2009 年 1 月 3 日，比特币第一个创世区块诞生，由此比特币成为第一款数字加密货币。但随着对比特币的逐渐认知，人们开始意识到，它并不能做到完全匿名。

每一笔比特币交易的发送方地址、接收方地址以及比特币的交易数量都公开可循，不能称之为完全的隐私。任何一个人都可以通过比特币区块链浏览器的公开信息，顺藤摸瓜查出来所有和它有往来关系的比特币账户。

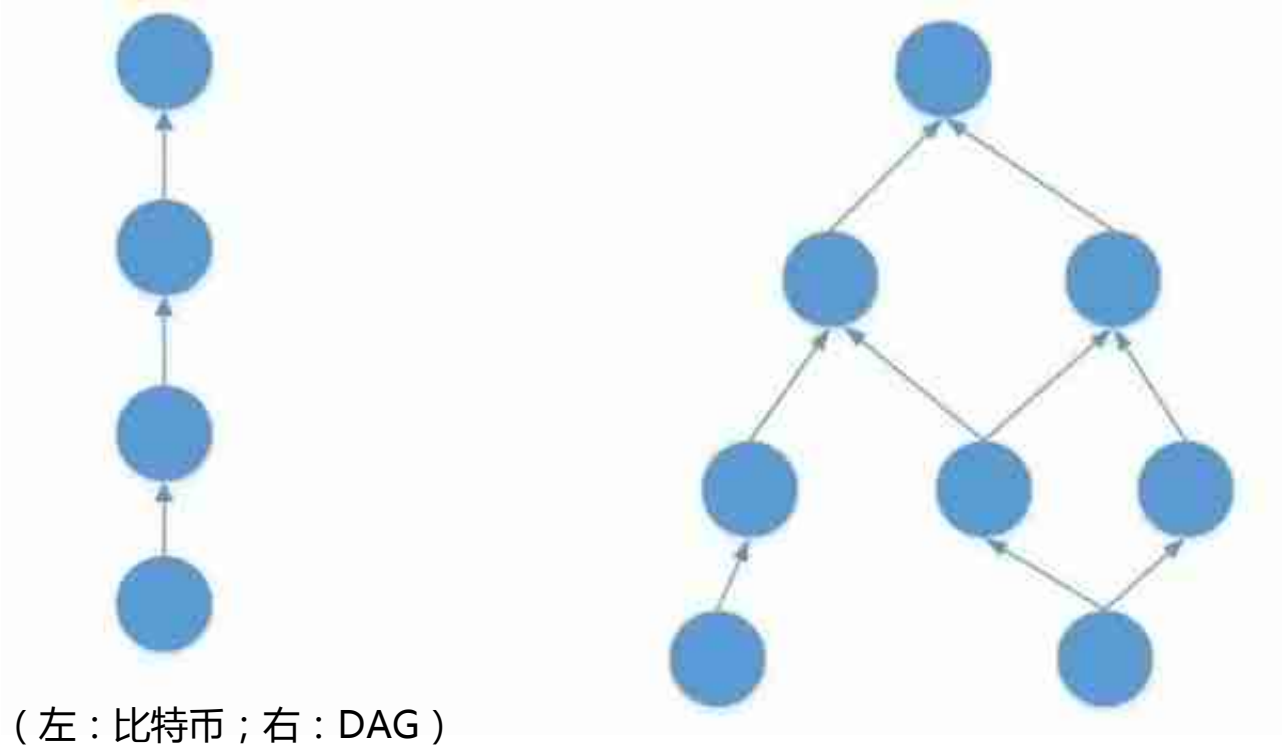
于是隐私性更强的匿名币应运而生，匿名币在匿名算法上做出了“改进”，这使得交易双方的身份和交易金额都被隐藏。Monero、Dash、Zcash 等都是知名度较高的匿名币。

最近，Odaily星球日报也报道了两个新晋匿名币——基于哈利波特魔法协议 MimbleWimble 的 Grin 和 Beam 。今天给大家介绍另一个新晋匿名币 Dero，有报道称其为“新匿名货币中的王者”。

多样的技术兼容：Dero

和 Grin 一样，Dero 是一个纯技术社区推动的币，看起来非常低调，几乎搜不到什么介绍文章。官网介绍 Dero 项目于 2017 年12 月启动，是一种新的实验性的区块链技术，专注于增强隐私和智能合约，同时保持区块链的透明度和安全性。

Dero 和比特币有相似的货币政策，恒定 1840 万供应量，挖矿奖励随时间递减。采用的是点对点匿名支付系统 Cryptonote 的工作量证明机制 CryptoNight 算法。CryptoNight 是一个内存难解（memory-hard）哈希函数，内存难解主要是指运算过程中需要大量的暂存器，因为成本过高一般的 GPU 或 ASIC 很难做到有这么大的内存空间，因此设计架构上对 GPU、FPGA 和 ASIC 不友好。



（左：比特币；右：DAG）

如图所示，传统区块链中，新发布的区块会加入到原最长链上，以所有节点认为的最长链为准无限延伸。而 DAG 中，每个新加入的单元，不仅仅只加入到长链里的一个区块，而是加入到之前的所有区块。相比较区块链而言，DAG 的可扩展性变得更好，处理能力会大幅度提升。区块链在处理交易的时候，必须全网达成共识才能出块。而 DAG 不必全网达成共识，只需要后面链接的交易来确认即可。

从数据结构体系来看，DAG 模式是一种典型的谣言传播算法（ Gossip 算法，代表杂乱无章），其核心机制即在于异步通讯。Gossip 算法是一种去中心化、容错而又最终一致性的算法，其收敛性不但得到证明还具有指数级的收敛速度。

需要注意的是，DERO 并不是第一个采用 DAG 技术的加密货币，此前还有 IOTA、ByteBall 等也用到了。随着各个币的发展，DAG 的技术弊端也随之显露：

- 交易时长不可控。DAG 的验证规则是后面的交易验证前面的交易，这就很容易出现最后的交易迟迟无法被验证的情况，尤其是在整个网络发展的初期节点数量比较少的情况下，造成交易时长无法预测。

- 异步通讯所带来最大的问题在于一致性不可控。
  在传统区块链结构中，只要一个区块出块后基本其交易的确认时间是相对可控的。但是由于在 DAG 中每个节点各自为政，它不存在一个全局的排序

机制，在运行智能合约时，这就很可能会出现节点间所存储的数据在运行一段时间以后出现偏差的情况，因此没有非常强有效的机制保证交易的确认时间。

- 安全性还没有得到大规模的验证。DAG 技术并不新鲜，但是应用到去中心化账本领域确是近几年的事情。并不像传统区块链已经经过长达 10 年的发展检验，所以其安全性还有待观察。

尽管如此，因为不需要单独的矿工通过挖矿来验证和确认交易，DAG 的采用有效地规避了 51% 攻击，可以更好地去中心化。没有了矿霸垄断算力的风险，转账手续费用也更低。2018 年 10 月，Monero 硬分叉部署了防弹协议（ BulletProof ）降低交易费用被认为是重大利好，但早在同年 6 月，Dero 就在主网上实现了防弹协议。

为加强安全，减少攻击面，开发团队还在 Dero 网络上实施了完全 SSL（ Secure Sockets Layer 安全套接层）。

想实现完全匿名：防弹协议 & 完全 SSL

2018 年 6 月，Dero 发布 Atlantis 测试，Atlantis 将加密协议、DAG 和防弹协议相结合。受控环境下，Atlantis 可以实现低至 3 秒的拥堵时间，每秒可处理 1000 笔交易，目前区块时间为 12 秒。

防弹协议由密码学家 Benedict Bunz 和 Jonathan Bootle 提出。从概念上讲，防弹协议可以被认为是一种更有效的零知识证明(Zero Knowledge Proof)形式。通过将信息聚合到新的数据结构中，使其以对数而不是线性的方式进行扩展，能够提供更大的存储空间、更合理的验证时间以及更低的费用。

Dero 项目已经构建了一种新的区块链技术，可以将隐私与智能合约结合在一个区块链上，而无需第二层或脱链解决方案。这使得所有数据真正地隐匿，这也解决了在无信任网络上通过机器信任而进行端对端匿名交易的问题。

为了保证网络传输过程中数据不被破坏和篡改，很多加密货币都在加密协议上做了相应的改进。比如 Monero 通过 Kovri 项目，被动网络监控无法揭示用户是否在使用门罗币，保证节点只是简单地传递消息，而不知道传递的消息的内容，也不知道节点是最终目的地或者最终目的地的中转路线。Dero

解决数据在传输过程中被监听的方法是节点间采用 SSL 链接解决这个问题。

网络上传输的数据非常容易被用户窃取，SSL 是利用数据加密、身份验证和消息完整性验证机制，为网络上数据的传输提供安全性保证的一种安全协议。实施完全 SSL 加密网络可以加密整个网络流量，从而大大减少攻击面，同时防止 ISP（互联网服务提供商） 或其他用户分析 Dero 的网络流量。

不仅仅是转账交易匿名，Dero 希望实现匿名智能合约。根据官方推特显示，智能合约（代号：Stargate ）于 1 月 4 日 开始测试。