道立名区块链

DaoLiName Blockchain

道立名公司

info@daoliname.com

https://github.com/DaoliName/daoliname

2019 年 6 月 22 日

首席摘要

区块链的技术本质为使用非线性 hash 单向函数，称之为 Lamport Signature[1]， 作为全系统唯一无信任中心的共识计算依据。道立名（DaoLiName）区块链还独特创新性使用了“双线性 hash 单向函数”，仍然为 Lamport Signature 无信任中心共识计算依据这一本质性原理。利用双线性 hash 函数的密码学语义可控性，道立名区块链首次将区块链用户链上的随机身份（钱包地址）完全性映射至同一用户在各种链下应用的真实身份，尤其是人脑易识别的用户身份或 IoT 设备的标识等，并且将这些身份或标识认证为用户或设备的去中心化身份即公钥（Decentralized Identity as Public Key, DID-PK）。DID-PK 在个人信息安全，网络安全，支付安全，万物安全互联等各种领域中有广泛的应用。DID-PK 在区块链领域是一个知名难题，道立名区块链有机组合使用双线性、非线性这两种 hash 函数，对应地有机组合了 Proof-of-Stake (PoS)、Proof-of-Work (PoW)这两种共识算法。这种有机组合实现了：（1）首次以分布式共识算法实现了链上随机身份与链下物理身份的完全性映射，（2）以链永不分叉

形式确保了共识算法的安全性，（3）PoW 挖矿的极小化使用有效降低了用户使用链服务的成本，同时也有效控制了挖矿能源的消耗。

1. 引言

自比特币的开拓性工作[2]起，在过去的十年中大量涌现出的区块链工作为密码学的广泛应用与发展贡献了非常宝贵的知识及有用的实践经验。如今数以十亿计的人拥有个人计算、存储和通讯设备（如台式机和智能手机）、正在无时不连无所不在地使用着并参与贡献互联网与云计算，其中有些人甚至直接享受到了区块链技术提供的真实价值。越来越多的人开始相信如下事实：当今的 IT 产能已经支撑得起全球规模用户以点对点方式实时广播所有支付交易，或更一般情况所有合同，到一个全球分布式分散的、去中心化的、只在尾部增加条目的帐本上。这种账本甚至可仅被个人拥有的物理设备形成的一个所谓去中心化自治组织（Decentralized Autonomous Organization, DAO)来构建运营维护。交易或合同的正确性判断以及被添加到账本尾部的决策由一个系统一致性共识算法做出，该算法由账本系统的所有参与对等节点共同执行。Leslie Lamport 于 1979 年提出的仅用密码学安全单向函数，如 hash 函数，可充分性构造数字签名，称之为 Lamport Signature[1]，成为区块链技术共识使用的系统一致性共识算法的不二选项。

道立名（DaoLiName）是“又一个”区块链。因此，它也含有一部分继承性地采用了与之前已经出现的许多区块链所用的通用技术、方法与知识。得益于之前区块链的探索与实践，道立名区块链吸取了之前工作积累的有用经验与教训。值得一提的是，道立名区块链作为后来者有着从先前工作中学习最佳实践，少走弯路的后发优势。例如，就共识算法而言，在了解 BitCoin 挖矿采用的工作证明（Proof-of-Work，PoW）算法仅消耗 CPU 时钟周期，可利用无内存设计的 ASIC 芯片取巧加速挖矿甚至建立矿池，而后出现了，例如以太坊[3]额外需要消耗内存甚至外部存储资源，更公平的挖矿方案。这些基于实践的知识有助于道立名区块链选择使用更合理的工作证明方案。再举一个例子，权属证

明（Proof-of-Stake，PoS）的提出，例如 Algorand [4]，EOS[5]，也为道立名区块链在提高区块链技术的效率和可扩展性方面提供了宝贵新知识的设计选项。

然而道立名区块链作为“又一个”新区块链项目，让我们对推出这个新区块链的必要性给出如下论证。我们观察到迄今为止出现的所有区块链皆存在一种可以称之为：“链上链下脱节”缺陷。链上的交易或合约参与方的身份与链下真实物理世界的交易或合约的参与方的真实身份不存在任何可证明的对应关系。此种对应关系的缺失对于比特币仅用于币交易应用来讲不仅不构成任何问题，恰相反却是一种非常有用的特征属性：交易的匿名性。然而对于现实世界一般性合约的去中心化要求，如以太坊，Algorand 等区块链愿景的服务应用场景，链上链下合约双身份对应关系的缺失不能被看作是一种有用属性。事实上，用户链上身份与链下身份关系的缺失是由于目前区块链技术的核心手段采用了非线性 hash 技术而无法对身份作有效共识控制，这是一种无奈被迫接受的必然做法，并非为一种可作为选项的有用属性。

与链上链下合约双方身份安全可靠的对应缺失相关，合约内容上链的共识算法也存在着安全性问题。我们可将区块链合约达成共识的安全原理简要叙述如下：一个合约的构建方与验证方仅信任一个公开算法（如 hash 函数）在系统分布执行得到多数一致结果达成共识，而无需依赖于任何第三方，格外具有某种权威性强制力量的，中间或中介实体的介入性服务作用。目前已知区块链技术通用的共识算法中，一方面，基于计算 hash 函数算力竞赛的 PoW 方案，仅用简单拼算力处于一种“蛮干”的原始状态，用低门槛很容易发生链分叉的共识分歧，而若为减少分叉概率而提高门槛则造成共识算法效率十分低下，还会因耗费巨量能源而造成服务不可持续。另一方面，基于坐拥资产多寡决定话语权重原理的 PoS 方案，如果因为链上对链下应用不敏感（链上对链下应用的敏感度与用户身份可识别性呈正比相关）而盲目采用资产权重决定共识，则很容易陷入少数寡头说了算的中心化局面，彻底违反了区块链去中心化的本源诉求与理念（少数人掌握多数财富是人类社会发展迄今的常态属性）。

为打通链上链下通道，有些链提出了使用“Smart Contracts”（“智能合约”）思路。所谓智能合约是一段可执行代码，广播到全链系统执行企图由算

法的唯一性期望能达到执行效果的一致性。以太坊上号称有 20 万种不同的智能合约能打通 20 万种不同的链下链上通道。智能合约的爱好者在鼓吹智能合约的神奇作用时其实正在把区块链去中心化任务推给了编写智能合约的程序员，完全不顾用户面对如此大量程序无能力判定程序员可能不经意或更糟糕故意引入错误会造成智能合约程序不可信这么简单的事实。

我们推出道立名区块链的重要目的是予以用户选择：将他们链上匿名的身份对应到他们在链下物理世界的身份。道立名区块链设计了完全去中心化的共识算法实现这种链上链下身份的对应。

2. 去中心化身份（Decentralized Identity, DID）问题

迄今为止的所有区块链（包括即将上线的道立名）技术皆无例外使用公钥算法让对等节点（peer nodes）在对等网络（peer-to-peer network）中建立匿名实体的安全匿名身份认证。对等节点在加入对等网络时生成自己的私钥，该私钥必须是一个随机数且从一个足够大空间选取而得，因此是一个高信息熵比特串。所有公钥算法必然使用一些单向和良好混淆函数（good mix function, Shannon 语）将私钥与公钥相关联，因此输出的公钥也必须是高熵的，即，不适于人脑消费受用。自 BitCoin 始，区块链行业将这样的对等身份公钥命名为“钱包的公开地址”。到目前为止已知区块链技术似乎不存在有效的去中心化共识算法构造或接受适合于人脑消费受用的低熵公开地址。Zooko Wilcox-O'Hearn[6]“猜想”任何区块链地址不可能同时（1）去中心化，（2）安全，（3）适宜于人脑受用。此断言被区块链业界称为所谓的“Zooko's Triangle”。迄今为止出现的所有区块链技术皆（事实上被迫）选择放弃属性（3）。

新近发布的 Libra 区块链白皮书[7]写道：“Libra 区块链是匿名的，允许用户持有一个或多个与现实世界身份无关的地址。”在我们看来，BitCoin 使用不适宜于人脑受用的高熵地址是希望用户消费具有匿名性，而 BitCoin 仅有花钱此唯一应用，因此用户匿名的确可被认为是 BitCoin 的有用性质。而对于其它有链下应用的区块链，如果匿名是一种“用户你要也得要，不要也得要”

硬塞给用户之类的货，那么这种性质实在是一种缺陷。特别考虑 Libra 区块链，如何让一个匿名用户建立他/她的个人财务或社会信用度，以说服贷方达成共识决定予以贷款？或大额跨境转账情况允许当局对资金流动的合法性实施监管？Libra 区块链若仅支持用户匿名，可能会令 Facebook 陷入一种两难境地：遵循行业规范 Know Your Customer（KYC）还是像其最近高调宣称：将转型至不再依赖“Make money out of mining user minute details”这一成就了 Facebook 的商业模式？

去中心化的低熵名称服务的需求其实由来已久。在 BitCoin 早期尚未广泛流行时，Namecoin[8]观察到了去中心化域名服务（Domain Name Service，DNS）的有用性：人脑可识别的低熵域名被解析为更高熵的 IP 地址。Namecoin 利用 BitCoin 分叉出来一个“先到先得”子链。为了给“域名蹲坑”（“DN Squatting”）增加一些难度，在收到一个 DN 注册请求时添加了时间戳，当请求发生一段时间后（假定此时间段内已经出了若干区块）才允许为此注册请求 DN 进行挖矿。显然此等质量的共识算法缺乏专业水准的 DN 管理和控制。Namecoin 的发起者已经放弃了他们的项目，留下由一群信徒组成的社区运营此点对点网络（所以 Namecoin 是一个货真价实的 Decentralized Autonomous Organization，DAO！）。以太坊域名服务（ENS）[9]也提供了一种去中心化域名服务，它指定了一些顶级域名，例如“.eth”，“.test”（类似于中心化顶级域名“.com”，“.net”）,成为某些智能合约的拥有者。智能合约执行的输出可将用户注册的 DN 绑定到用户请求 IP 地址。事实上这些智能合约的拥有者形成了一些中心化的权威，的确一般用户是没有能力从复杂的智能合约识别或判定为什么 ENS 比 DNS 去中心化。我们认为合约不应该过于聪明而具有某种魔术功能，恰相反应该非常简单易懂让大多数用户能够确切地理解为啥这段复杂的代码有其宣称的魔术功能，而非病毒！　去中心化建立的 ID（DID）作为公钥也并非什么新需求。去中心化公钥基础设施 DPKI[10]提案不仅仅试图服务于 DNS 域名，DPKI 本质上是一个区块链时代重新构造的，在线服务版的，Pretty Good Privacy Web of Trust，PGP-WoT [11]。PGP 当 WoT 具有规模时可以看作是一种去中心化的分布式证书认证公钥系统。区块链时代是一个在线服务时代，原本作为离线软件产品的 PGP 因用户得不到专业服务而始终不能形成规模

化应用，因而从未脱离业余质量。如今区块链时代 PGP 当然应该作为在线服务重新推出尝试能否将 WoT 做成有规模的用户相互认证群。然而证书认证是一种依赖于第三方签名的计算，这种对第三方计算的依赖从根本上违背了区块链去中心化共识计算原理。另外基于公钥认证体系中证书撤销仍然是一个非常棘手的问题。

此白皮书的剩余部分将详细描述一种独特且有用的去中心化共识算法，首次对链上用户匿名随机身份，与同一用户在链下物理世界应用的，适宜于人脑受用的身份形成完全性映射。我们用 Good-ID 表示用户在链下应用中适合于人脑受用的低熵 ID，用 Good-DID 表示由去中心化共识算法认证的 Good-ID，用 Good-DID-PK 表示 Good-DID 还是用户可在链下应用中使用的一个公钥。道立名区块链提供了一种构建 Good-DID-PK 的独特新颖实用的公链服务。

3. 基于身份的密码学

Adi Shamir 于 1984 年开创性地提出的基于身份的签名方案[12]，此工作突破了传统公钥认证体制基于 Directory Reference 的限制。基于身份的密码学(IBC)可以将任何适宜于人脑识别的低熵字符串制作成公钥。Shamir 开创性的工作激发了 IBC 研究兴趣，IBC 成为密码学的一个重要研究方向,终于在世纪更替时出现了实用的 IBC 方案[13,14]。这些实用的 IBC 方案使用了一种非常有用的密码学算法基础构建，称为双线性对，由 Victor Miller[15]从数学领域（The Weil Pairing）引入至密码学领域。

双线性对是从有限域上定义的椭圆曲线上两个点的加法群到有限域乘法群的一种同态映射。假设 G_1 和 G_2 为素数阶 q 下的两个双线性对友好可计算的椭圆加法群，G_T 是具有相同素数阶 q 的乘法群，$\hat{e}$ 为双线性对映射：

$$\hat{e} : G_1 \times G_2 \rightarrow G_T$$

对所有 G_1 上椭圆曲线点 U, V，G_2 上椭圆曲线点 U', V'，以下双线性等式成立并可被高效率快速计算：

$$\hat{e}(U + V, U') = \hat{e}(U, U') \times \hat{e}(V, U')$$
$$\hat{e}(U, U' + V') = \hat{e}(U, U') \times \hat{e}(U, V')$$

令用户 Alice 使用一个易识别的低熵 ID，简单表示为“Alice”，其中引号表明为比特串。在区块链应用中，Alice 可以是一个区块链钱包的拥有者或持有者。令 $k_{\text{Alice}} < q$ 是随机生成的大整数，作为 Alice 的私钥。令 H_1 表示从任意比特串到 G_1 上椭圆曲线点的确定性映射函数，H_2 表示从任意比特串到 G_2 上椭圆曲线点的确定性映射函数，表示如下：

$$H_1(\text{"Alice"}) \in G_1$$
$$H_2(\text{"Alice"}) \in G_2$$

这两个 hash 函数的输出分别是 G_1 和 G_2, 上的两个椭圆曲线点，每个都被命名为：“ID hash 映射至曲线点”。作为 IBC 用户 ID 的例子包括，众所周知的通信应用可寻址的身份，如：手机号，手机/电脑的 MAC 地址，电子邮箱地址，社交媒体账号，域名等。由于道立名区域链的主要应用为打通链上匿名身份与链下应用真实身份的关系，我们的技术格外涵盖用户 ID 为更普遍事物的情况，如：照片，学位证书，身份证，车牌号，文档等。幸好所有这些事物的数码表达皆可确定性唯一性 hash 到椭圆曲线的某一点上。

将 Alice 的身份确定性的 hash 到椭圆曲线点后，Alice 的钱包可计算输出以下四元组（包含 i=j 的特殊情况）：

$$< \quad H_1(\text{“Alice}_i\text{”}), \quad [k_{\text{Alice}}]H_1(\text{“Alice}_i\text{”}) \quad > \text{in } G_1$$
$$< \quad H_2(\text{“Alice}_j\text{”}), \quad [k_{\text{Alice}}]H_2(\text{“Alice}_j\text{”}) \quad > \text{in } G_2$$

根据上面列出的双线性等式，可推导出以下”双线性对 Diffie-Hellman 四元组”（BPDHQ) 验证等式：

$$\hat{e}(H_1(\text{" Alice}_i\text{" }), [k_{\text{Alice}}]H_2(\text{" Alice }_j\text{" })) = \hat{e}([k_{\text{Alice}}]H_1(\text{" Alice}_i\text{" }), H_2(\text{" Alice }_j\text{" }))$$

因为两者皆等于

$$\hat{e}(H_1(\text{" Alice}_i\text{" }), H_2(\text{" Alice }_j\text{" }))^{k_{\text{Alice}}}$$

使用 Miller 算法[15]qualifies 公钥算法单向和良好混合属性。可以在不需要知道 Alice 私钥 k_{Alice} 的情况下有效计算 BPDHQ。Miller 算法这一重要属性对 IBC 是非常重要的，对 BPDHQ 的等式验证成立意味着曲线点对

$$< H_{1,2}(\text{“Alice}_j\text{”}), \quad [k_{\text{Alice}}]H_{1,2}(\text{“Alice}_j\text{”}) >$$

可以用作 Alice 的适宜于人脑识别的低熵值公钥。这个观察将构成道立名新区块链在线算法的诀窍，该算法输出一个一致的断言，即 Alice 的钱包可以具有适宜于人脑受用的有意义的低熵公钥或地址。

上面这对公钥密码学的价值是很容易表达并已为业界采纳为加密标准的。例如，让 Bob 将消息 m 加密到 Alice，其中 m 是长度不超过配对的可计算椭圆曲线的坐标的位串。Bob 随机选取 $r < q$，并进行计算:

$U = [r]H_1(\text{“Alice”}), V = m \text{ “bit-wise-xor” } (x \text{ coordinate of } [r][k_{\text{Alice}}]H_1(\text{“Alice”}))$

由于 〈 U, V 〉是被 Bob 的随机值 r 随机化的，所以从对中提取消息 m 具有不可行的计算复杂度。但是 Alice 可以使用她的私钥 k_{Alice} 在椭圆曲线点 U 上标量乘，计算输出椭圆曲线点$[k_{\text{Alice}}][r]H_1(\text{“Alice”})$，然后用 V 对该点的 x 坐标进行“位-xor”来解密消息 m。使用她的私钥对消息进行数字签名更容易演示，然而让我们将此演示延迟至下一节中给出。

4. 道立名区块链

所有已知区块链技术仅皆使用非线性 hash 函数，道立名区块链额外还使用第 3 节中介绍的双线性对映射 $\hat{e} : G_1 \times G_2 \rightarrow G_T$。Miller 双线性对映射算法是一个优良混淆函数，还因具有压缩性质也是一个单向映射函数，所以可被称之为“双线性 hash 函数”。道立名区块链用户钱包的公钥算法使用双线性对友好的椭圆曲线。在我们的应用中，令 G_1 如同所有现有的区块链中应用一样，发挥椭圆曲线加密算法的通常作用。令 G_2 提供一种新的独特有用的功能：从用户链下应用的 Good-IDs 到 G_2 曲线点坐标的散列映射。

我们指出道立名区块链将以完全公开挖矿算法方式导出所有系统公共使用的密码学应用参数。例如，令椭圆曲线的定义参数为公开 hash 函数的输出。设 P 为 G_1 中素数阶 q 的一个固定公共点。记 Alice 钱包的私钥为 k_{Alice}。Alice 先以匿名方式加入道立名区块链，这一步用户上链方式可以像所有已出现区块链情况一样，然而我们建议这一步上链无需挖矿，所谓上链只不过让用户钱包加入区块链 P2P 网络，使得钱包公钥活动可被广播至全网。在这一步“通常”上链情况，Alice 钱包仅需使用 G_1；她的公开地址是 $[k_{\text{Alice}}]P$。注意，这个 G_1 地

址是一个通常区块链的高熵地址。Alice 可以选择保持匿名使用道立名区块链，就像在所有其它区块链中一样匿名所作所为。

有些 Alice 当然会选择让道立名区块链认证她们在链下应用中需要用的 Good-IDs（出名当然要用好身份）。这样“想出名”的 Alice 可发起一个“想出名交易”请求，向所有节点广播以下 Trustlessly Agreeable Diffie-Hellman Quadruple (TADHQ, 无须信任即可认同 Diffie-Hellman 4 元组)：

$$\text{TADHQ} = < \quad P, \quad [k_{\text{Alice}}]P, \quad H_2(\text{“Alice”}), \quad [k_{\text{Alice}}]H_2(\text{“Alice”}) \quad >$$

之所以将这个 4 元组命名为“无须信任即可认同的 Diffie-Hellman 4 元组”，是因为将这个 4 元组输入到“双线性对 hash”算法公式（见第 2 节，使用常数散列函数 $H_1(\text{“Alice”}) = P$ ）将得到 TRUE 为输出，实施这种验证，验证方可以在不需要知道 Alice 的私钥 k_{Alice} 的情况下公开进行，完全遵从区块链共识算法仅信任公开的 hash 算法的原则。

与 Libra 区块链或 EOS 区块链使用多个特权节点情况类似，道立名区块链也会组织一群（Proof-of-Stake，PoS）俱乐部成员节点，叫做验证节点，从事验证 Alice 的“想出名交易”所提供参数的正确性。例如，如果“Alice”是一个电子邮件地址，那么 PoS 俱乐部成员应该包括可发收邮件的验证节点。其他形式的“Alice”（及对应的验证者）包括：社交媒体帐户（社交媒体服务提供商）、智能手机号码（运营商短信）与/或网卡（智能手机操作系统提供商），域名（域名注册服务商）等。这些情况都是在线管理的身份。“Alice”的一些形式可能是线下的，例如：学校毕业证书（学校）、组织成员雇员（组织、雇主），政府-公民-服务关系，IoT 设备识别号（IoT 设备提供商）等。

记 Bob 为这样的一个 PoS 验证节点。对于 i = 1，2，令 IDi 表示将“Alice”散列映射到 Gi 群的椭圆曲线点。下面的两个公式也构成两个 TADHQ 4 元组的双线性对 hash 函数的验证，而且事实上还构成了验证者 Bob 对 Alice 的 Good-IDi 身份所做的数字签名：

$$\hat{e}([k_{\text{Bob}}]\text{Alice}_1, \text{Bob}_2) = \hat{e}(\text{Alice}_1, [k_{\text{Bob}}]\text{Bob}_2)$$
$$\hat{e}([k_{\text{Bob}}]\text{Bob}_1, \text{Alice}_2) = \hat{e}(\text{Bob}_1, [k_{\text{Bob}}]\text{Alice}_2)$$

PoS 验证者 Bob 的以上签名构成了 Bob 对 Alice 在 G_1 群中的匿名身份与她的“想出名交易”请求在 G_2 群中的表达她的 Good-ID 身份做出了关联声明。当

然在给出这样的身份关联声明之前，Bob 应当对 Alice 的链下应用身份做 Alice 对其身份真实拥有事实的调查。道立名区块链中对用户链上链下身份映射正确性的验证者 Bob 之所以被称为 PoS 节点，正是因为要求 Bob 对用户链下应用身份真实拥有性调查是尽职的，是一种基于奖惩机制尽职设计。这种设计可以要求验证者将验证出错风险所对应的资产予以抵押。提供正确身份验证是有利可图的商业服务提供，而错误的身份验证将以没收验证者抵押的资产作为惩罚。

道立名区块链设计的 PoS 验证具有区块链流线型方式工作：Bob 可以用发起一个交易请求（称之为“验证交易”）的区块链标准方式提交以上 TADHQ 公式的数字签名。所有 P2P 广播网中的节点皆可收到验证者的验证成功交易请求。当对给定 Alice“出名交易”身份真实性验证的“验证交易”数量达到一个事先设定的门限阈值时，针对 Alice“出名交易”TADHQ 4 元组的 PoW 挖矿工作开始进行，成功挖矿将输出 Alice 链上 G_1 曲线群的匿名身份与链下应用 G_2 曲线群的真实身份，而且还都是 Good-ID-PK。我们在此格外提醒读者注意：挖矿输出的链上链下身份对应的链下应用验证工作仅要求链下应用验证者仅信任公开 hash 函数，非线性与双线性对的。道立名的此种链下验证身份共识算法与之前所有已知企图用区块链技术提供 DID 服务的工作不同，之前已知 DID 工作的最佳知识限于 PGP-WoT 在线服务证书方式，那样的“共识”无法避免验证者必须在某个环节信任某个第三方。

由于道立名区块链的 PoW 挖矿工作仅对达到了 PoS 阈值的 Alice“想出名交易”TADHQ 4 元组进行，出块时可能出现的分叉不具有攻击区块链安全的恶意利用价值，当出现分叉时系统可任选一叉作为合法 block head，同时向非恶意分叉矿工按正常出块成本支付出块费用。所以道立名区块链不存在链分叉攻击。我们需要指出：此种链安全性质得益于道立名链应用仅限于注册管理自己服务用户的 Good-DID-PK 身份。

从此开始，Alice 可在各种链下应用中方便自如地使用她的 Good-ID-PK。

我们注意到一些区块链项目，如 Libra，也提出要考虑在其共识算法使用某种形式的门限阈值签名，例如 BLS 聚合门限签名[16]。这种聚合门限签名允许任意多个签名者共同参与一个多方计算协议，协议最终输出的签名不扩展表达签名比特串的长度。道立名区块链提出的 TADHQ 公式签名允许多个验证节点

以一种非时间敏感的方式输出门限阈值签名，每一个签名简单由一个通用区块链交易表达。由于链下身份防盗、真实性的验证工作可能涉及到离线步骤，因此将共识算法设计成非时间敏感是有必要的。十分幸运的是，在区块链技术中，虽然链的逻辑长度可以是任意长的，但物理长度总是恒定被压缩为常数1。简单的基于通用交易公式的阈值门限签名达到的共识机制，虽然看起来不那么智能，听起来也不那么通得过某种学术评审者已经习惯了的规范，却能以一种优雅的方式服务于链下应用所需的在线离线身份真实性核查。

由于道立名区块链建立的Good-DID-PK是一种在线服务提供，撤销密钥对是在线服务的一个简单副产品。

用户在G_1曲线群中的匿名身份是道立名区块链的一个默认属性。如果用户还希望在G_2曲线群中也使用匿名身份，双线性对是可以轻松而有效地实现非交互零知识证明，像多个PoS验证者证明Alice在两个曲线群中的公钥身份共用了她的私钥。

5. 讨论

1. 道立名区块链使用双线性对密码学技术作为一种共识可信的公开线性hash算法，可在无中心化信任方的环境公开验证Diffie-Hellman四元组，将任意数量适宜于人脑受用识别的低熵值比特串确定性映射至高熵值公钥或区块链钱包地址。

2. 道立名区块链使用online-offline PoS-PoW结合的共识算法，实现去中心化共识算法以完成Good-DID-PK认证。

3. 自从20世纪80年代IBC概念被提出以来，具有密钥托管性质的所谓“Private Key Generator”PKG可被看作是一个黑洞引力量级的被攻击和单点故障中心，事实上造成了IBC应用基本缺失。道立名区块链工作完全去除了IBC的这个应用不可行缺陷。

4. 利用完全同样的双线性对hash映射算法，可将Alice多个设备分布的钱包中独立不同的公钥（对应独立不同的私钥）映射到同一个链下应用身份，可以使Alice钱包的安全性得到有效加强。

5. 区块链时代的 IBC 能够在主流的公钥加密应用中发挥其应有的作用。

6. REFERENCES

[1] Leslie Lamport, *Constructing digital signatures from a one-way function*, Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, Oct. 1979.
en.wikipedia.org/wiki/Lamport_signature

[2] Satoshi Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2009, url:www.bitcoin.org/bitcoin.pdf

[3] Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, url: github.com/ethereum/wiki/wiki/White-Paper

[4] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich, MIT CSAIL, url:people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf

[5] EOS.IO Technical White Paper v2, url:github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[6] Zooko's triangle, url:en.wikipedia.org/wiki/Zooko%27s_triangle

[7] An Introduction to Libra, url:libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf

[8] Namecoin — Decentralized secure names, url:namecoin.org

[9] Ethereum Name Service, url:ens.domains

[10] Christopher Allen, Arthur Brock, Vitalik Buterin, et. al., Decentralized Public Key Infrastructure, url:danubetech.com/download/dpki.pdf

[11] Alfarez Abdul-Rahman, The PGP Trust Model, url:ldlus.org/college/WOT/The_PGP_Trust_Model.pdf

[12] Adi Shamir, Identity based cryptosystems and signature schemes, Advances in Cryptology, Proceedings of CRYPTO' 84, Lecture Notes in Computer Science 196, pages 48-53, SpringerVerlag, 1985.

[13] R. Sakai, K. Ohgishi, and M. Kasahara, Cryptosystems based on pairing, In Proceedings of 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 2000.

[14] D. Boneh and M. Franklin, Identity based encryption from the Weil pairing. Advances in Cryptology, Proceedings of CRYPTO’01, Lecture Notes in Computer Science 2139, pages 213229, Springer-Verlag, 2001.

[15] Victor S. Miller, Short programs for functions on curves, Unpublished manuscript, vol. 97, pages 101－102, 1986.

[16] Dan Boneh, Ben Lynn, Hovav Shacham, Short Signatures from the Weil Pairing. ASIACRYPT 2001. pages 514-532. See also J. Cryptology 17(4): 297-319 (2004).