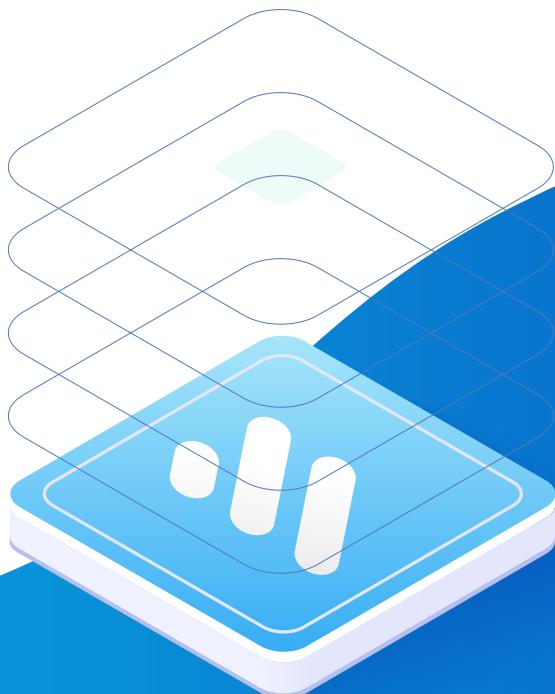


# MetaPay



## Meta Financial Payment Ecology

NFT trading platform supported by Meta Finance



# Content

<b>Preface</b>	<b>3</b>
<b>Background</b>	<b>4</b>
DeFi	5
History of Cross-chain Development	5
The proposal of Meta Finance	6
<b>Vision</b>	<b>7</b>
<b>MetaPay Introduction</b>	<b>9</b>
MetaPay	10
Meta NFT	11
Meta DAO	11
MetaPay Token	12
<b>MetaPay Cryptographic Algorithm</b>	<b>13</b>
Elliptic Curve Discrete Logarithm Problem (ECDLP)	14
Hash function algorithm	17
Zero-knowledge proof of non-interactive zk-SNARKs	18
<b>MetaPay</b>	<b>19</b>
Implementation	24
<b>Meta NFT</b>	<b>26</b>
Meta NFT Features	28
Implementation	28
Minting Custom Coins	29
Community integration	30
<b>Meta DAO</b>	<b>31</b>
Definition	32
Met Global Governance Model	32
Implementation	32
<b>Roadmap</b>	<b>34</b>
<b>References</b>	<b>36</b>
<b>Laws &amp; Regulation</b>	<b>38</b>



# Preface

With the continuous upgrading of "Internet +" and the continuous demand of improvement of the pursuit of the quality life, the centralized and large-scale corporate commerce and manufacture are declining. The era of multidimensional competition with perfectionism and ecologicalization is coming with dividing demand and splitting business is getting deeper and deeper, and the organizational model is bound to move from a single vertical control type to a meshed and platformized one, and individuals will get more empowerment.

According to a survey, millennials are more able to accept new changes. Although they have their own ideas and motivations for this move, they are generally optimistic and support the continuous development of open source distributed blockchains.

Crypto algorithms, blockchain, and DeFi may be the most important inventions in the past 500 years and the next 100 years. It is possible to truly realize the liberals' utopia represented by people like Satoshi Nakamoto, but the process must be tough.

The most likely way to reach the milestone of liberalism is DeFi (Decentralized Finance). Most people think that DeFi is just a series of smart contracts. In fact, the meaning of DeFi goes far beyond smart contracts.

DeFi can be any decentralized financial protocol, such as decentralized lending, payment, pledge, mining, NFT aggregator, etc.

In the future, the implementation of DeFi must develop tools that support continuous management, decision-making, and code execution.



# Background





# Background

## DeFi

The word "decentralized finance" (DeFi) refers to an alternative financial infrastructure based on blockchain. DeFi uses smart contracts to create a new agreement that replicates existing financial services in a more open, interoperable, and transparent way.

The most basic concept of smart contract was proposed by Szabo in 1994. He used the concept of vending machines to further explain and believed that many agreements could be "embedded in the hardware and software in a way that allows defaulters to pay a high price for default." Buterin (2013) proposed that a decentralized blockchain-based smart contract platform can solve any trust issues related to the operating environment, thereby ensuring a safe state in whole situation. In addition, the platform allows interaction and mutual construction between contracts. This concept was further finalized by Wood (2015) and implemented in the name of Ethereum.

## History of Cross-chain Development

### 2009–2012 Single-chain development stage

This period is the budding stage of Blockchain technology. It is inspired by Bitcoin. It is widely believed that the performance optimization and technology upgrade of Blockchain can be completed in a single chain. Once the members of the chain cannot agree on the project development, only Can be solved by permanent divergence, which also lead to permanent divergence of bitcoin and other chains.

### 2012–2014 Side chain proposal

The development of Bitcoin is severely constrained by the limitations of Bitcoin in terms of block time, block size and smart contracts. With the emergence of Litecoin, BitShares and Ethereum, the Bitcoin core development team felt the crisis. In 2012, Ripple Labs proposed the Inter ledger protocol to connect different accounts and achieve synergy between them.

### 2014 Cross-chain proposal

The earliest proposal of cross-chain technology can be traced back to the BlockStream team's research on Bitcoin side chain technology in 2014. Subsequently, there are lightning network, Raiden Network application of hash time lock HTLC technology, Ripple to notary public mechanism and HTLC. The comprehensive practice of the agreement, and now Wanchain, Cosmos, Polkadot and other projects on the cross-chain platform's unremitting pursuit and practice.



## The proposal of Meta Finance

Meta is called meta in the computer field, such as Metadata. verse is the abbreviation of universe, which means to explore the reconstruction of the virtual world outside the real world, including all virtual worlds, AR and the Internet.

Looking at the payment tools we use, the core function of payment tools is "value measurement, circulation means". When the Internet industry has not yet prospered, the existing payment methods can fully meet the needs of the society. However, with the rapid development of Internet technology and related industries, the current payment function has become weak and cannot fully cover the demand of global payment. Traditional payment methods are based on centralized data storage. In the face of irreversible cyber attacks, assets will suffer infringements and losses, and centralized payment methods can easily leak personal information, making it difficult to guarantee privacy and security.

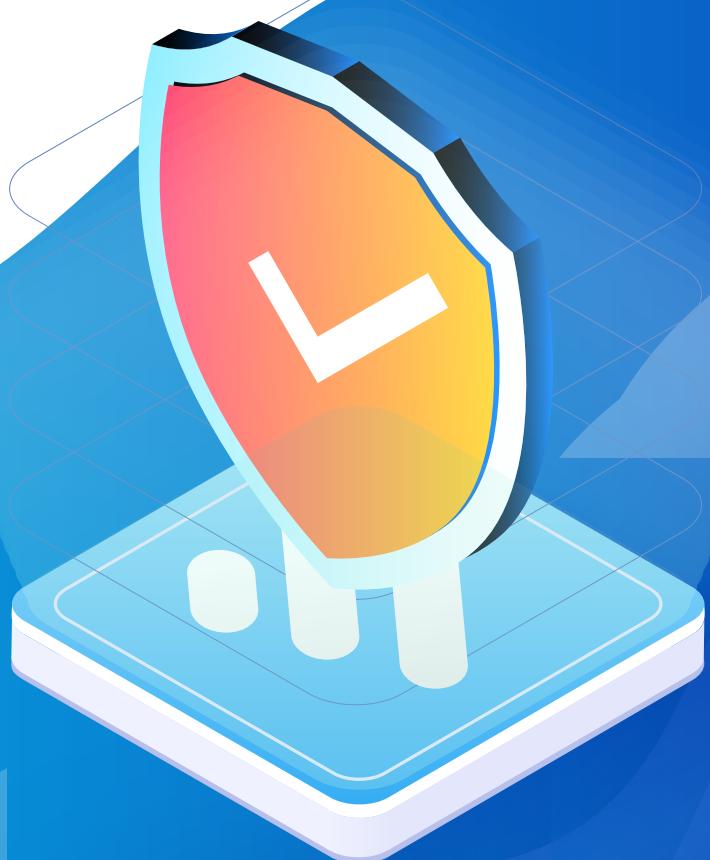
With the development of decentralized finance and cryptocurrency, payment tools that can meet the needs of the new era will follow.

In 2021, more and more communities and individuals hope to use more flexible financial payment tools to adapt to the development of the virtual meta universe. MetaPay was born.





# Vision





# Vision

The Metaverse originated from the hypothesis of American writer Neal Stephenson: through equipment and terminals, humans can enter the virtual three-dimensional "reality" of computer simulation through connections in the future. Everything in the real world is digitally copied, and people can be in the virtual world through digital identity. you can do anything in real life, and actions in the virtual world will also affect the real world.

MetaPay hopes to reconstruct mobile payment and break the cross-chain barriers of the existing payment industry. It tries to couple with various public chains and protocols. Assets on the existing BTC, ETH, DOT, ATOM, BSC, HECO, OKT, TRON chains are free trade and lightening exchanged, so as to truly realize cross-chain payment.

Meanwhile, MetaPay is committed to providing one-stop decentralized NFT technical support for diversified crypto assets, such as animation IP, artwork, collection cards, personal time or services, games, domain names, real estate, etc. that can be tokenized real or virtual "assets".

The MetaPay cross-chain payment function will provide a strong foundation for Meta NFT transactions.

As the core value of MetaPay, Mep integrates the characteristics of decentralized finance and NFT, bringing together different ecological participants, so that all participants have the opportunity to demonstrate themselves in MetaPay and participate in ecological integration.

MetaPay is committed to the infrastructure and technical support of Meta finance, applied to payment, transaction, pledge, mining, NFT transactions and other fields. At the same time, combined with a highly autonomous DAO governance solution, MetaPay hopes to enable all geeks to be efficient and low-cost use of blockchain decentralization technology, thereby creating more decentralized ecological benefits for the world.

Meta NFT is committed to building the highest quality and most active NFT community and asset trading platform to promote the liquidity and trading of global artworks, animation IP, and even NFT real estate.

Meta DAO advocates decentralized governance and community power. Code is law once became the core principle of DAO governance. However, obviously, we are not ready to enter a thorough DAO because people's consciousness and habits cannot adapt to this development. Only by allowing DAO to form a large economy of scale in the society can the development of the global DAO network be truly activated, including the improvement of corresponding governance mechanisms, tools and technologies, as well as the development of people's general awareness and habits. Meta DAO hopes to promote the role of DAO in global governance.

# MetaPay Introduction





# MetaPay Introduction

MetaPay is a safe and efficient Meta financial payment ecosystem based on the Ethereum Layer 2 expansion protocol developed by genius blockchain technology geeks. The main direction is cross-chain payment and ecological construction of virtual assets, including decentralized payment , pledge, liquidity mining, NFT aggregator, etc.

MetaPay adopts a completely decentralized DAO autonomous mechanism, and transfers the right of control to Meta DAO to achieve decentralization and creates an effective model of sustainable development. In Meta DAO, the membership of DAO is open, not limited to a specific group. DAO members/shareholders can propose and vote to decide which changes to make. There is no situation where a central agency can hinder or change its decision.

## The realization of MetaPay is mainly divided into three stages:

**The first stage:** MetaPay —— Meta financial payment ecology

**The second stage:** Meta NFT——Decentralized NFT asset transaction aggregator

**The third stage:** Meta DAO ——decentralized autonomous mechanisms

In order to allow as many audiences as possible to introduce the demand for blockchain technology to the public, the MetaPay platform will be provided in the form of a mobile application or a web page. The application will be run and maintained by the Meta team; The first phase of MetaPay will be developed based on OKT. Unlike other DeFi platforms developed on single-chain, MetaPay is multi-chain governance, and will also support ecosystems such as BSC, Heco, Polkadot, Ethereum and TRON, etc.

## MetaPay

MetaPay uses a highly scalable payment protocol based on Ethereum layer2. The decentralized network is provided by the blockchain smart contract, and the smart contract function is used to realize instant payment across the network. Flash Payment, developed by MetaPay, uses real blockchain transactions and smart contract language scripts to create a secure network which can conduct a large number of high-speed transactions.



## Meta NFT

Meta NFT aims to build the world's largest NFT asset and financial derivatives trading platform with the richest ecology and the strongest technical strength.

Meta NFT will include four major sectors: NFT Asset Exchange, On-chain Exhibition Hall, Decentralized NFT Community and NFT Pledging & Issuance Platform. In the future, Meta NFT will expand according to market demand to meet the needs of more collectors, and will support auction transactions for all NFT projects.

Meta NFT is integrating more than 100 animation IP and 1,000 global artists and collecting more than 5,000 contemporary artworks as a reserve. Meta NFT will be a bridge for communication and transactions between east and west, but also the new cradle of world art.

The Beta version of Meta NFT will display the core function of the platform---NFT asset exchange. Users will be free to trade NFT assets in Meta NFT. NFT one-stop issuance, asset management and other functions will be updated later.

## Meta DAO

MetaPay adopts the method of on-chain governance. Participants can research and formulate proposals, then vote on the proposals through the blockchain, and finally count the voting results. Initiating proposals and participating in voting will be rewarded.



# MetaPay Token

MetaPay adopts the method of on-chain governance. Participants can research and formulate proposals, then vote on the proposals through the blockchain, and finally count the voting results. Initiating proposals and participating in voting will be rewarded.

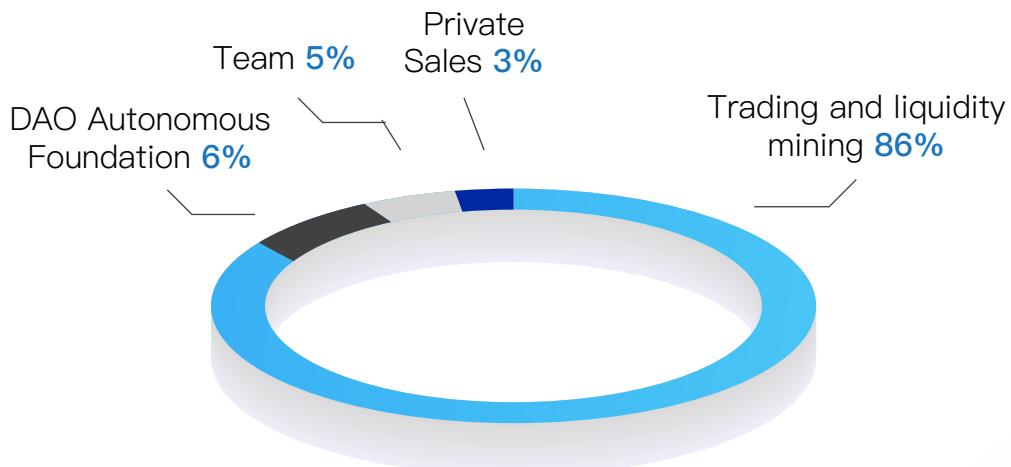
Mep is the native governance token of MetaPay. As a decentralized autonomous organization, MetaPay advocates decentralized governance and community power. The Map token incorporates the development team's expertise in token economics and blockchain governance.

Every application in MetaPay will initially run with Mep tokens. Unlike other pre-mining and ICO projects, the value of Mep tokens is directly related to its ability to provide credit for governance and financial value.

**Name of Token:** MetaPay

**Token abbreviation:** Mep

**Total of issuance:** 919,000,000



# MetaPay

# Cryptographic

# Algorithm





# MetaPay Cryptographic Algorithm

The cryptographic algorithm used by MetaPay is the discrete logarithmic encryption and elliptic curve encryption which are commonly used in modern public key crypto systems.

## Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve  $E$ , consider the primitive  $P$  and another element  $T$ . Then the DL problem is to find the integer  $d$  ( $1 \leq d \leq \#dE$ ), which satisfies:

$$\underbrace{P + P + \dots + P}_d = dP = T. \quad (9.2)$$

In the crypto system,  $d$  is usually an integer and is also a private key, and the public key  $T$  is a point on the curve with coordinates  $=(x_T, y_T)$ . The two keys in the DL problem in  $Z_p$  are integers. The operation in equation (9.2) is also called point multiplication because the result can be written as  $T = dP$ . However, this term is somewhat misleading because the integer  $d$  cannot be directly multiplied by a point  $P$  on the curve. So  $dP$  is only a simple representation of the group operation of the group operation repeated in equation (9.2).

Let's look at an example of an ECDLP.

We perform a dot multiplication on the curve  $y^2 = x^3 + 2x + 2 \pmod{17}$ . Assume that you want to calculate

$$13P = P + P + P \dots + P$$



Where  $P = (5, 1)$ . In this case, you can directly use the pre-compiled table and get the result:

$$13P=(16,4)$$

Point multiplication is similar to an exponential operation on a multiplicative group. In order to efficiently calculate the point multiplication, we can directly use the square-multiplication algorithm; the only difference is that the square becomes doubling and the multiplication becomes the addition of  $P$ . The algorithm process is as follows:

Double-and-Add algorithm in point multiplication  
Input: elliptic curve  $E$  and point  $P$  on the elliptic curve  
Scalar

$$d = \sum_{i=0}^t d_i 2^i, \text{ and } d_i \in \{0, 1\}, d_t = 1$$

Output:  $T = dP$   
initialization:  
 $T = P$   
algorithm:

```
1      FOR i=t-1 DOWNTO 0
1.1    T=T + T mod n
        IF di=1
1.2    T= T + P mod n
2      RETURN (T )
```



For a random scalar of length  $t + 1$  bits, this algorithm requires an average of  $1.5t$  point doubling and point addition. Briefly, the algorithm scans the bit representation of the scalar  $d$  from left to right and performs a double doubling in each iteration; it only performs a  $P$  addition if the current bit has a value of 1. Let's look at an example.

For scalar multiplication  $26P$ , its corresponding binary representation is: This algorithm scans each scalar bit in turn from the leftmost  $d_4$  until the rightmost  $d_0$  bit.

#0	$P=1_2P$	Initialization settings, the bits being processed are: $d_4=1$
#1a	$P+P=2P=10_2P$	DOUBLE, the bit being processed is: $d_3$
#1b	$2P+P=3P=10_2P+1_2P=11_2P$	ADD, due to $d_3=1$
#2a	$3P+3P=6P=2(11_2P) =110_2P$	DOUBLE, the bit being processed is: $d_2$
#2b		No ADD, due to $d_2=0$
#3a	$6P+6P=12P=2(110_2P) =1100_2P$	DOUBLE, the bit being processed is: $d_1$
#3b	$12P+P=13P=1100_2P+1_2P=1101_2P$	ADD, due to $d_1=1$
#4a	$13P+13P=26P=2(1101_2P) =11010_2P$	DOUBLE, the bit being processed is: $d_0$
#4b		No ADD, due to $d_0=0$

This process is a very intuitive reflection of the binary representation of the exponential transformation process. It can be seen that doubling the point will move the scalar one bit to the left and 0 to the rightmost position. Performing an addition of  $P$  inserts a 1 at the rightmost position of the scalar. Compare the way the highlighted index is transformed in each iteration.

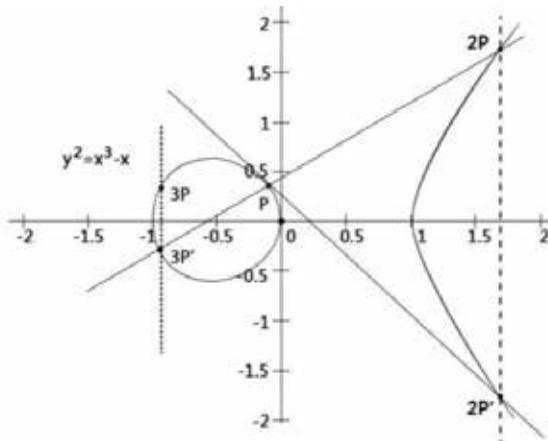


The geometric interpretation of ECDLP is also very simple:

Given a starting point P (public parameter), you can effectively calculate  $2P$ ,  $3P$ , ...,  $dP = T$  (public key) by jumping back and forth on the elliptic curve;

Then publish the starting point P and the ending point T. In order to decipher the crypto system, the attacker must figure out the frequency of “jumping” on the elliptic curve;

The number of times this jump is the password d, the private key.



## Hash function algorithm

The hash function algorithm is widely used in the chain of MetaPay.

The hash function is also called a hash function, a message digest function, and the like. Its purpose is to compress a message  $m$  of any length into data of a specified length  $H(m)$ .  $H(m)$  is also known as the fingerprint of  $m$ .

More hash function algorithms are used. For example: message authentication, pseudo-random functions, and so on.



The hash function has the following characteristics:

- I) Anti-first originality The hash function has unidirectionality, and  $H(m)$  is known. It is impossible to calculate the  $m$  value by  $H(m)$ .
- II) Violence Crack For the  $n$ -bit hash value, the exhaustive scale is 2 to the  $n$ th power.
- III) Collision Resistance The possible values for each element in the hash function are  $n^2$ , where  $n$  is the output width of  $H()$ . The number of hash operations  $t$  needed to find a conflict is expressed as a function of the hash output length  $n$  and the collision probability  $\lambda$ .

$$t \approx 2^{(n+1)/2} \sqrt{\ln\left(\frac{1}{1-\lambda}\right)}$$

For a hash function with an output length of 256 bits, to find a collision pair with a probability of success of 50%, 2129 hash calculations are required. Assuming that the computer can perform 10,000 hash calculations per second, it will take 1027 years to complete these hash calculations.

## Zero-knowledge proof of non-interactive zk-SNARKs

MetaPay uses a non-interactive zk-SNARKs zero-knowledge proof system to completely address the issue of transactions being traced to expose user privacy.

zk-SNARKs is an encryption method based on purely mathematical theory. It is the same as the nature of Blockchain. The advantage of this method is that it does not need to rely on the external operating environment to be self-contained, so it has a wide range of application scenarios.



Its basic meaning is "zero knowledge Succinct Non-interactive Argument of Knowledge", to see what they mean:

- zero knowledge: Zero knowledge, that is, does not reveal any insider in the process of proof;
- succinct: Concise, mainly means that the verification process does not involve a large amount of data transmission and the verification algorithm is simple;
- non-interactive: No interaction, technique attempts to completely avoid interactions.

In a nutshell, zk-SNARK is a kind of technology that proves that I know the inside story. It is simple and easy to operate. The most important thing is that you can get the conclusion that it is correct, and you don't know anything about the content of the message or transaction, so this process can achieve privacy and anonymous.

It is worth noting that MetaPay chose a BLS12-381 curve with a higher safety level when specifically selecting the zk-SNARK zero-knowledge proof curve.

Barreto–Naehrig curves vs Barreto–Lynn–Scott curves

The same pairing-friendly elliptic curve, BN128 and BLS 12-381 are still different.

<b>KSS curves:</b> $k = 18$ , $\rho \approx 4/3$ $p(z) = (z^8 + 5z^7 + 7z^6 + 37z^5 + 188z^4 + 259z^3 + 343z^2 + 1763z + 2401)/21$ $r(z) = (z^6 + 37z^3 + 343)/343$ , $t(z) = (z^4 + 16z + 7)/7$
<b>BN curves:</b> $k = 12$ , $\rho \approx 1$ $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ $r(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1$ , $t(z) = 6z^2 + 1$
<b>BLS12 curves:</b> $k = 12$ , $\rho \approx 1.5$ $p(z) = (z - 1)^2(z^4 - z^2 + 1)/3 + z$ , $r(z) = z^4 - z^2 + 1$ , $t(z) = z + 1$
<b>BLS24 curves:</b> $k = 24$ , $\rho \approx 1.25$ $p(z) = (z - 1)^2(z^8 - z^4 + 1)/3 + z$ , $r(z) = z^8 - z^4 + 1$ , $t(z) = z + 1$



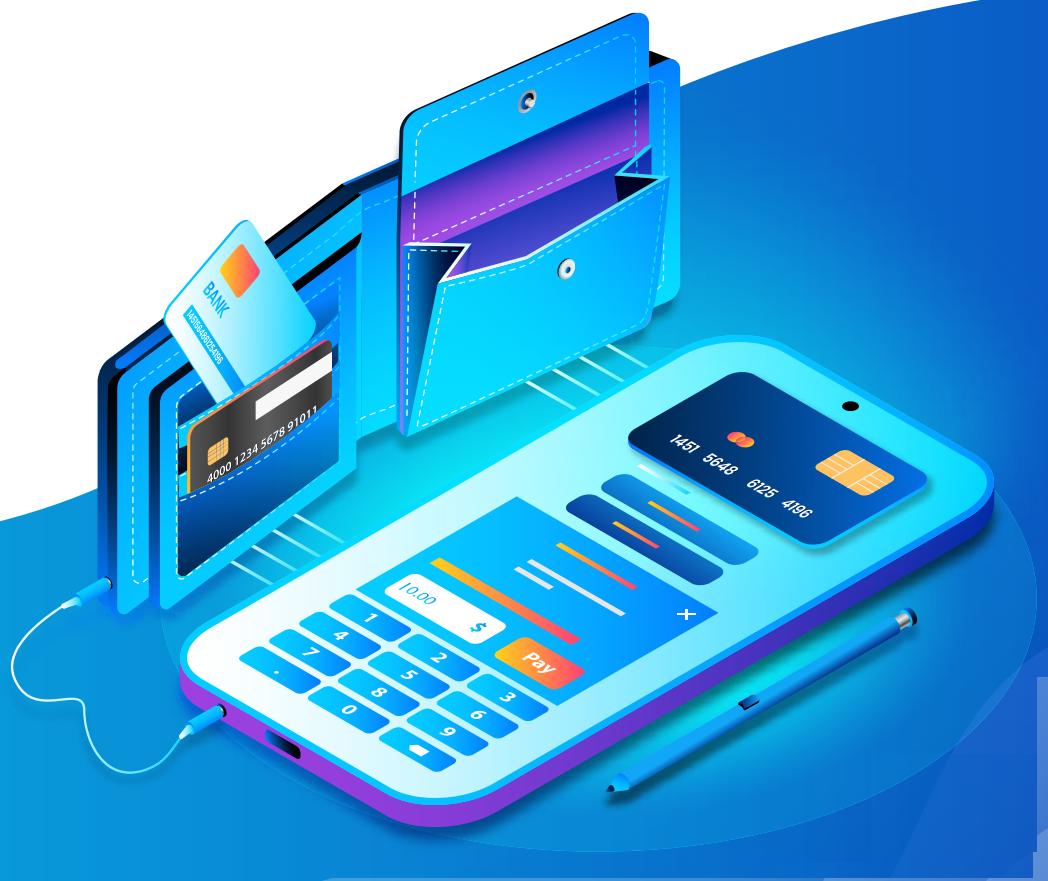
According to the corresponding parameters in the paper "Implementing Pairings at the 192-bit Security Level" are as follows:

According to the description in <https://electriccoin.co/blog/new-snark-curve/>, the BN128 curve is conservatively estimated, and the safety factor that can be achieved is only 110-bit, which is not the 128-bit security previously mentioned. To achieve 128-bit security,  $q \approx 2384$  is required, and the order  $r$  value of the corresponding BN curve will be increased to 2384. The increase of  $r$  value will affect the performance of multi-exponentiation, FFT, etc., thus affecting the execution efficiency of zk-SNARKs and secure multiparty computing also affects the unnecessary increase of key files.





# MetaPay



**MetaPay** Meta Financial Payment Ecology



# MetaPay

MetaPay adopts the Layer 2 technology based on Ethereum, and achieves a flash payment experience comparable to Internet products through expansion of the off-chain channel. In addition to the extremely fast payment experience, there is no handling fee in the off-chain channel, which effectively solves the problems of slow speed and high gas fee of the Ethereum. The decentralized network is provided by the blockchain smart contract, and the smart contract function is used to realize instant payment across the network. The Flash Payment, developed by MetaPay team, uses real blockchain transactions and smart contract language scripts to create a secure network who can conduct a large number of high-speed transactions.

It is mainly achieved through the following three aspects:

## Two-way payment channel

Two participants create a ledger entry on the blockchain, which requires the two participants to sign any fund expenditures. Both parties create transactions that return ledger entries to their respective allocations, but do not broadcast them to the blockchain. They can update the personal distribution of ledger entries by creating many transaction expenditures from the current ledger entry output. Only the latest version is valid, which is enforced by smart contract scripts that can be analyzed by the blockchain. By broadcasting the latest version to the blockchain, any party can close the entry at any time without any trust or custody.

## Lightning Network

By creating a network of two-party ledger entries, you can find a path across the network, similar to routing data packets on the Internet. The nodes on the path are not trusted because the payment is executed through a script that enforces atomicity (the entire payment succeeds or fails) by decrementing the time lock. In order to expand Lightning Network in Layer 2, MetaPay incorporates two basic protocols, RSMC (Revocable Sequential Maturity Contract) and HTLC (Hash Clocked Contract) in the transaction verification process of the underlying protocol which is to build the Fund pool on Layer 2 and the establishment of payment channels.



The Lightning Network on Layer 2 has many advantages. The first is instant determinism. As long as the signatures of all parties pass the status update, the status will be “confirmed” without waiting for block confirmation on the blockchain; Secondly, The status update is off-chain, and peer-to-peer communication can guarantee privacy. Only the final status will be submitted to the blockchain. Finally, there is a low gas fee. The Lightning Network only needs to settle and clear the fees on the blockchain when the channel is opened and closed. At other times, no matter how the two parties update in the channel, the transaction is free.

## Blockchain arbitration mechanism

It is possible to conduct transactions outside the blockchain without restrictions. It is also possible to conduct off-chain transactions with the confidence that it is executable on the blockchain. This is similar to the way one person enters into many legal contracts with others, but there is no arbitration every time a contract is signed. By making transactions and scripts parseable, smart contracts can be executed on the blockchain. Only in the case of non-cooperation, arbitration will be intervened. But for blockchain, the result is certain.

Through the above three functions, the congestion of existing Ethereum network transactions can be broken, and the optimal transaction speed of the entire network can be achieved.

Instant payment. Lightning payment, no need to worry about block confirmation time. Security is implemented by blockchain smart contracts without the need to create transactions on the blockchain for personal payments with the payment speed in milliseconds.

**Scalability.** Millions to billions of transactions can be processed through the network every second. Capacity has eliminated many traditional payment barriers. Now there is no need for a custodian to attach payment by clicking the action.

**Low cost.** Through the transaction and settlement off-chain, the Lightning Network can achieve extremely low fees, which can be used for emerging use cases, such as instant micropayments.

**Cross-chain.** Cross-chain atomic swaps can happen immediately off-chain through heterogeneous blockchain consensus rules. As long as the chain can support the same password hashing function, transactions can be carried out across blockchains without trusting a third-party custodian.



## Implementation

We use the transfer path of three people to explain the working principle of MetaPay Layer 2:

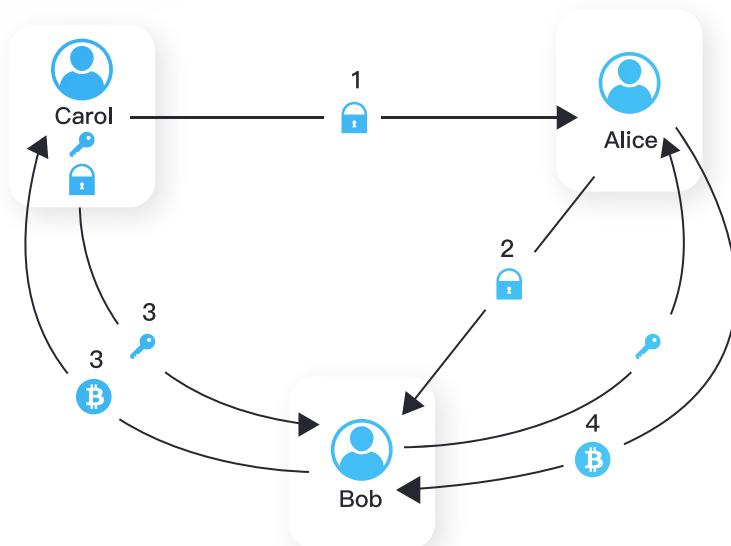
Carol, Alice and Bob are the three parties to the transaction. Alice and Bob have established "Alipay" payment channels, and Bob and Carol have established "WeChat" payment channels. If Alice wants to conduct a transaction with Carol, there are two schemes. The first is to establish an "Apple" payment channel between Alice and Carol, and the other is to bridge the payment through Bob through Alice and Carol. Both parties to any transaction need to establish a one-to-one channel, which will obviously bring a lot of trouble. Lightning Network supports intermediaries to bridge the establishment of payment channels. The steps are as follows:

1. Alice wants to pay Carol in cash and has to bridge the payment through an intermediary. But the intermediary is not necessarily reliable, so Carol and Alice agreed on a "puzzle". If the "answer" received by Alice from Bob can solve the "puzzle", it means that Bob has really given the funds to Carol.
2. Alice gives Bob the "puzzle" and transfer information.
3. Bob and Carol negotiate the transfer. If Carol tells Bob the "answer", Bob will transfer the money to Carol. This is actually the same as entering a secret to make a payment.
4. Alice and Bob make the same negotiation transfer. If Bob tells Alice the "answer", Alice transfers the money to Bob.

It should be noted that the sequence of steps 3 and 4 is that Bob advances the funds first, and then Alice gives the funds to Bob. In other words, Alice needs to pay Carol and needs to use the funds on the entire value transmission path. When there was only one middleman, Bob, both Alice and Bob's funds were used passively. If there are 10 intermediaries, then the amount of funds used is 11 times that of Alice's direct payment to Carol.



🔒 Hash    🔑 Value



MetaPay Layer 2 solution hopes to find a balance among the following three:

### Scalability:

Adding a participant/node will increase the overall network performance.



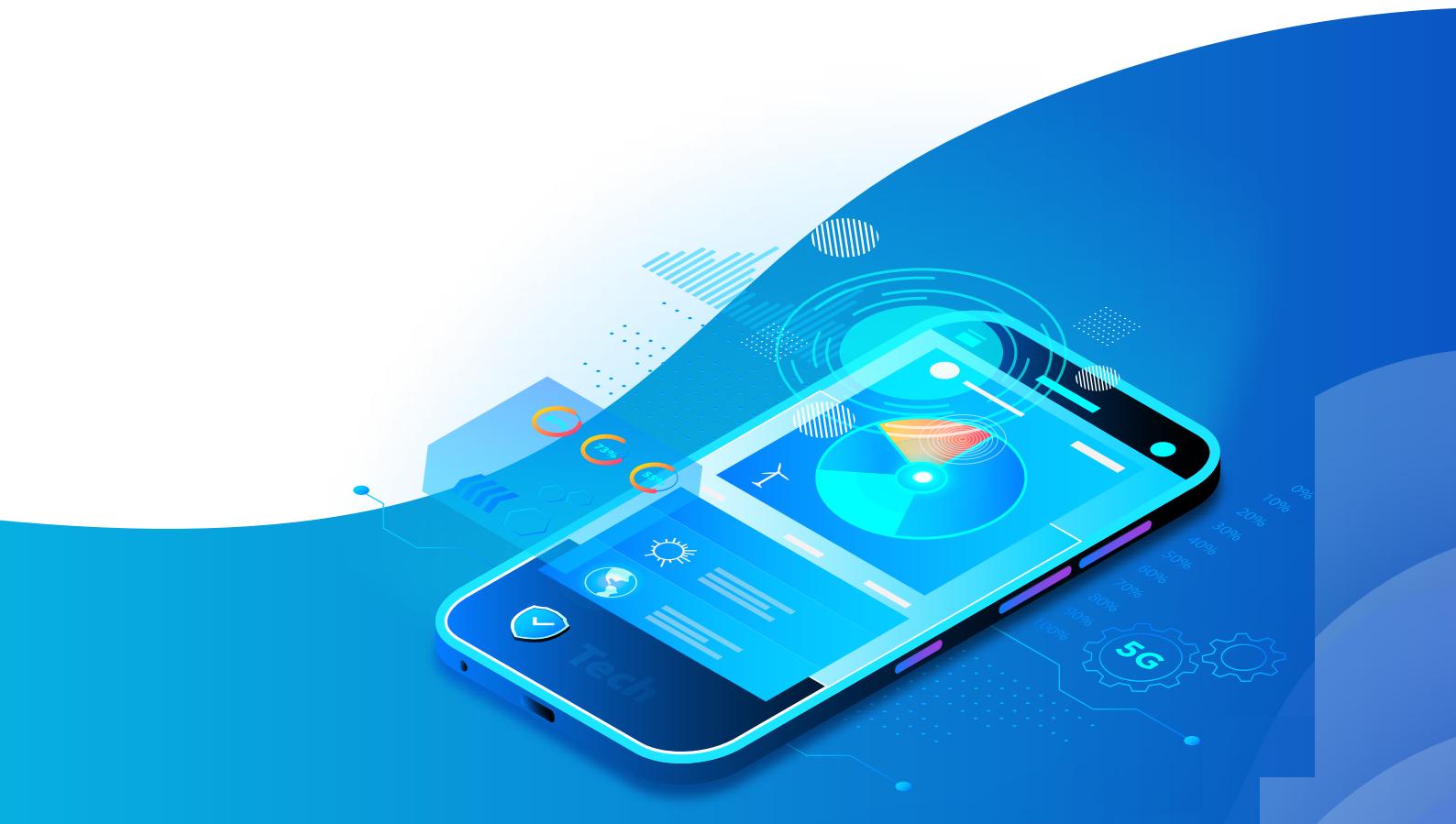
### Availability

Users need to stay online once within a specified period of time.

### Liquidity

The two parties involved in the transaction and the intermediate nodes need to bet a large amount of funds on the Layer 1.

# Meta NFT





# Meta NFT

Currently, many projects are exploring the financial properties and derivatives of NFT assets, such as NFT fragmentation transactions and NFT mortgage lending.

How NFT products be priced? And why do most of the NFT assets have a premium part?

NFT value = Intrinsic Value + Utility Value + Premium

The premium of NFT assets = protection of rights brought by smart contracts + economic incentive mechanism brought by blockchain + interoperability brought by blockchain

The incentive mechanism and interoperability of smart contracts and blockchains are important sources of NFT asset premiums.

The use NFT cases cover real or virtual “assets” that can be tokenized, such as artworks, collection cards, personal time or services, game projects, real estate and domain names.

The reason why NFT is attractive in so many fields is because of its uniqueness, scarcity, provability of ownership, transferability and indivisibility. NFT technology embeds metadata, which can be used to prove authenticity. The number of NFTs can be limited by coding, ownership can be proven on the blockchain, and item transfer can be realized with just a click of a button.



## Meta NFT Features

### Ownership

Meta NFT uses unique blockchain traceability technology for ownership tracking and protection.

### Transferability

In Meta NFT, any asset that can be tokenized can be freely transferred.

### Authenticity

Blockchain technology ensures the authenticity of the NFT assets of the transaction and prevents fraud.

### Uniqueness

Meta NFT adopts the ERC721 Non-Fungible asset standard to ensure the uniqueness of assets.

## Implementation

The Beta version of Meta NFT will display the core function of the platform---NFT asset exchange. Users will be free to trade NFT assets in Meta NFT. NFT one-stop issuance, asset management and other functions will be updated later.

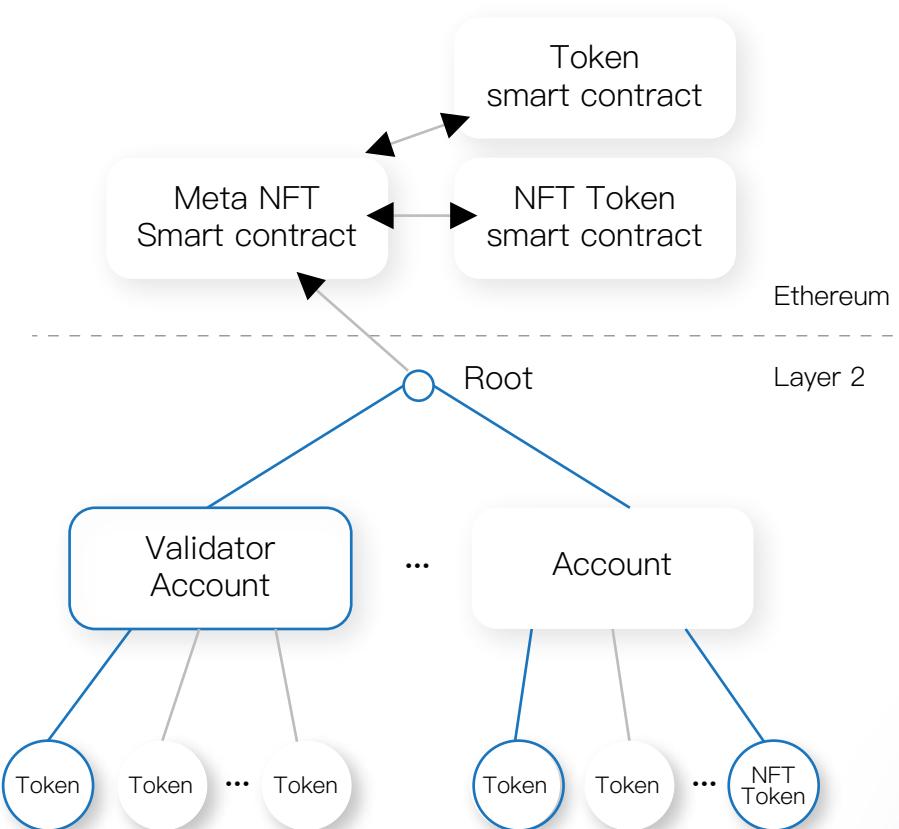
Each NFT asset release and transaction event can include asset title and detailed description to provide more information about the event. For those who want to transmit information at the blockchain level, we include them. The default assets in the system must reach a minimum threshold, and there is no maximum amount. The amount is determined by both parties freely. If the seller's minimum goal is not reached during the transaction, the user can withdraw his funds by interacting with the smart contract. Since the token address parameter is specified when creating a proposal, our smart contract can usually be used with any token. On our platform, we may use Mep and require creators and owners to use Mep to drive demand.



## Minting Custom Coins

Users can directly create NFTs in Meta NFT Layer 2, and the changes in the state of the world in the system are similar to recharging NFTs. Web, Mobile App and API-based user interfaces to the Mint smart contract will be developed to make asset creation and management a simple process. The following parameters define a new custom asset:

- Name
- Icon
- Maximum Supply
- Decimal Places
- Exchange Rate
- Access List
- Data





## Community integration

Mep features will be integrated across the entire MetaPay platform and natively supported by over 450,000 existing gaming websites.

Going past the system, MetaPay will develop phpCB, McBulletin and other forum and integrations as part of the open-source Platform API that will allow even more internet communities to easily adopt Mep into their websites and games.

The following functions will be included:

### Rewards Automations

The existing automation system on the MetaPay Platform can reward tokens to user accounts based on powerful combinations of conditions and triggers. Various reward system can be setup for user participation on the forum and other website activities.

### Forum Boards

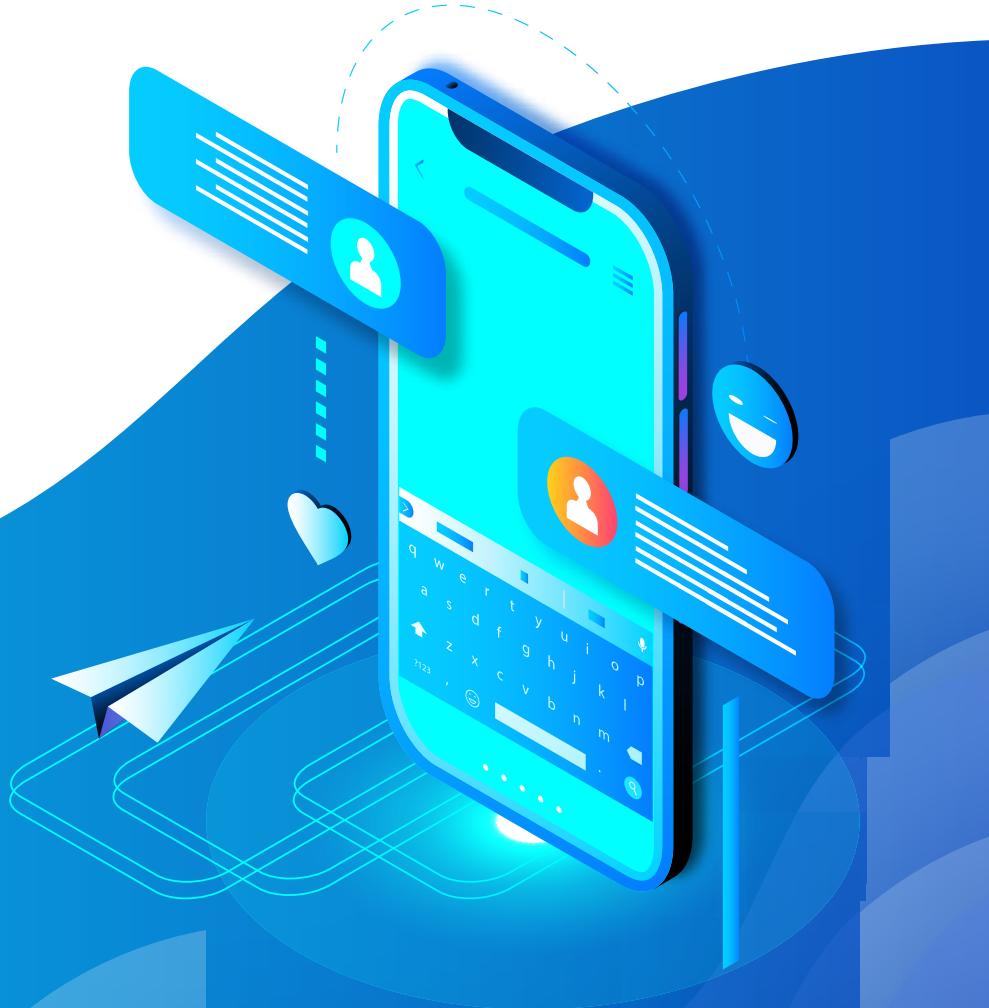
The MetaPay includes an incredibly feature-rich forum system, currently powering everything from small teams to giant communities with over a million users participating on their message boards. Forum votes and points will be extended with the ability to display Custom Tokens. Tipping will be added to the Forums so that coins can be tipped to users with a few simple clicks (and this action would be displayed on the thread).

### Donation & Group Pay

Many websites accept donations instead of using a store – especially smaller eSports clans or guilds made up of friends. Meps will now be a payment option in the Donation module and Stretch Goals.

As a representative of the new generation of Layer 2 technology, Meta NFT has achieved zero gas fee transfers and transactions on the second-layer network through Rollups technology, and has done a lot of optimization work in the field of zero-knowledge proof, realizing the rapid withdrawal from Layer 2 to Layer 1. Meta NFT's Layer 2 NFT protocol will solve the shortcomings of expensive issuance and slow transfer in the NFT field. At present, NFT platforms based on Ethereum can seamlessly switch to the Layer 2 protocol, thereby achieving 0 Gas issuance and transfer of NFT, and no transaction capacity limitation. In the future, Meta NFT will continue to promote the development of the Layer 2 protocol layer and provide Layer 2 infrastructure for more fields, such as Layer 2 stable coins and Layer 2 lending protocol.

# Meta DAO





# Meta DAO

## Definition

In order to build a decentralized network with extensive influence and high retention, ecological construction will become the core of the MetaPay. With the aid of the DAO organizational structure, a fair and efficient ecological construction framework will be established. Mep is the first sustainable DeFi token that incorporates the elements of proof of equity into its powerful DAO representative governance model.

## Mep Global Governance Model

Mep holders can voluntarily participate in the Mep Global Governance Model, and Mep serves as the proof of stake of representative governance. Under the Mep PoS ecosystem, MetaPay candidates for the council will run for community council. Community directors will serve on the MetaPay Representative Council and have the ability to make suggestions or vote on Meta DAO changes. Reaching a consensus requires the approval of a majority of the community directors.

## Implementation

**Equity-weighted Voting:** Voting in the Mep Global Governance Model is equity-weighted, that is, its final statistical voting results will be based on the amount of tokens held instead of the number of nodes.

**The structure of MetaPay Represents:** Numbers of members are between 11–21, and the number of personnel is odd, depending on community votes. Representatives in MetaPay Represents have different duties, including execution, supervision and review, financial management, and overall operation. Members of MetaPay Represents must pledge a certain amount of tokens as a disciplinary cost for possible improper behavior.

**Planning and Proposals:** Mep holders (amount greater than 10,000) can publish Punk-related proposals, including but not limited to financial or technical support for ecological applications, main network technology upgrades, online and offline marketing activities planning, etc. All aspects of the operation of a decentralized project are welcome.

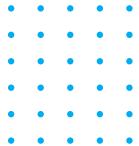


**Release and Voting:** If the total number of supported tokens exceeds 10,000, it can be released for voting. If the number of support votes exceeds 50%, the proposal will enter the feasibility analysis stage.

**Feasibility Analysis:** The MetaPay Representative Council will analyze the feasibility from various perspectives (including finance, legal affairs, practicality, difficulty of implementation, short, medium and long-term value, etc.), and vote, and more than half can enter the implementation stage. The feasibility analysis report needs to be published to public.

**Execution:** The MetaPay Representative Council will be responsible for the implementation of operations, control, and docking of partners. Ecological supporters such as OKT will be given priority for cooperation.

**Monitoring and review:** All MetaPay holding nodes can participate, and MetaPay Representative is responsible for publicizing the proposal implementation process and results.



# Roadmap





# Roadmap





# References

- [1] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell; Enabling Blockchain Innovations with Pegged Sidechains;2014.10.22
- [2] Vitalik Buterin; Chain Interoperability;14,9,2016
- [3] BitCoin Timelock; <https://en.bitcoin.it/wiki/Timelock#Relativelocktime>
- [4] Hashed-Timelock Agreements (HTLAs); <https://interledger.org/rfcs/0022-hashed-timelock-agreements/#simple-payment-channels>
- [5] MONACO J V. Identifying Bitcoin users by transaction behavior[C]//The SPIE DSS, April 20–25, 2015, Baltimore, USA. Baltimore: SPIE, 2015.
- [6] GENNARO R, GENTRY C, PARNO B, et al. Quadratic span programs and succinct NIZKs without PCPs [C]//The 32nd Annual International Conference on the Theory & Applications of Cryptographic Techniques, May 26–30, 2013, Athens, Greece. [S.l.:s.n.], 2013: 626–645.
- [7] PARNO B, HOWELL J, GENTRY C, et al. Pinocchio: nearly practical verifiable computation[C]//The 2013 IEEE Symposium on Security & Privacy, May 19–22, 2013, San Francisco, USA. Washington, DC: IEEE Computer Society, 2013: 103–112.
- [8] REID F, HARRIGAN M. An analysis of anonymity in the Bitcoin system[C]//The 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust, October 9–11, 2011, Boston, USA. Piscataway: IEEE Press, 2011: 1318–1326.
- [9] ANDROULAKI E, KARAME GO, ROESCHLIN M, et al. Evaluating user privacy in Bitcoin[C]//The 17th International Conference on Financial Cryptography and Data Security, April 1–5, 2013, Okinawa, Japan. Heidelberg: Springer, 2013: 34–51.
- [10] CHAUM D. Untraceable electronic mail, return addresses and digital pseudonyms[J]. Communications of the ACM, 2003: 211–219.



- [11] Johnny Dilley, Andrew Poelstra, Jonathan Wilkins, Marta Piekarska, Ben Gorlick, Mark Friedenbach, Strong Federations: An Interoperable Blockchain Solution to Centralized Third Party Risks, 2017.1.
- [12] J. Aspnes, C. Jackson, and A. Krishnamurthy, Exposing computationally-challenged Byzantine impostors, Tech. Report YALEU/DCS/TR-1332, Yale University, 2005, <http://www.cs.yale.edu/homes/aspnes/papers/tr1332.pdf>.
- [13] Merkle tree: <https://brilliant.org/wiki/merkle-tree/>
- [14] Whitepaper of ELA: [https://www.elastos.org/wp-content/uploads/2018/White%20Paper/elastos\\_sidechain\\_whitepaper\\_v0.3.0.6\\_ZH.pdf?\\_t=1526918341](https://www.elastos.org/wp-content/uploads/2018/White%20Paper/elastos_sidechain_whitepaper_v0.3.0.6_ZH.pdf?_t=1526918341)
- [15] Whitepaper of Cosmos: <https://github.com/cosmos/cosmos>
- [16] DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]// The 12th Annual International Cryptology Conference on Advances in Cryptology, August 16–20, 1992, Santa Barbara, USA. Piscataway: IEEE Press, 1992: 139–147.
- [17] Whitepaper of Bytom: <https://bytom.io/wp-content/themes/freddo/-book/BytomWhitePaperV1.1.pdf>
- [18] Joseph Poon, Vitalik Buterin, Plasma: Scalable Autonomous Smart Contracts, 2017.8
- [19] Anna Osello, Andrea Acquaviva, Daniele Dalmasso, BIM and Interoperability for Cultural Heritage through ICT, 2015
- [20] Whitepaper of Wanchain <https://wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf>
- [21] SHENTU Q C, YU J P. A blind-mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm[J]. Computer Science, 2015.
- [22] Whitepaper of Polkadot: 《POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK DRAFT 1》



# Laws & Regulation

Certain parts of MetaPay Lending business are subject to state and federal regulations in the United States, as well as foreign laws and regulations. Loans arranged through the MetaPay platform are provided by SEC registered investment advisors or other board-registered banking entities.

MetaPay Lending Holdings, Inc. and loans provided through the MetaPay platform must comply with applicable state and federal lending and usury laws, such as the Federal Consumer Credit Protection Act, the Loan Truth Act, and the Equal Credit Opportunity Act , Fair Debt Collection Act, Dodd–Frank Wall Street Reform and Consumer Protection Act, Service Personnel Civil Relief Act, Military Loan Act, Bank Secrecy Act, American Patriot Act , Electronic Funds Transfer Act, Global and National Commerce Act (ESIGN) in electronic signatures and other federal and state laws regarding privacy, data security and prohibiting unfair or deceptive business practices.

As a non-bank entity, MetaPay Lending Holdings, Inc. and its affiliate MetaPay Platform have developed a wide range of best practice policies and procedures designed to ensure compliance with laws and regulations.

MetaPay Lending Holdings, Inc. and its affiliate MetaPay Platform may be subject to inspection, supervision and other regulatory enforcement measures by national agencies responsible for monitoring consumer credit, trade, and commerce; and responsible for the administration of the US federal consumer protection law, trade and commercial federal agencies, such as the Consumer Financial Protection Agency and the Federal Trade Commission.