

8th 面向可持续发展目标 (SDGs) 的

2024 年 TICC 国际会议 整合不同学科的视角，满足当前和新出现的

社会需求

2024 年 2 月 1st - 2nd，泰国曼谷

凭证控制余额：从银行到比特币、以太坊的通用区块链账户模型摘要

外部自有账户和账户抽象

焦慧峰、Nathapon Udomlertsakul 博士、Anukul Tamprasirt 博士

清迈大学数字创新国际学院，泰国清迈，50200¹ 电子邮件：huiheng_jiao@cmu.ac.th,
nathapon.u@icdi.cmu.ac.th, anukul@innova.or.th

摘要

区块链市场价值曾达到 3 万亿美元的峰值，后跌至 1 万亿美元，然后回升至 1.5 万亿美元，并再次上升。在这个巨大的市场中，区块链账户确保了大部分链上资产的安全（Web-12）。本文通过对区块链账户发展的全面回顾，从学术界和业界的角度出发，提出了一个**通用的区块链账户模型**。本文采用**模型分析方法**分析账户进展，**创建高水平的新账户模型**。并采用**系统的文献综述方法**，对有关**账户模型**的论文进行了检索、筛选、分析和评价，并分析了相关的**技术权衡**。本研究在WOS、Scopus以及比特币和以太坊社区资料库中搜索关键词：区块链、账户、私钥和安全，深入了解从传统银行账户到比特币、EVM适配和抽象账户等账户模型的设计和评估。通过数据驱动的账户模型**比较**（安全性、成本、采用率），本研究还探索了未来的方向，并提供了跨模型账户理论概述，为进一步的区块链研究提供指导。本文对模型变化的驱动因素、应用技术的进步进行了深入探讨。

关键词： 区块链账户、私钥、安全、隐私、大规模采用

1 引言

账户是一个常识性概念，因为银行账户就在您的日常生活中。理查德和彼得的论文列出了几种银行账户类型。例如，有存款账户和托管账户。它们依赖于三大银行服务。这些服务包括支付、保险和中间业务（Davies，2010 年）。与早期的银行账户一样，区块链账户现在也是一种存款和支付账户类型。它将发展成为像银行账户一样更复杂的账户类型。这将与区块链的未来相适应。中本聪在比特币白皮书中定义了区块链和第一个区块链账户（Nakamoto, n.d.）。区块链账户持有数字签名，控制比特币余额，这为所有权提供了强有力的控制。

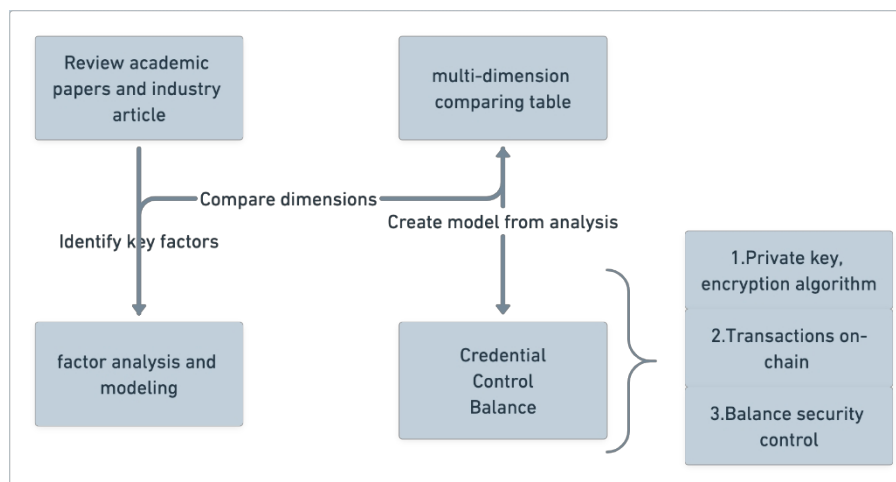


图 1：研究流程

加密货币市场是一个正在崛起的市场，它将成为影响每个人的重要市场。抛开投机和泡沫



不谈，加密货币市场的繁荣也反映了加密货币行业的持续增长。

图 2：2023 年 11 月加密货币市场总市值

区块链账户在不断发展。数字签名（Diffie & Hellman，2021 年）和应用算法 RAS（Rivest 等，1978 年）、Merkle 哈希算法（Debnath 等，2017 年）技术、ECDSA（椭圆曲线数字签名算法）（Johnson 等，2001 年）等等，都在提高账户的安全级别。但仍有一些问题有待解决（Web-10）。这些问题包括严重的安全问题、TPS（每秒交易量）低和验证时间长。此外，交易流程复杂、私钥易丢失、技术使用门槛高、气体成本高也是问题所在。安全、连续性/UX（用户体验）和成本，这些挑战可能会阻碍人类在数字未来中广泛受益。

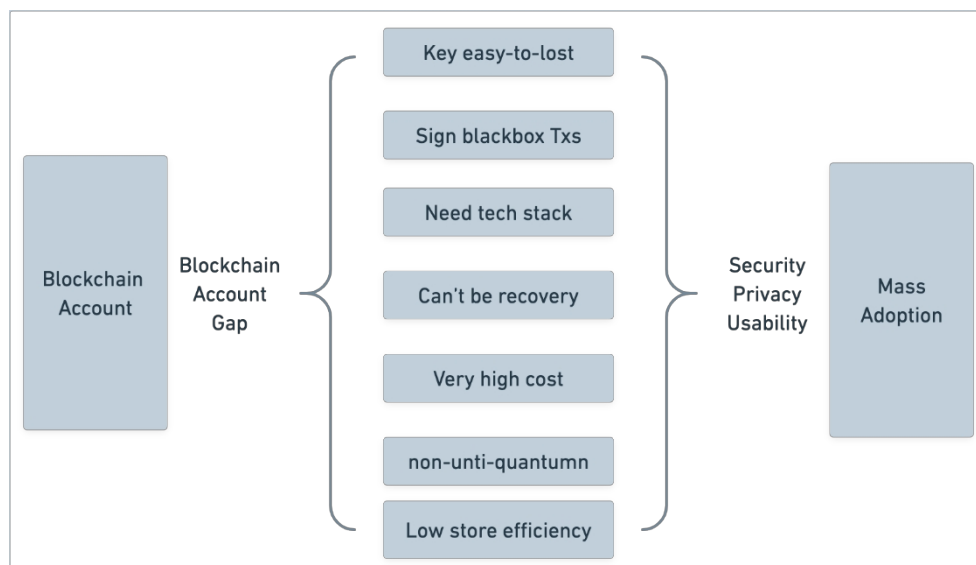


图 3：现在账户与未来账户之间的差距

我们可以根据常识经验建立一个假设模型：**凭证控制余额**。这一模型基于银行账户的抽象。区块链账户将围绕这些推出许多能力。

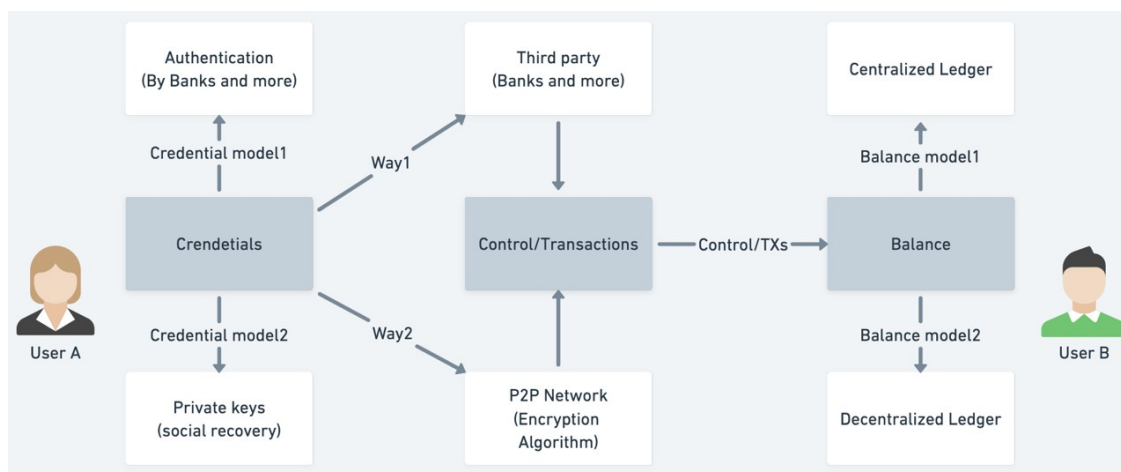


图 4：全民账户概念模型

比特币账户模型（也称区块链账户模型）包括凭证模型、控制模型和余额模型。**凭证子模型**是基于分散共识的数字签名。**控制子模型**是基于 PoW 网络（工作证明）和签名验证方法的哈希算法和交易。**余额子模型**是UTXO（未花费交易输出），它就像很多面额可变的钱。它既安全又不会重复消费。比特币账户模式实现了“**无需可信第三方**”的点对点交易（Nakamoto, n.d.）。

EOA（外部自有账户）是以太坊（Web-11）的第二类区块链账户，但容易丢失和被黑客攻击。EOA保留了EVM适应链的大部分资产。EIP55(Web-4)协议遵循继承自BIP39(Web-1)等的账户计算惯例。它使用 ECC（椭圆曲线加密）/Secp256k1（安全椭圆曲线加密参数）（Web-13）（

Brown, n.d.) 和 SHA256 (安全散列算法) (Web-7) 散列加密。

计算私钥和公钥的方法更安全。您必须小心保管您的私人密钥。丢失一次，损失全部。

AA（账户抽象）（Web-10）是 EVM 适应链中的一种开发账户类型。它出现在以太坊、Layer1、Layer2 等链中。它通过将交易流分解成许多模块来扩展其能力，从而实现大规模采用。由私钥产生的所有者地址是链上合约的一个插槽。社会恢复可以改变它。合约可以接受不同的签名算法。气体支付可以由外部资源委托。它有许多改进之处，但也存在一些问题。例如，它有一个复杂的系统架构。它很难构建，也很难保持地址的一致性。此外，它的燃气费也很高。UTXO、EOA 和 AA 是目前流行的区块链账户模式。

区块链是一个新兴产业。目前有许多公有链，如以太坊、Optimism、BSC（Binance 智能链）、Arbitrum 等。大多数区块链都遵循比特币的模式：使用密钥对（包括私钥）签署数字签名，使用公钥验证签名和交易执行，这些都是由加密算法产生的。













Name	Protocols	Addresses	1d Change	7d Change	1m Change	TVL	Stables
1  Ethereum	1004		-0.77%	-0.49%	+11.12%	\$32.985b	\$71.486b
2  Tron	29		-0.06%	-4.06%	-6.14%	\$7.804b	\$52.174b
3  BSC	690		+0.30%	-3.05%	+8.98%	\$3.488b	\$32.58m
4  Arbitrum	526		-1.32%	-0.72%	+7.98%	\$2.589b	\$2.125b
5  Solana	123		+1.94%	-3.71%	+33.98%	\$1.368b	\$1.919b
6  Polygon	513		+0.55%	-4.27%	-2.65%	\$850.44m	\$1.31b
7  Optimism	218		+0.37%	-7.41%	-2.89%	\$839.51m	\$606.12m
8  Avalanche	359		-0.16%	-7.76%	-14.43%	\$804.13m	\$1.104b
9  Manta	32		-0.32%	+3.63%	+659%	\$429.17m	
10  PulseChain	34		-2.61%	+96.70%	+182%	\$412.22m	
11  Base	208		-0.35%	-6.63%	-10.76%	\$401m	\$297.29m
12  Cardano	33		-0.13%	-5.69%	-15.68%	\$351.87m	\$19.12m

图 5：Defilama 上区块链的总锁定值排名

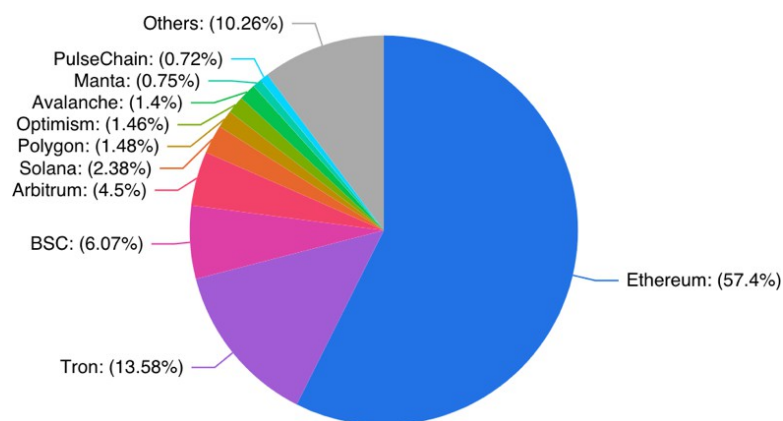


图 6：市场份额饼图

本文采用了系统的文献综述方法。它收集并研究了大多数关于区块链账户的论文。研究目的是对区块链账户的发展进行全面回顾。本文还对**账户模型**进行了评估。它使用统计表方法比较了不同账户模型的**权衡**。同时，我们还通过模型图来阐明账户的基本操作和交互流程。我们将对区块链账户的学术史进行回顾。

这项研究分析了不同时期区块链账户模式的所有结构。它提出了一个新概念--**通用区块链账户**：即区块链使用哈希函数和椭圆曲线数字签名作为账户的唯一秘密凭证。并使用区块聚合所有交易的哈希值来保证您资产的控制权。使用UTXO、Merkle树和Verkle树来快速、安全地存储和更改您的余额。它将用三角形来评估每种模式：安全性、便利性和成本。这些模式应满足未来大规模采用的需求。

2 文献综述

账户的概念经历了几个世纪的演变，从简单的纸质分类账到现代数字银行账户，再到现在的区块链世界。这一历程标志着一个关键的转变：信任和责任正在从中心化的机构转向技术赋权的个人。

传统上，账户依赖于集中验证和保证（想想理查德和彼得的会计（Davies，2010 年））。中本聪（Satoshi Nakamoto，n.d.）首创的区块链技术以加密证明和分布式共识取而代之，正如数字信任和签名方面的著作所探讨的那样（Debnath et al.）对隐私和控制的担忧（在比特币白皮书（Nakamoto，n.d.）和相关研究（Debnath et al., 2017）中得到了强调）助长了这一转变，为账户管理的新时代铺平了道路，用户可以直接控制自己的资产，同时保持系统的完整性。

但是，我们如何确保区块链网络内的安全互动呢？创建独一无二的安全区块链账户凭证是关键。数字签名和哈希函数等加密工具是账户安全的基础。用户根据 RFC2459 等标准生成一对密

钥（私钥和公钥），无需依赖中央机构（Housley et al.）公钥经过散列后变成一个唯一的标识符，成为用户的区块链地址。

在分散式系统中丢失这些凭证可能会造成毁灭性的后果。严格的恢复和备份最佳实践至关重要。有关数字签名的文献强调使用记忆性短语从安全词表（Web-2）和分层确定性（HD）钱包（Web-3）中衍生出来，以实现

从丢失的私钥中恢复。更新的协议，如无记忆符号的社交恢复，有望在区块链系统中实现更强大的自我主权身份管理。

区块链技术的核心意义在于能够在没有中心化可信实体的环境中管理资产余额并促进交易。与传统的银行账户不同，金融机构是余额管理和交易验证的可信中介，而区块链网络则利用去中心化的共识机制来实现同样的目标。比特币网络的未花费交易输出（UTXO）模式是这一原则最早、最突出的体现，也是中本聪的开创性白皮书（Nakamoto, n.d.）开创的新范式。每个UTXO代表一种未使用的离散数字货币，实际上是一种无记名票据。用户通过消耗这些UTXO并在链式区块中生成新的UTXO来进行交易，从而确保每个单位的加密货币都以一定的容量被唯一地记录在网络分类账中（Chakravarty et al.）这种机制通过建立不依赖中介机构而依赖加密验证的交易历史，从本质上促进了审计工作。同时，文献还指出了一系列基于账户的模式，包括以太坊平台，在该平台上，个人账户余额随每笔交易更新，就像传统的银行分类账一样；不过，这些更新是通过共识在全网传播的，不需要可信的第三方（Chakravarty 等人，2020 年）。基于区块链的机制不仅要消除金融业务中的中心化，还要为网络中的每个参与者提供隐含的安全性和透明度。

区块链生态系统中的账户基础设施会有很大差异，表现为不同的交易处理和状态维护模式。比特币方法的核心是未支出交易输出（UTXO）模式，这一创新将比特币的每一部分都细致地编入已支出或未支出的目录，从而确保余额计算的准确性，并防止重复支出，而无需可信的机构（Nakamoto, n.d.）。相比之下，以太坊采用了基于账户的模式，主要是通过外部自有账户（EOA）和最近的账户抽象（AA）模型。EOA 的运作方式类似于传统的银行账户，采用基于非 Cee 的交易排序，简化了状态转换逻辑，但矛盾的是却提高了密钥管理不善和丢失的风险（Li 等人，2020 年）。账户抽象（Account Abstraction）试图通过将用户账户转化为智能合约来改善这一问题，允许更复杂的访问控制选项，包括恢复机制和交易费支付授权，这对用户的可访问性和安全性至关重要（Web-10）。还有其他一些区块链账户模式。互联网计算机（ICP）创建了一个内部构建账户模型，具有强大的账户功能，如与不同的DApps（去中心化应用程序）建立即时子账户，以实现高隐私性（Web-5）。

在密码学领域，账户访问和安全性已开始与生物识别模式交织在一起，努力提升用户体验，同时加强安全保障。FIDO（快速身份在线）协议就是这种扩展的缩影，它支持生物识别解决方案，如指纹识别，用于验证区块链操作，在解决可用性问题的同时又不影响安全性（Merkle, 1987）。各种平台正在超越传统凭证：互联网计算机协议（ICP）利用用户指纹进行账户验证，从而将与生俱来的生物特征与加密过程交织在一起，这是一个前沿领域，在隐私影响和包容性方面还没有完全明确（Farrugia et al.）以太坊社区也在基于 ERC4337 发展账户模型。他们试图通过内置客户端协议建立一个原生账户抽象，从而提高效率和安全性，降低复杂性和成本（Web-6）。

另外，StarkNet 和 Polygon 等 Layer2 解决方案正在探索可扩展性和效率，这表明它们正朝着更精细的账户模型迭代发展，以同时保证功能性能和用户安全（Ma 等人，2021 年）。一些 ZK-SNARKs 链尝试使用 ZK 证明来验证数据或交易，同时又不泄露原始数据，从而找到一种更具隐私性的账户模型（Guan 等人，2022 年）。每种模式都有其独特的优势和局限性，映射出区块链账户基础设施向安全、实用性和包容性的微妙平衡靠拢的多样化格局。

区块链技术的一个重要方面是，它能够维持一个点对点的账户余额系统，而无需可信实体的中介--这与传统金融系统对中央机构的依赖截然不同。这种去中心化的基石是账户余额的维护是共识机制的巧妙应用。这种机制促进网络参与者就有效交易达成一致，有效确保了余额更新的完整性和可验证性。其中最主要的是工作证明（PoW）和权益证明（PoS）等协议，尽管它们的操作策略各不相同，但都服务于分布式信任的统一目标（Cao 等人，2020 年）。文献揭示了这些范例，如 "信任与电子声誉"，更多的组织和个人在声誉探索中尝试在电子声誉上建立信任（Web-8）（Zinko 等人，2007 年）（Web-9）。

"PKI信任模型概述"以及更多的公钥基础设施（PKI）（Buchmann等人，2013年）（S. Khan 等人，2023年）（Perlman，1999年），阐明了与认证机构（CA）不断发展的数字信任概念。但在区块链信任网络中，单个节点集体承担了传统上由银行或 CA 承担的角色，技术信任取代了机构信任。然而，对纯技术共识的依赖也带来了挑战，特别是可扩展性三难问题，即去中心化、安全性和速度之间的微妙平衡。因此，区块链账户继承了数学形式的 PKI，使用私钥和公钥系统（Koblitz，1994 年）。这些资料深入探讨了共识驱动的平衡管理的复杂性，对现状提出了精辟的观点，并设想了数字分类账的潜在改进方案。

安全考虑是区块链账户模型的核心，因为这些系统的完整性和可信度是其被广泛接受和取得成功的关键。多年来，已经发现了各种安全漏洞和漏洞，从智能合约中的代码漏洞到针对私钥的社交工程攻击（Atzei et al.）值得注意的事件凸显了严格的安全措施的重要性，促进了对区块链系统稳健性和潜在攻击表的研究。例如，一些研究侧重于检测区块链网络上的非法活动，揭示了改进监控和欺诈检测机制的必要性（Farrugia 等人，2020 年）。为降低此类风险，有人提出采用先进的加密技术，包括带有阈值签名的椭圆曲线数字签名算法（ECDSA）（Goldfeder et al. 此外，多重签名方法（带阈值签名）也受到了关注，因为它们要求多方在交易上签名，从而增加了一层额外的安全性，以防止未经授权的资产转移（Goldfeder 等人，2014 年）。这种方法分散了与单一私钥控制相关的风险，这种设计已被证明能显著增强区块链账户的安全态势（Andrychowicz 等人，2016 年）。加密标准的不断演进和多签名钱包的推出，体现了为确保区块链账户安全以应对所面临的各种威胁而做出的不懈努力。

隐私在区块链开户送体验金无需申请中的重要性怎么强调都不为过，因为它是用户自主性和安全性原则的基础。在区块链背景下，零知识证明和 ZK-SNARKs 等密码学工具的出现为区块链系统中的隐私增强提供了重要信息（Ma 等人，2021）（Guan 等人，2022）。零知识证明允许在不泄露底层交易数据的情况下验证交易，因此在保护隐私的同时，还能提高区块链系统的安全性。

保持事务的完整性。ZK-SNARKs--非交互式知识论证--通过最大限度地减少计算开销和证明者之间的交互，进一步简化了这些证明。

和验证器。基础研究表明，这种方法可以稳健地应用于账户模型，在赋予交易数据隐私性的同时，还能确保问责制和可验证性，而这正是区块链的关键所在（Ma 等人，2021 年）（Guan 等人，2022 年）。

而隐私权的实现需要权衡利弊。加密协议的计算强度大，可能会对区块链网络的可扩展性和延迟带来挑战，可能会影响交易吞吐量，导致成本上升。隐私保护技术的复杂性可能会提高用户理解和参与的门槛，从而有可能影响交易吞吐量并导致成本增加。

影响广泛采用。现在，零知识技术提供了令人信服的隐私保护能力。在人类数字化的未来，它可以帮助创建像电子邮件账户一样的大规模应用。

区块链未来能否被大规模采用，取决于区块链账户是否依赖于技术和以人为本的障碍。**可用性**非常重要；用户与区块链技术的交互必须直观、无缝，才能获得广泛接受（Brünjes & Gabbay, 2020）。研究表明，潜在用户对区块链的认知和理解深刻影响着他们采用该技术的意愿（Tsai 等人，2018 年）。事实上，区块链的复杂性可能会让非技术用户感到恐惧，从而阻碍其主流应用。**安全性**通常是用户最关心的问题，这是一种不影响可用性的强大保护措施。**隐私**也是一个重要的考虑因素；用户必须确信他们的交易和余额是保密的。然而，实现高水平的安全性和隐私性往往要以牺牲易用性为代价，这也是研究人员和开发人员必须权衡的问题。因此，区块链系统的设计者们面临的挑战是如何找到一个平衡点来解决这些因素，确保数字资产的安全和隐私管理不会因为复杂性而阻止潜在用户的使用。

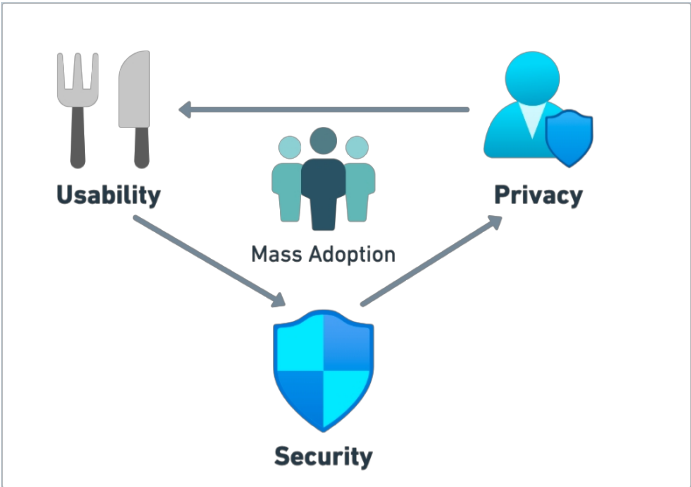


图 7：账户权衡模式

尽管有关区块链的研究越来越多，但明显缺乏专门针对区块链账户模式的全面通用模型（Wood & others, 2014）。这种疏忽是至关重要的；随着数字交易系统数量的增加，了解账户模式的全部内容--从老式银行账户到实用的区块链变体--变得更加重要。从传统银行系统到去中心化架构的演变

我们需要深入研究区块链模式的内在核心组成部分。可用性、安全性和隐私之间的权衡随着时间的推移而不断变化。因此，在基本银行原则和区块链技术引入的创新模式之间架起桥梁的广泛分析不仅有保障，而且至关重要。这种差距凸显了研究界开发通用账户模型的必要性，该模型不仅可以**解释**账户演变过程中的技术机制，还可以**解释**可能影响账户管理和治理未来**发展的**范式转变。

区块链账户的未来既要保持系统信任的不可变核心原则，又要满足不断发展的用户期望。

不可更改的交易和加密区块链网络仍然是用户信心和技术完整性的基础。最近的趋势，尤其是在增强用户体验和提供监管合规性方面，预示着未来区块链账户必须在安全性和便利性之间取得平衡（Atzei 等人，2017 年）。可扩展性解决方案，无论是链上进步还是链下协议，都在不断发展，以满足未来的需求。

用户群不断扩大（D. Khan 等人，2021 年）。区块链技术与各行各业的融合

从金融到医疗保健--鼓励多学科研究，旨在建立一个通用账户模型，简化用户交互，同时保持强大的安全措施。学者和企业

因此，从业人员的任务是为大规模采用区块链技术开辟道路，设计复杂但用户友好的界面，并确保不同区块链生态系统之间的互操作性（D. Khan 等人，2021 年）。这种通用账户模式希望成为大规模应用的蓝图，体现技术能力与用户需求之间的权衡与协同。

3 方法

本研究的方法对于解决区块链账户技术中根深蒂固的各种挑战的有效性和连贯性至关重要。**系统的文献综述**方法是本研究的关键点，它经过精心挑选，可以剖析和驾驭**学术文章**和**行业领域**中错综复杂的安全、隐私和障碍问题。

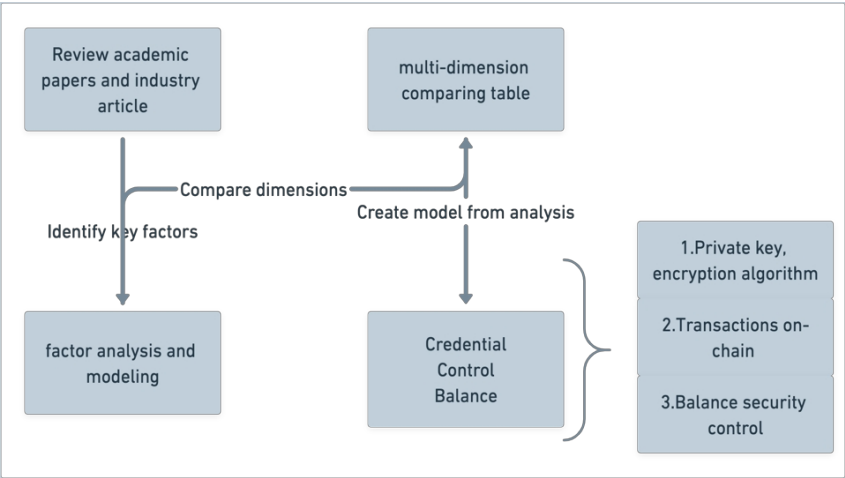


图 8：通用概念账户模型

这种方法符合全面性、客观性和可复制性等学术要求，对于建立一个能够研究区块链账户的演变和采用的强大框架至关重要。这种方法的灵活性使其能够囊括各种不同的观点，形成一种全面的理解，既能阐明区块链账户技术的技术复杂性，又能阐明其社会影响。除了单纯的评论之外，本书还旨在构建一个知识网络，为未来的创新、政策制定和学术研究提供有效的信息，帮助人们了解区块链账户技术不断拓展的数字领域。

区块链账户是加密货币行业的一种实践模式，因此我们采用**模型分析法**对账户相关模型进行分析和评估。分析对象包括五个行业阶段：银行账户、比特币账户、EOA 账户及其他、抽象账户（合约账户）和其他 EVM 账户。它代表了账户的原始来源和发展路线。

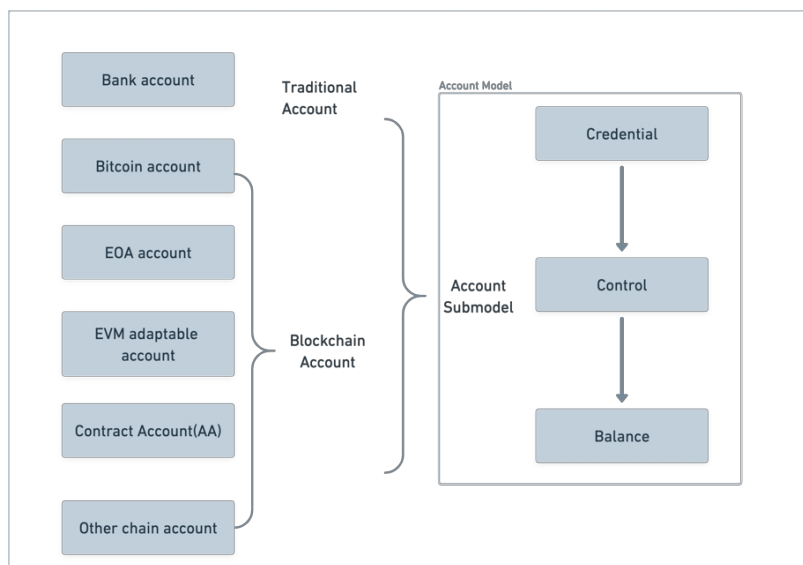


图 9：通用概念账户模型

本文通过对账户历史的分析，将账户分为三个子模块：**凭证、控制和平衡**。这可以为后续工作提供更精确的分析对象和决策视角。我们使用了一个三维评估模型：安全性、便利性和成本，将隐私作为安全性的一部分，并将可用性分为便利性和成本。

本系统性文献综述的数据收集策略取决于对探究区块链账户技术复杂性的行业改进建议和学术文章的细致**汇总**。通过考虑区块链行业提供的技术文档和实证研究结果，特别是白皮书和改进协议，本综述综合了大量数据点，形成了安全、隐私和可用性随时间发展的全面图景。为此，我们设计了一个**庞大的表格矩阵**，以有效比较各种区块链账户模式的特点、优势和弱点。这个详细的表格不仅可以清晰直观地比较各个研究目标，还可以阐明每种模式的演变和范围，从而为分析和讨论提供一个总体接入点。

为了阐明区块链账户模型中固有的复杂相互关系，我们的分析方法结合使用了可视化和表格表示法。**图表**是一种基础工具，可直观地阐明每个模型中区块链账户各组成部分（凭证、控制和余额）之间错综复杂的关系。通过这些示意图，可以直观地理解不同模型之间的细微动态和结构差异。

此外，我们还构建了综合表格，便于对所研究的区块链账户模式进行并列**比较**。这些表格有助于突出差异、划定**权衡**、对比相对优缺点，尤其是在安全、隐私和易用性方面。通过这种**双重策略分析**，我们努力对收集到的数据进行清晰易懂的综合，以满足视觉学习者和喜欢详细量化评估的人的需求。

通过这种方法，我们将对私钥的制作、签名的制作和验证、交易的建立和出块方法、余额的修改以及资产在多账户之间的流动进行**多维度的审查**，并给出一些变化的路径。这些步骤中的安全技巧、这些复杂流程中的交互便利性、这些账户模式行为的隐私和成本权衡。

4 结果与讨论

总结凭证、控制、平衡，讨论这三个子模型的不同模型细节。一些参考资料。

区块链账户确保了区块链上数万亿加密资产的安全。但我们却苦于开设新区块链账户的高科技要求、私钥易丢失等诸多当代问题。而关键问题在于未来的大规模应用。在安全性、便利性和成本方面会有很多问题。我们需要对区块链账户进行全面审查和改进。

区块链账户也遵循基本的账户认知：凭证控制平衡。区块链必须提供去中心化的凭证，以消除第三方的信任。不同的区块链账户模式使用不同的技术来实现去中心化。因此，"凭证控制余额"变成了"d-ledger 中的 d-credential d-control balance"。第一个字母"d"表示去中心化。

这些使用变体技术的模型中的权衡受到不均衡规则的影响。比特币使用UTXO平衡模型来避免双重消费，这是在密码学邮件列表中讨论最多的问题。在比特币之前，戴伟发明了B-money，其重点是分配和密码学安全。尼克-萨博（Nick Szabo）发表了比特黄金（Bit Gold）概念，重点关注计算追索权消耗（Popper, 2015）。

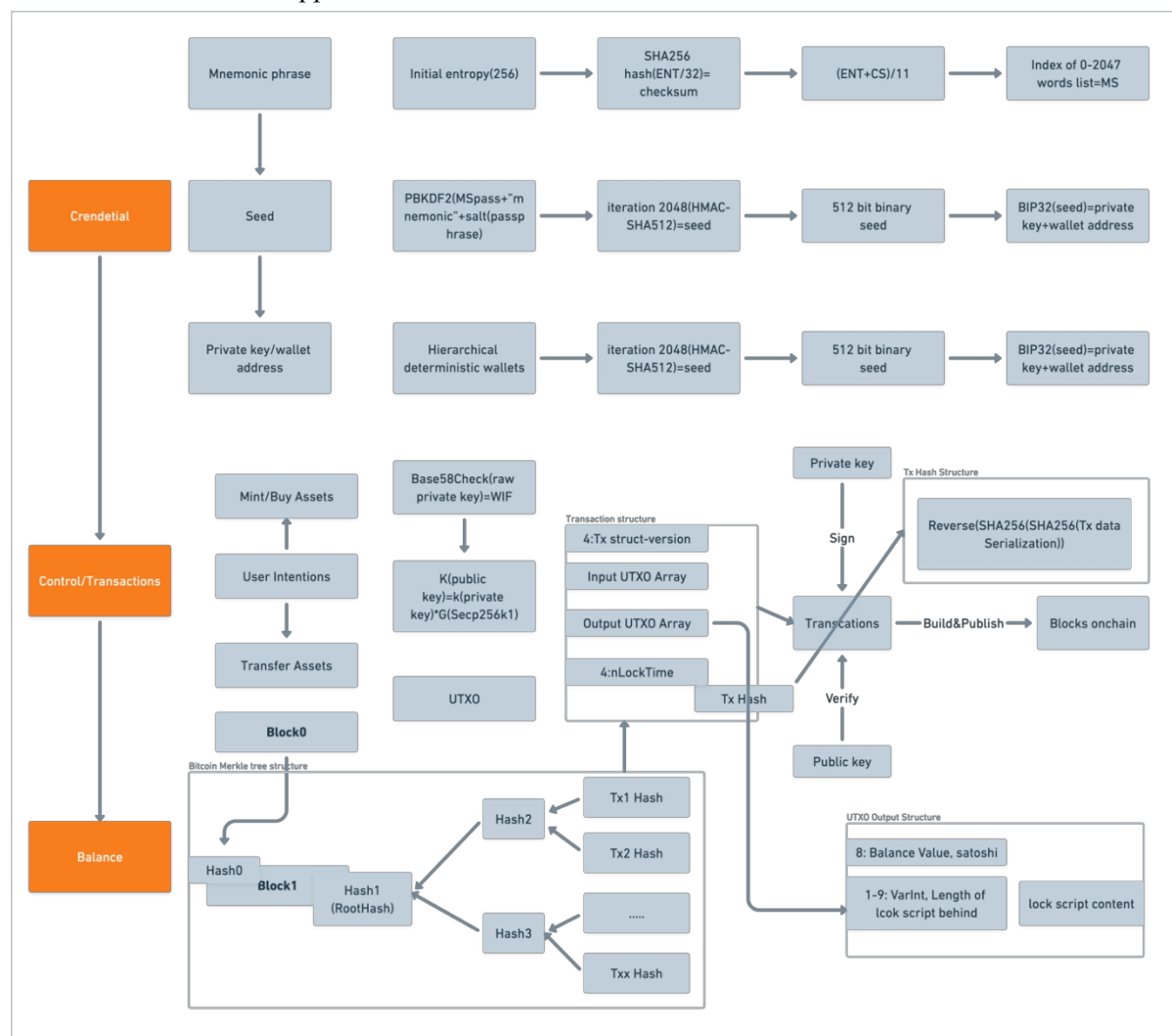
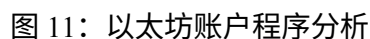


图 10：比特币账户程序分析

EOA 注重工程便利性，因此继承了凭证模型，改变了一些算法和方法，如控制模型 HD Wallet（分层确定性钱包）、使用 Merkle 树的平衡模型。并将控制模型扩展到带有签名的 EVM（以太坊虚拟机）。



上图是以太坊账户机制的详细回顾，你也可以在这里（Web-17）（Web-18）（Web-19）查看真实的链上区块和交易。

账户抽象注重系统的可扩展性，不仅是余额模型，它还注重安全性，如社会恢复机制、不同签名算法支持、入口点合约监控等。它注重便利性，如支持第三方支付燃气费，支持会话密钥、死人开关、指纹 2FA、支持复杂个人或企业流程的多重签名等。我们可以查看普通 EOA 交易和合同账户交易之间的简单对比。

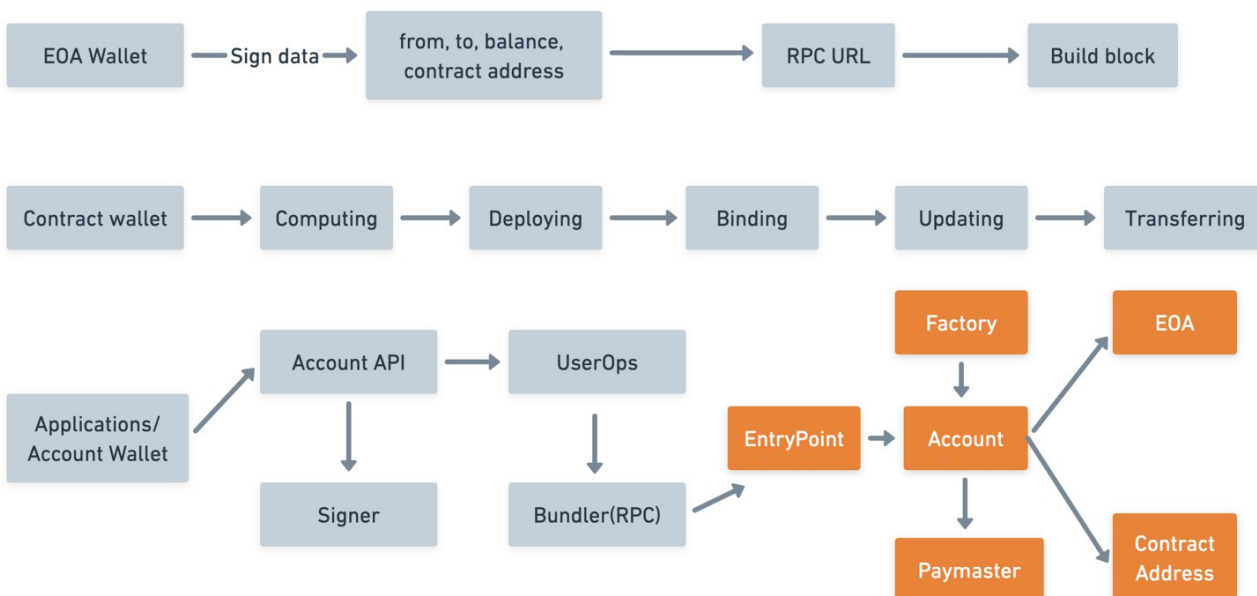


图 12：以太坊合约账户程序分析

账户抽象，它还需要在成本和可组合性方面进行更多的修订，并平衡评估三角：安全性、便利性和成本。否则，以太坊的区块链模式无法支持未来数十亿用户的大规模应用。业界正试图推出 RIP7560（Web-6）来构建原生账户抽象，但我们还需要更多的努力。因此，我们应该深入这一研究领域，以应对这一挑战。

这项研究采用了一系列尖端软件工具和技术。Visual Studio Code是一款可扩展的代码编辑器，为编写脚本和测试我们的分析算法提供了一个高效的生态系统。此外，我们还使用了人工智能编码助手 Code Pilot，它通过建议代码片段和方便调试智能合约代码来帮助简化开发流程。这些工具的结合使我们的分析保持了较高的精确度。我们对数据处理和评估工作流程中的每一步都进行了细致的记录，以便于复制我们的研究，从而维护我们系统审查的完整性和有效性。我们所采用的算法和测试方法既透明又全面，确保研究人员和行业从业人员能够忠实地探索和测试我们的研究结果和结论。

我们通过系统的文献回顾和模型分析来选择和创建区块链账户模型，我们选择那些对行业影响最深远的模型，并在安全、隐私和采用领域提供最广泛的见解。因此，我们的调查涵盖了比特币基于UTXO的系统和以太坊基于账户的框架等重要模型，因为这些生态系统代表了区块链技

术的重要里程碑，并在学术界和业界得到广泛认可。除此之外，我们还考虑了其他可能影响区块链账户技术未来发展轨迹的新兴模式和非传统模式。通过调查这些不同的模式，我们的研究涵盖了不同的人群，从早期的

从嵌入比特币网络的采用者到高级以太坊智能合约平台的参与者，再到其他区块链基础设施的用户。这些模型与我们的研究目标相关，因为它们对区块链领域做出了巨大贡献，帮助我们了解不同的账户结构如何应对安全、隐私和大规模采用等挑战。

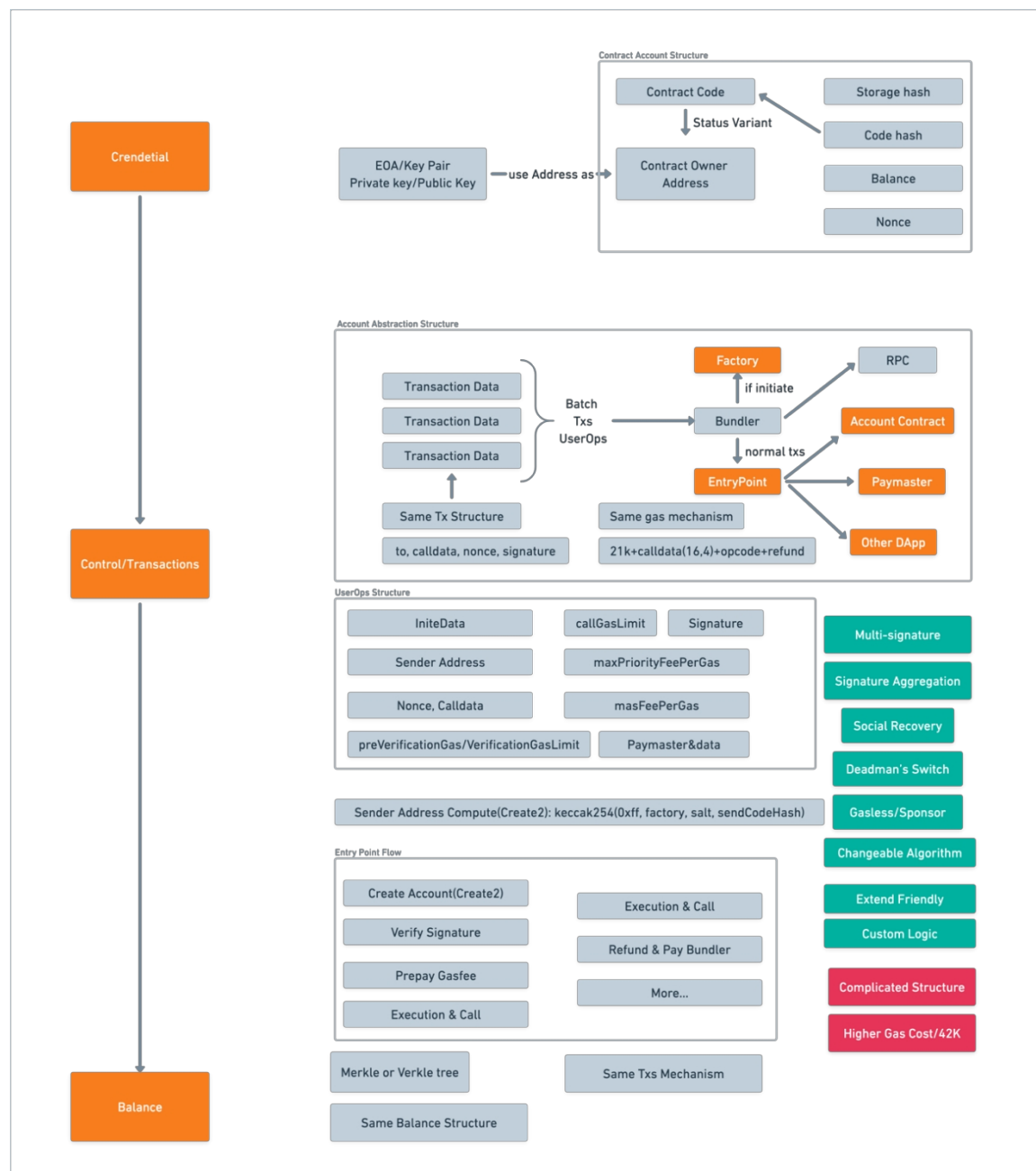


图 13：以太坊账户抽象程序分析

我们的分析框架将区块链账户剖析为三个基本子模块：凭证、控制和平衡，从而为账户模型的复杂性提供了一个细化的视角。凭证 "子模块侧重于确保合法所有权的认证机制，通常是通

过加密密钥管理。控制 "子模块涉及如何管理交易的机制。

包括共识算法和智能合约。最后, "余额"子模块反映了维护和更新资产所有权记录的方法。这些子模块构成了我们比较模型审查的主干, 通过协同互动产生账户的运行概况。为了全面评估这些组成部分, 我们采用了安全性、便利性和成本三维视角--这是评估大规模采用区块链技术倾向的基本标准。这一多维评估模型揭示了区块链账户模型内部和之间存在的权衡和相互依存关系, 从最终用户采用的角度深入分析了它们的能力和局限性。通过这种结构化的分解和评估方法, 我们的研究旨在揭开区块链账户安全性和可用性错综复杂的结构, 为更明智的设计决策铺平道路, 从而促进更广泛的接受。

Submod	Behavior	Attributes/Tradeoffs	1: Bank Account	2: Bitcoin Account	3: EOA of Ethereum
Credential	Create	Who create the key Random number	Centralized Authorities No	Mathematics and Encryption Algorithm(MEA)	MEA
	Encrypt	How to encrypt	Personal password	PBKDF2(MSPass+"mnemonic"+salt(passphrase))	PRNG()=Hex(32Byte);ECDSA(32 PrivateKey)
	Keep	How to keep	keeping using rights	memonic or bare piate key or json file	keystore
	Transaction	Who can launch Tx	User/Authorities	Only User with Private Key(OUPk)	OUPk
Control	Encrypt	Txs with encryption	bare database	spec256k1(ECDSA)	spec256k1(ECDSA)
	Verify	How to verify	Trust Authorities	Trust encryption and key pair verification	Trust encryption and key pair verification
Balance	Logic	Where is the number	Centralized ledger	Decentralized ledger with scattered UTXOs	Decentralized ledger with different account changing Merkle tree
	Storage	How to save	RDBS	Blocks include Merkle tree and Txs, Secp256k1, SHA256	Blocks include Merkle tree and Txs, secp256k1, keccak_256
	Index	Search and interacte	RDBS	Merkel tree	Merkel tree

图 14：账户权衡比较演变表第 1 部分

Submod	Behavior	Attributes/Tradeoffs	4: AA of Ethereum	5: Other Blockchain Account	6: Universal Blockchain Account
Credential	Create	Who create the key Random number	MEA	MEA	MEA
	Encrypt	How to encrypt	the same with EOA	like keccak and ECDSA	changeable; like keccak and ECDSA
	Keep	How to keep	EOA keystore & contract field with social recovery	EVM adaptable are keystore	keystore and social recovery and public guardians
	Transaction	Who can launch Tx	OUPk and relation	OUPk	OUPk and trust network
Control	Encrypt	Txs with encryption	spec256k1(ECDSA)	spec256k1(ECDSA) and other way	spec256k1(ECDSA) and changeable encryption algorithms
	Verify	How to verify	Trust encryption and key pair verification and social relation	Encryption or MPC or mix method	Trust encryption and key pair verification and social relation and DTrust network
Balance	Logic	Where is the number	Same with EOA	Like EOA	Like AA with more friendly interface
	Storage	How to save	Same with EOA; improve Verkle tree future	Like EOA and other encryption algorithms	Like EOA and AA with changeable encryption algorithms
	Index	Search and interacte	Verkle tree	Merkle tree or other index	Merkle tree and future Verkle tree and multi-layer index

图 15：账户权衡比较演变表第 2 部分

本文所采用的研究方法旨在系统地研究区块链账户技术的前景, 但也不乏特定的范围限制。其中最重要的一点是, 本文决定将重点放在账户模型本身, 而不是探究在安全性、便利性和成本方面进行权衡的多方面原因。因此, 本研究在对区块链账户类型--从加密基础到运行动态--进行细

化分析的同时，并未深入探讨更广泛的应用层选择，如去中心化交易所（DEX）和其他综合账户结构的战略利用。

此外，所选用于审查的账户模型虽然代表了重要的行业里程碑，但并不包括所有潜在或新生模型的详尽清单。排除这些模式的理由是多方面的，包括在研究时间框架内的可行性、行业采用的当前阶段，以及对读者了解区块链账户安全性和可操作性的当前状态的实用性。明确承认这些限制是为了保持本综述预期范围的清晰度，并为后续研究工作提供机会范围。

5 结论

本文回顾了学术文章和行业技术提案和文件。它从银行模型、比特币账户模型、以太坊账户等方面创建了一个**通用模型**。它立足于区块链行业账户发展的整体视角，以指导未来的研究。

核心结论不仅是一个通用模型，可以用一个模型解释所有区块链账户：**凭证控制平衡**。而且还包括一个具有**权衡三角**模型的通用模型，以保持进化平衡。这是一个**安全、隐私、可用性的三角模型**，以便在未来大规模采用。

而且，这项研究还得到了一系列**对比表格**，这些表格引领着方向，**规范着模型演化得失的权衡**。这个表格包含了每个子模型的**基本行为和属性**项目。我们必须根据这些属性和行为的不同变化来衡量和选择最基本的**决策**。

本文发现，区块链账户包括**三个子模型：凭证、控制和余额**。从比特币到 EOA，再到 AA 和 Native AA，区块链账户都在努力提高其安全性和便利性。尽管在安全性、便利性和未来大规模应用的成本方面还存在许多问题。这也是对账户模式的简单**描述**：凭证控制余额。

但重要的是要全面**考虑三个要素：安全性、隐私性和可用性**。数以万亿计的资产受到区块链账户的保护，数十亿用户将使用这些人类数字公共产品。这项研究指出，这些便利性和成本之间的权衡是复杂的，应谨慎对待区块链账户的去中心化改进。

我们认为账户抽象的路线图是正确的。我们面临的**挑战**是，在改善**便利性**和降低使用**成本**这两个短板的同时，还要同步改善由此带来的安全性降低问题。否则，就不可能与未来的大规模应用相匹配。

可以利用这种通用的区块链账户模式来分析和**改进**现实中的账户模式。我们使用**对比表**来演化 AirAccount 项目模型，平衡安全性、隐私性和可用性。

就让我们像忍者神龟一样，以合作的心态探索区块链的未来吧（Web-14）。

6 致谢

作者衷心感谢以下人员对本作品所做的贡献：我的导师 Anukul 博士，感谢他对我的项目 AirAccount 的鼓励和支持。

我的合作导师 Nathapon 博士，感谢他在论文和研究过程中给予的指导和支持。感谢 4Seas

社区在举办工作坊和黑客马拉松时提供的资助和支持。感谢我们的同学 FengHan、Lily 和 Miko、YT 提供的有益建议和反馈。
我的家人，感谢他们的爱和鼓励。

参考文献

Debnath, S., Chattopadhyay, A., & Dutta, S. (2017, November).安全哈希算法之旅简评。In [2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix) (pp. 1-5).IEEE.

Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, Ł.(2016).比特币上的安全多方计算

。 *ACM 通信*》, 59(4), 76-84. <https://doi.org/10.1145/2896386>

Atzei, N., Bartoletti, M., & Cimoli, T. (2017)。以太坊智能合约攻击调查 (SoK) 。 In M. Maffei & M.

Ryan (Eds.), *Principles of Security and Trust* (Vol. 10204, pp. 164-186).https://doi.org/10.1007/978-3-662-54455-6_8

Brown, D. R. L. (n.d.).*SEC 2: Recommended Elliptic Curve Domain Parameters*.

Brünjes, L., & Gabbay, M. J. (2020).UTxO- vs 基于账户的智能合约区块链编程范式。 In T. Margaria

& B. Steffen (Eds.), *Leveraging Applications of Formal Methods, Verification and Validation :*

应用》 (第 12478 卷 , 第 73-88 页) 。 Springer International Publishing.

https://doi.org/10.1007/978-3-030-61467-6_6

Buchmann, J. A., Karatsiolis, E., & Wiesmaier, A. (2013)。 *Introduction to Public Key Infrastructures*.

Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-642-40657-7>

Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. (2020).基于 PoW、 PoS 和 DAG

的区块链性能分析与比较。 *Digital Communications and Networks*, 6(4), 480-485.

<https://doi.org/10.1016/j.dcan.2019.12.001>

Chakravarty, M. M. T., Chapman, J., MacKenzie, K., Melkonian, O., Peyton Jones, M., & Wadler, P.

(2020).The Extended UTXO Model.In M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A.

Maurushat, P. B. Rønne, & M. Sala (Eds.), *Financial Cryptography and Data Security* (Vol. 12063, pp. 525-539).https://doi.org/10.1007/978-3-030-54455-3_37

Davies, R. (2010).*Evolution of the UK banking system*.

Debnath, S., Chattopadhyay, A., & Dutta, S. (2017)。安全哈希算法之旅简评。2017 第四届光电子学

与应用光学国际会议 (*Optronix*) , 1-5。 <https://doi.org/10.1109/OPTRONIX.2017.8349971>

Diffie, W., & Hellman, M. (2021). 密码学的新方向（1976 年）。In H. R. Lewis (Ed.), *Ideas That*

Created the Future (pp. 421-440). <https://doi.org/10.7551/mitpress/12274.003.0044>

Farrugia, S., Ellul, J., & Azzopardi, G. (2020). 通过以太坊区块链检测非法账户。

<https://doi.org/10.1016/j.eswa.2020.113318> Goldfeder, S., Bonneau, J., Kroll, J., & Felten, E.

(2014). 通过阈值保护比特币钱包

签名。

Goldfeder, S., Gennaro, R., Kalodner, H., Bonneau, J., Kroll, J. A., Felten, E. W., & Narayanan, A.

(2015). 通过新的 DSA/ECDSA 门限签名方案确保比特币钱包安全。In *Et al.*

Guan, Z., Wan, Z., Yang, Y., Zhou, Y., & Huang, B. (2022). BlockMaze: An Efficient Privacy-

Preserving Account-Model Blockchain Based on zk-SNARKs. *IEEE Transactions on Dependable and Secure Computing*, 19(3), 1446-1463. <https://doi.org/10.1109/TDSC.2020.3025129>

Housley, R., Ford, W., Polk, W., & Solo, D. (1999). *Internet X.509 Public Key Infrastructure Certificate*

and CRL Profile (RFC2459; p. RFC2459). RFC 编辑。 <https://doi.org/10.17487/rfc2459>

Johnson, D., Menezes, A., & Vanstone, S. (2001). 椭圆曲线数字签名算法（ECDSA）。 *International*

Journal of Information Security, 1(1), 36-63. <https://doi.org/10.1007/s102070100002>

Khan, D., Jung, L. T., & Hashmani, M. A. (2021). 区块链可扩展性挑战的系统性文献综述。 *Applied*

Sciences, 11(20), 9372. <https://doi.org/10.3390/app11209372>

Khan, S., Luo, F., Zhang, Z., Ullah, F., Amin, F., Qadri, S. F., Heyat, M. B. B., Ruby, R., Wang, L.,

Ullah, S., Li, M., Leung, V. C. M., & Wu, K. (2023). 关于 X.509 公钥基础设施、证书撤销及其

在区块链和账本技术上的现代实现的调查。 *IEEE Communications Surveys & Tutorials*,

25(4), 2529-2568. <https://doi.org/10.1109/COMST.2023.3323640>

Koblitz, N. (1994). *A course in number theory and cryptography* (Vol. 114). Springer Science & Business Media.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020).区块链系统安全性调查。未来 新 一 代

计算机 Systems、 107, 841-853.

<https://doi.org/10.1016/j.future.2017.08.020>

Ma, S., Deng, Y., He, D., Zhang, J., & Xie, X. (2021).通过账户模型区块链进行隐私保护交易的高效

NIZK 方案。 *IEEE Transactions on Dependable and Secure Computing*, 18(2), 641-651.

<https://doi.org/10.1109/TDSC.2020.2969418>

Merkle, R. C. (1987).基于传统加密函数的数字签名。 *密码技术理论与应用会议*, 369-378。

Nakamoto, S. (n.d.).*比特币：点对点电子现金系统*。

Perlman, R. (1999).PKI 信任模型概述。 *IEEE Network*, 13(6), 38-43. <https://doi.org/10.1109/65.806987>

Popper, N. (2015).*Digital Gold：比特币不为人知的故事*》。企鹅图书有限公司。

<https://books.google.com.sg/books?id=zYQeBwAAQBAJ>

Rivest, R. L., Shamir, A., & Adleman, L. (1978).A method for obtaining digital signatures and public-

key cryptosystems.*ACM 通信*, 21 (2) , 120-126。 <https://doi.org/10.1145/359340.359342>

Tsai, W.-T., Zhao, Z., Zhang, C., Yu, L., & Deng, E. (2018).CBDC 的多链模型。 *2018 第五届可依赖系*

统及其应用国际会议 (DSA) , 25-34。 <https://doi.org/10.1109/DSA.2018.00016>。

Wood, G. & others.(2014).以太坊：安全的去中心化通用交易总账。 *以太坊项目黄皮书* , 151 (

2014) , 1-32。

Zinko, R., Ferris, G., Blass, F., & Laird, M. (2007).Toward a Theory of Reputation in Organizations. *人事*

与人力资源管理研究》, 26, 163-204。 [https://doi.org/10.1016/S0742-7301\(07\)26004-9](https://doi.org/10.1016/S0742-7301(07)26004-9)

- Brown, D. R. L. (n.d.). *SEC 2: Recommended Elliptic Curve Domain Parameters*.
- Buchmann, J. A., Karatsiolis, E., & Wiesmaier, A. (2013). *Introduction to Public Key Infrastructures*. Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-642-40657-7>
- Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. (2020). 基于 PoW、PoS 和 DAG 的区块链性能分析与比较。 *Digital Communications and Networks*, 6(4), 480-485. <https://doi.org/10.1016/j.dcan.2019.12.001>
- Chakravarty, M. M. T., Chapman, J., MacKenzie, K., Melkonian, O., Peyton Jones, M., & Wadler, P. (2020). The Extended UTXO Model. In M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, & M. Sala (Eds.), *Financial Cryptography and Data Security* (Vol. 12063, pp. 525-539). https://doi.org/10.1007/978-3-030-54455-3_37
- Davies, R. (2010). *Evolution of the UK banking system*.
- Debnath, S., Chattopadhyay, A., & Dutta, S. (2017). 安全哈希算法之旅简评。 *2017 第四届光电子学与应用光学国际会议 (Optronix)*, 1-5. <https://doi.org/10.1109/OPTRONIX.2017.8349971>
- Diffie, W., & Hellman, M. (2021). 密码学的新方向 (1976 年)。 In H. R. Lewis (Ed.), *Ideas That Created the Future* (pp. 421-440). <https://doi.org/10.7551/mitpress/12274.003.0044>
- Farrugia, S., Ellul, J., & Azzopardi, G. (2020). 通过以太坊区块链检测非法账户。 <https://doi.org/10.1016/j.eswa.2020.113318>
- Guan, Z., Wan, Z., Yang, Y., Zhou, Y., & Huang, B. (2022). BlockMaze: An Efficient Privacy-Preserving 基于 zk-SNARKs 的账户模型区块链。 *IEEE Transactions on Dependable and Secure Computing*, 19(3), 1446-1463. <https://doi.org/10.1109/TDSC.2020.3025129>
- Housley, R., Ford, W., Polk, W., & Solo, D. (1999). *Internet X.509 Public Key Infrastructure Certificate*

and CRL Profile (RFC2459; p. RFC2459).RFC 编辑。 <https://doi.org/10.17487/rfc2459>

- Johnson, D., Menezes, A., & Vanstone, S. (2001).椭圆曲线数字签名算法 (ECDSA) 。 *International Journal of Information Security*, 1(1), 36-63. <https://doi.org/10.1007/s102070100002>
- Khan, S., Luo, F., Zhang, Z., Ullah, F., Amin, F., Qadri, S. F., Heyat, M. B. B., Ruby, R., Wang, L., Ullah, S., Li, M., Leung, V. C. M., & Wu, K. (2023).关于 X.509 公钥基础设施、证书撤销及其在区块链和账本技术上的现代实现的调查。 *IEEE Communications Surveys & Tutorials*, 25(4), 2529-2568. <https://doi.org/10.1109/COMST.2023.3323640>
- Koblitz, N. (1994). *A course in number theory and cryptography* (Vol. 114).Springer Science & Business Media.
- Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020).区块链系统安全性调查。 *未来 新 一 代 计算机 Systems*, 107, 841-853. <https://doi.org/10.1016/j.future.2017.08.020>
- Ma, S., Deng, Y., He, D., Zhang, J., & Xie, X. (2021).通过账户模型区块链进行隐私保护交易的高效 NIZK 方案。 *IEEE Transactions on Dependable and Secure Computing*, 18(2), 641-651. <https://doi.org/10.1109/TDSC.2020.2969418>
- Merkle, R. C. (1987).基于传统加密函数的数字签名。 *密码技术理论与应用会议*, 369-378。
- Nakamoto, S. (n.d.). *比特币：点对点电子现金系统*。
- Perlman, R. (1999).PKI 信任模型概述。 *IEEE Network*, 13(6), 38-43. <https://doi.org/10.1109/65.806987>
- Zinko, R., Ferris, G., Blass, F., & Laird, M. (2007).Toward a Theory of Reputation in Organizations. *人事与人力资源管理研究》* , 26, 163-204。 [https://doi.org/10.1016/S0742-7301\(07\)26004-9](https://doi.org/10.1016/S0742-7301(07)26004-9)

网站：

网络-1：

BIP39: [https://github.com/bitcoin/bips/blob/master/bip-](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki)

[0039.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki) Web-2：

BIP 记忆词表:<https://github.com/bitcoin/bips/blob/master/bip-0039/bip-0039-wordlists.md> Web-3：

BIP32: <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>

Web-4：

EIP55: <https://github.com/ethereum/ercs/blob/master/ERCS/erc-55.md>

Web-5：

ICP 账户和令牌标准: <https://github.com/dfinity/ICRC-1/tree/main/standards/ICRC-1> Web-6：

RIP7560: 以太坊 mgician 论坛中的原生账户抽象: <https://ethereum-magicians.org/t/rip-7560-native-account-abstraction/16664>

Web-7：

NIST 标准安全散列函数: <https://csrc.nist.gov/projects/hash-functions> Web-8

:

Joseph Jr, M. (2005).[电子市场中的信任：密码学家与经济学家的融合：]

<https://firstmonday.org/ojs/index.php/fm/article/view/1509/1424>（最初发表于 1996 年 8 月）。

First Monday.

Web-9：

"走向 a 理论 声誉理论 声誉理论"、魏 Dai、1995, 赛

弗朋克 邮件 list: <https://cypherpunks.venona.com/date/1995/11/msg01043.html>

网络-10：

Vitalik 谈账户抽离和 ERC4337: <https://medium.com/infinity/erc-4337-account-abstraction-without-ethereum-protocol-changes-d75c9d94dc4a>

Web-11：

Buterin, V. (2013).Ethereum white paper.: <https://ethereum.org/en/whitepaper> GitHub repository, 1, 22-23.

网络-12：

[全球加密货币市值图: <https://coinmarketcap.com/charts/#market-cap> Web-13：

Bitcore 存储库: <https://github.com/bitcoin-core/secp256k1>

Web-14：

布特林 V. (2023).Make 以太坊 赛弗朋克 再次

: <https://vitalik.eth.limo/general/2023/12/28/cypherpunk.html>

网络-15：

最近的一个比特币区块:___

<https://www.blockchain.com/explorer/blocks/btc/826537> Web-16：

区块 826537 的一次交易:___

<https://www.blockchain.com/explorer/transactions/btc/073c3138f020d2180a634ca4994bd5572e9098af9489f1a748d30b9760e120d4>

Web-17:

最近的以太坊区块: <https://etherscan.io/block/19047413>

Web-18:

区块 190747413 的一次正常转账交易:

<https://etherscan.io/tx/0xe7a17deb4db3af40c57059c8027c56dad90fb8045e3ebef54178b7e63fe26082>

Web-19:

一份 Uniswap 合同 内部交易区块 190747413:

<https://etherscan.io/tx/0xb86b96dc9b45a8f575c1eda550e89c38e649462d20afe47898823bc254ad1d42>