基于哈希锁定的多方跨链协议研究

张诗童[1]，秦波[1]，郑海彬[2,3]
（1. 中国人民大学信息学院，北京100872;
2. 北京航空航天大学电子信息工程学院，北京 100191;
3. 信息保障技术重点实验室，北京 100072）

摘 要：区块链技术是当前热门的互联网技术之一，因其去中心化、可追溯、不可篡改和不可伪造等优良特性，被广为熟知与应用。当前，在区块链技术面临的诸多挑战中，区块链之间的互通性问题因为链的特异性强、种类繁多而日益凸显。跨链技术是解决这一问题的关键所在。论文提出了一种基于哈希锁定的多方跨链协议，用于解决多方跨链资产转移的清结算问题。文中的“边着色”自动撮合交易算法，可以在多方多链情况下快速匹配交易，实现交易所的去中心化，解决现有交易所因中心化而产生的信任问题。论文还提出了一种价格磋商机制，在保证公平性的前提下求出了多方交易多种货币时的最优价格

关键词：区块链；跨链技术；哈希锁定；原子交换协议
中图分类号：F274;TP311.5 **文献标识码：**A

Research on the protocol of multiple cross-chains based on the hash lock

Zhang Shitong[1], Qin Bo[1], Zheng Haibin[2,3]
(*1. School of Information, Renmin University of China, Beijing 100872;*
2. School of Electronic and Information Engineering, Beihang University, Beijing 100191;
3. Science and Technology on Information Assurance Laboratory, Beijing 100072)

Abstract: Blockchain technology is one of the most popular Internet technologies. Blockchain is well known for its excellent characteristics, such as decentration, traceability, immutability and unforgeability. At present, Among the challenges of blockchain technology, the interoperability between blockchains is becoming more and more important because of the variety of blockchains. The cross-chain problem is a key to solve the interoperability of Blockchains. In this paper, the protocol of multiple cross-chains based on the hash lock is proposed to solve the problem of multi-party transaction between different blockchains. By providing an algorithm of auto-transaction, called colour for edge, decentralized exchange can be possible, which solves the problem of trust because of exchanges' centralization. We also provide a price negotiation mechanism, figure out the best price when multi-party transaction with multi-currency, which can be prove this price is equitable for each one of parties.

Key words: blockchain; cross-chain; hash lock; protocol of atomic swaps

1 引言

自2008年中本聪发明比特币[1]至今，已有近10年时间。在这10年间，源自于比特币的底层技术，区块链技术逐步成长为一项独立、扩展性强、应用范围广的新型互联网技术。随着公有链、私有链、联盟链[2]的发展，区块链研究呈现百花齐放的态势，各大机构公司纷纷涉足，希望找到适合于自身的区块链发展路径。区块链技术有四大技术特点，分别是去中心化、不可篡改、可追溯和不可伪造。

与此同时，因脱离区块链1.0技术的区块链2.0智能合约[3]广泛的应用性，全球范围内的新型区块链项目如雨后春笋，数量与日俱增。根据Coinmarket Cap（数字货币数据分析网站）的数据显示，现有流通数字货币已有2071种，总市值高达1467亿美元，相当于一个中等国家的GDP总量。随着区块链项目的增多，区块链的互通性问题成为搭建区块链价值网络的核心问题。

2 区块链的跨链需求及技术难点

区块链是一种分布式的总账，一种区块链是一个独立的账本，两种区块链是两个相互独立的账本。对于某个特定的用户而言，如何把一种区块链上的价值转移到另一种区块链上，就要涉及到两个独立账本之间的价值流通，也就是我们所说的跨链问题。如果链与链之间无法实现互通互联，那么区块链网络恐成一个个价值孤岛。跨链技术是链接区块链的桥梁和纽带，如果说各个币种是区块链生态的血液，那么跨链技术就是区块链生态的血管。

现有的跨链技术主要有四类：公证人机制、侧链/中继、哈希锁定以及分布式私钥控制。公证人机制例如Ripple[4]的Interledger协议。著名的侧链BTC Relay[5]是一种基于以太坊的智能合约，将比特币和以太坊以一种安全去中心化的方式连接起来。Wanchain[6]和Fusion[7]是两种目前较为流行的分布式私钥控制跨链方案，虽然在一定程度上实现了多链间价值转移，但因基于智能合约，能够实现的交易类型还非常有限。

2013年5月，Tier Nolan提出了原子交换的思路[8]，实现跨链交易的原子性。Tier Nolan的技术方案经过改进升级后被称为哈希锁定，并成为跨链的一种主要技术手段。除了Bitshares、Stellar、Loopring等去中心化交易所，关于讨论多方交易行为的论文还有[9]最早探讨假设中介的物物交换协议[10]；分析数字货币网络链下交易方式与效率[11]；不可分割商品交易探索[12]；分析多方交易存在的流动性风险[13]；具有惩罚效应和安全现金分配的分摊多方计算的有效协议[14,15]；]尝试在比特币线下搭建双重微支付渠道解决多方交易问题[16]；提出了一种针对多方电子支付订单撮合的新算法。在利用图论理论阐述交易协议问题方面，IOTA[17]和Byteball[18]利用有向无环图，提高了系统交易效率，Maurice Herlihy提出用强有向连通图证明了双方HTLC的原子性[19]。

3 协议设计

从三方的跨链协议说起，首先用一个简单的故事描述这种交易需求：有三个交易方，即Alice、Bob、Cindy。Alice想用兰博基尼换取15万元的人民币；Bob想用比特币换取兰博基尼；Cindy想用15万元的人民币换取比特币，如图1所示。

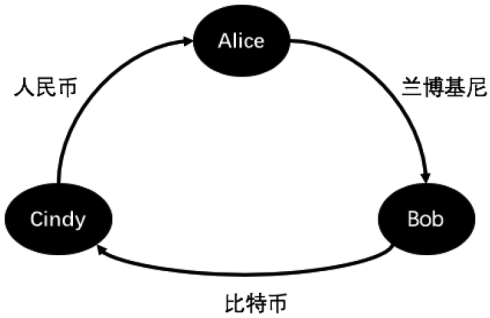

图1 三方原子交换协议

3.1 三方协议

下面假设Alice、Bob、Cindy的强有向连通图(V,E)已经通过系统自动匹配的方式建立完毕，系统生成三个参数：第一个是V中点的个

数3；第二个是2*3*Δ记为Time Lock时间锁定值；第三个是Alice、Bob、Cindy三者中的一个随机参与方。具体协议是双方原子交换协议的一种平凡扩展，具体详见[19]。协议中设立一种激活函数，是协议的每一个参与方交易需要触发的条件。经过六步操作，假设每一步操作至多Δ时间，且整个协议在6Δ内完成。当计时结束后，确认三个激活函数都激活完毕。若计时结束后，其中一个激活函数未激活完毕，则协议不会发送交易单，此时交易失败。

3.2 n方协议设计

3.2.1 n方协议的数学建模

为了将n方协议的过程表达清楚，首先运用矩阵与图论的数学方法对n个交易方m种数字货币的交易问题进行建模。

定义1：矩阵$A=\{A_1, A_2,\ldots, A_n\}T$为交易矩阵，第i个交易方的资产交换需求被描述为$Ai=(a_{i1}, a_{i2},\ldots, a_{ij},\ldots,a_{im})$。其中$a_{ij}\in Z$，表示第i个交易方对与第j种数字货币的需求情况。例如$a_{i1}=2$，表示第i个交易方想要买入2个第一种数字货币，如果$a_{i1}=-2$，则表示第i个交易方想要卖出2个第一种数字货币。

例如3个交易方三种数字货币的交易矩阵A如下：

定理1：交易矩阵A是一个可交易矩阵当且仅当交易矩阵A满足$\sum_{j=1}^{m} a_{ij}=0$且$\sum_{i=1}^{n} a_{ij}=0$。

根据定义1，可以将交易矩阵A交易的过程，被描述为矩阵A的每一列变为零向量的过程。这有助于后续对“边着色”算法进行优化时从矩阵变换的角度优化问题。

定义2：图G是一个有序二元组(V,E)，其中V为顶集(Vertices Set)，E为边集(Edges set)，将交易方定义为顶，双方的交易表示为边，E边集按照交易数字货币的种类划分为$E=\{E_1, E_2,\ldots, E_m\}^T$。定义交易矩阵中$a_{ij}$为正的值为图的该顶点的入度，$a_{ij}$为负的值为图的该顶点的出度。

定义3：矩阵V为价格期望矩阵V，例如三个交易方3种数字货币的价格期望矩阵如下：

$$\begin{pmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{pmatrix}$$

其中V_i是第i个交易方的价格期望向量$V_i=(v_{i1}, v_{i2},\ldots, v_{ij}, v_{im})T$，$v_{i1}$为第i个交易方对于第一种数字货币的价格期望，该期望是一种比例数。例如，假设交易平台的平台币与美元等值，即一个交易平台的平台币可以换取1美元，那么对于比特币，其价格期望为对应交易方对于比特币兑换美元的价格期望。某交易方的比特币的价格期望可以填写为4503.72。

若交易平台没有平台币，则可以假设第一种数字货币为基准，比如以比特币为第一种数字货币且为基准，第二种数字货币为以太坊，则某交易方对于第一种数字货币比特币的价格期望为1，第二种数字货币以太坊的价格期望为0.033，表示该交易方愿意用0.033个比特币换取一个以太坊。

3.2.2 n方协议过程

将三方协议扩展至n方时，首先要考虑的是，n个交易方的需求如何匹配的问题。若想要n个交易方之间能够在保证每个人都不亏钱的情况下进行资产交易完成各自的需求，矩阵A需要满足下面两个条件：

a) $\sum_{j=1}^{m} a_{ij}=0$，即每个交易方买入与卖出的资产等价，如果将交易方看作图中的顶点，则本条件需要使每个顶点的入度和等于出度和。

b) $\sum_{i=1}^{n} a_{ij}=0$，即每种货币的买入与卖出相同，才能保证市场是均衡的，交易可实现。

假设上述两个条件在我们的交易环境中能够被满足，那么如何执行协议能够实现所有交易方的交易需求。先考虑一种简单情况：有甲、乙、丙、丁四个交易方，A、B、C三种数字货币，每个交易方的需求如表1所示。

从加总列和加总行可以得知，该矩阵满足交易的两个前提条件，即该交易环境能实现所有

表1 4方数字货币需求

	A	B	C	加总
甲	2	-1	-1	0
乙	0	3	-3	0
丙	-4	3	1	0
丁	2	-5	3	0
加总	0	0	0	0

交易方的交易需求。然后进行协议算法。

a) 从表的第一列开始，选择第一列从上往下的第一个正数a_{11}为起点，第一列从当前正数往下的第一个负数a_{31}为终点，箭头的权重为2，表示甲将2个A给乙。因为2-4=-2，所以a11的值变为0，同时a_{31}的值变为-2。

b) 变换表格，继续从第一列从上往下进行选择，选择第一个正数a_{41}为起点，第一个负数a_{11}为终点，表示丁将2个A给丙。此时，a_{41}的值变为0，a_{31}的值也变为0。

c) 经过前两步，第一列的所有值都变为0，结束对第一列的计算，第二列按照第一列的算法进行计算，直至第二列都变为0。

d) 第三列同理。

以交易者为图的顶点，交易为边，用不同的颜色表示不同的货币品种对图进行着色，按照步骤进行“边着色图”如图2所示。

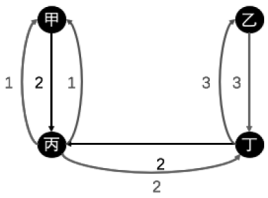

图2 4方原子交换协议

上面是问题2在4个交易方3种货币下的算法举例，下面说明n个人m种货币时的算法步骤：

a) 从i=1开始遍历所有a_{i1}，当a_{i1}>0时，令a=a_{i1}，再从j=1开始遍历所有a_{j1}，当a_{j1}<0时，令b=a_{j1}。

b) 若|a|≤|b|，则a_{i1}=0，a_{j1}=|a|-|b|；若|a|>|b|，则a_{i1}=|a|-|b|，a_{i1}=0。

c) 重复步骤a)和b)，当 i [1,n],a_{i1}=0时，第1种货币交易结束。

下面用同样的方法处理其它m-1种货币，下面叙述第k种货币的情形：

d) 从i=1开始遍历所有a_k，当a_{ik}>0时，令a=a_{ik}，再从j=1开始遍历所有a_{jk}，当a_{jk}<0时，令b=a_{jk}。

e) 若|a|≤|b|，则a_{ik}=0，a_{jk}=|a|-|b|；若|a|>|b|，则a_{ik}=|a|-|b|,a_{jk}=0。

f) 重复步骤d)和e)，当 i [1,n],a_{ik}=0时，第k种货币交易结束。

当 i [1,n],k [1,m],a_{ik}=0时,则所有货币的交易完成。

关于自动撮合交易的算法需要依据图的搜索策略。平面图的搜索策略包括广度优先搜索、深度优先搜索和启发式搜索三种。Dijkstra算法是一种特殊的广度优先搜索，也是最经典的一种最短路径搜索算法，但基于我们的问题，要保持行向量和为零的条件下进行搜索与上面三种搜索方法都不尽相同，更优化的路径还需要等待我们继续深入研究才能得到。

3.2.3 n方协议的价格磋商机制

“边着色”算法解决了当不同货币等值的情况下，交易的匹配问题，但真实的情况往往是非等值的情况，例如按照目前市场价格，1个比特币大约可以换取30个以太坊。本文提出一种关于n方协议的价格磋商机制，用于解决在不同货币不等值的情况下交易的匹配问题。

设m种货币之间的价值比为：(v_1, v_2,..., v_m)，例如比特币与以太坊的价值比可表示为（30,1），即：

$$\frac{1_{btc}}{1_{etc}}=\frac{30}{1}.$$

此时，问题1中，交易的可执行条件中的第一个条件，变成了：$\sum_{j=1}^{m} a_{ij} \cdot v_j = 0$

即第i个交易方买入与卖出的资产等价，既不能亏钱也不能获利。现实情况是，并没有放之天下皆准的定价规则，所以对于(v_1, v_2,..., v_m)一千个交易方中就有一千种答案，交易所需要对一千个交易方的答案进行均衡，在保证公平的前提下完成交易。在我们的场景中，对于每个交易方的价格期望，对应交易矩阵，产生

了下面的价格期望矩阵V，例如：

$$\begin{pmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{pmatrix}.$$

其中，V_i是第i个交易方的价格期望向量$V_i=(v_{i1}, v_{i2},\ldots, v_{ij},\ldots, v_{im})^T$,m仍然表示交易的货币种类数量。接下来，需要处理的问题是，n个交易方m种货币，交易矩阵A与价格期望矩阵V已知，且满足$\sum_{i=1}^{n} a_{ij}=0$的条件下，如何对n个交易方进行交易匹配，在保证公平的前提下完成交易。

这里，还需要提出一些隐含的假设，确保协议的有效性，也便于为后续的探索理清思路。

a) 假设进行交易的交易方填写的交易矩阵A和价格期望矩阵V都是自己真实想要交易的情况。

b) 我们假设存在一种平台币，使得每个交易方对于各个币种的价格都能有一定的衡量尺度，例如将第一列的货币设为平台币，则每个交易方的价格期望向量中的第一项变为1，即$v_{i1}=1$，$\forall i \in [1,n]$。

为了在公平的状况下实现交易，那么平台必须通过对每个交易方的价格期望矩阵进行折衷，取得一个使所有人的损失最小的价格进行交易。设这个价格为$P=(p_1, p_2,\ldots, p_j,\ldots, p_m)^T$.则每个交易方的损失可以被表示为$\Delta=\sum_{j=1}^{m} a_{ij}\cdot(v_j-p_j)$.下面的问题转化为，如何取P使得$\Delta=\sum_{i=1}^{n}\Delta_i$最小.化简Δ：

$$\Delta=\sum_{i=1}^{n}\Delta_i=\sum_{i=1}^{n}\sum_{j=1}^{m} a_j\cdot(v_j-p_j)=$$

$$\sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}\cdot(v_j-p_j)=\sum_{j=1}^{m}[\sum_{i=1}^{n} a_j\cdot v_j-p_j\sum_{i=1}^{n} a_j]$$

因为$\sum_{i=1}^{n} a_{ij}=0$，故$\Delta=\sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}\cdot v_j$与P值无关，故价格的选取只与每个交易方想要交易的数量和价格期望有关。为了保证公平性，还需要考虑的因素是所有交易方的方差。方差体现交易方交易损失的均衡情况，方差越大，表示交易方损失之间的差别越大，方差越小，表示交易方损失较为均衡。下面，先定义方差的公式：

令σ定义为n个交易m种货币交易状态下的方差，则：

$$\sigma=\sum_{i=1}^{n}\sum_{j=1}^{m}|a_{ij}|\cdot(v_j-p_j)^2$$

展开得到：

$$=p_1^2\cdot\sum_{i=1}^{n}|a_{i1}|-2p_1\cdot\sum_{i=1}^{n}|a_{i1}|\cdot v_{i1}+\sum_{i=1}^{n}|a_{i1}|v_{i1}^2$$

$$p_2^2\cdot\sum_{i=1}^{n}|a_{i2}|-2p_2\cdot\sum_{i=1}^{n}|a_{i2}|\cdot v_{i2}+\sum_{i=1}^{n}|a_{i2}|v_{i2}^2$$

$$+\cdots+p_n^2\cdot\sum_{i=1}^{n}|a_{in}|-2p_n\cdot\sum_{i=1}^{n}|a_{in}|\cdot v_{in}+\sum_{i=1}^{n}|a_{in}|v_{in}^2$$

上式是关于p_1到p_n的多元二次函数，因为$\sum_{i=1}^{n}|a_{ij}|>0$，所以二次函数开口向上，函数有最小值，可以求得，方差取最小值时，p_1到p_n的值为：

$$p_1=\frac{\sum_{i=1}^{n}|a_{i1}|\cdot v_{i1}}{\sum_{i=1}^{n}|a_{i1}|},p_2=\frac{\sum_{i=1}^{n}|a_{i2}|\cdot v_{i2}}{\sum_{i=1}^{n}|a_{i2}|},\cdots,p_n=\frac{\sum_{i=1}^{n}|a_{in}|\cdot v_{in}}{\sum_{i=1}^{n}|a_{in}|}\quad(1)$$

方差的最小值为：

$$\sigma_{\min}=\sum_{j=1}^{m}\frac{\sum_{i=1}^{n}|a_{ij}|\cdot\sum_{i=1}^{n}|a_j|\cdot v_j^2-(\sum_{i=1}^{n}|a_j|\cdot v_j)^2}{\sum_{i=1}^{n}|a_j|}$$

至此，首先提出所有交易方损失的总和与选取的P值无关，其次证明了当P取(1)值时，所有交易方损失的方差最小，也就是交易达到了公平原则。

此时，n方协议“边着色”算法按照每种不同货币进行交易，所以每种币的价值并不影响我们的算法，算法可以如期进行。n方协议的意义在于：不需要第三方交易所，而可以在去中心化的交易所为n个人m种货币交易进行需求匹配，且保证交易的公平性与原子性。

4 结束语

本文提出了一种基于哈希锁定的多方跨链协议，用于解决多方跨链资产转移的清结算问题。

首先，通过对双方原子交换协议进行扩展，提出了三方至n方的原子交换过程。

其次，本文对n方交易进行建模，定义了交易矩阵和价格期望矩阵，解决了n方协议的价格磋商问题，证明了总损失只与交易矩阵和价格期望矩阵有关，与平台提供的最终交易价格无关。为了保证交易的公平性，本文求出了总损失最小时的最优交易价格。

最后，基于最优交易价格，本文提出了一种自动撮合交易算法，可以在多方多链情况下匹配交易，实现无需第三方的交易协议。本文的创新点在于用数学建模的方法将n方交易的复杂问题模型化，并提出了最优交易价格，在保证公平的前提下，实现了交易所的去中心化。

比特币诞生10年，人们一直在追逐却从未真正超越比特币。它理论的完美性，源于它对于人性的挖掘。数据层、网络层、共识层、激励层、合约层层层相扣，缺一不可。中国数字货币研究所所长姚前教授，曾在一篇名为《去中心化资产交易：一种新的金融市场模式》的文章中指出，随着技术的发展深入，业界希望对现行模式作出变革，即真正发挥区块链技术的特点实现去中心化资产交易。

基金项目：

1.科技部国家重点研发计划（项目编号：2017YFB1400700）；

2.国家自然科学基金面上项目（项目编号：61772538和61672083）；

3.国家自然科学基金重点项目（项目编号：91646203和61532021）；

4.信息保障技术重点实验室开放基金项目（项目编号：61421120305162112006）；

5.十三五国家密码发展基金密码理论课题（项目编号：MMJJ20170106）。

参考文献

[1] Nakamoto Satoshi. Bitcoin: A Peer-To-Peer Electronic Cash System. 2009.

[2] Vitalik Buterin. On Public and Private Blockchains. 2015.

[3] Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper. 2014.

[4] David Schwartz, Noah Youngs, Arthur Britto. The Ripple Protocol Consensus Algorithm. 2014.

[5] BTC Relay. https://github.com/Ethereum/btcrelay. 2018.

[6] Jack Lu, Boris Yang, Zane Liang, Ying Zhang, el al. WanChain. https://www.chainwhy.com/upload/default/20180615/3dd1f9350b626b6b5371906f2acdaa78.pdf. 2017.

[7] Fusion Foundation. An Inclusive Cryptofinance Platform Based on Blockchain. https://www.chainwhy.com/upload/default/20180619/299dd7eb20e20760b4e53dd5b6c05a6e.pdf. 2017.

[8] Tier Nolan. Alt Chains and Atomic Transfers. 2013.

[9] Matt Franklin, Gene Tsudik. Secure Group Barter: Multi-Party Fair Exchange with Semi-Trusted Neutral Parties. 1998.

[10] Rami Khalil, Arthur Gervais. Revive: Rebalancing Off-Blockchain Payment Networks. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS ’17. 2017.

[11] Lloyd Shapley, Herbert Scarf. On Cores and Indivisibility. Journal of Mathematical Economics.

[12] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, et al. Enabling Blockchain Innovations with Pegged Sidechains. 2014.

[13] Iddo Bentov, Ranjit Kumaresan, Andrew Miller. Instantaneous Decentralized Poker. https: //arxiv.org/abs/1701.06726. 2017.

[14] Christian Decker, Roger Wattenhofer. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. Springer International Publishing. 2015.

[15] Matthew Green, Ian Miers. Bolt: Anonymous Payment Channels for Decentralized Currencies. Cryptology ePrint Archive: Report 2016/701. 2016.

[16] Randy M. Kaplan. An Improved Algorithm for Multi-Way Trading for Exchange and Barter. Electronic Commerce Research and Applications. 2011.

[17] Serguei Popov. The Tangle. http://www.descryptions.com/Iota.pdf. 2018.

[18] Anton Churyumov. Byteball: A Decentralized System for Storage and Transfer of Value. 2016.

（下转第67页）

[3] 刘明月.新形势下高校信息安全的管理策略研究[J].山东工业技术,2018(5).

[4] 刘瑞礼,张长森,梁博.大型企业网络安全探索与研究[J].网络空间安全,2015.

[5] 丛晓颖,计算机网络信息系统安全问题的分析与对策[J].网络空间安全,2016.

作者简介：

刘明月（1989-），女，汉族，山东济宁人，北京大学，研究生，工程师；主要研究方向和关注领域：信息系统的安全与管理。

（上接第62页）

[19] Maurice Herlihy. Atomic Cross-Chain Swaps. arXiv preprint arXiv:1801.09515. 2018.

作者简介：

张诗童（1993-），女，汉族，宁夏吴忠人，中国人民大学，在读研究生；主要研究方向和关注领域：新兴信息系统安全、应用密码学。

秦波（1977-），女，汉族，湖北十堰人，博士，中国人民大学，副教授；主要研究方向和关注领域：新兴信息系统安全、数据安全与隐私保护、云计算安全、应用密码学。

郑海彬（1989-），女，汉族，山东聊城人，北京航空航天大学，博士研究生；主要研究方向和关注领域：公钥密码学、区块链与数字货币系统、信息与网络安全。