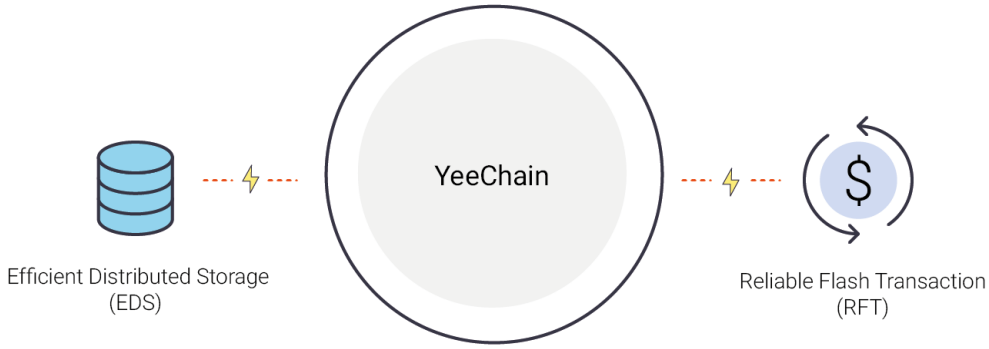
2 YeeChain

In the initial stage, Yee will be operated on public Ethereum network. However, it should be clear that to support the efficient and stable operation of a distributed communication network, the current Ethereum network still has many problems:

- A great deal of calculation is wasted because of its current consensus mechanism, and it will create some barriers when applied to mobile phones.
- Network partition will lead to the phone's frequent disconnecting and connecting to the network, therefore undermines the stability of communication mechanism.
- Slow transaction: the average confirmation time (or block time) is about 30 seconds (December 2017). This processing speed can hardly be applied in daily life circumstances.

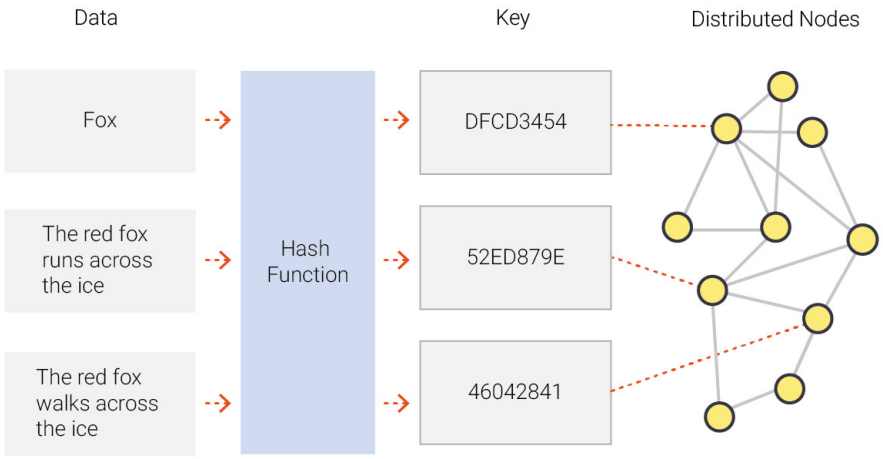
- The amount of data on the chain is too large, which means great consumption of phone storage space if it is fully stored on the phone.
- Ethereum blockchain needs to pay for every transaction, which causes barriers for ordinary users paying with Ethereum cryptocurrency.

In order to solve all these problems, we are committed to creating a YeeChain, which can be operated on current blockchain base, and try to achieve high-efficiency storage and fast transaction.



• High-efficiency Storage (local storage can be decreased by 99.99%)

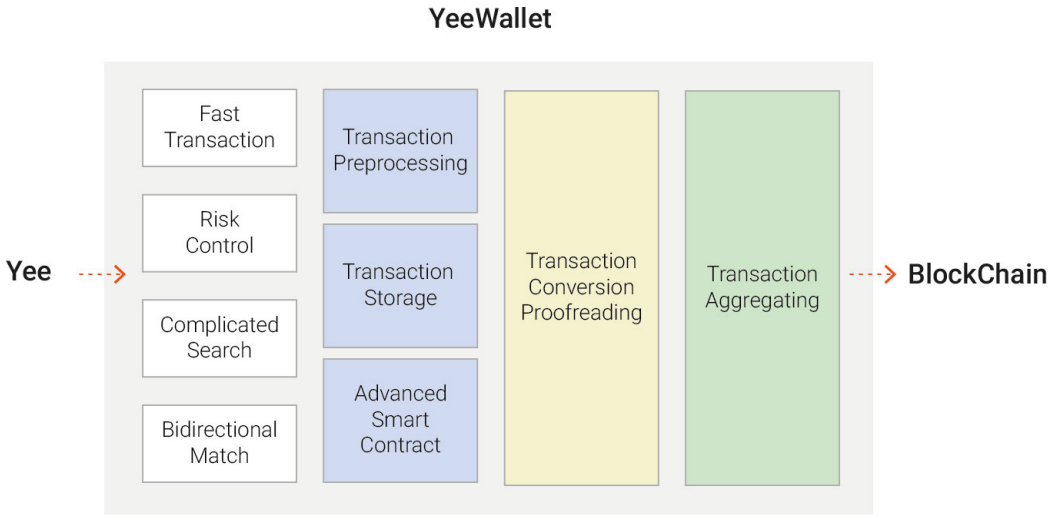
All the nodes within a blockchain can shared by the whole network. With the guarantee of secure verification, a person can choose to save only a small part of each node and certain blocks that are concerned and in use. When other blocks are needed, they can be downloaded from other nodes. The double verifications of Hash(SHA512)'s result and context can make sure that the blocks acquired from the distributed network are not tampered.



For the code within the upper layer's blockchain, the local network still owns all the blocks and the logic is the same as before. For the blockchain network supporting frequent transactions, local storage can be decreased by 99.99%.

• Fast Transaction

Introduce the credible third party YeeWallet: To the public blockchain, transaction fees and speed are two difficult problems. However, the credible third party can combine the advantages of public blockchain and that of private blockchain to let users choose which one they want to use. In this way, the user experience can be significantly improved, and users' rights and interests, as well as the security and tamper-resistance of Yee can be ensured. The credible third-party YeeWallet can gather a great amount of small transactions and submit them to the blockchain at one time. Meanwhile, as the intermediary, YeeWallet can protect and promote transactions as long as both of the transacting parties trust YeeWallet (Alipay and PayPal have created essential value to their own communities). As a community platform that has a great number of users, YeeCall itself is a credible platform to its users. After introducing YeeWallet, users can use YEE conveniently.



3 YeeNet

Although building an efficient and real-time communication network is so complicated, YeeCall team has been working to update the product over the past three years:

•Initial Phase

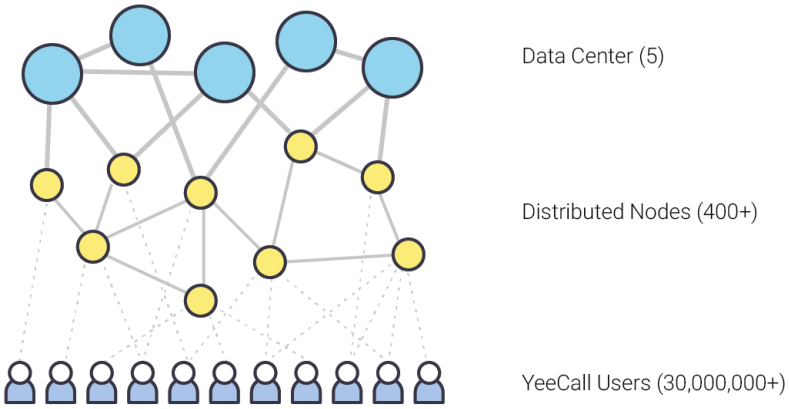
YeeCall completed its communicational deployment in every country around the world by supporting message and other asynchronous communications and using centralized networking mode.

• Developing Phase

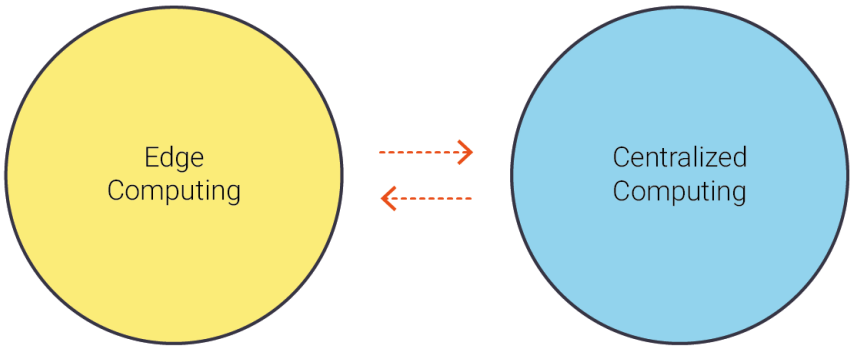
On the basis of realizing asynchronous communication, YeeCall enhanced its peer-to-peer chat, group chat and other synchronous communication models, and supported live broadcasting mode on the bottom layer. Meanwhile, YeeCall established 5 big data centers and more than 400 relay nodes around the world, covering 227 countries and more than 1000 operators. Due to all of these efforts, YeeCall has become a perfect high-efficiency communication network that supports both synchronous and asynchronous communications.

• The Current Phase

YeeCall has been updated to a "distributed + centralized" hybrid cloud communication network. Now, 70% of the data traffic can be efficiently completed through P2P communication. Now YeeCall is taking steps to enter the IoT area.



※Current YeeCall Network Structure

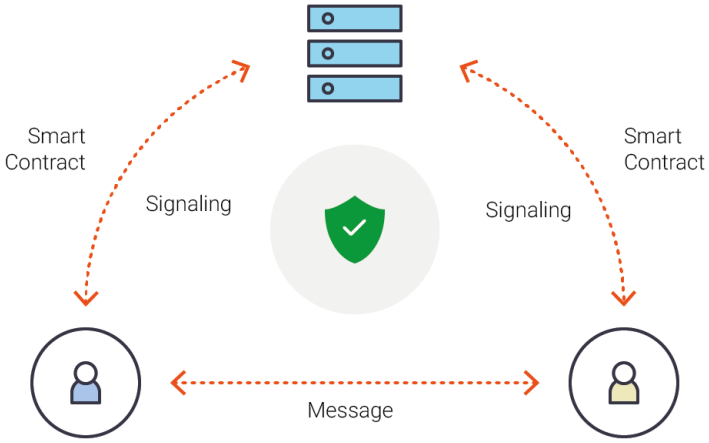


※Current YeeCall Computing Structure

For such a communication network covering the whole world, the next step is to provide a more secure architecture and more privacy-respected product in the light of decentralized consensus mechanism.

The birth of blockchain technology brings us some new ideas like:

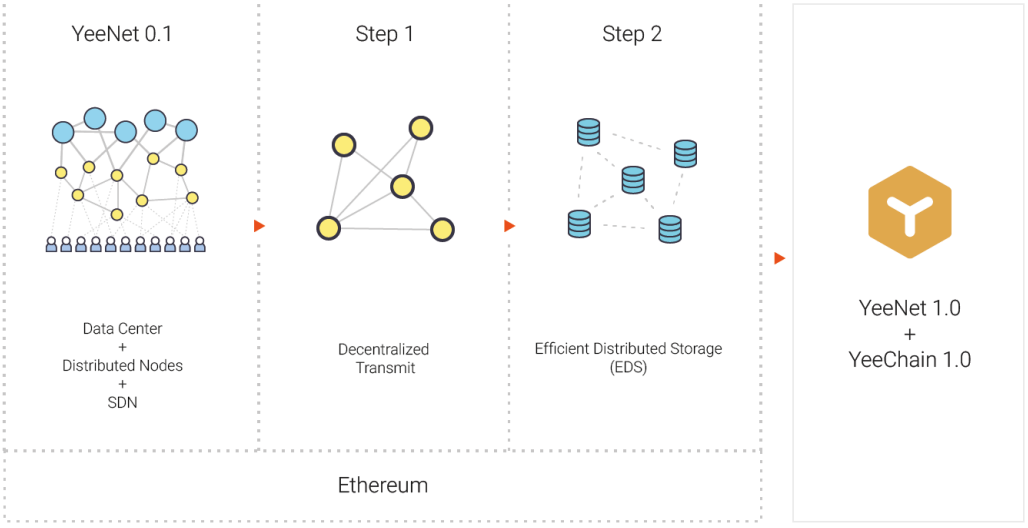
Encrypted communication: The traditional encrypted communication is to encrypt the transport channels from end to end, but there still exists a possibility of being attacked at the tip node. What's more, the signaling of communication has to go through the server, which cannot convince people as blockchain's consensus mechanism does. We are planning to realize encrypted communication through the smart contract of the blockchain. The smart contract will be formed once a message is sent out, and the message will be destroyed on the server as soon as it is read. By this means, transport channel encryption plus smart contract-based destroy system will truly solve the problems of encrypted communication.



Encrypted Communication Based on YeeNet

On the basis of the current YeeCall communication network, we will gradually improve and update this network by using blockchain technology and finally make it a decentralized autonomous communication network YeeNet.

The expected update process:



YeeNet 1.0 will support peer-to-peer chat, group chat, live broadcasting and IoT communication and it is combined with YeeChain 1.0, which solves current blockchain's core problems of great storage space cost and low transaction speed. Finally, it will become a distributed, open, efficient and stable communication network.

The combination of IoT and blockchain is an important research topic around the world. Since YeeNet has already had basic ability in terms of edge computing and IoT network architecture, Yee Foundation will continue to conduct research in this area to find a better integration scheme.

In the future, YeeNet will be applied in many communication circumstances. For example, the encrypted communication based on consensus, paid service of destroying message after being read (if one sends a paid message, the other must pay first to read the message and the message will be automatically destroyed after being read) and tracing to the source of things on IoT application.

4 Technical Consideration

This section introduces the general technical considerations over the application of Yee ecosystem on public Ethereum network and technical innovation of YeeChain and YeeWallet.

4.1 Platform Limitation and Off-chain Solution

Although the future version of Ethereum will focus on improving throughput and scalability, when Ethereum network runs on the "Proof of Work" blockchain and then applies in Yee Ecology, it will face the following problems:

- The current consensus mechanism causes a great deal of computing power being wasted, thus hindering the operation of the applications on the phone.
- Network partition causes the phone connecting and disconnecting from the Internet frequently, thus affecting the reliability of communication mechanism.
- Relatively slow transaction speed: the current average confirmation time (or block time) is around 30 seconds (2017 December), which makes it difficult to apply to everyday life scenes.
- The amount of data on the chain is so large that full storage consumes a large amount of mobile space.
- The Ethereum blockchain needs to pay the fees for each transaction, which creates a barrier for ordinary users to pay with Ethereum cryptocurrency.

Given these obstacles, YeeWallet will first implement the semi-centralized, hybrid on-chain and off-chain transaction service in order to realize scalable interaction with YEE cryptocurrency. In the future, we will work hard to develop YeeChain that supports efficient storage and fast transaction. Specifically, our technological innovation will focus on the following points:

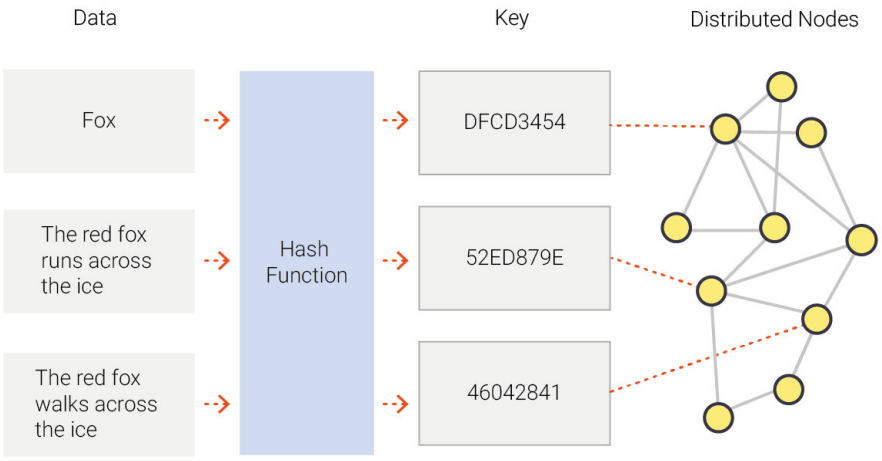
- YeeChain will adopt the "Proof-of-Stake" method to build consensus mechanism based the new blockchain agreement of Ethereum, which is similar to the partition solution of Cosmos Internet of BlockChains and supports smart contract.
- Meanwhile, transform the underlying storage, and achieve the distributed storage of blockchain; but as for the upper-level program, it seems that it has been stored locally.
- Transform the transaction, introduce YeeWallet as the trusted third party through which users can choose to employ advanced functions, such as revocable transaction; they can also choose to trade directly on BlockChain at normal speed.

4.2 Technical Innovation

Since a large number of developers have already come up with "Proof-of-Stake" and partition solution of Cosmos Internet of BlockChains, we will not go through the details here. Here we mainly explain the underlying storage transformation and transaction optimization.

4.2.1 Underlying Storage

Core Concept:
All the nodes within a blockchain are whole-network sharing. With the guarantee of secure verification, a person can choose to save only a small part of each node and certain blocks that are concerned and in use. When other blocks are needed, they can be downloaded from other nodes. The double verifications of Hash(SHA512)'s result and context can make sure that the blocks acquired from the distributed network are not tampered.



For the code within the upper layer's blockchain, the local network still owns all the blocks and the logic is the same as before. For the blockchain network bearing frequent transactions, local storage can be decreased by 99.99%.

Core Algorithm:
Node distance: the distance between any two nodes or the keys of two data.
d is defined as:
d = SHA512 (node-id 1) XOR SHA512 (node-id 2)

Routing Table Rule:
The distance d has 512 bits in total; from high to low, every 4 bits is one group, and they can be divided into 128 groups. The nodes in different distance, according to the value of d, from high to low, can be uniquely assigned to a certain group. In this way, the high groups have many nodes; but because of its far distance, there is less interaction with this node. The low groups have fewer nodes; but because of the close distance, there is a closer connection with this node.

Define a constant k; in each group, save the position of k other nodes (IP: PORT) to form a chain table as the access node list for subsequent access. When accessing nodes in each group, there are cached hot nodes that can be directly accessed. Meanwhile, if the nodes to be accessed are not on the list, initiate a node query to any node of the k nodes in this group and then find the actual location of the node. This dynamic node list can be updated at any time, thus effectively preventing the node failure or the problems caused by the attack.

Node Query:
Node query should be designed to be executed asynchronously.
The steps can be expressed by pseudo code as follows:

```
find_node(dest_node_id){
d = distance(my, dest_node_id)
//According to the grouping algorithm mentioned above, find a non-empty group with the smallest difference from d.
group = find_min_distance_and_not_empty_group(d) query_nodes=nodes in group
//The algorithm will be over when have found the target, or when the queried intermediate result does not change (it means that the target to be queried is not in the network)
while( ! find_dest && query_nodes changed){ query_result.clear()
for(node in query_nodes){
//Each intermediate node reports the k points it knows closest to dest_node_id
 query_result.addAll( query(node, dest_node_id))
}
//From this round of results, find the k nodes that closest to the queried node query_nodes =
```

```
 find_min_k_distance_from(query_result,dest_node_id)
} }
```

Data Query:
Data query and node query are highly similar, except that the node **id** becomes the key value data "**Hash"**. The difference is that, during the query process, once one node has saved this data, it will report directly that it has found this data. Then the query will be over directly, and the data can be acquired from this node. Because it is very similar to find_node, pseudo code will not be attached here.
But data storage will simultaneously initiate the storage to the closest k nodes during the storing of the actual storage nodes. In this way, if one of the k nodes is online, the data can be accessed.

```
//Initiate the storage
Store_data(data_key,data){ node=find_node(data_key) store_if_not_exists(node,data_key,data)
}
//Actually storage data in this node
on_store_data_in_myself(data_key,data){ d = distance(my, data_key)
//According to the above grouping algorithm, find a non empty group with the least difference from d
group = find_min_distance_and_not_empty_group(d) nodes=nodes in group
for(node in nodes) store_if_not_exists(node,data_key,data)
}
```

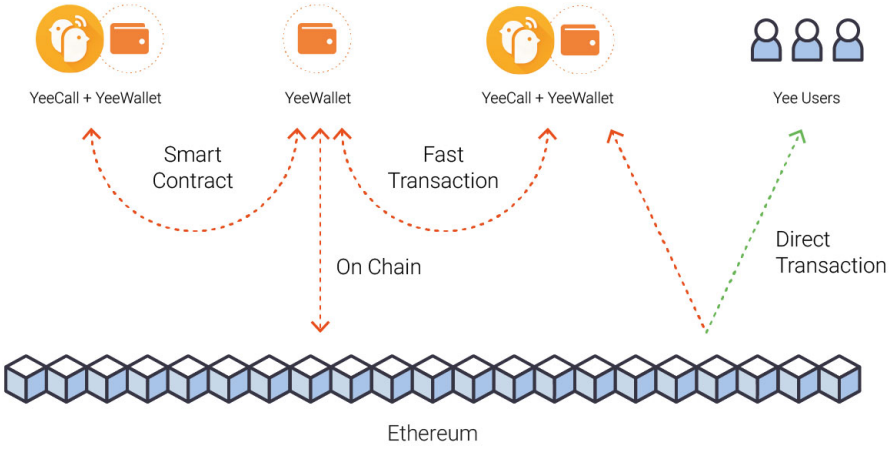
For hot data that is accessed frequently, when it is accessed by actual storage node, it can also ask for being diffused (i.e. be cached). Specifically speaking, ask for the node that initiated the query to cache this data on the node queried in the last round.

Mathematical Analysis of Algorithm:
Supposing that there are n nodes using this storage engine, respectively marked as x1…xn (x is A numerical value with the length of d bits). Then, for any x□{x1…xn}, define Di(x) as the set of numerical value with the same d-i length prefix.

Define Txy as the query time required to find y from x, then it can be proved that(The proving is omitted):
Where **sup** is the upper bound and Hk is the kth Harmonic number. When k tends to infinity, Hk / logk tends to be 1, so the expected upper bound of Txy is , and the average algorithm complexity can be considered as .

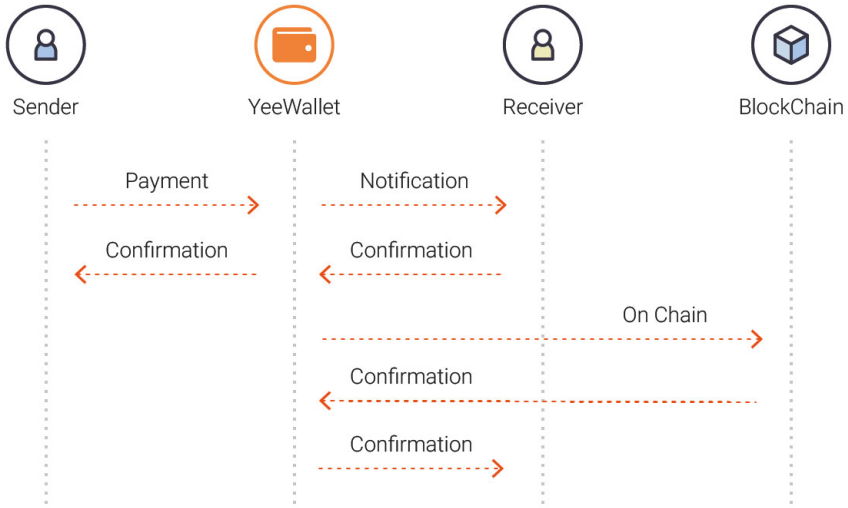
4.2.2 Transaction Methods

Introduce the credible third party YeeWallet: To the public blockchain, transaction fees and speed are two difficult problems. However, the credible third party can flexibly combine the advantages of public blockchain and that of private blockchain to let users choose which one they want to use. In this way, the user experience can be dramatically improved, and users' rights and interests, as well as the security and tamper-resistance of Yee can be ensured. The credible third-party YeeWallet can gather plenty of small transactions and submit them to the blockchain at one time. Meanwhile, as an intermediary, YeeWallet can protect and promote transactions as long as both of the transacting parties trust YeeWallet (Alipay and PayPal have created essential value to their own communities). As a community platform that has a great number of users, YeeCall itself is a credible platform to its users. After introducing YeeWallet, users can use YEE conveniently.



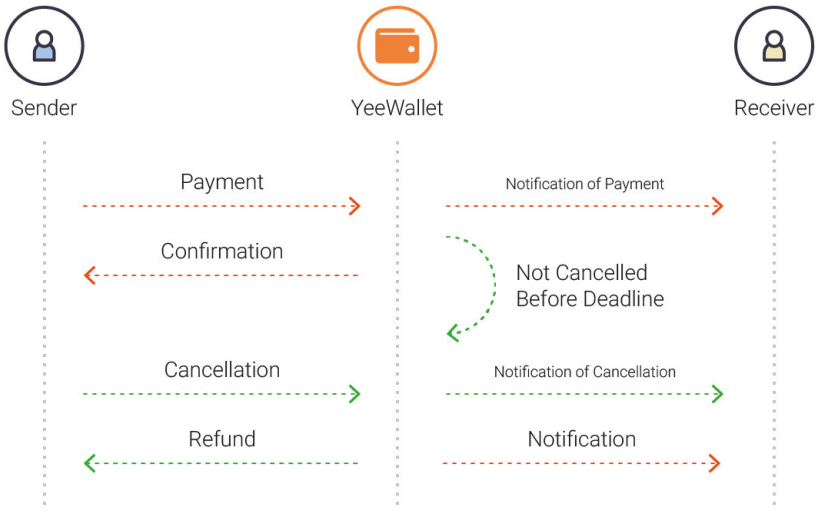
Core Business Logic Implementation:

- One-way payment with no need to be reconfirmed. Representative transaction: tips, purchase system service. YeeWallet fast payment (payer should have the balance in YeeWallet): YeeWallet of the payee will show received payment. Transactions can be finished instantly in YeeWallet. If the payee needs, YeeWallet will intensively submit to the blockchain after a period of time. Status change is visible to the users.

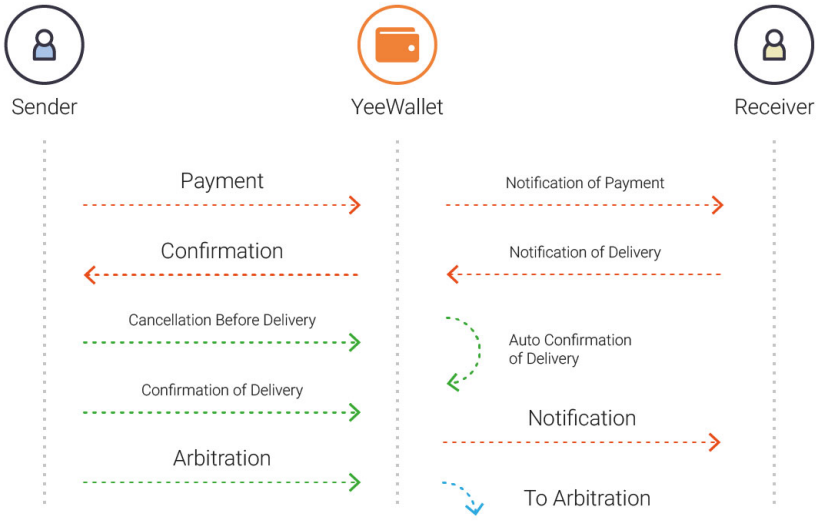


Because transferring to blockchain is an independent operation, we will not introduce the relevant processes.

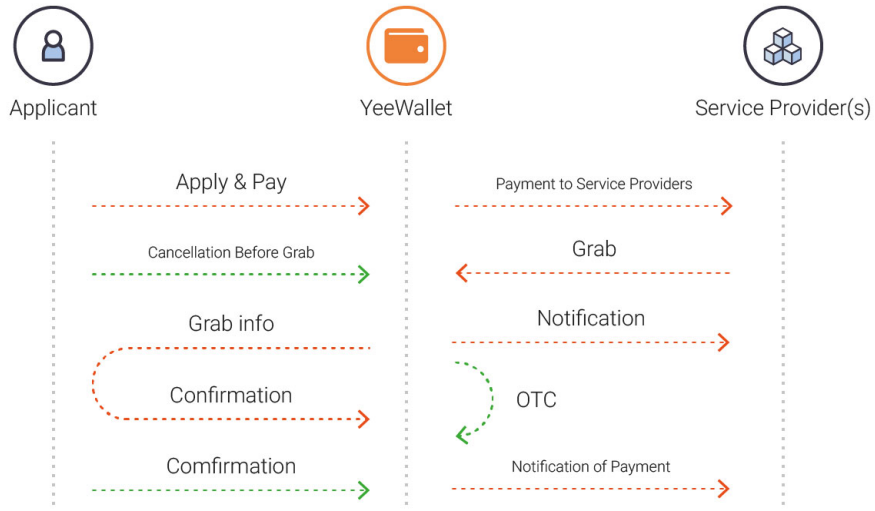
- One-way virtual goods transaction that needs to be confirmed. Representative transaction: purchase group membership right, purchase third party sticker and other virtual goods transaction. YeeWallet revocable payment: the payer pays to YeeWallet first and the payee will receive the payment reminder in advance (but not credited yet). The payer can revoke the payment before the specified time limit. After the time limit, if not be revoked, the payment will arrive the payee's YeeWallet account.



- Physical transaction that needs to be confirmed. Representative transaction: C2C commodity transaction. Use YeeWallet to pay periodically: The payer will pay to YeeWallet first, and the payee will receive payment reminder in advance (but not credited yet). Before the payee submits the proof of delivery to YeeWallet, the payer can apply for revoking the payment, but the revocation will be delayed. If the payment is not revoked after submitting the proof of delivery, it cannot be revoked any more (but can initiate the arbitration). If the transaction is successful, or if the payer does not confirm in a long period of time, the payment will arrive the payee's YeeWallet account. If there is a dispute in the subsequent transaction, both parties can submit the arbitration request to the third party arbitration organization, attached with arbitration fee. The arbitration fee of the losing party will be vested to the third-party arbitration organization.



- Bidirectional matching transaction. Representative transaction: various real-time order-snatching transaction, such as currency exchange intermediary service. The exchanger initiates the order and pays the corresponding Yee token to YeeWallet. After the order is initiated, the corresponding organization that can take this order or the third party will snatch the order. The exchanger need to confirm that the order-snatchers are service providers. After confirmation, they will transact offline. After completing the transaction, the order initiator confirms or the order taker uploads agreed evidence to complete the transaction, and Yee token will be paid to the order taker from the YeeWallet.



- Portfolio transaction: such as the transaction type of personal information exchange. Information transaction exchange is that the publisher firstly initiates a one-way payment with no need to be reconfirmed to the system, the system will make a price according to the requirements of broadcast range and others. When the information is read, the reader performs a one-way virtual goods transaction with need to be confirmed to information provider. The more information is read, the greater the benefit is.

In summary, in order to solve some practical problems, Yee will launch a credible third-party payment and guarantee organization YeeWallet, and will develop and host a centralized off-chain ledger book, which will provide API that apply to all digital service partner. This will (1) improve the user experience that is affected by the delay, (2)reduce network cost in the transaction between users, (3) avoid stressing on the public network due to heavy volume of transactions, (4) adapt to the unique transaction scene of YeeCall users.