Bitmark:数字环境中的产权系统

Christopher Hall, Casey Alt, Lê Quý Quốc Cường, and Sean Moss-Pultz

2016.11.7

摘要

本文提出了一种数字产权系统，涵盖了数字和实物资产，在去中心化的情况下，实现了安全认证和从一方到另一方的转让。数字签名提供了在此数字产权系统内进行发行和转让被称为“bitmarks”的标识的方法。使用区块链算法、分布式共识可以实现确认资产的所有权关系。数字资产可以通过密码学中的摘要算法进行唯一确定。实物资产则可以通过细节特征进行唯一确定。标识通过 P2P 方式转让、验证，并创建不可伪造的所有权链（溯源）。

关键词

产权系统、数字产权、所有权、数字资产、安全来源、中本聪区块链、去中心化系统

1、简介

在正式的产权系统中，最重要的功能之一就是将资产由不可达状态转化为可以有效访问的状态，使得所有权可以在一个更广泛的网络中进行有效的传递和重组。

将一所房子等资产转化为资产所有权等抽象概念需要一个复杂

系统来记录和组织所有权相关的社会、经济有效属性。将资产具化为产权标识并记录进共有账本的行为有利于用户之间达成关于资产持有方式、使用、交易等方面的共识[1]。

数百年来，产权系统已经演化为在现实世界中持有资产，从土地、建筑甚至包括创意。随着计算技术的发展，数字产权系统成为可能，律师天然尝试使用现有产权系统掌控他们的数字资产，然而这已经被证明相比整合知识产权困难的多。（我们在同一时间点拥有相同的创意，针对这一现实，数字化可以衍生出多个具有独特经济特性的信息）。企业试图通过将所有权转换为许可来找到解决数字产权难点的可行方案。但是就像房屋出租不同于固定资产，数字资产使用许可也不同于开发产权。我们对数字产权的定义就会被破坏，也无法修复。

数字产权目前遇到的自身结构性问题与许多社会领域跨越式进步时遇到的问题及其类似。当牛顿力学不能充分描述亚原子粒子的运动时，物理学家首先想到在原有基础上进行扩展，但只有当他们打破原有规则并完全改变角度，他们才能发现一个新的领域量子力学，才能解释亚原子粒子的运动以及将牛顿力学描述现象在更大范围内进行解释。我们需要定义一种新的数字产权系统，类似的可以描述目前存在的各种所有权关系。

新系统需要从数字视角构建，重新定义数字产权——包括独有真实标识的真正数字产权——包括实物资产。新系统通过标识掌控实物和数字资产，“标识”作为抽象的容器将与数字产权绑定并用于确认

[1] Hernando de Soto Polar, The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else, 2003

所有权。

我们计划使用基于独特表层质地特征的“对象细节特征”（ ObjectMinutiae[2]）架构来安全识别物理资产。密码学安全的摘要算法用于获取数字资产指纹。数字签名技术支持发行和转让标识（bitmarks），通过采用区块链算法[3]、分布式共识可以达成确认持有标识的具体用户。标识的转让通过 p2p 方式，可以进行验证并创建了不可篡改的链上所有权关系（可信溯源）。

不需要中心化权威机构进行操作和维持安全，提高了整个系统的效率、降低成本，并且不容易受到欺诈和丢失数据。数字资产的稀缺性可以容纳物理世界的概念和法律框架[4]。

不能混淆上述技术与“数字版权管理系统”（DRM[5]）。本文不讨论 DRM。人们认可资产所有权记录基于资产的具体特征和法律规定。这里提出的方法只解决：安全的确认“谁拥有什么”。通过赋予所有资产同样的不可篡改、伪造的数字身份、标识，我们可以充分描述实物资产、知识、数字资产的所有权。

2、交易

一个“bitmark”被定义为由一个发行记录和一个或多个转让记录组成的数字签名链。

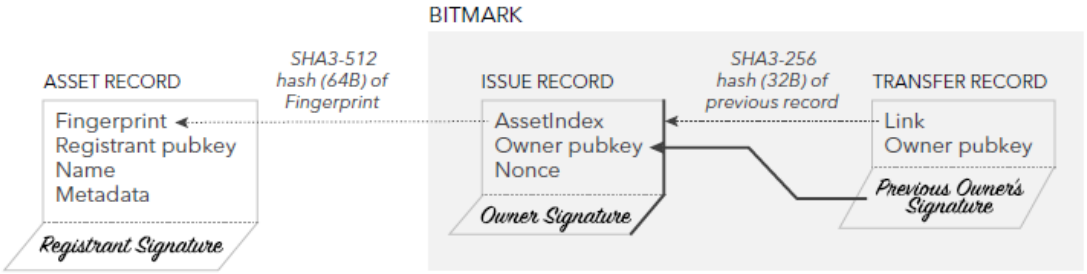
---

[2] Tzu-Yun Lin, Yu-Chiang Frank Wang, Sean Moss-Pultz, “ObjectMinutiae: Fingerprinting for Object Authentication”, 2015.

[3] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2008.

[4] Nick Szabo, “Scarce Objects”, http://szabo.best.vwh.net/scarce.html, 2004-5.

[5] Wikipedia, “Digital rights management”, http://en.wikipedia.org/wiki/Digital_rights_management



本系统中，用户通过 Ed25519 公钥识别[6]。一条资产记录包括能够在 Bitmark 系统内指定一个物理或者数字资产的独有资产指纹元数据。资产记录包括一下字段：

Fingerprint：一件物理实体的数字代表或者数字文件的摘要。

Registrant:用户注册这件资产的公钥（Ed25519）

Name:短 utf-8 格式标识符

Metadata:用于识别被 NULs 分离的 utf-8 格式文本的键值对

Signature:注册此资产的用户私钥对以上字段的签名。

一条*发行记录*从一条资产记录创造出一个新的 Bitmark。发行记录建立了资产与系统中数字信息的联系。发行记录拥有如下字段：

AssetIndex:相关资产记录中 Fingerprint 字段的 SHA3-512 哈希值（64bytes）。AssetIndex 作为独有的资产记录标识符，在针对同一资产记录创建的所有发行记录中完全相同。采用资产记录的 Fingerprint 字段进行哈希取值，是为了保证数据大小的一致性，忽略指纹值得原始大小。

Owner：创建新的发行记录的用户的公钥（Ed25519），一条新的

[6] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, Bo-Yin Yang, “High-speed high-security signatures”, http://ed25519.cr.yp.to/ed25519-20110926.pdf, 2011.

发行记录自动属于发行者所有。

Nonce：一个无符号整数，用于区分同一资产记录的多次发行。

Signature：发行此资产的用户私钥对以上字段的签名。

转让记录记录了 bitmark 所有权的变化。转让记录包含以下字段：

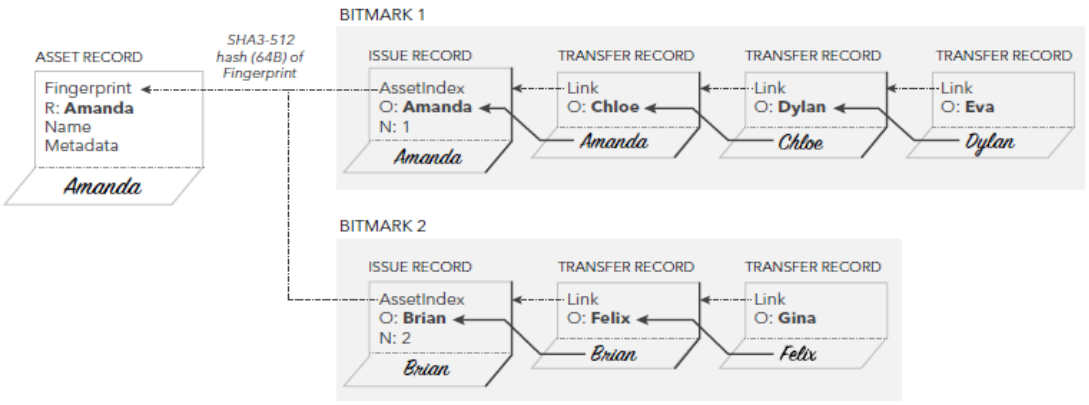
Link：前一记录所有数据（包含 Signature）的 SHA3-256 哈希值（32bytes），在 bitmark 的所有权链中指明了前一条记录。前一记录可以是发行记录，也可以是另一条转让记录。取前一记录的哈希值是为了确保数据大小一致性，忽略前一记录的原始大小。

Owner：此 bitmark 转让接收者的公钥（Ed25519）

Signature:前一记录所有者私钥对以上所有字段的签名。

bitmark 的当前所有者（所有权链最右边的记录）通过数字签名进行验证。如果一条转让记录的签名与其前一记录所有者的公钥相匹配，则此转让记录被认为有效并且被记录到区块链中。如果不匹配，无效的转让记录被丢弃。原始资产记录则通过验证其真实对象对应的索引指纹。

资产记录是自签名的，所以，任何用户可以为同一资产发行新的 bitmarks。



以上案例中，Eva 和 Gina 都是当前拥有者。避免指向同一资产的具有不同签名的发行记录进行所有权主张冲突，必须在系统外部进行产权判定。Bitmark 区块链记录了所有的产权交易，并因其不可篡改的特性，将作为重要证据。

3、操作

注意：本章节假定您已经熟悉中本聪区块链，读者可以在 Bitcoin Wiki[7]获得专题介绍。

Bitmark 系统通过 P2P 网络处理交易。用户可以通过以下软件进行操作。

Client（GUI）

- 通过 JSON RPC 连接到 bitmarkd，并发送交易；
- 产生密钥并存储。

Server（bitmarkd）

- 通过 JSON-RPC 监听 Client 提交交易；
- 自定义二进制 P2P 协议，进行区块链和交易广播；
- 通过 JSON-RPC 监听管理员命令；
- 自定义旷工协议；
- 采用 LevelDB 存储数据（使用前缀字节区别单个表）。

Client 连接到 bitmarkd 的 RPC 端口，并通过 JSON-RPC 请求发送交易。Bitmarkd 验证交易签名。*资产记录*和*发行记录*都是自签名，而

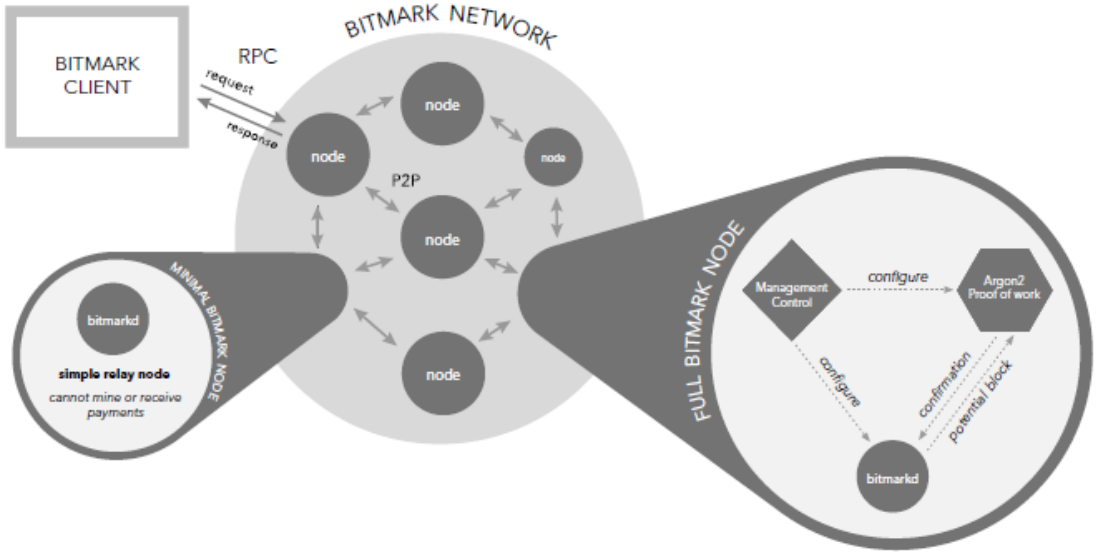
[7] Bitcoin Wiki, “Block chain,” https://en.bitcoin.it/wiki/Block_chain.

*转让记录*则必须通过前一记录的拥有者私钥签名。无效签名和不正确的记录连接会被拒绝。有效交易被作为未支付条目存储下来并通过 P2P 网络广播到其他服务器。

每一个未支付发行交易，bitmarkd 会返回一个支付 id 和支付所需数据——货币种类以及付款地址——网络将接受挖掘交易方式支付 fee。另外，包括支付随机数和难度值，以让 Client 可以挖矿。类似的，每一个未支付转让交易，bitmarkd 会返回一个支付 id 和支付所需数据——货币种类以及付款地址——网络将接受挖掘交易方式支付 fee。两者不同的是，转让交易没有支付随机数和难度值。

多个发行交易可以通过支付一笔经过换算过的交易费或者挖掘转换过难度值的随机数进行合并支付。转换基于每次提交支持最大 100 笔的发行交易，交易费则相比每次发送一笔发行交易进行折算。

作为响应，Client 构建一笔支付交易并发送到 bitmarkd 进行验证和传达。Servers 为记录设置一小时支付等待时间，超时则认为记录无效，在一小时内一旦收到支付确认，则挖掘记录。



虽然大部分 Bitmark 系统已经直接采用 Bitcoin 区块链开发，但是不可撤销的将一个产权系统绑定到一个主要设计用于支付的网络上不是长期可持续的策略。

挖矿过程独立于 bitmarkd，采用自定义协议。每个 bitmarkd 服务器存储可用的交易列表并且计算交易摘要的 Merkle 树，在发行记录验证时确保已经存在对应的资产记录。（比如：相关资产是否已经被前一个区块挖掘或者是否被本 bitmarkd 记录）。

区块头包含区块编号、64bit 时间戳和一个包含区块拥有者收款地址的基础记录，遍历 Merkle 树并广播到订阅的旷工，如果一个旷工成功，则返回其挖到的随机数。Bitmarkd 创建完整头部，基于 Merkle 树，验证难度值符合，此区块编号比当前区块编号大 1。满足这两个条件的区块将被并入当前区块链。

基础 Bitmark 记录发布此块的收款地址，让发行者和转让者使用。

区块头数据结构如下：

Block Number：8bytes，小端

Timestamp：8bytes，小端（UTC Unix time in seconds）

Merkle Root：32bytes，Merkle 树的根值。

Difficulty：8bytes，此时区块挖矿的难度值

Transaction Count：8bytes，旷工用

Previous Block Hash：32bytes，前一区块的 Argon2[8]哈希值

[8] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich, “Argon2: the memoryhard function for password hashing and other applications”, https://github.com/P-H-C/phc-winner-argon2/blob/master/argon2-specs.pdf, 2016.

Nonce：8bytes，旷工用

基础记录数据结构如下：

Extra Nonce：8bytes，旷工用

Currency Name：0..16bytes，小写 ASCII 货币名称（例如：bitcoin）

Payment Address：0..64bytes，旷工的 ASCII 地址，用于接受付款（例如：Base58 Bitcoin address）

Bitmarkd 服务器收到额外交易，将定期把新任务广播到连接的旷工。挖出的区块将使其所包含的交易处于已挖掘状态，进而将这些交易从可用池移除。服务器继续基于剩余可用交易工作。

以下条件发生时，挖矿将暂停，服务器进入恢复模式，直到可用交易池被完全重建：

- 收到一个新区块，并且此区块编号大于下一个预期区块；
- 服务器掉线一段时间（或者只是错过了一些区块）；
- 区块链分叉；

服务器在获取到最长可用区块时恢复，通过从相邻服务器从高到低获取，覆盖旧的区块，直到与相邻服务器的区块链一致。

一旦收到所有区块，并且相应交易已经被设置为已挖掘状态，则可恢复挖矿。

4、轻所有权验证

不需要全节点，系统可以验证任何 bitmark 的当前所有者。服务器内部维护一个包含每条 bitmark 当前所有者的表格，从而可以通过

查表方法对来自 Client 的所有权查询进行验证。

查表法有一些漏洞，这种方法只在由诚信节点控制网络的时候是有效的。所以，频繁进行转让和接收 bitmarks 的参与者应该运行他们自己的完全节点。运行本地完全节点能够更好的独立安全快速的进行验证。

5、激励

所有产权系统存在一种天然激励：参与者通常认为具有标识的资产比没有的更具价值。标识代表资产的一种潜在价值，标识赋予一种基本的能力，比如转售、租借、捐献。

任何人都可以基于任意资产发行 bitmarks，但是发行记录的不可篡改特性将避免恶意参与者针对有产权争议的资产进行发行 bitmarks。当发生法律纠纷，每一个来源都会作为证据用于解决冲突的所有权主张。

旷工通过收取交易费获利，比如比特币支付，并有助于防止对系统的滥用。交易费是支付交易的输入值与输出值的差额。

6、隐私和身份

系统仍有必要公开进行所有交易，隐私可以通过保持公钥的匿名性得到保障。每个发行可以启用新密钥作为一种额外的预防措施，防止关联到一个所有者。

所有者可能希望在系统内展示他们的身份。像博物馆这样的机构

往往希望他们的控股者了解他们在系统中的身份。Client 可以通过 PKI 来验证某个公钥属于特定的实体。

7、结论

本文介绍了一种全球性的产权系统，通过给所有资产赋予一个数字身份可以充分描述所有权。产权的创建和转让必须遵循协议，并且采用中本聪区块链生成不可伪造的记录源。在结构上，对 Bitcoin 的关键技术的利用使得支付去中心化。

该解决方案扩宽了产权网络的可操作性，它足以管理数字、知识和物理资产。系统的去中心化结构可以防止欺诈，并使它能跨政治、经济环境运作，从而创造最广泛的所有权认证、交易和管理网络。

更改日志

- 2016.11.7——修订了区块链的结构和挖矿协议；将物理资产的验证方法由 PUFs 修改为 ObjectMinutiae。
- 2015.4.7——初始版本

致谢

Timothy Chen, Mike Hearn, Casey Reas, Bunnie Huang, Amy Whitaker, Peter Schwabe, Jenny Pat, Agnes Yen