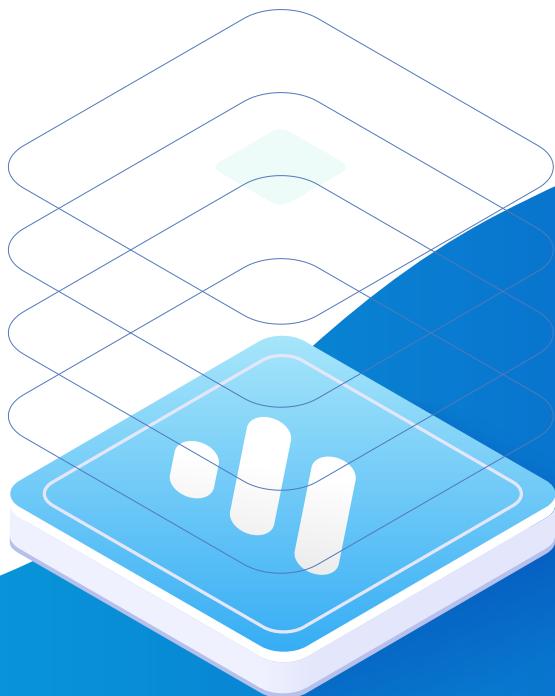


MetaPay



元金融支付生态

元金融支持的NFT交易平台



目录

序	3
背景	4
DeFi发展	5
跨链发展史	5
Meta Finance元金融的提出	6
愿景	7
MetaPay 介绍	9
Meta Pay	10
Meta NFT	11
Meta DAO	11
MetaPay 令牌	12
MetaPay 密码学	13
椭圆曲线离散对数问题(ECDLP)	14
杂凑函数算法	17
非交互式的zk-SNARKs的零知识证明	18
MetaPay	19
实施方案	24
Meta NFT	26
Meta NFT 特点	28
实施方案	28
铸造自己的NFT资产	29
社区联动推动市场需求	30
Meta DAO	31
定义	32
Mep全球治理模型	32
实施方案	32
路线图	33
参考文献	35
法律法规	37



序

随着“互联网+”的不断升级以及大众生活品质追求的不断提升，中心化规模化的公司型商业和企业生产正在趋向衰退，极致化、生态化的多维竞争时代正在到来，需求细分，业务拆分正在日益深化，组织模式势必由单一垂直管控型走向网状化、平台化，个体将得到更多的赋权赋能。

据一份调查显示，千禧一代更能够接受新兴的行业动态。尽管他们此举有着各自的想法和动机，但是他们普遍看好并支持开源的分布式区块链不断向前发展。

加密算法、区块链和去中心化金融可能是过去500年和未来100年最重要的发明，要真的实现以中本聪为代表的自由主义者的信仰乌托邦不是不可能，但过程一定曲折。

而最有可能达到自由主义这一里程碑的是通过去中心化金融——DeFi (Decentralized Finance)。我们目前认为DeFi只是一些智能合约，其实DeFi的含义远远超出智能合约。

DeFi可以是任何去中心化的金融协议，比如去中心化借贷、支付、质押、挖矿、NFT聚合器等等。

未来DeFi的落地，必须要开发出支持持续管理、决策制定及像代码执行那样落实协定的工具。



背景





背景

DeFi 发展

“去中心化金融”(DeFi)一词，指基于区块链的替代性金融基础设施。DeFi利用智能合约创造了新协议，该协议以更开放、更具互相操作性、更透明的方式复制了现有金融服务。

最基础的智能合约概念是由Szabo (1994) 提出的。Szabo (1997)用自动售货机的概念来进一步解释并认为许多协议能“以一种让违约者支付高昂违约代价的方式，嵌入到我们使用的硬件和软件中。” Buterin (2013) 提出，一个去中心化的基于区块链的智能合约平台能解决任何关乎操作环境的信任议题，从而确保了安全的全局状态。此外，平台允许合约间互动和互相搭建（可组合性）。此概念被Wood (2015) 进一步定型并用以太坊的名义落地。

跨链发展史

2009年-2012年 单链发展阶段

这个时期是区块链技术的萌芽阶段，受比特币思想启发，行业内普遍认为区块链的性能优化和技术升级完全可以在单一链上完成，一旦链内成员就项目发展无法达成一致，只能通过硬分叉来解决，这也为比特币及其他链频繁出现分叉埋下了伏笔。

2012年-2014年 侧链提出

正因为比特币在出块时间、区块容量还有智能合约方面的限制，比特币的发展受到了严重的制约。而随着莱特币、比特股和以太坊的出现，比特币核心开发组感受到了危机。瑞波实验室在2012年曾提出Interledger协议旨在连接不同账本并实现它们之间的协同。

2014年 跨链提出

跨链技术最早方案提出者可以追溯到2014年BlockStream团队对比特币侧链技术的研究，随后相继有了闪电网络、雷电网络对哈希时间锁HTLC技术的应用，Ripple对公证人机制以及HTLC等协议的综合实践，再到现在Wanchain、Cosmos、Polkadot等项目对跨链平台不懈的追求与实践。



Meta Finance 元金融的提出

Meta在计算机领域称之为元，如Metadata元数据，verse是宇宙universe的缩写，意为探讨在现实世界外重建虚拟世界。包括所有虚拟世界、AR和互联网。

纵观我们使用的支付工具，支付工具的核心功能是“价值衡量，流通手段”，在互联网产业还未兴盛和繁荣时，现有支付方式充分发挥这八个字的职能，并完全满足社会需求。但随着互联网技术及相关联产业的高速发展，在全球经济一体化的前提下，支付功能出现疲态，无法全面覆盖全球支付需求面。传统的支付方式都是基于中心化数据存储完成的，在面临不可逆转的网络攻击时，资产将遭受侵害和损失，并且中心化支付方式极易泄露个人支付信息，难以保证交易隐私和安全。

随着去中心化金融及虚拟货币的发展，能够承载新时代需求的支付工具也随之而来。

2021年，越来越多的社区及个人希望可以使用更灵活的金融支付工具以适用虚拟元宇宙的发展。MetaPay由此产生。



愿景





愿景

Metaverse元宇宙缘起美国作家Neal Stephenson的假设：未来通过设备与终端，人类可以通过连结进入计算机模拟的虚拟三维“现实”，现实世界的所有事物都被数字化复制，人们可以通过数字分身在虚拟世界中做任何现实生活中的事情，虚拟世界的行动还会影响现实世界。

MetaPay元金融希望重构移动支付，打破现有支付行业的跨链壁垒，它试图与各公链、各协议耦合，在现有的 BTC、ETH、DOT、ATOM、BSC、HECO、OKT、TRON等不同链上的资产都实现自由交易及闪电兑换，从而真正实现跨链支付。

同时，MetaPay致力于为多元化的资产提供一站式去中心的NFT技术支持及交易流转，包括动漫IP、艺术品、收藏卡、个人时间或服务、游戏项目、域名等可以代币化的真实或虚拟“资产”。

MetaPay跨链支付功能将会为Meta NFT 交易提供强大的支付基础。

Mep作为MetaPay 的核心价值体现，融合了去中心化金融和NFT的特点，将不同的生态参与者汇聚一堂，让所有参与者有机会在MetaPay 施展自己并落地参与生态融合。

MetaPay 致力于元金融的基础设施及技术支持，应用于支付、交易、质押、挖矿、NFT交易等领域，同时，结合了高度自治的DAO治理方案，MetaPay 希望让所有极客们能够高效并且低成本使用区块链去中心化技术，从而为世界创造更多去中心化的生态红利。

Meta NFT致力于打造最优质、最活跃的NFT社区及资产交易平台，从而推动全球艺术品、动漫IP，甚至是NFT房产的流转及交易。

Meta DAO 倡导去中心化治理和社区力量，Code is law 一度成为DAO治理的核心准则，但是，显然，我们还没准备好进入彻底的DAO，这是因为人们的意识和习惯还无法适应这种发展。只有让 DAO 在社会范围形成规模效应，才能真正激活全球化 DAO 网络的发展，包括相应的治理机制、工具和技术的完善，以及人们普遍意识和习惯的养成。Meta DAO希望可以推动DAO在全球治理中发挥的作用。

MetaPay 介绍



MetaPay 元金融支付生态



MetaPay介绍

MetaPay是由天才级的区块链技术极客开发的基于以太坊Layer 2扩展协议搭建的安全高效元金融支付生态，主要方向是做虚拟资产的跨链支付与生态搭建，包括去中心化支付、质押、流动性挖矿、NFT聚合器等。

MetaPay采用完全去中心化的DAO自治机制，将控制权交给Meta DAO来实现真正的去中心化，创建出一个可持续发展的有效模型。在Meta DAO内，DAO的成员资格是开放的，不仅限于某个特定群体内部。DAO的成员/股东可以提议、投票决定要做出哪些变动，不存在有某个中央机构能够阻碍或更改其决策的情况。

MetaPay 的实现主要分三个阶段：

第一阶段：MetaPay ——元金融支付生态

第二阶段：Meta NFT——去中心化NFT资产交易聚合器

第三阶段：Meta DAO ——去中心化自治组织

为了使尽可能多的受众接触并向公众介绍对区块链技术的需求，Meta 平台将以移动应用程序或者网页端的形式提供。该应用程序将由Mep团队运行和维护；第一阶段的MetaPay 将会基于OKT开发，和其他单链治理的DeFi平台不同的是，MetaPay 是多链治理，后期还将支持BSC、Heco、波卡、以太坊、波场等多个生态。

Meta Pay

MetaPay的支付采用了在以太坊layer2基础上的高扩展性支付协议。由区块链智能合约提供去中心化的网络，使用智能合约功能来实现跨参与者网络的即时付款。MetaPay自行研发的Flash Payment，通过使用真实的区块链交易并使用智能合约语言脚本，可以创建一个安全的参与者网络，这些参与者能够进行大量、高速的交易。



Meta NFT

Meta NFT 旨在打造全世界规模最大，生态最丰富，技术实力最强的 NFT 资产及其金融衍生品交易平台。

Meta NFT 旨在打造全世界规模最大，生态最丰富，技术实力最强的 NFT 资产及其金融衍生品交易平台。

Meta NFT 将会包含 NFT 资产交易所、链上展览馆与去中心化社区 NFT Community、NFT 资产质押借贷平台与多元化 NFT 发行平台四大板块。在未来，Meta NFT 将会根据市场需求进行扩容，满足更多对 NFT 资产感兴趣的收藏家们的需求，将会支持所有NFT项目的拍卖交易。

Meta NFT 正在整合超过100个全球动漫IP、1000名全球艺术家，收集5000多幅当代作品作为储备库。Meta NFT 不仅会成为东方艺术与西方世界沟通与交易的桥梁，同时也会成为世界艺术运动与思潮的发源地。

Meta NFT 的 Beta 版本将开放平台的核心功能---NFT 资产交易所，彼时用户将可以自由地在 Meta NFT 中交易 NFT 资产。NFT 一站式发行、资产管理、等功能将在随后更新。

Meta DAO

MetaPay 采取链上治理的方式，参与者可以研究并制定提案，然后通过区块链对提案进行投票，最后统计投票结果。发起提案、参与投票都会得到奖励。



MetaPay 令牌

MetaPay 采取链上DAO治理的方式，参与者可以研究并制定提案，然后通过区块链对提案进行投票，最后统计投票结果。发起提案、参与投票都会得到奖励。

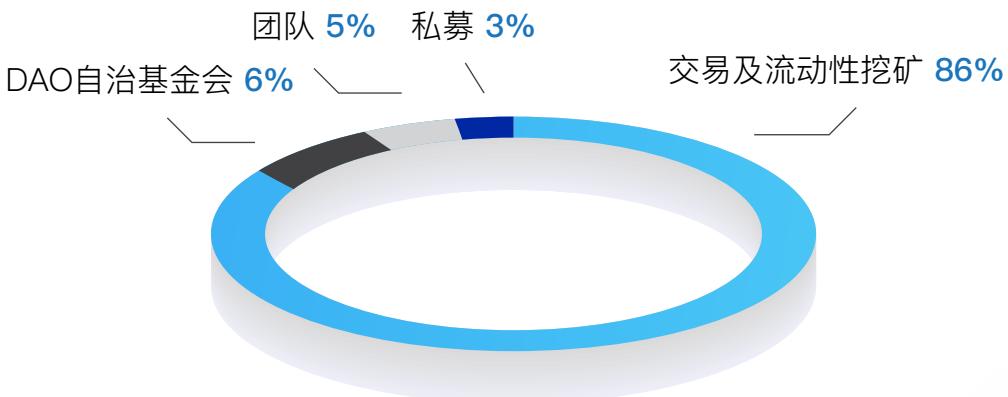
Mep是MetaPay的原生治理代币。作为一个去中心化自治组织，MetaPay 倡导去中心化治理和社区力量。Mep 代币融合了开发团队在代币经济学和区块链治理方面的专业知识。

Meta APP和将来的Web应用程序中的每个平台最初都将使用 Mep 令牌运行。与其他预挖矿和ICO项目不同，Mep 令牌的价值直接与其提供治理和财务价值的信贷的能力直接相关。

通证全称：MetaPay

通证简称：Mep

总发行量：919,000,000 枚



MetaPay 密码学



MetaPay 元金融支付生态



MetaPay密码学

MetaPay使用的密码学算法是现代公钥加密系统中常用的离散对数加密和椭圆曲线加密。

椭圆曲线离散对数问题(ECDLP)

给定一个椭圆曲线E，考虑本原元P 和另一个元素T。则DL问题是找到整数d ($1 \leq d \leq \#E$)，满足：

$$\underbrace{P + P + \dots + P}_{d \text{次}} = dP = T. \quad (9.2)$$

在密码体制中，d 通常为整数，也是私钥，而公钥 T 是曲线上的一点，坐标为 (x_T, y_T) 。而Zp 内DL问题中的两个密钥都是整数。等式(9.2) 中的操作也称为点乘法，因为其结果可以记作 $T = dP$ 。但是，这个术语有一定的误导性，因为整数d 与曲线上的一点P 无法直接相乘。所以dP仅是对等式(9.2) 中重复应用的群操作的一个简单表示符号3。

下面来看一个ECDLP的例子。

我们对曲线 $y^2=x^3+2x+2 \bmod 17$ 执行一个点乘。假设要计算

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



其中 $P = (5, 1)$ 。这种情况下可以直接使用预先编译好的表，得到结果为：

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

点乘类似于乘法群上的指数运算。为了高效地计算点乘，我们可以直接使用平方-乘算法；唯一的区别在于，平方变成了点加倍(doubling)，乘法变成了 P 的加法。算法过程如下：

点乘中的Double-and-Add算法

输入：椭圆曲线 E 及椭圆曲线上的点 P

标量

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

输出： $T = dP$

初始化： $T = P$

算法：

```
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 )
```



对于一个长度为 $t + 1$ 位的随机标量，此算法平均需要 $1.5t$ 次点加倍和点加法。简单地讲，该算法从左到右依次扫描标量 d 的位表示，并在每次迭代中执行一个点加倍；只有当前位的值为1 时，它才会执行一个P 的加法。下面来看一个示例。

对于标量乘法 $26P$ ，它对应的二进制表示为：

此算法从最左边的 d_4 开始依次扫描各个标量位，直到最右边的 d_0 位为止。

#0	$P=1_2P$	初始化设置， 被处理的位为： $d_4=1$
#1a	$P+P=2P=10_2P$	DOUBLE, 被处理的位为： d_3
#1b	$2P+P=3P=10_2P+1_2P=11_2P$	ADD, 因为 $d_3=1$
#2a	$3P+3P=6P=2(11_2P) =110_2P$	DOUBLE, 被处理的位为： d_2
#2b		没有ADD, 因为 $d_2=0$
#3a	$6P+6P=12P=2(110_2P) =1100_2P$	DOUBLE, 被处理的位为： d_1
#3b	$12P+P=13P=1100_2P+1_2P=1101_2P$	ADD, 因为 $d_1=1$
#4a	$13P+13P=26P=2(1101_2P) =11010_2P$	DOUBLE, 被处理的位为： d_0
#4b		没有ADD, 因为 $d_0=0$

这个过程非常直观地反映了指数的二进制表示变换的过程。从中可以看出，点加倍会使标量向左移动一位，并在最右边的位置填上0 。执行一个P 的加法则会在标量最右边的位置上插入一个1 。请比较高亮显示的指数在每轮迭代中的变换方式。

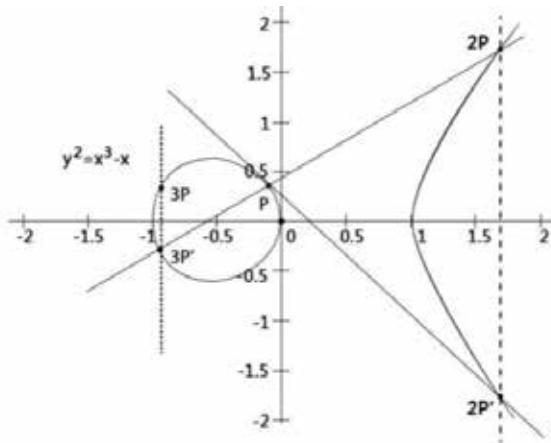


ECDLP的几何解释也非常简单：

给定一个起点P（公开参数），可以通过在椭圆曲线上来回跳跃，有效地计算 $2P$, $3P$, ..., $dP = T$ （公钥）；

然后发布起点P 和终点T。为了破译密码体制，攻击者必须弄清楚在椭圆曲线上“跳跃”的频率；

而这个跳跃的次数就是密码d，即私钥。



杂凑函数算法

在链中广泛使用了杂凑函数算法。

杂凑函数又称为Hash函数、报文摘要函数等。其目的是将任意 长度的报文m压缩成指定长度的数据 $H(m)$ 。 $H(m)$ 又称为 m 的指纹。

中使用了较多的杂凑函数算法。例如：消息认证、伪随机函数等。



杂凑函数有以下特性:

I)抗第一原像性 杂凑函数具有单向性, 已知 $H(m)$, 试图通过 $H(m)$ 计算 m 值是不可能的。

II)暴力破解 对于 n 位的 hash 值, 穷举的规模是 2 的 n 次方。

III)抗碰撞性 哈希函数中每个元素对应的可能值为 n^2 个, 其中 n 为 $H(\cdot)$ 的输出宽度。寻找一个冲突所需哈希操作 t 的数目表示为哈希输出长度 n 和冲突概率 λ 的函数。

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

对于输出长度为 256 位的哈希函数, 要找到碰撞对成功概率为 50%, 需要 2129 次哈希计算。假设计算机每秒能进行 1 万次哈希计算, 则需要 1027 年才能完成这些哈希计算。

非交互式的zk-SNARKs的零知识证明

MetaPay 采用了非交互式的 zk-SNARKs 的零知识证明体系, 目的是彻底解决交易被追踪从而暴露用户隐私的问题。

zk-SNARKs 是基于纯数学理论实现的加密手段, 和区块链的本质一样, 这种方式的好处在于使用它不需要依赖外部的运行环境而自成体系, 因而具备十分广泛的应用场景。



它的基本含义是“zero knowledge Succinct Non-interactive Argument of Knowledge”，分别来看看他们的含义：

- zero knowledge：零知识，即在证明的过程中不透露任何内情，如上文的例子所示；
- succinct：简洁的，主要是指验证过程不涉及大量数据传输以及验证算法简单；
- non-interactive：无交互。上文中举的两个例子虽然实现了零知识证明，但Prover和Verifier之间需要经过多次交互才能取得满意的可靠性，而此技术试图彻底避免这些交互。

合起来，zk-SNARK是一种“证明我知道内情的技术，简单、易操作，最关键的是你除了能够得到结论是正确的，对于消息或者交易的内容一无所知，从而真正实现隐私和匿名。

值得注意的是，在具体选择zk-SNARK零知识证明曲线的时候，MetaPay选择了安全系数更高的BLS12-381曲线。

BN128曲线 (Barreto–Naehrig curves) vs BLS 12–381曲线
(Barreto–Lynn–Scott curves)

同为pairing-friendly椭圆曲线，BN128和BLS 12–381还是有所区别的。



根据论文《Implementing Pairings at the 192-bit Security Level》中相应的参数如下：

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

根据 <https://electriccoin.co/blog/new-snark-curve/> 中说明，BN128曲线保守估计，所能达到的安全系数只能到110-bit，并不是之前所称的128-bit security. 若想要达到128-bit security，需要 $q \approx 2384$ ，相应的BN曲线的order r值也会提高到2384量级，r值的增大，会影响multi-exponentiation, FFT等运算性能，从而影响zk-SNARKs以及安全多方计算的执行效率，同时也会影响key文件不必要的增大。



MetaPay



MetaPay 元金融支付生态



MetaPay

MetaPay采用了基于以太坊的Layer2技术，通过链下通道扩容来实现可与互联网产品媲美的秒级支付体验。除了极快的支付体验以外，链下通道内无手续费，有效解决了以太坊公链速度慢、成本高等问题。由区块链智能合约提供去中心化的网络，使用智能合约功能来实现跨参与者网络的即时付款。MetaPay自行研发的Flash Payment，通过使用真实的区块链交易并使用智能合约语言脚本，可以创建一个安全的参与者网络，这些参与者能够进行大量、高速的交易。

主要通过以下三个方面来实现：

双向支付渠道

两名参与者在区块链上创建一个分类帐条目，这要求两名参与者签署任何资金支出。双方都创建了将账本条目退还给他们各自分配的交易，但不将其广播到区块链。他们可以通过从当前分类帐分录输出中创建许多交易支出来更新分类帐分录的个人分配。只有最新版本有效，这是由可区块链分析的智能合约脚本强制执行的。通过向区块链广播最新版本，任何一方都可以在没有任何信任或保管的情况下随时关闭该条目。

闪电网络

通过创建由两方分类帐条目组成的网络，可以找到跨网络的路径，类似于在Internet上路由数据包。路径上的节点不受信任，因为付款是通过脚本执行的，该脚本通过递减时间锁来强制执行原子性（整个付款成功或失败）。为了扩展Layer 2的闪电网络，MetaPay在底层协议的交易验证过程中融入了RSMC(可撤销的顺序成熟度合同)和HTLC (哈希的带时钟的合约) 两个基础协议,用于构建Layer 2的资金池和支付通道的建立。



Layer 2上的闪电网络就具有了非常多的优势，首先就是即时确定性，只要各方签名通过状态更新，状态就被“确认”，而不需要如区块链上等待区块确认；其次，状态更新在链下，点对点通信能够保证隐私，仅最终状态会提交到区块链上；最后是低手续费，闪电网络只在通道打开和关闭的时候需要区块链上结算清算的手续费，而其他时间，不管双方在通道内如何更新、交易都是免费的。

区块链仲裁机制

可以不受限制地在区块链外进行交易。可以在区块链上具有可执行性的信心下进行脱链交易。这与一个人与他人订立许多法律合同的方式类似，但是每次签订合同时都不会上仲裁。通过使交易和脚本可解析，可以在区块链上执行智能合约。只有在不合作的情况下，仲裁才被介入。但是对于区块链来说，结果是确定的。

通过以上三点，可以打破现有以太坊网络交易的拥堵性，实现全网最优的交易速度。

即时付款。闪电般快速的区块链支付，无需担心区块确认时间。安全性是由区块链智能合约实施的，而无需为个人支付创建区块链上的交易。付款速度，以毫秒为单位。

可扩展性。每秒可通过网络处理数百万至数十亿笔交易。容量使传统的支付障碍消失了多个数量级。现在无需保管员即可按操作/点击附加付款。

成本低廉。通过交易和结算链下链，闪电网络可实现极低的费用，从而可用于新兴的用例，例如即时小额支付。

跨区块链。跨链原子交换可以通过异构区块链共识规则立即在链外发生。只要链条可以支持相同的密码哈希功能，就可以跨区块链进行交易而无需信任第三方保管人。



实施方案

我们用三人的转账路径来做解释MetaPay Layer 2的工作原理：

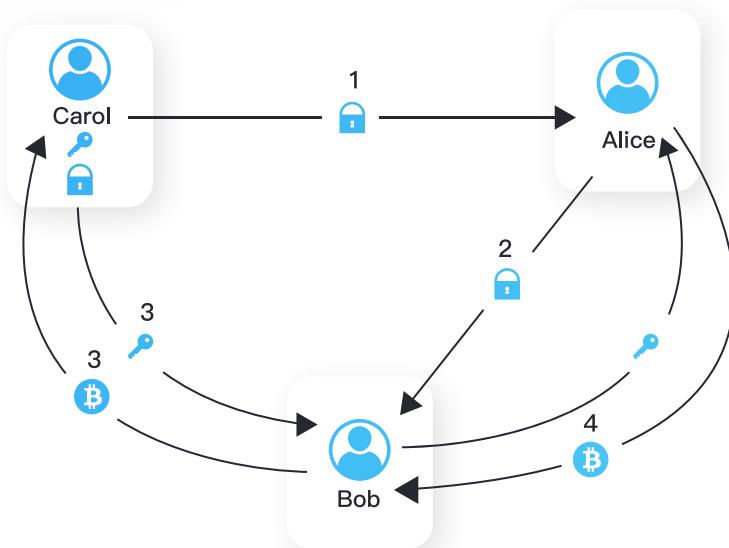
Carol、Alice和Bob分别是交易的三方，Alice 和 Bob 已经建立“支付宝”支付通道，Bob 和 Carol 已经建立“微信”支付通道。如果 Alice 给 Carol 之间要进行交易，有两种方案，第一种是 Alice 和 Carol 再建立一条“Apple”支付通道，另外一种方案是通过 Alice 和 Carol 通过 Bob 进行桥接支付。任何交易双方都需要建立一个一对一的通道，这显然会带来很多麻烦。闪电网络支持中间人桥接建立支付通道，步骤如下：

1. Alice 要给 Carol 支付现金，要通过中间人进行桥接支付。但是中间人不一定可靠，那么 Carol 就和 Alice 约定一个“谜题”，如果 Alice 从 Bob 哪里收到的“答案”能够解开“谜题”，就说明 Bob 真正的把资金给了 Carol。
2. Alice 把“谜题”和转账信息给了 Bob。
3. Bob 和 Carol 进行协商转账，如果 Carol 把“答案”告诉 Bob，Bob 就把钱给 Carol 转过去。这实际上也就和输入秘密进行支付一样。
4. Alice 和 Bob 进行了同样的协商转账，如果 Bob 把“答案”告诉 Alice，Alice 就把钱给 Bob 转过去。

需要注意的是，第 3 步和第 4 步的先后顺序，是 Bob 先垫付的资金，然后 Alice 才把资金给了 Bob。也就是说 Alice 需要给 Carol 支付，需要动用整条价值传输链路上的资金。在只有一个中间人 Bob 的时候，Alice 和 Bob 的资金都被动用了。如果有 10 个中间人，那么动用的资金量就是 Alice 直接支付给 Carol 的 11 倍。



🔒 哈希 🔑 价值



MetaPay的Layer 2解决方案希望可以在下列三者中找到平衡：

可扩展性

增加一个参与者/节点，
网络整体性能也随之增加。



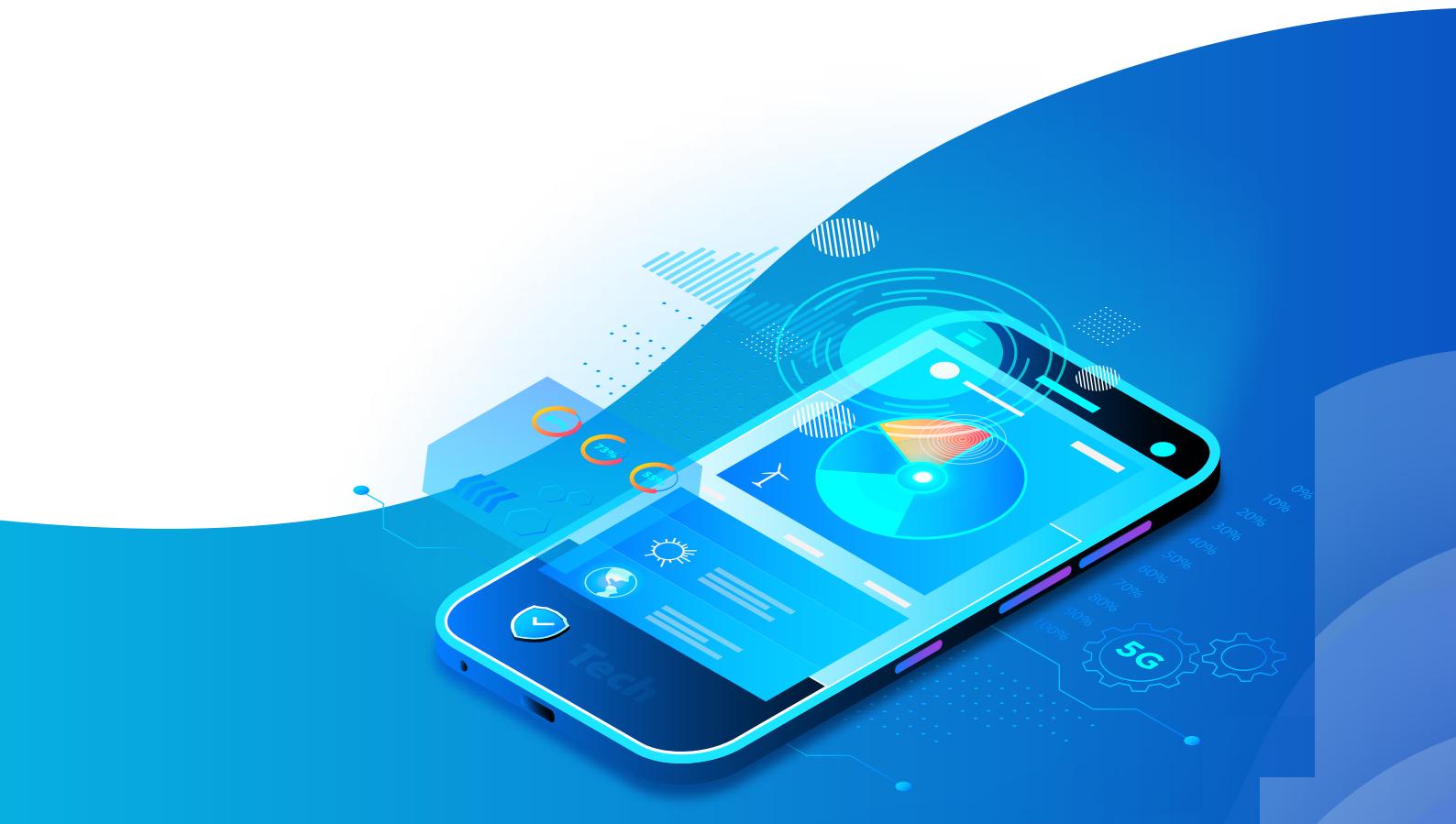
可用性

用户需要在某个指定时间内
保持一次在线。

流动性

参与交易双方和中间节点的需
要将大量的资金押注在Layer1层。

Meta NFT



MetaPay 元金融支付生态



Meta NFT

当前，很多项目在探索NFT类资产的金融属性和衍生品，比如NFT分片化交易，NFT抵押借贷等。

NFT产品将如何定价？而为什么大部分的NFT资产都会有溢价的部分？

NFT价值 = Intrinsic Value（内在价值） + Utility Value（使用价值） + Premium（溢价）

NFT资产的溢价 = 智能合约带来的权利保障 + 区块链带来的经济激励机制 + 区块链带来的互通性

智能合约和区块链的激励机制以及互通性是NFT资产溢价的重要来源。

NFT 的用例涵盖了艺术品、收藏卡、个人时间或服务、游戏项目、域名、房产等可以代币化的真实或虚拟资产。

NFT 之所以在这么多领域产生吸引力，是因为其具有独特性、稀缺性、所有权可证明性、可转移性以及不可分割性。NFT 技术嵌入了元数据，可以用来证明真实性，NFT 的存在数量可以通过编码来进行限制，所有权可以在区块链上得以证明，点击一下按钮就可以实现物品转让。



Meta NFT 特点

所有权

Meta NFT 通过独有的区块链溯源技术进行所有权追踪及保障。

可转让性

在Meta NFT，任何可以代币化的资产可以进行自由转让。

真实性

区块链技术确保交易的NFT资产真实性，防止欺诈行为。

唯一性

Meta NFT采用ERC721不可分割资产标准，确保资产的唯一性。

实施方案

Meta NFT 的 Beta 版本将开放平台的核心功能---NFT 资产交易所，那时用户将可以自由地在 Meta NFT 中交易 NFT 资产。NFT 一站式铸造、发行、资产管理等功能将在随后更新。

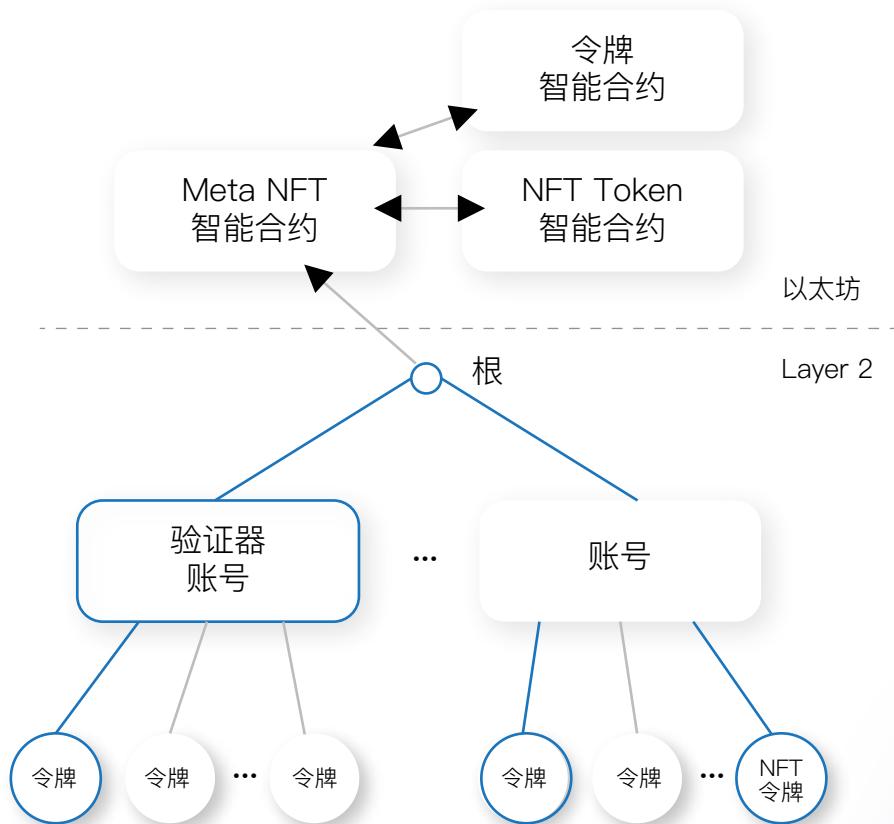
每个NFT资产发布及交易事件可以包含资产标题和详细描述，以提供有关该事件的更多信息。对于那些希望在区块链级别传递信息的人，我们将它们包括在内，系统内默认的资产必须达到一个最低阈值，并且金额没有最高金额，金额由自由买卖的双方共同决定。如果在交易期间未达到卖家的最低目标，则用户可以通过与智能合约进行交互来收回其资金。由于创建提案时会指定令牌地址参数，因此我们的智能合约通常可以与任何令牌一起使用。在我们的平台上，我们可能会使用Mep，并要求创作者及拥有者使用Mep 来推动需求。



铸造自己的NFT资产

用户可在Meta NFT Layer 2直接创建NFT，系统中世界状态的变化和充值 NFT 类似。将开发基于Web，移动应用程序和基于API的Mint智能合约的用户界面，以使资产创建和管理变得简单。将会根据名称/图标/最大供应量/小数位/兑换率/访问列表及资产的详细资料等参数定义新的自定义资产：

- 名称
- 图标
- 最大供应量
- 小数位
- 汇率
- 访问列表
- 数据





社区联动推动市场需求

Mep功能将整合到整个MetaPay 中，并由超过450,000个现有游戏网站提供本机支持。

作为开源平台API的一部分，MetaPay 将开发phpCB, McBulletin, 以及其他论坛和集成，这将使更多的互联网及区块链社区轻松地将Meta Tokens纳入他们的网站和游戏中。而且，Mep将会实现以下功能。

奖励自动化

MetaPay 上现有的自动化系统可以基于条件和触发器的强大组合将Token奖励给用户钱包内。可以为用户参与论坛讨论和其他网站活动设置各种奖励系统。

论坛板

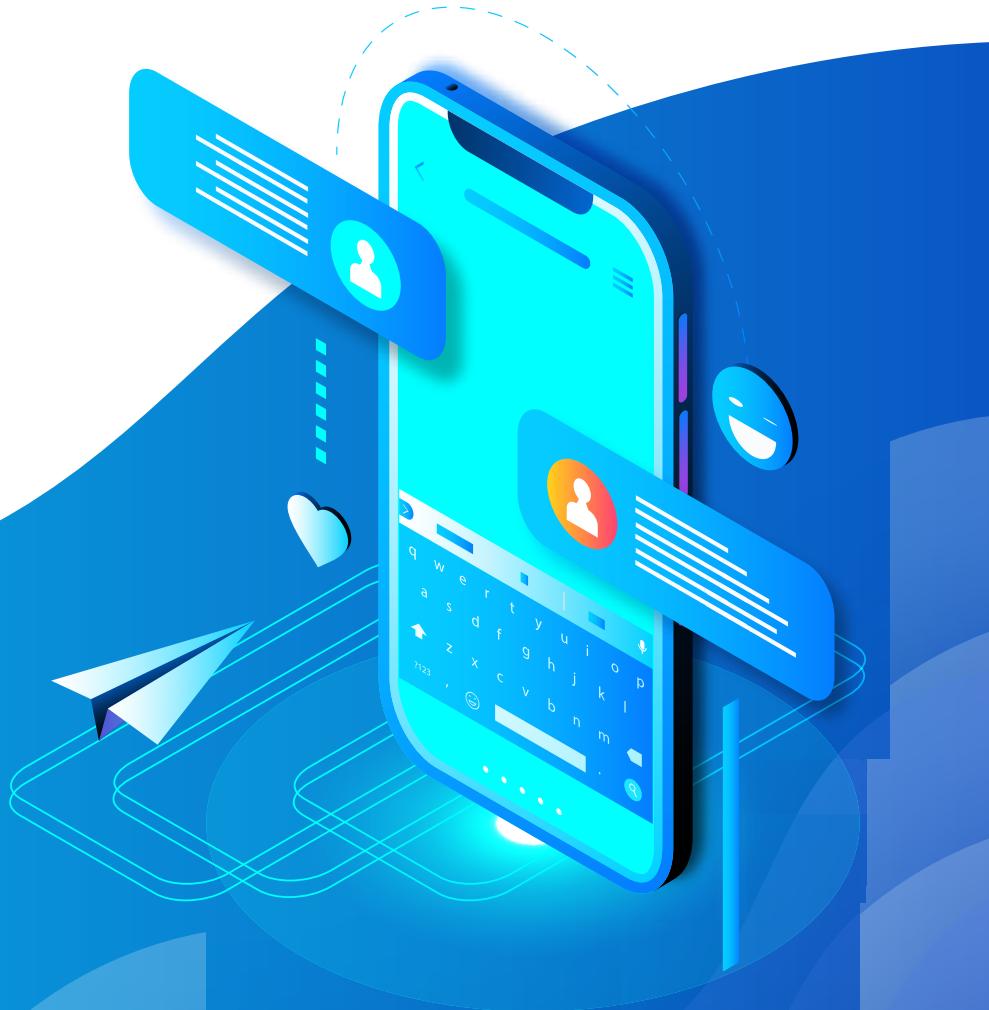
MetaPay 包含一个功能强大的论坛系统，目前为从小型团队到拥有超过一百万用户参与其留言板的巨型社区的各种功能提供支持。论坛投票和积分将通过显示自定义Token的功能得到扩展。奖励将添加到论坛中，以便只需单击几下即可向用户显示余额（此操作将显示在主题上）。

捐款和团体付款

许多网站接受捐赠而不是使用商店，尤其是由社区组成的小型电子竞技比赛或者会议。现在，Mep将成为“捐赠”模块和“付款”中的一种付款方式。

Meta NFT 作为新一代Layer2技术的代表，通过 Rollups 技术实现了二层网络的0 gas费转账和交易，并且在零知识证明领域做了大量的优化工作，实现了Layer2 提现到Layer1的快速提现。Meta NFT 的Layer2 NFT协议，会解决NFT领域的发行贵和转账慢的缺点，目前基于以太坊搭建的NFT平台都可以无缝切换到该Layer2 协议，从而实现0 Gas 发行和转移NFT，并且没有交易容量的限制。未来， Meta NFT 将继续推动Layer2 协议层的发展，为更多领域提供Layer2 的基础设施，如Layer2 的稳定币和Layer2 的借贷协议等。

Meta DAO



MetaPay 元金融支付生态



Meta DAO

定义

为建设拥有广泛影响力和高留存的去中心化网络，生态建设将成为MetaPay 的核心，借力于 DAO 组织架构，公平又高效的生态建设框架将被建立。Meta 是第一个将权益证明要素纳入其强大的DAO代表治理模型的可持续DeFi代币。

Mep全球治理模型

Mep代币持有者可以自愿参加Mep全球治理模型，Mep作为权益证明的代表治理。在Meta PoS生态系统下，Meta 代表理事会的候选人将竞选社区理事。社区理事将在Meta代表理事会中任职，并有能力对Meta DAO的变更提出建议或投票。达成共识需要获得社区理事的多数批准。

实施方案

权益加权投票：Mep全球治理模型内的投票是经过权益加权的，也就是说，其最终统计的投票结果将根据持币量而非节点数。Meta 代表理事会架构：成员介于 11-21 人之间，人员个数为单数，视社区投票而定。生态Meta 代表理事会拥有不同职能，包括执行、监察审核、财务管理、统筹运作。Meta 代表理事会成员须质押一定的代币，作为可能存在的作恶的惩戒成本。策划与提案：Mep 的持有者（额度大于 10000 枚）可发布与 MetaPay 相关提案，包括但不限于对生态应用的资金或技术支持、主网技术升级、线上线下营销活动策划等，涉及到一个去中心化项目运转的方方面面。发布与投票：总支持代币数超过 10000 即可通过发布，进行票选阶段。支持票数超过 50% 即可进入可行性分析阶段。可行性分析：Meta Pay代表理事会将从各个角度（包括财务、法务、可落地性、执行难度、短中长期价值等）分析可行性，并进行投票表决，超过半数即可进入执行阶段。可行性分析报告需进行公示。执行：MetaPay代表理事会将负责运营、把控、对接合作方等落地执行工作，MetaPay与BSC等生态支持者将获得合作的优先级。监察与审核：MetaPay 持币节点皆可参与，MetaPay 代表理事负责将提案执行流程与结果进行公示。

路线图





路线图





参考文献

- [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.I.: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
- [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》



法律法规

MetaPay Lending业务的某些部分受美国境内的州和联邦法规以及外国法律法规的约束。通过MetaPay 平台安排的贷款是由SEC注册投资顾问或其他董事会注册银行实体提供的。

MetaPay Lending Holdings, Inc.以及通过MetaPay 平台提供的贷款必须遵守适用的州和联邦贷款与高利贷法律，例如：《联邦消费者信贷保护法》，《贷款真相法》，《平等信贷机会》法案，《公平债务追收行为法案》，《多德-弗兰克华尔街改革和消费者保护法案》，《服务人员民事救济法案》，《军事贷款法案》，《银行保密法案》，《美国爱国者法案》，《电子资金转移法案》，《全球和国家商务法》（ESIGN）中的电子签名以及其他有关隐私，数据安全并禁止不公平或欺骗性商业行为的联邦和州法律。

作为非银行实体，MetaPay Lending Holdings, Inc. 及其关联公司MetaPay Platform已制定了广泛的最佳实践政策和程序，旨在确保法律和法规合规性。

MetaPay Lending Holdings, Inc.及其关联公司MetaPay Platform可能会受到负责监视消费者信贷，贸易和商业的国家机构的检查，监督和其他监管执行措施；以及负责管理美国联邦消费者保护法，贸易和商业的联邦机构，例如消费者金融保护局和联邦贸易委员会。