区块链隐私保护读书报告

摘要：本文从分层结构的角度出发探讨了当前区块链的隐私保护技术。针对不同的技术的特点及利弊做了一定的调研，并调研了当前一些隐私保护技术的应用。大多数的隐私保护技术的出发点基于对既定系统的补足，缺乏系统性前瞻性的分析。

关键词：区块链；隐私保护

1. 引言

作为公共记账本，区块链记录了交易的所有信息，包括账户余额、交易金额和交易双方的信息等。但是，区块链的这一特性也带来了严重的隐私问题。由于区块链上的节点可以访问查看区块链上记录的所有交易信息，所以通过分析大量数据，攻击者可以推断出交易所涉及的相关账户的个人信息。此外，永久记录在区块链上的交易信息也将会导致另一个问题：一旦某笔历史交易泄露了某个用户的真实身份，与该用户相关的所有交易记录中的信息也都将被泄露。因此，保护区块链隐私显得尤为重要[1]。

大多数关于区块链的安全和隐私研究都集中在两个方面：（1）迄今为止发现的一些基于区块链的系统遭受的攻击；（2）提出了针对此类攻击采取一些最新对策的具体建议。但是，几乎没有做出任何努力来提供对安全性和安全性的深入分析[2]。当然，对于系统安全性完善效率来说，通过解决实际遭受攻击比未雨绸缪的分析系统漏洞更高效。但若能够从根本上分析系统的安全性和隐私漏洞，揭示当前区块链部署模型中漏洞的根本原因，便可以进一步强化或者创新当前的安全和隐私技术。

1. 区块链分层隐私保护

按照层次结构特点对区块链隐私保护分类，主要可以分为三类，分别是网络层隐私保护、交易层隐私保护和应用层隐私保护[3]。

* 1. 网络层隐私保护

区块链网络层可能存在的安全威胁主要是网络中的通信数据可能被恶意节点监听。以比特币为例，节点的IP地址、节点之间的拓扑关系以及网络传输信息可被恶意节点所获。将交易信息和源节点的IP地址关联，来分析出用户的实际身份，这是一种可能的攻击手段。

保护区块链数据免于被攻击者接触是网络层隐私保护的主要手段，目前的技术手段主要分为限制接入、恶意节点检测和网络层数据混淆三类[3]：

限制接入机制对不同区块链节点进入区块链网络给与不同的权限，没有得到区块链系统授权的节点不能访问网络中的交易数据。例如在区块链应用超级账本hyperledger中，在进入区块链网络前，节点必须通过认证中心 CA 节点的身份验证[4]。

检测恶意节点的一种方法是基于行为模式聚类的检测方法，通过分析分布式节点的行为模式来快速定位和剔除恶意节点，可筛选恶意节点以降低其对区块链网络的危害[5]。

数据混淆方法中，研究人员提出区块链应用应该在可以隐藏 IP 地址的专用网络上使用。而数字加密货币门罗币采用匿名通信协议 I2P，因为 I2P 使用多条网络信道发送数据、接受数据，增加网络信道可以更好地隐藏 IP 地址，避免攻击者溯源交易信息。

* 1. 交易层隐私保护

区块链的交易信息永久记录在区块链上，节点都可以查看交易明细。若有恶意节点根据区块链中的交易数据，通过分析交易的源头流向，可推测分析出节点的身份信息等隐私信息，损害用户隐私。

交易层隐私保护的关注重点是在现有的区块链验证机制和共识算法下，使用能够隐藏交易信息的技术，防止而已节点通过分析交易数据推测出有价值的敏感信息。

交易层隐私保护机制是在不改变区块链已有的共识算法和验证机制前提下，防止恶意节点获得准确的交易数据。根据数据保护技术的特点，保护技术可以分为三种类型：

基于数据失真的技术：重点是对交易数据内容进行混淆，主要是混币思想

基于数据加密的技术：在不妨碍区块链系统原有的共识算法和验证机制的前提下，采用技术手段对交易信息加密，保护交易数据不被攻击者获取。例如门罗币、零币等

基于限制发布的保护方案：指在区块链中选择性地公开相关数据。例如闪电网络是比特币协议中采用的微支付技术[6]，该技术在线下进行交易的部分步骤，不必再线上完成交易的所有步骤，在线上只记录与交易相关的必要参数，可降低被而已节点利用推测隐私的可能性。

* 1. 应用层隐私保护

应用层主要涉及使用区块链应用的用户和提供区块链服务的服务商。用户和服务商都有可能泄露隐私。

应用层隐私保护的研究方向是提升用户的安全意识、提高区块链服务商的安全防护能力。目前也出现了很多针对隐私保护的区块链客户端。例如已有的在线钱包和多重签名技术，离线钱包技术。

1. 区块链隐私保护技术及利弊

3.1、 混合机制

混合机制，也称作混币思想，是指在不改变交易最终结果的原则下改变交易的过程。混币思想将在多个发送和接收方之间的具体交易信息进行隐藏。主要分为需要和不需要第三方节点的两种方法[3]。

在使用第三方节点方法中，第三方节点可能会被攻陷导致混币过程泄露。针对中心化混币方法的缺陷研究人鱼提出了许多解决方案，例如具审计功能的中心化混币方案、中心节点不能知晓混币具体信息的盲签名机制等优化方案。

不使用第三方节点的混币方法是指混币过程由分布式节点自行协调和运作，如CoinJoin机制。在 CoinJoin[7] 思想中，混币过程的具体实行由分布式节点自行商定，导致混币过程中可能存在很多安全隐患，例如在节点协商的过程中攻击者可能获取其他节点的交易信息。

针对这些威胁，CoinShuffle[8]在去中心化混币机制的基础上提出了一种输出混淆协议，混淆协议的参与者无法分析出其他参与者的信息，也不能分析出输入地址和输出地址之间的对应关系。且混币参与方在混币过程中必须同时在线，因此比较难以抵御拒绝服务攻击。

3.2、 匿名签名

数字签名技术由多种变体开发而成。一些签名方案本身具有为签名者提供匿名的能力，我们称这种签名方案为匿名签名。在匿名签名方案中，较早提出了组签名和环签名，它们是两个最重要和最典型的匿名签名方案。

组签名在一个组内，其任何成员都可以使用个人密钥为整个组匿名签名消息，并且具有该组公共密钥的任何成员都可以检查和验证生成的签名，并确认某些组成员用于签署消息的签名。签名验证的过程除了该组的成员身份之外，没有透露任何有关签名者真实身份的信息。小组签名有一个小组管理员，负责管理添加小组成员，处理纠纷事件（包括透露原始签名者）。在区块链系统中，我们还需要一个授权实体来创建和撤消该组，并向该组动态添加新成员，以及从该组中删除或撤消某些参与者的成员资格。由于组签名需要组管理员来设置组，因此该组签名适用于联盟区块链。

环签名是一种匿名数字签名，交易的发送方可以将自己的账户地址隐藏在一个匿名集（环）中，可以验证交易的签名确实来自于匿名集（环）中的某一账户，但是不知道具体是哪一个账户。

但是，交易的不可链接性过于依赖匿名集（环），在用户使用的匿名集合比较小的情况下，其他恶意用户可以通过分析多个匿名集和交易记录，利用匿名集合间的差集，将相关交易信息与真实用户身份关联起来。

以太坊在2015年添加了环签名，为用户提供了匿名性，如门罗币。

3.3、 同态加密

同态加密是指无需对加密数据解密就能进行密文运算的一种密码学技术，根据支持运算的种类不同可分为加法同态、乘法同态以及支持任意运算的全同态加密[9]。

随着对同态加密算法的研究深入，一些实际应用成果也取得了不错的效果。目前，在云安全、多方计算、移动代码、匿名访问等领域内，同态加密算法技术得到广泛应用。在如今越来越受重视的区块链研究中，同态加密技术也正得到学者研究人员们的重视。目前，同态签名、基于同态加密的电子投票等方案已经得到广泛应用。但当前的全同态加密技术效率低下，要达到大规模的应用难度较大。但是对于计算时长要求不高或是数据规模本身就不大的业务场景，全同态加密有着重要的应用价值[10]。

3.4、 零知识证明

零知识证明是指证明者可以向验证者证明某些断言是准确的，而无需向验证者提供任何有用的信息。在数字货币中，交易发送方可以使用零知识证明来证明交易是有效的，并且有权在不泄露身份信息和交易金额的情况下使用相对应的加密货币。

传统的零知识证明需要可信的初始化设置，这一初始化设置必须由可信的第三方执行。并且在初始化过程中，通常会产生额外变量，如果这些额外变量被攻击者获取，它们可以被用来生成无法被检测出来的假证明。另外，传统的初始化设置是针对特定电路的一次性可信设置，电路发生变化后，需要重新执行一次初始化设置。

为了解决上述问题，有学者设计了公开透明的初始化设置，生成一个没有额外变量的公共参考字符串（CRS）[11]。但是这样的新设置以为他们的证明大小比传统的设置方案要大，所以无法实际应用到区块链。另外，有学者设计可以对通用的初始化设置优化[12]，这些初始化设置使用额外变量创建了结构化参考字符串（SRS）。SRS是一种通用的、可更新的结构化参考字符串，它支持无限数量的任意电路。即电路发生变化后，不需重新进行初始化设置。

3.5、 基于属性的加密（ABE）

ABE是一种加密方法，其中属性是定义使用用户的私钥加密的密文的因素。如果用户的属性与密文的属性一致，则可以使用用户密钥解密加密的数据。抗串通性是ABE的重要安全属性。它确保了当恶意用户与其他用户串通时，他无法访问其他数据，但可以用其私钥解密的数据除外。

基于属性的加密功能非常强大，但由于缺乏对核心概念和有效实现的理解，迄今为止尚未有应用程序对其进行部署[2]。

3.6、 多方安全计算

多方计算（MPC）模型定义了一种多方协议，允许他们在不破坏其输入隐私的情况下共同对其私有数据输入进行一些计算，而仅获知联合计算的输出。

近年来，MPC已在区块链系统中用于保护用户的隐私。比特币系统上设计并实现了安全的多方计算协议。

一种名为Enigma[13]的去中心化SMP计算平台采用了可验证的秘密共享方案来保证其计算模型的私密性。 此外，使用修改后的分布式哈希表对共享机密数据进行编码，以实现高效存储。 它利用外部区块链作为事件的防腐败记录，并利用对等网络的监管者进行身份管理和访问控制。 类似于比特币系统，Enigma提供了对个人数据的自主控制和保护，同时消除了可信第三方的必要性和依赖性。

此外在基于区块链的可验证计算方面，由于区块链、安全多方计算和可验证同态秘密分享都是为了在不可信环境中创造可信信息分享，所以区块链与安全多方计算和可验证同态秘密分享的结合具有先天优势[14]。

3.7、 基于受信任的执行环境（TEE）的智能合约

如果执行环境提供了用于应用程序执行的完全隔离的环境，则该执行环境称为TEE，这可以有效防止其他软件应用程序和操作系统篡改并了解其中运行的应用程序的状态。英特尔Software Guard eXtensions（SGX）是实现TEE的代表性技术。例如，Ekiden [15]是用于保护机密合同的基于SGX的解决方案。 Ekiden将计算与共识分开。它在链上的计算节点上的TEE中执行智能合约计算，然后使用远程证明协议来验证链上计算节点的执行正确性。共识节点用于维护区块链，不需要使用受信任的硬件。 Enigma 在其当前版本中利用TEE允许用户使用分散的信用评分算法来创建保护隐私的智能合约。信用评分会加权多个因素，例如帐户的数量和类型，付款历史和信用使用率。

3.8、 基于游戏的智能合约

基于游戏的智能合约验证解决方案是最近的研究发展，以TrueBit [16]为代表。

TrueBit使用交互式“验证游戏”来确定计算任务是否正确执行。 TrueBit提供奖励以鼓励玩家检查计算任务并查找错误，以便智能合约可以安全地执行具有可验证属性的计算任务。此外，在每一轮“验证游戏”中，验证程序都会递归检查越来越小的计算子集，这使TrueBit大大减少了其节点上的计算负担。

Arbitrum设计了一种激励机制，供各方就虚拟机的行为达成链下协议，因此它仅要求验证者验证合同的数字签名。对于试图掩盖虚拟机行为的不诚实方，Arbitrum设计了一种有效的基于挑战的协议来识别和惩罚不诚实方。虚拟机行为的链下验证的激励机制已大大改善了智能合约的可扩展性和隐私性。

1. 近年隐私保护技术的研究

4.1、 匿名签名

Chunpei Li[17]等提出了一种基于群组签名思想的区块链模型，以许可区块链为底层架构，旨在消除区块链技术中隐私保护与监管之间的矛盾，并设计了三种方案，分别称为GroupSig，GroupCT和Semi-Stealthaddress。并分析了Groupchain系统的正确性，匿名性，可追溯性和组成Groupchain的各个部分的效率。

4.2、 零知识证明

管章双[1]基于零知识证明针对账户模型区块链设计了一种名为BlockMaze的隐私保护方法。利用了承诺机制的隐藏和绑定特性，并提出了一个双余额模型以记录零知识余额和明文余额。结合零知识证明机制设计了两步资金转移操作以隐藏交易双方间转账关系。通过实验测试，BlockMaze的性能能够满足较快速的计算和处理交易。

Benedikt B[18]等提出一种基于账户模型的完全去中心化的保密支付方案，利用ElGamal加密有效隐藏了交易金额。为了在使用ElGamal加密的情况下进行零知识证明，作者提出了无需可信设置的零知识证明机制Σ-Bullets。作者还提出了一个扩展方案，不仅可以做到保密交易还可以做到匿名交易，利用匿名集隐藏交易发送者和接受者的地址。两种隐私方案均可与以太坊及其他之智能合约平台兼容，不会有像基于UTXO模型的方案那样有状态无限增长的情况，且可以防止非正常预先交易和重放攻击。

4.3、 同态加密

李建珍[10]设计了基于Paillier同态加密的以太坊隐秘交易方案，并设计了金额隐藏方案。基于密文交易合法性验证原理，设计了交易验证方案，可以对交易完成后的账户余额进行更新。经测试得出该方案不仅能够有效隐藏交易金额，还能在保证足够高的安全性的前提下，表现出较好的存储性能和时间性能，适合应用在区块链隐私保护中。

马平[9]改进NHTU-FHE17方案。利用改进方案将敏感交易数据加密为对应密文。为保证敏感交易数据加密前后在智能合约中的数据类型不变，设计了改进方案密文向量整数化算法及其逆算法用于完成交易验证。该方案首次将词法分析和全同态加密与区块链智能合约结合，一定程度上解决了区块链隐私保护问题。

Shunli Ma[19]等提出了一种同态加密方案，并构造了一个紧凑的NIZK方案来证明交易的有效性。在其中的NIZK自变量系统中，public参数用作公共参考字符串，对于多个证明仅生成一次。在安全性方面，可以在标准CRS模型中实现零知识属性，而在RO模型下可以获得稳健性。基于NIZK方案，作者描述了一种在帐户模型下隐藏了余额和交易金额的去中心化智能合约系统的框架。

4.4、 多重签名

Manu D[20]等针对在权益证明（PoS）区块链中后验腐败构成了共同的威胁，因为对手在验证一个区块并使用其签名密钥来验证另一个区块后会破坏委员会的验证者的问题。作者介绍了Pixel，这是一种基于配对的正向安全多重签名方案，已针对区块链进行了优化，可大幅节省带宽，存储要求和验证工作。像素签名由两个组元素组成，与签名者的数量无关，可以使用三个配对和一个乘幂进行验证，并支持将单个签名非交互式聚合为一个多重签名。像素签名也是前向安全的，并且允许签名者随时间发展其密钥，从而使得新密钥不能用于在旧块上签名，从而防止对区块链的后验破坏攻击。Pixel在存储，带宽和块验证时间方面产生了显着的节省。尤其是，Pixel签名将1500笔交易的区块大小减少了35％，并将区块验证时间减少了38％。

4.5、 多方安全计算

针对现有的MPC协议都不能在不显着牺牲性能的情况下运行大规模计算问题，Ruiyu Zhu[21]等开发了nanoPI，它在时间和空间上都非常有效。协议基于WRK，但引入了有趣且必要的修改，以解决一些重要的编程和密码挑战。作者通过构建和运行一系列基准测试应用程序，展示了nanoPI的可扩展性和性能，其中包括主动安全的四方逻辑回归（涉及47亿个AND和89亿个XOR），该过程在不到28小时的时间内完成了四个小型的内存机器。

Assi B[22]等介绍了第一个用于在最终用户之间部署大规模MPC协议的端到端自动化系统，称为MPSaaS（用于MPC系统即服务）。系统使各方能够预先注册即将进行的MPC计算，然后通过在VM实例上运行软件（例如，在Amazon中）或通过在移动应用程序中运行协议（在其浏览器中的Javascript中）来参与，甚至在物联网设备上。系统包括一个用于部署MPC协议的自动化系统，一个用于设置MPC计算和邀请参与者的管理组件以及一个用于在实际的最终用户环境中运行MPC协议的最终用户组件。作者为运行安全轮询和调查的特定应用演示了系统，其中安全计算端对端运行，而各方实际上都在运行协议（即，无需依赖一组服务器来运行协议）。

1. 总结与展望

（1）没有任何单一技术是区块链安全和隐私的灵丹妙药。因此，应基于安全性和隐私要求以及应用程序的上下文来选择适当的安全性和隐私技术。通常，多种技术的组合比使用一种技术更有效。例如，将最先进的加密技术SMPC和硬件隐私技术TEE与区块链相结合，以提供对加密数据的大规模计算。

（2）没有技术在各个方面都没有缺陷或完美无缺。当我们将新技术添加到复杂的系统中时，它总是会导致其他问题或新的攻击形式。这需要仔细注意将某些安全和隐私技术集成到区块链中所引起的陷阱和潜在危害。

（3）迄今为止发现的一些基于区块链的系统遭受的攻击。但是，几乎没有做出任何努力来提供对安全性和安全性的深入分析。若能够从根本上分析系统的安全性和隐私漏洞，揭示当前区块链部署模型中漏洞的根本原因，便可以进一步强化或者创新当前的安全和隐私技术。

（4）在安全性，隐私性和效率之间始终存在折衷。我们应该在区块链上倡导那些安全性和隐私性。

参考文献：

1. 管章双. 基于零知识证明的账户模型区块链系统隐私保护研究[D]. 山东大学计算机科学与技术学院，2020.
2. Zhang, Rui，Xue, Rui，Liu, Ling. Security and Privacy on Blockchain . ACM Computing Surveys, Volume 52, Issue 3July 2019, Article No.: 51, pp 1–34. https://doi.org/10.1145/3316481.
3. 郁鑫. 区块链隐私保护关键技术研究与应用[D]. 南京邮电大学计算机科学技术，2019：2-6.
4. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the Thirteenth EuroSys Conference. ACM, 2018: 30.
5. Huang B , Liu Z , Chen J , et al. Behavior pattern clustering in blockchain networks[J]. Multimedia Tools and Applications, 2017, 76(19):20099-20110.
6. Joseph P, Thaddeus D. The bitcoin lightning network: Scalable Off-Chain instant payments [EB/OL]. [2018-12-12], http://lightning.network/lightning-network-paper.pdf
7. Gregory M. CoinJoin: Bitcoin privacy for the real world[EB/OL]. [2018-12-11]. http://bitcointalk.org/index.php?topic=279249.0
8. Kyle T. CoinShuffle aims to improve privacy in bitcoin[EB/OL]. [2018-12-23]. http://insidebitcoins.com/news/coinshuffle-aims-to-improve-privacy-in-bitcoin/29269
9. 马平. 基于词法分析与全同态加密的区块链隐私保护研究[D]. 云南大学数学与统计学院，2019.
10. 李建珍. 基于Paillier同态加密的区块链交易隐私保护的应用研究[D]. 东南大学软件工程，2019.
11. Chiesa A, Ojha D, Spooner N. Fractal: Post-quantum and transparent recursive proofs from holography[J]. IACR Cryptology ePrint Archive, 2019.
12. Mailer M, Bowe S, Kohlweiss M, et a1. Sonic: Zero-knowledge SNARKs from linear-size universal and updatable strucW red reference strings[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019: 2111-2128.
13. Guy Zyskind, Oz Nathan, and Alex Pentland. 2015. Enigma: Decentralized computation platform with guaranteed privacy. Comput. Sci. (2015).
14. 周李京. 区块链隐私关键技术研究[D]. 北京邮电大学网络空间安全学院， 2019.
15. Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah M. Johnson, Ari Juels, Andrew Miller,and Dawn Song. 2018. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contract execution. CoRR abs/1804.05141 (2018).
16. Jason Teutsch and Christian Reitwießner. 2017. TrueBit: A scalable verification solution for blockchains.）和Arbitrum（Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten. [n.d.]. Arbitrum: Scalable, private smart contracts. In USENIX Security 2018. 1353–1370.
17. Li C , Wang L E , Xu Q , et al. Groupchain: A Blockchain Model with Privacy-preservation and Supervision[C]// HP3C 2020: 2020 4th International Conference on High Performance Compilation, Computing and Communications. 2020.
18. Benedikt Bünz, Agrawal S , Zamani M , et al. Zether: Towards Privacy in a Smart Contract World[M]// Financial Cryptography and Data Security. 2020.
19. Ma S , Deng Y , He D , et al. An Efficient NIZK Scheme for Privacy-Preserving Transactions over Account-Model Blockchain[J]. IEEE Transactions on Dependable and Secure Computing, 2020, PP(99):1-1.
20. Manu Drijvers, Sergey Gorbunov, Gregory Neven, Hoeteck Wee. Pixel: Multi-signatures for Consensus[R]. Proceedings of the 29th USENIX Security Symposium. August 12–14, 2020, 978-1-939133-17-5.
21. Ruiyu Zhu, Darion Cassel, Amr Sabry, Yan Huang. NANOPI: Extreme-Scale Actively-Secure Multi-Party Computation[J]. CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications SecurityOctober 2018, pp 862–879https://doi.org/10.1145/3243734.3243850
22. Assi Barak, Martin Hirt, Lior Koskas, Yehuda Lindell. An End-to-End System for Large Scale P2P MPC-as-a-Service and Low-Bandwidth MPC for Weak Participants. CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications SecurityJanuary 2018 Pages 695–712https://doi.org/10.1145/3243734.3243801