捍卫隐私：匿名技术的兴起

——区块链技术引卷之十

专题报告　　宏观研究

2019.07.10

通证通研究院
区块链研究报告

通证通 x FENBUSHI DIGITAL

分析师：宋双杰，CFA

Email:master117@bqbase.org

分析师：田志远

Email:tianzhiyuan@bqbase.org

分析师：金佳豪

Email:jinjiahao@bqbase.org

特别顾问

沈波

Rin

更多研究请关注通证通公众号获取

通证通研究院　　FENBUSHI DIGITAL

请务必阅读最后特别声明与免责条款

导读：针对 BTC 在隐私性方面的问题，各种各样的匿名通证应运而生，并迅速在数字通证市场占据了一席之地。

摘要：作为数字通证的先行者，BTC 已历经十年起伏，具备良好鲁棒性的同时也逐渐显露出隐私保护的局限性。近年来，随着区块链技术、隐私计算技术、密码学技术等方面的发展，基于各种新兴技术为保护交易隐私而创立的匿名通证相继出现。

2012 年 12 月，第一个针对数字通证隐私问题的协议——**CryptoNote** 问世。该协议介绍了两种技术：隐私地址技术和环签名技术，分别提供对数据接收方和发送方的隐私保护。

2013 年 1 月，BTC 开发商 Gregory Maxwell 为提高 BTC 的隐私性提出了 **Coinjoin 技术**，Coinjoin 使用多重签名技术，交易者需各自独立分散完成签名，只有提供了所有签名的交易才能被判定合法，并被网络接收。

2013 年 5 月，约翰霍普金斯大学教授 Matthew D. Green 等人提出了 **Zerocoin 协议**。此协议提议允许销毁并重新生成数字通证，以保证通证交易匿名化且无需可信第三方参与。次年 5 月 Matthew Green 等人在 Zerocoin 的基础上创建了 **Zerocash**，并提出了一种经典的零知识证明法——zk-SNARKs。

2015 年 10 月，Monero 研究实验室的 Shen-Noether 提出 **RING-CT**，该技术基于 CryptoNote 协议发展而来，是一种隐匿交易金额的技术，该技术同时可加快交易速度。

2016 年 7 月，Tom Elvis Jedusorand 提出 **Mimblewimble**，该技术保留了 BTC 基于 PoW 共识的优越特性，同时针对 UTXO 集合进行了优化，在大幅提升匿名性的同时，能够极大地节省区块链存储空间。

风险提示：监管不确定性，匿名性或影响性能

目录

图表目录

1 匿名伊始——BTC 的“提尔锋”

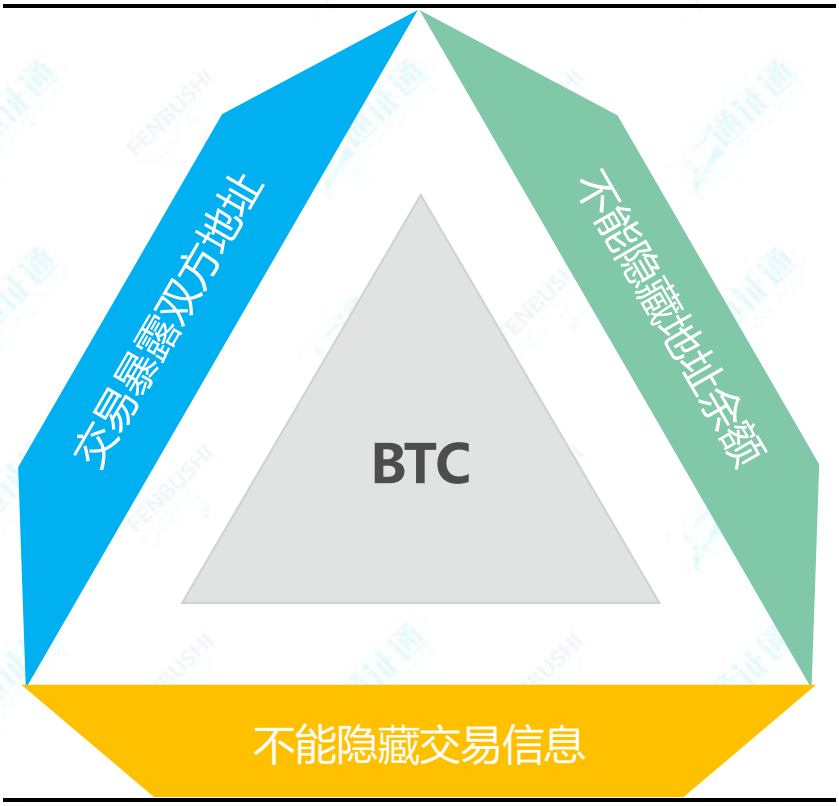
2008 年，中本聪发表了闻名遐迩的《Bitcoin: A Peer-to-Peer Electronic Cash System》（BTC：一个点对点的电子现金系统）并于次年挖掘出第一枚 BTC，数字通证的概念第一次从设想成为现实。彼时正值金融危机爆发，人们对于法定货币的信心大幅削减，而 BTC 的**非中心化（Decentralized）、抗通胀、公开透明、不可逆性（Immutable）和匿名性（Anonymous）**等特征似乎符合人们对于理想货币的设想。

1.1 BTC 的隐私策略

在 BTC 初露锋芒之际，媒体和投资者对于数字通证褒贬不一。一部分人的关注点在于数字通证是否为一种新型的“庞氏骗局”；而另一部分人则聚焦于 BTC 的各种优越特性，包括非中心化、匿名性、不可逆性等。随着对数字通证的认识越来越深入，公众对于前者渐渐形成了共识——开源共享、自由查看的 BTC 不具备庞氏骗局的典型特征。但 BTC 在运行过程中也逐渐暴露出一些问题，其中之一便是隐私问题。

进行 BTC 交易无需提供真实信息，只需提供与真实信息无关的虚拟信息（地址），但由于区块链记载了每一笔交易的相关地址和金额，因此追踪者可以在多次交易中匹配到相同的地址并将它们相关联。正因如此，BTC 的隐私策略被称为**“假名”（Pseudonymity）。**

图表1：BTC 隐私保护的局限性



资料来源：Crypto Ramble，通证通研究院

2017 年 9 月，美联邦当局通过 BTC 地址在亚特兰大机场抓捕了法国毒枭 Gal Vallerius，这在当时引起了广泛关注。调查人员发现暗网大毒枭 OxyMonster 多次使用同一 BTC 地址收款，并且该地址

的 17 次转出交易中有 15 次关联到法国公民 Gal Vallerius。执法部门注意到这条线索，进一步分析开源数据后定位到了 Vallerius 的 Instagram 和 Twitter 账号，对 OxyMonster 和 Vallerius 的写作风格进行对比后，最终确定其身份。

除了存在隐私方面的问题，“假名”策略还损害了 BTC 的**可替换性（Fungibility）**。

1.2 BTC 的“提尔锋”

可替换性是指某种物品的独立单位本质上可以互换，黄金和法币都具有可替换性，相同重量的黄金之间、相等面额的法币之间都是等价的，不因黄金是否经手海盗或者钞票是否曾在黑市流通（钞票虽然具有编号，但很少会有人注意这些编号）而改变其价值。

BTC 的“假名”策略导致其丧失了“可替换性”这一特性。交易记录的公开透明、可追溯和不可篡改是 BTC 作为数字通证深受赞誉的特点，区块链上保存了从“创世块”（Genesis block）至今所有的交易记录。

但是这些特点如今成为了 BTC 的“提尔锋”。持有者绝不希望陷入被相关部门冻结通证之类的麻烦，因此交易接收方通常会拒绝收入“被污染的”（例如曾有过非法交易历史）的 BTC，更倾向于持有干净的 BTC，其中价值最高的就是第一次从矿工手上流出的 BTC。

注：提尔锋：北欧神话中的魔剑，无坚不摧百发百中，但同时也诅咒所有者步向灭亡。

为加强数字通证交易的隐私性，ByteCoin，一种基于 BTC 发展而来的加密通证应运而生。

1.3 “匿名通证”应运而生

作为第一个基于 CryptoNote 协议的匿名通证，Bytecoin 使用隐私地址技术（Stealth Address）和环签名技术（Ring Signature）应对 BTC 在隐私保护方面的缺陷。自 Bytecoin 之后，各种匿名通证如雨后春笋般涌现，并且吸引了众多投资者，其中 Monero、Dash 等匿名通证的市值在所有数字通证中稳居前列（依据 CoinMarketCap2019 年 6 月 24 日市值排名，Monero 居第十三，Dash 居第十五）。

目前市场上比较有代表性的匿名通证包括已经过几年时间验证的 **Monero、Dash、Zcash** 等，由匿名通证硬分叉而来的 **Zencash** 等，以及 **Grin、Beam、Dero** 等数字通证圈的新宠。这些匿名通证在信息技术、匿名技术、密码学等方面各有突破，下文将对目前市场上常见的匿名技术进行介绍。

2 常见的匿名技术

针对 BTC 的隐私性问题，世界各地的学者们展开了研究，迄今为止已经提出了许多比较完善的解决方案且已在实际区块链项目中得到应用。

目前比较常见的匿名技术包括 CryptoNote、Coinjoin、Zerocoin（以及次年基于 Zerocoin 发展而来的 Zerocash）、RING-CT、Mimblewimble 等。

图表2：常见匿名技术及匿名通证

资料来源：Crypto Ramble，通证通研究院

2.1 CryptoNote 协议——首个数字通证隐私协议

2012 年 12 月，第一个针对数字通证隐私问题的协议——CryptoNote 问世。该协议介绍了两种技术：**隐私地址技术和环签名技术，分别提供对数据接收方和发送方的隐私保护。**2013 年 10 月名义撰写人 Nicolas van Saberhagen 更新了 CryptoNote 第 2 版。基于 CryptoNote 协议的匿名数字通证有很多，包括 Bytecoin、Monero 和 Particl（Monero 和 Particl 使用 RING-CT 协议，此协议基于 CryptoNote 发展而来）。

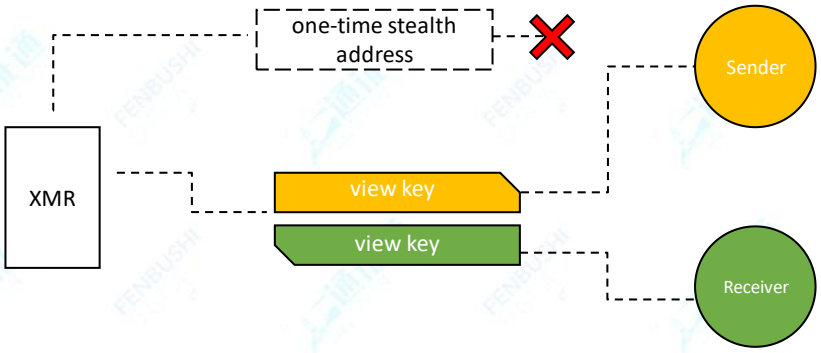
2.1.1 隐私地址技术

隐私地址技术是隐藏实际交易地址的技术，该技术主要提供对数据接收方的隐私保护。

用户进行 BTC 交易时将在公共区块链上生成一份标准的 BTC 交易记录，记录交易包含接收方的地址，BTC 使用假名技术保护接收方的地址隐私，但是区块链的公开透明性使追踪者能够将特定假名的所有交易相关联，进而结合其他信息和方法可能追踪到实际交易者。

CryptoNote 的**隐私地址技术使用一次性隐匿地址（后称混淆地址）降低不同交易之间的关联性，发送方和接收方可通过查看密钥确认交易是否有效。**

图表3：隐私地址技术示意图



资料来源：通证通研究院

相较于其他的隐私策略，隐私地址技术具有**多重密钥**的特性。**接收方具有私钥 b 和公钥 B（B=bG）**，G 为 Ed25519 曲线上的一个点。发送方在交易时取得接收方的公钥 ***B***，生成混淆地址 ***P***。该地

址由两部分构成，一部分由接收方的公钥 B 经过哈希生成，这一过程加入了只有发送方拥有的随机数 r；一部分为接收方的公钥 B。

$$P = H_s(rB)G + B$$

在交易的开始阶段，支付方 Alice 获得接收方 Bob 的查看公钥 A 和支付公钥 B，结合随机数 r 经过哈希和椭圆算法获得混淆地址。混淆地址 P 生成后被矿工记录上链。接收方可以在链上获取随机数 r 经椭圆算法运算后的 R（$R=rG$），且 $bR=brG=rbG=rB$，根据此等式接收方可使用查看私钥和支付公钥生成相同的混淆地址：

$$P' = H_s(bR)G + B$$

接收方通过 R、**私钥 b 和公钥 B** 检验区块链上的**所有交易地址**以确认是否存在自己的交易。检查等式如下：

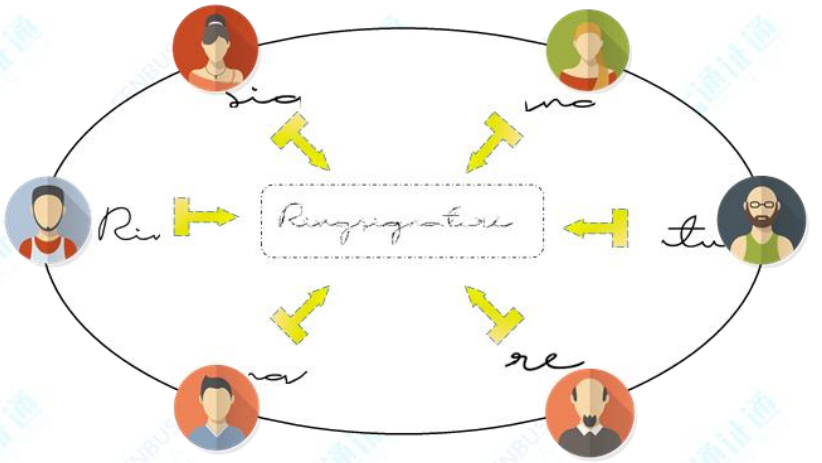
$$P = P'$$

隐私地址技术使用一次性的隐匿地址，极大地增强了交易接收方的安全性，保证通信接收方的信息隐私。

2.1.2 环签名技术

相比于隐私地址技术，**环签名技术**能够提供对**数据发送方**的隐私保护。环签名技术借用**无法追溯来源的共同签名实现数字通证交易签名混淆化。**共同签名混合一群信息发送方的签名，其中之一是信息真正的发起者，其余来自于区块链网络。后者从区块链曾记录的无数签名中提取而来，被称为**诱饵（decoy）。**

图表4：环签名技术示意图



资料来源：通证通研究院

环签名技术涉及密码学中的单向陷门函数，该函数**首先是一个单向函数**，通过不对称算法保证不可逆性（即正向计算容易而反向计算困难，例如函数$y = f(x)$，若已知x 欲求 y 很容易，而已知 y 欲求$x = f^{-1}(y)$则很困难）。**其次具有一个特定陷门（也称后门）**，若知道陷门 m 可以很容易地计算出$x = f^{-1}(m)$。在基于单向陷门函数的公开密钥密码体制中，公钥是公开可查的，可用于加密信息，且仅有拥有私钥的接收方可以使用私钥对加密信息进行解密。

生成签名。利用发送方**私钥与一组区块链上的随机公钥**进行运算形成环签名。首先，发送方从区块链上获得 r 个混淆公钥 P_i（$i=1, 2, \ldots, r$），生成随机数 x_i（$i=1, 2, \ldots, r$）并通过 r 个公钥加密生

成 y_i **($i=1, 2, \ldots, r$)。**然后选取随机数 v，并通过特定算法（此算法中，v 和 y_i 为参数）生成 y_s。作为私钥的拥有者，发送者可以很容易地利用私钥和 y_s 计算得到 x_s。**最终的环签名 P 由以下参数组成（其中 P_s 是发送方的公钥）：**

$$P = (P_1, P_2, \ldots, P_r, P_s; v; x_1, x_2, \ldots, x_r, x_s)$$

验证签名。验证者使用环签名中的参数 x_i ($i=1, 2, \ldots, r$)，x_s 经过各自对应的单向陷门函数（即 P_i，P_s），求得相对应的输出值 y_i ($i=1, 2, \ldots, r$)，y_s，最后将 y_i，y_s 经过上述特定算法的逆运算得到v'，对比验证环签名中**$v = v'$，若等式成立则环签名有效。**

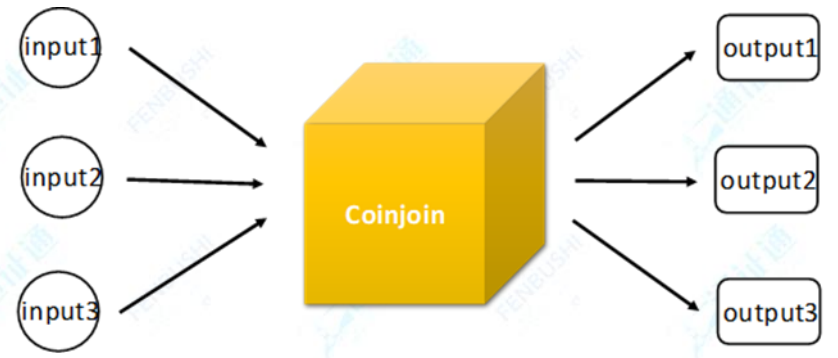
环签名技术在信息发送环节加入了不可分辨的无效信息，从而能够保护发送方的信息隐私。**在签名验证环节通过验证整体的签名即可确认交易信息的有效性。**

2.2 Coinjoin——非中心化的“混币”方案

2013 年 1 月 28 日，BTC 开发商 Gregory Maxwell 为提高 BTC 的隐私性提出了 Coinjoin 技术，其基础为“混币”技术。

“混币”是一种较朴素的通证匿名技术，指将多个交易者的输入进行混合后输出。观察者无法根据混币后的输出关联到交易输入，从而混淆数字通证流向。然而，早期的“混币”需要可信第三方的参与，存在中心化风险和信任问题。在此基础上发展起来的 **Coinjoin 则是非中心化的混币方案。**

图表5：Coinjoin 技术示意图



资料来源：通证通研究院

Coinjoin 使用多重签名技术（Multisig），交易者需各自独立分散完成签名，只有提供了所有签名的交易才能被判定合法，并被网络接收，否则，便会悉数分别退回个体的资产。

相比早期的混币服务，Coinjoin 能够有效化解第三方信任风险，避免了第三方盗窃与泄露混币信息的可能。CoinJoin 是非中心化混币机制的基础，主流匿名通证中的 Dash 便应用了此协议。

但是，即便 Coinjoin 在设计上不需要可信第三方参与，但为保证混币的效果，需要有充足数量的数字通证。这依然导致对数字通证集中持有者的依赖性。Zerocoin 协议针对此问题提出了改进方案。

2.3 Zerocoin、Zerocash——巧用密码学领域的高级证明法

2013 年 5 月，为了改进 Coinjoin 需要第三方参与的缺陷，约翰霍普金斯大学教授 Matthew D. Green 等提出了 **Zerocoin 协议。此协议提议允许销毁并重新生成数字通证，以保证通证交易匿名化且无需第三方参与。**

2014 年 5 月，**Matthew D. Green 等人基于 Zerocoin 创建了 Zerocash 协议。**该协议利用密码学领域的高级证明——**零知识证明方法**对 Zerocoin 进行了完善和改进。**Zerocash 提出了一种经典的零知识证明方法——zk-SNARKs。**

本系列前文已经提到，**零知识证明是密码学的高级证明**（详见《隐私计算：动态的加密技术——区块链技术引卷之八》）。**证明者在不透露隐私数据的情况下，可以向任意第三方证明自己确实拥有特定数据。零知识证明具有完备性、稳定性、零知识性的特点。**理论上，零知识证明是匿名程度最好的隐私计算技术，其学术资本较强。

zk-snark（Zero-knowledge succint non-interactive arguments of knowledge）是一种经典的零知识证明法，发送方可以在不泄露交易的金额、地址等细节的前提下向验证者证明交易的合法性。

zk-SNARKs 的验证过程主要包含三部分。

第一：抽象编码。证明者需要向验证者证明他知道某一事实，这一逻辑在第一步被抽象为证明者需要向验证者证明一个多项式成立。例如：

$$f(x) \cdot g(x) = h(x) \cdot w(x)$$

第二：简单随机抽样。验证者虽无法直接确认多项式成立，但可使用评估点进行评估。验证者选取随机的评估点 s，若在评估点上等式成立（即 $f(s) \cdot g(s) = h(s) \cdot w(s)$），则说明含参多项式具有一定可信度。通过多次选取评估点能不断提升可信度。

第三：零知识证明。为了确保证明者不会因为透露 ***f(s)***、***g(s)***、***h(s)***、***w(s)***的值而泄露安全信息，证明者使用同态加密技术将上述值加密。例如使用同态加密函数 E 将上述值加密为 ***E(f(s))***、***E(w(s))***、***E(h(s))***、***E(w(s))***，验证者被授权验证加密后的值，如果加密后的值符合下式，则验证成功。

$$E(f(s)) \cdot E(w(s)) = E(h(s)) \cdot E(w(s))$$

但是，**zk-SNARKs 有两个明显的缺陷。第一，依赖于可信的初始设置。**基于此方法的数字通证交易要求每一对证明者和验证者都提供一组公共参数以进行零知识证明，而这组公共参数是由协议开发者共同设置的，拥有这些公共参数意味着拥有了造假权。换言之，**zk-SNARKs** 无法避免开发者风险，开发者可能由于不同的原因泄露公共参数。**第二，zk-SNARKs 的加密技术基于椭圆曲线密码**，目前的计算机无法暴力破解。但随着计算机性能的提高，尤其是量子计算机的进步，**这种不具备量子抵抗能力的方法可能会在将来被暴力破解。**

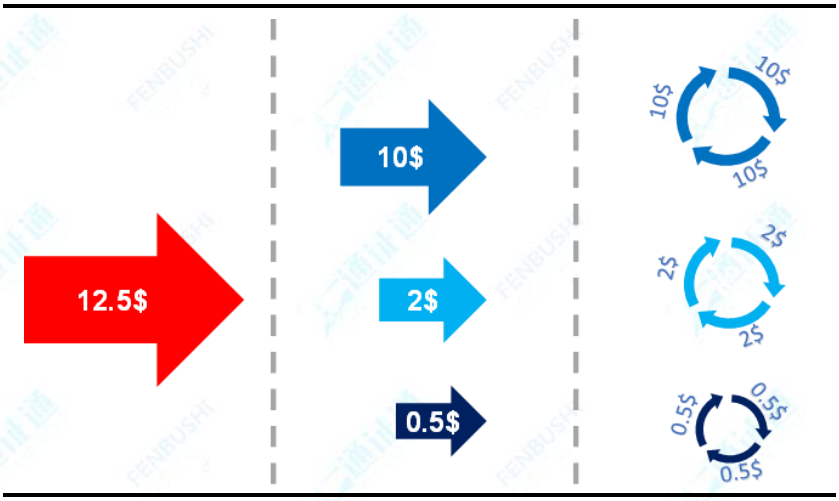
zk-stark（Zero-knowledge Scalable Transparent Argument of Knowledge），一种零知识、可扩展、透明的知识论证正在研究当中。

该方法能够保证生成证明的所有参数都是公开并随机生成的，同时还具备量子抗性。

2.4 RING-CT——CryptoNote 的继任者

RING-CT（Ring Confidential Transactions）是一项隐匿交易金额的技术。这项技术于 2015 年 10 月由 Monero 研究实验室的 Shen-Noether 提出。在最初的 Monero 交易中，为了保证环签名有充足的数据来源，交易往往需要被拆分为特定面额，以保证环签名技术的混淆能力。

图表6：采用环签名技术需要分割交易



资料来源：通证通研究院

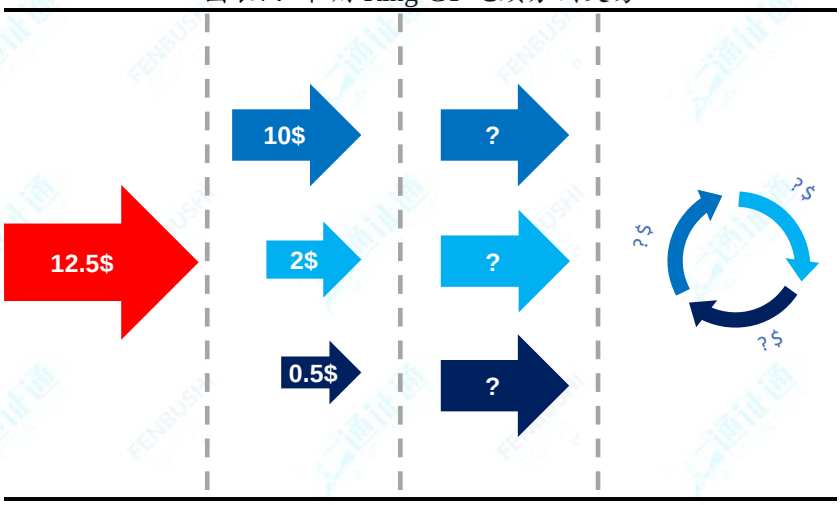
然而，通证的交易数额也属于交易双方的隐私。基于这一理念，Ring-CT 技术被提出并得到了广泛应用。应用 Ring-CT 协议之后，数字通证**只有从区块链中奖励给矿工时会显示数额，其后的所有交易将遮罩交易面额**，转为在交易中提供一个数字 ***RCXXX*** 作为交易金额输出。

$$RCXXX = random + m\ （真实交易金额）$$

交易输出由两部分组成，一是随机数，用来遮罩真实金额，由钱包自动产生；另一部分为真实交易金额。矿工不能从 ***RCXXX*** 中得到交易具体数额，但可根据 ***RCXXX*** 验证**交易输入是否等于交易输出，**以确认没有伪造产生通证。在整个环节中，不论矿工还是其余观察者都无从得知确切的交易金额信息。

Ring-CT 同时解决了环签名技术需要分割交易的问题。公开交易金额削弱了环签名的混淆能力，而隐匿交易金额能弥补这一缺陷，同时由于交易金额隐匿后无需分割交易，因此在提升了交易隐匿性的同时，也能够加快数字通证交易速度。

图表7：采用 Ring-CT 无须分割交易



资料来源：通证通研究院

2.5 Mimblewimble——优化 BTC 的神奇咒语

Mimblewimble 取名于哈利波特中的魔法咒语，于 2016 年 7 月被匿名撰稿人 Tom Elvis Jedusorand 提议并于 2016 年 10 月由 Andrew Poelstra 进一步扩展。其研究之初的目的是为了改进 BTC 的隐私性，同时节省存储空间。**Mimblewimble 基于 BTC 去粗存精，保留了 PoW 的优越特性的同时，针对 UTXO 集合进行了优化。**目前基于 Mimblewimble 的数字通证代表是 Grin 和 Beam——两位数字通证界的新宠。

机密交易（Confidential Transactions）是 Mimblewimble 的一项核心技术，其主要原理基于以下公式：

$$C = r \times G + v \times H$$

其中 C（Pedersen Commitment）是经过椭圆算法 ECDSA 得到的加密交易金额，矿工透过 Pedersen Commitment 的同态加密特性，即使不知道具体的输入和输出金额，但依然可以利用加密后的值确认输入值等于输出值，确认交易有效性。

其次，矿工利用 Range Proof 来验证交易值没有溢出，即交易双方没有凭空创造额外的通证。比如 Alice 持有 5 枚 BTC，Bob 持有 0 枚 BTC，则交易后 Bob 不可能拥有超过 5 枚 BTC。

最后，Mimblewimble 针对优化矿工存储空间设计了 Cut-through（核销）特性，能够降低区块链的大小。随着时间的推移，区块链会不可避免地扩增、臃肿，但 Mimblewimble 通过 Cut-through 能够删除无用信息从而有效压缩区块链大小。例如，BTC 的区块链上记录了两条信息：

1. Alice 支付 1BTC 给 Bob
2. Bob 支付 1BTC 给 Charlotte

在这个例子中，BTC 区块链记录了两笔交易，第一笔交易记录了来自 Alice 的输入信息和发送向 Bob 的输出信息，第二笔交易记录了来自 Bob 的输入信息和发送向 Alice 的输入信息。但在交易完成后，Bob 的输出和输入信息是过期的无效信息。Cut-through 技术允许删除中间无效信息，从而能够大幅压缩区块链体积，此外中间信息的丢弃也提高了交易的隐私性。

但需要指出的是，目前基于 Mimblewimble 的实际项目 Grin、Beam 虽然实现了 Cut-through，但矿工能够根据需要剔除相应代码，因此 Cut-through 通过删除中间信息加强数字通证交易隐私性的设想并没有完全实现。

本文详细介绍了主要的隐私交易技术，在后续专题中，我们将对各种隐私通证技术进行对比，并对使用各种隐私交易技术的匿名通证的生存环境和未来发展作出分析。

附注：

因一些原因，本文中的一些名词标注并不是十分精准，主要如：通证、数字通证、数字 currency、货币、token、Crowdsale 等，读者如有疑问，可来电来函共同探讨。

免责声明

本报告由通证通研究院和FENBUSHI DIGITAL提供，仅供通证通研究院和FENBUSHI DIGITAL客户使用。本报告仅在相关法律许可的情况下发放，所提供信息均来自公开渠道。通证通研究院和FENBUSHI DIGITAL尽可能保证信息的准确、完整，但不对其准确性或完整性做出保证。

本报告的完整观点应以通证通研究院和FENBUSHI DIGITAL发布的完整报告为准，任何微信订阅号、媒体、社交网站等发布的观点和信息仅供参考，通证通研究院和FENBUSHI DIGITAL不会因为关注、收到或阅读到报告相关内容而视相关人员为客户。

本报告所载的资料、意见及推测仅反映通证通研究院和FENBUSHI DIGITAL于发布本报告当日的判断，相关的分析意见及推测可能会根据后续发布的研究报告在不发出通知的情形下做出更改，投资者应当自行关注相应的更新或修改。

市场有风险，投资需谨慎。本报告中的信息或所表述的意见仅供参考，不构成对任何人的投资建议。投资者不应将本报告为作出投资决策的唯一参考因素，亦不应认为本报告可以取代自己的判断，通证通研究院或FENBUSHI DIGITAL、通证通研究院或FENBUSHI DIGITAL员工或者关联机构不承诺投资者一定获利，不与投资者分享投资收益，也不对任何人因使用本报告中的任何内容所引致的损失负责。

通证通研究院和FENBUSHI DIGITAL对本免责声明条款具有修改和最终解释权。