区块链隐私保护机制发展方向

作者：Gate.io 研究院 Eric Fu，Jill Chow

摘要

随着网络技术的发展，用户对于隐私问题的关注度日益增大。与传统技术不同，区块链作为去中心化账本，用户个人信息无需提交于第三方，对用户隐私保护有着天然的优势。而链上数据信息全部公开透明却又引发了新的隐私保护问题。本文通过对区块链隐私安全机制优缺性进行对比，深入探讨现阶段提高区块链隐私机制的方案并对区块链隐私性未来发展方向进行展望。

要点总结：

- 与传统技术相比，区块链技术去中心化的特点取缔了用户对第三方高信任度机构的依赖，提升了用户信息隐私性。
- 区块链通过点对点传播、去中心化、地址匿名化等方式提高了用户的隐私安全，然而链上数据透明化也为攻击者提供了获取、分析用户数据信息的途径。
- 提高区块链安全隐私机制可以从网络层、交易层、应用层三方面入手，分别对应为：在网络层可以对节点进行安全验证、使用匿名网络；在交易层使用混币机制、零知识证明等技术；应用层选择安全隐私机制高的区块链等方式。
- 单一隐私保护机制很难做到尽善尽美，未来区块链隐私安全性的提高可以从多种安全方案进行配合的方向上进行思考。同时密码学的加速发展以及链下扩容方案与隐私机制的融合也为提高用户隐私安全性提供了更多的可能。

1 区块链构架及基础知识介绍

区块链作为当下最前沿的技术之一始终是热门话题，自比特币面世以来，人们通过不断完善、优化区块链的各种机制，以便区块链技术的早日普及。

作为去中心化账本，用户可以不通过第三方高信用度机构直接与另外一个用户进行点对点交易。也就是说，用户通过使用区块链进行交易同时不必提交与自己相关的信息资料。但如此一来，由于区块链本身没有第三方高信用度机构进行中心化管理，如何保障用户隐私不被泄露变成区块链发展道路上一个很重要的课题。

在区块链当中隐私性涵盖范围很大，如比特币般通过 hash 函数生成交易地址只能称作为匿名化，可以被认作是保护用户隐私的一种手段，这并不代表用户的隐私性得到了万全的保障。

区块链逻辑架构

图片制作：Gate.io 研究院

如左图所示：传统区块链的架构可以分为数据层、网络层、共识层、激励层、合约层与应用层。数据层为区块链最底端架构，用来存储交易记录、哈希值、时间戳等。网络层则搭建起点对点交易体系。交易方可以通过合约层提供的智能合约，以相同的共识进行交易。应用层为交易方提供了交易的方法。根据对区块链逻辑构架不同层面进行归类，除去数据层作为去中心化账本的核心数据必然公开之外，整个体系的隐私保护机制可以从网络层、交易层（共识层、激励层、合约层）、应用层三个层面进行提高。下文将对其进行具体介绍。

2 区块链在隐私性方面的优缺点

传统 IT 行业中存在第三方高信任度监管机构，用户在使用时需要提交个人信息才可以进行交易活动，因此一旦信息泄露则会导致用户个人隐私泄露。相比传统 IT 行业，区块链技术对于保护用户的隐私性具有很大的优势，去中心化的设计理念可以使交易用户无需提交个人信息给他人便可以进行交易。这也意味着，传统 IT 行业对于用户隐私性的保密机制在区块链系统中不再适用。同时为了保证交易的公正性，区块链上的交易数据需要公开透明化，也就是说在区块链构架数据层面上用户的一些交易信息是无法做到完全保密的。下文将从网络层、交易层与应用层对区块链隐私性的优缺点进行分析。

2.1 网络层

在网络层面上讲，区块链采取 P2P 的交互模式，节点发起交易信息广播后，首先会传播给邻居节点，邻居节点收到信息会继续以此方式进行广播直至扩散到全网。通过这种方式进行信息传播，攻击者很难以传统监控流量的方式追踪交易信息的来源与去向。

然而，要保护这种交互方式的安全性需要整个区块链网络中存在大量足够活跃的节点用户。同时，由于网络中不存在中心化节点，系统无法依靠保护几台中心服务器的安全来保障安全性，这就需要每个节点都有足够的安全保障措施，如果存在安全防护性较低的节点，攻击者则可以直接针对这个低安全性节点进行侵入攻击，获取 IP 地址、分析网络拓扑从而获取用户的隐私信息。

2.2 交易层

用户在区块链上交易时会使用公钥加密算法生成交易地址，生成的交易地址为哈希字符串，此地址与用户身份信息毫无关联，可以使交易用户匿名化（Anonymous），因此攻击者很难直接通过交易地址获取交易用户信息。

然而地址匿名化只是保护用户隐私性的其中一种方式，仅仅依靠匿名化依旧无法确保用户隐私性的安全。由于链上的交易信息会全部储存在公开透明的去中心化账本上，所有人都可以获取全部交易信息，攻击者有可能通过对交易之间的关联性进行分析从而降低匿名化程度获取用户交易隐私信息。

2.3 应用层

区块链技术属于分布式网络技术，没有中心化节点，每一个节点用户都相当于一个小型的服务器，攻击者很难通过攻击某个特定节点得到用户全部隐私信息。

然而无法保障每个节点的安全防御机制都做到如中心化服务器一样安全，安全防护意识不足的节点用户可能会遭受到黑客攻击导致隐私信息泄露。此外，区块链服务商对区块链安全机制的研发也会对用户隐私安全性造成影响，使用具备隐匿特性的区块链对隐私信息保护会更有效果。

2.4 优缺点对比

如下表所示，区块链对于用户的隐私性保护是创新性的。用户通过点对点交易和交易身份匿名化等匿名技术充分保护了个人隐私，区块链无需依赖第三方信任机构的特点更是从本质上保障了用户的隐私性。然而基于区块链系统的底层构架，交易数据的公开透明化仍存在暴露用户个人隐私的风险，攻击者或可通过对交易数据进行分析从而挖掘到更多的用户个人信息。区块链

隐私机制的不足同样会对用户隐私安全性带来隐患。

优点	缺点
1. 点对点交易，广播式传播 2. 地址匿名化，与真实身份无关 3. 节点去中心化，无第三方机构掌握隐私信息	1. 单个节点安全防护性高低存在差异，安全性低用户容易遭到攻击 2. 交易数据公开透明化，攻击者可以藉此分析交易相关性 3. 区块链服务商的安全机制设定影响用户隐私安全性

来源：公开资料 表格制作：Gate.io 研究院

基于上述情况，区块链开发者们一直致力于提高区块链系统安全隐私性，下文将对现阶段区块链安全隐私提高技术加以介绍分析。

3 提高区块链隐私性的机制

3.1 网络层

通过上文中对网络层隐私安全性优缺点的分析可知，如果单个节点的安全性不足，攻击者可以通过对低安全性节点进行侵入从而获取用户的 IP、交易信息以及网络拓扑结构从而得到用户的隐私信息。也就是说防御方向主要为防止攻击者恶意接入节点以及对交易信息的加密。目前来看有两种安全机制适用于提高网络层安全性。

■ 限制接入、恶意节点屏蔽

在区块链中系统设置接入节点验证，并对恶意节点加入黑名单。系统可以对接入节点进行验证，如此一来便大大降低了攻击者攻破节点获取信息的几率。而这种限制机制多用于私链当中，公链构架由于本身设定原因无法限制节点加入。虽然公链无法限制节点接入公网，但是可以采取

节点检验机制，一旦发现节点出现异常行为，便以将其列入黑名单的方式限制该节点对系统的安全威胁。

■ 匿名网络

使用匿名网络对用户信息来源进行混淆。由于在网络层中，攻击者通过侵入节点获取网络拓扑结构可以得出用户的隐私信息。将区块链布置在具有隐私保护特性的匿名网络上，该网络可以通过对数据进行多层加密并由多个路由器转发数据包使得攻击者无法直接判断对应的输入源与输出目的地的方式保护节点用户信息安全性。目前运用比较广泛的匿名网络有两种，一种为 Tor（The Onion Router：洋葱路由），另外一种为 I2P。

如下图所示，Tor 的用户可以启用洋葱代理模式对数据进行加解密。

① 首先它会在目录服务器中获取所有的节点信息

② 随机选取节点通过网桥建立安全通道。

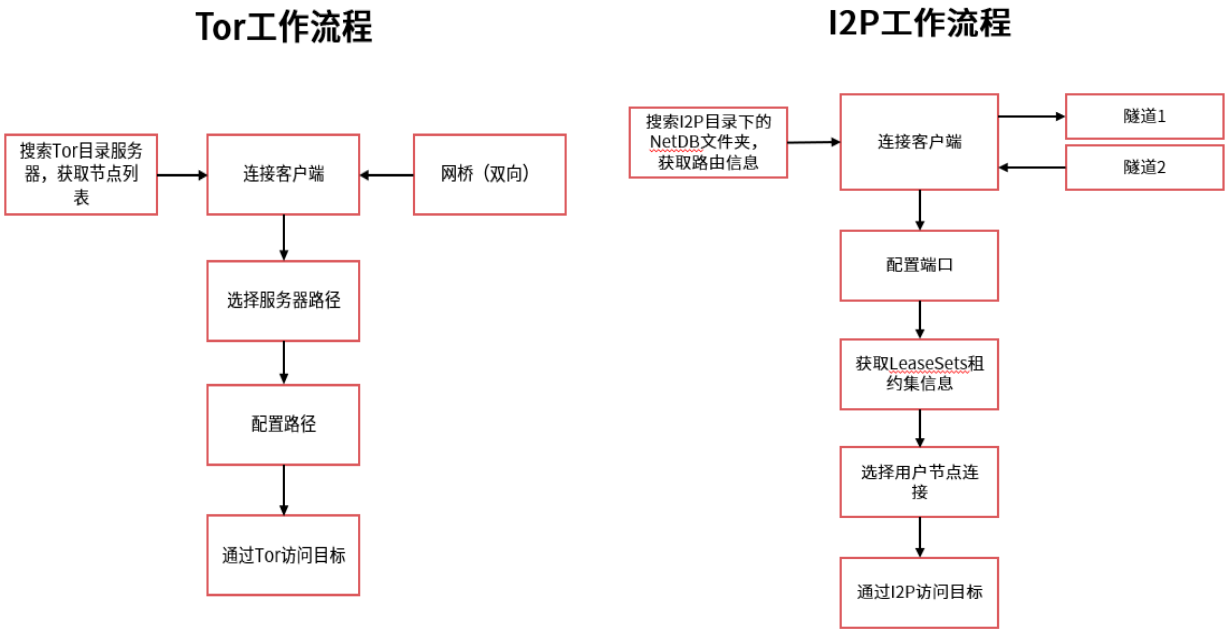
③ 其次选择目标服务器

④ 配置路径

⑤ 最后访问目标。

这个过程中用户与 Tor 建立的通道会继续拓展至其他 Tor 节点并对信息进行层层加密。之后在传输过程中，每经过一个随机 Tor 节点会通过密钥交换的方式进行层层解密最终将信息传输到目的地。对于攻击者来说除非掌握了所有的 tor 节点，否则很难获取通信中的明文。

相比于 Tor，I2P 网络的安全性要更高。Tor 采取的是双向电路通信，I2P 则采取了单项隧道通信。如下图所示，I2P 在 NetDB 中获取所有路由节点信息，通过单项隧道的方式建立客户端，这个过程中信息入站与出站选择的是两条不同的隧道，并且每两条隧道的建立间隔时间为 10 分钟，同时 I2P 网络的出站的端口是被隐藏的。



图片制作：Gate.io 研究院

匿名网络属于在区块链应用层面上提高安全机制的一种技术。它与区块链的结合提升了攻击者通过攻击用户节点获取 IP 分析流量的难度。

3.2 交易层

在交易层面，区块链系统可以使交易用户实现匿名化。然而匿名化只是保护用户隐私性的其中一种方式。攻击者即使无法通过破解交易用户地址直接获取用户隐私信息，但仍然可以通过对用户交易记录的分析获取其隐私信息。基于此，目前主流的可以提高用户在交易层的信息安全性的机制大概为混币机制与信息加密机制两种。

3.2.1 混币机制

混币机制是指在交易的过程中，用户可以把交易信息进行加密得到 A1，然后使用某个中间方提供的公钥对已加密信息以及交易目的地址进行二次打包得到加密信息 A2。二次加密后将 A2

发送给中间方。当中间方接收到这个交易信息 A2 时，使用私钥对信息进行解密再次得到 A1 以及交易目的地址，解密完毕后中间方通过交易将加密信息 A1 发送到目的地。

	混币机制	费用	额外消耗	资金盗窃风险	混币过程中隐私泄露风险	DDoS 攻击风险性
中心化	Mix	√	交易时间长	高	高	低
	MixCoin	√	交易时间长	中（审计）	高	低
	BlindCoin	√	盲签名计算开销	中（审计）	低（使用盲签名）	低
	Dash	√	押金	中（惩罚机制）	高	低
去中心化	CoinJoin	×	×	×	高	高
	CoinShuffle	×	参与人员同时在线	×	低（地址洗牌机制）	高
	Xim	√	×	×	高	低
	CoinParty	×	×	×	高	低
	Monero	×	环签名额外开销	×	低（使用环签名）	低
	TumbleBit	×	需要至少两个交易	×	低（不可链接支付通道）	低

来源：公开资料 表格制作：Gate.io 研究院

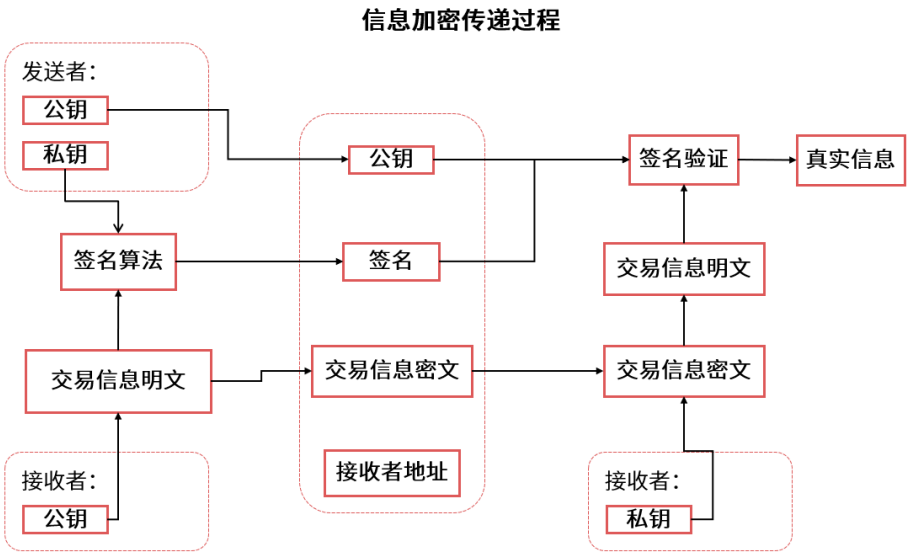
如上图所示。混币机制分为两种，一种为中心化混币机制，其中包括 Dash 币、BlindCoin 以及 Mixcoin 等。另外一种为去中心化混币机制，其中包括 CoinJoin、Xim、门罗币等。

通过对比可以发现，中心化混币机制的优点是受到 DDoS 攻击 [1]的风险比较低，然而若要保障用户资金不被盗窃则需要一些其他安全机制作为保障，如 Dash 币要求第三方节点提交高额押金以保证信用。

相比于中心化混币机制，大部分去中心化混币机制无需向混币服务商缴纳服务费，同时由于不存在第三方的缘故，资金盗窃风险几近为零，但仍无法保证所有参与用户不泄露其他用户的隐私信息。因此，去中心化混币机制同样需要追加其他安全机制来保障参与用户的个人隐私安全，如环签名或地址洗牌机制等。

3.2.2 加密机制

加密机制是另外一种保护用户交易时隐私安全性的可行方法。如下图所示：



图片制作：Gate.io 研究院

传统区块链的交易过程是使用接收方公钥对交易信息原文进行加密，再对交易信息原文进行 Hash 并使用交易发送方自己的私钥对 Hash 值进行签名，在此之后将密文、签名、发送方的公钥同时发往交易接收方完成交易。在这个过程中可以看到交易信息的安全性是有保障的，然而交易地址也是公开的。如此一来攻击者可以通过分析交易之间的关系窥探用户的个人隐私。基于此种情况，门罗币（Monero）提出一种解决方案。交易发送方在发送交易信息时会随机产生一个参数，这个参数可以与交易接收方的公钥结合加密后得到一个新的地址，由于随机参

数是不公开的，所以攻击者无法通过这个新生成的地址观察出资金的流向从而保障了交易用户的信息隐私。

此外，零知识证明技术（Zero-Knowledge Proof）同样可以保障用户信息隐私性。简而言之，零知识证明可以让验证者在不检查被验证人私钥的情况下得出某个结论的正确性。比如，验证者提供了随机数 A，在不知道具体验证方法的情况下，验证者使用被验证人的公钥对未知验证方法求解并得到这个随机数 A，则证明被验证者没有问题。

这之中 Zcash 使用的 zkSNARK（zero-knowledge succint non-interactive arguments of knowledge）技术就是对零知识证明的一种运用。使用 Zcash 的交易过程中，用户可以完全匿名化交易，交易的基本原理是交易双方通过签订“支票”的方式进行交易，交易时验证者无需看到具体“支票”内容，只需要确认票号是否存在于“支票”列表或“作废支票”列表中便可确认交易的真实性。

3.3 应用层

应用层面上提高隐私安全性的方式大致可以分为两方面：一方面用户提高自身安全意识，使用安全性高的程序加强本身节点服务器的安全性。另一方面交易时可以选择具有隐私保护机制的应用。

目前具有交易隐私保护机制的应用大体可以分为链上与链下两类。

3.3.1 链上（Layer1）

比特币作为第一代区块链应用在交易隐私保护方面存在着不足，此后人们意识到交易隐私对于用户的重要性，相继开发了多种具备不同隐私保护机制的区块链项目。如下表所示：

区块链	类型	隐私保护策略	评价
Dash	公链	混币	形成第三方中心化网络，存在资金窃取、泄露混币过程的可能
Monero	公链	混币、数据加密	利用环签名方式使参与者无法获取其他用户的交易信息，提供隐私保障
Zcash	公链	零知识证明	保障交易数据链上校验的同时保护用户隐私信息，非常有发展前景
EOS	公链	pEOS（类似 Monero 使用技术）	
Fabric	联盟链	限制节点接入、限制数据发布	
SERO	公链	零知识证明	保障交易数据链上校验的同时保护用户隐私信息（加入智能合约，开发难度较大）
Grin	公链	Mimblewimble 隐私协议	引入致盲因子，通过零和验证、私钥确认安全性并保护用户隐私，交易过程中没有地址
Beam	公链	Mimblewimble 隐私协议、Bulletproof	除了使用 Mimblewimble 隐私协议之外追加 Bulletproof 签名，保护用户隐私

来源：公开资料 *表格制作：Gate.io 研究院*

大多数具备隐私保护机制的区块链项目属于公有链，限制节点接入方案并不可行。目前多以使用混币机制、数据加密为主。零知识证明技术的出现进一步提升了用户隐私安全的可行性。

3.3.2 链下（Layer2）

从应用角度上看，很多区块链项目采取不同的隐私保护机制提高用户隐私信息安全性，但越发复杂的链上机制在一定程度上可能会限制区块链的扩展性，此时一些于链下提高隐私性的方案被提出。

如闪电通道的交易方式不去记录用户之间所有的交易记录，只将初始交易状态与最终交易状态上传到链上，通过隐蔽中间多次交易流向的方式来保障用户的隐私性。

而 AZTEC 是一种基于以太坊的隐私保护方案，使用零知识证明加密技术。其基本交易原理是交易用户通过 AZTEC 协议进行交易时，具体余额会被隐藏并通过转化为“票据（Notes)”的形式进行交易，通过对“票据”的多次拆分达到隐藏具体交易信息的目的。

4 隐私性机制未来发展方向

随着区块链技术的发展速度越发加快，用户对于区块链隐私保护性的要求也越来越高。目前来看每一种隐私保护机制都有各自的优缺点，隐私保护技术仍在不断完善中。由于区块链本身去中心化的特点，单一的保护机制很难做到尽善尽美。未来区块链隐私保护机制可以在不影响区块链基本运行构架的基础上从多个层面进行提高，同时针对不同应用场景发挥不同隐私机制的最大优势。

从实用性的角度出发，达世币与门罗币等专门针对隐私保护的项目为对有强烈隐匿性需求的人群提供了很好的选择。密码学的突破使得用户隐私性的提升存在更大的可能，零知识证明通过不需要直接验证用户私钥便可认证信息真实性为提升区块链隐私性机制新方向。

同时，由于链上空间过于拥堵、负担过大导致很多扩容技术出现，闪电网络等链下扩容技术的

出现不仅可以缓解链上拥堵问题，与链下隐私保护机制结合亦不失为一种可行的发展方向。

5 总结

本文通过对区块链逻辑架构分层为网络层、交易层与应用层三个层面，并详细阐述了区块链技术中隐私性的优缺点。

由于区块链使用点对点的方式进行传播且没有中心化节点，在网络层中，攻击者很容易通过对单个低安全性节点发动攻击获取其 IP 以及网络拓扑结构从而获得用户隐私信息。将区块链与匿名网络结合可以有效提高系统的安全性，增加攻击者攻破用户 IP、分析用户数据的难度。

在交易层中，区块链会对用户交易地址进行匿名化，攻击者无法直接通过匿名化地址获取用户信息，与传统 IT 构架相比用户隐私性得到了提高。然而攻击者仍然可以通过用户的交易数据、交易流向对用户进行分析从而获取用户隐私信息。基于此，混币机制与加密机制相继被提出以提高用户隐私安全性。前者通过混淆数据流向使攻击者无法确认交易的来源与输出方向从而达到匿名的目的。数据加密则是通过使用交易接收者公钥以及交易发送者提供的随机数对交易地址进行加密使攻击者无法分辨真正的交易地址达成匿名化。

除此以外，目前有很多区块链项目针对隐私机制进行研发，达世币、门罗币以及 Zcash 对提高用户隐私性都有明显的效果。鉴于目前链上拥堵等情况，链下扩容方案的不断提出，融合隐私性机制于链下扩容方案中也不失为一种可行的方案，闪电网络目前的主要发展方向便是为保护用户隐私安全。

随着区块链技术的发展，对于交易隐私安全的要求越来越高。单一的隐私安全机制很难做到尽善尽美，未来提高区块链安全隐私性可以通过多种隐私机制配合的形式来完成。随着扩容方案

的不断改进，交易隐私方案亦可融入至链下进行以便于减轻链上的负担。密码学的突破、零知识证明技术的崛起也为隐私安全技术打开了一扇的新的大门。

6 参考资料

6.1 参考资料

1. 张宪，蒋钰钊，& 闫莺. (2017). 区块链隐私技术综述. *信息安全研究, 3*(11), 981-989.
2. 祝烈煌，高峰，沈蒙，李艳东，郑宝昆，& 毛洪亮等. (2017). 区块链隐私保护研究综述. *计算机研究与发展, 054*(010), 2170-2186.
3. Khan, N. , & State, R. . (2019). *Lightning Network: A Comparative Review of Transaction Fees and Data Analysis. Blockchain and Applications*.
4. 李旭东，牛玉坤，魏凌波，张驰，& 俞能海. (2019). 比特币隐私保护综述. *密码学报, 006*(002), 133-149.
5. 祝烈煌，董慧，& 沈蒙. (2018). 区块链交易数据隐私保护机制. *大数据*.
6. 杨云，李凌燕，魏庆征. 匿名网络 Tor 与 I2P 的比较研究. *网络与信息安全学报*[J], 2019, 5(1): 66-77 doi:10.11959/j.issn.2096-109x.2019008
7. Cramer, R. , & Ivan Damgård. (2004). Secret-Key Zero-Knowlegde and Non-interactive Verifiable Exponentiation. *Theory of Cryptography, First Theory of Cryptography Conference, Tcc, Cambridge, Ma, Usa, February*.
8. Eberhardt, J. , & Tai, S. . (2018). ZoKrates - Scalable Privacy-Preserving Off-Chain Computations. *IEEE International Conference on Internet of Things & IEEE Green Computing & Communications & IEEE Cyber*. IEEE.

6.2 名词解释

[1] DDoS 攻击：分布式拒绝服务攻击（Distributed Denial of Service），指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。由于攻击的发出点是分布在不同地方的，这类攻击称为分布式拒绝服务攻击。区块链中分布式节点比较多，容易发动类似攻击。

声明

因出具该研究报告，特做出如下声明：

- 本研究报告是内部成员通过尽职调查和客观分析得出的结论，旨在对区块链隐私保护机制进行分析总结，并不能完全以此来预测未来区块链隐私保护机制的发展情况。
- 本研究报告非衡量研究对象本身价值、以及其发行代币价值的工具，不构成投资者做出最终投资决策的全部依据。

本研究报告中引用的项目资料来源自内部认为可靠、准确的渠道，因为存在人为或机械错误，信息均以获取时态为准。内部成员对研究报告中所依据的相关资料的真实性、准确度、完整性以及及时性进行了必要的核查与验证，但对其不做任何明示或暗示的陈述或担保。