voidcoin: 一种点对点的电子发行系统

Void Sleep
voidcoin@gmail.com
www.voidcoin.com

天下万物生于有，有生于无。——《道德经》

摘要. void 在程序中表示可以任意进行转换的空类型，voidcoin 也具有相似的属性，可以生成不同类型的子币，子币具有透明和半中心化的属性，子币的作用决定于发行者的属性和如何对其解读。
voidcoin 的目标不是替代现有信用体系，而是通过把母币作为权力媒介，赋予现有信用体系全新的信任度、透明度以及开放的竞争性。

1. 简介

本体系基于比特币的原理，尝试构建一种兼顾去中心化和半中心化，兼顾信用体系和非信用体系的电子发行系统。网络通过工作量证明挖矿产生母币，母币可以进行自由流通，同时母币代表了子币的铸币权，任何人集到足够数量的母币，就可以通过摧毁母币发行属于自己的子币，子币发行数量不限，子币的价值由发行人的信用和市场决定。子币发行后归发行人所有，子币可以在网络上和母币一样自由流通，但不具有进一步铸币的能力。发行人拥有对子币的交易确认权，可以通过架设子币确认服务器达到瞬间确认的中心化效果。发行人可以多次筹集母币进行适合数量子币的增发。发行人自行负责子币的流通和增发工作，由于数据透明，滥发将造成发行人的信用降低。

2. 铸币权

a) 母币

母币通过原始挖矿生成，并可自由交易。任意帐号积攒到足够发行权的母币，便可以向网络广播销毁母币，同时生成任意数量的子币。每个帐号生成的子币均不同，同一种子币如需要增发，必须用同一个帐号再次销毁母币，增发数量由发行帐号自行决定。

b) 子币

子币由特定帐号通过销毁母币生成，每个帐号发行的子币都不同，属于完全不同的货币。同一个帐号可以发行若干种子币。子币最小单位为 1，不可继续分割，不可用于生成下一代子币。子币由发行人负责分配给其他人。

子币分为 2 类，一种不带有数据功能，可以作为通用货币或股票的形式存在。一种拥有一定的数据携带能力，可以标识每一枚子币特定的意义，可用于所有权表示等作用。每一枚子币携带的数据只能进行一次初始化，后续不可修改。具有数据功能的子币需要更多的母币进行发行。

3. 增发子币

如果某种子币有增发需求，必须使用发行地址的私钥签名再次销毁母币进行增发，

增发数量不限，增发次数不限，增发的子币类型和之前发行的一样。由于数据的公开性，发行人必须自行保证发行量不影响自己的信用。信用降低的发行人将会被自由竞争出局。

4. 货币销毁

a) 母币

母币和子币都允许做销毁操作，母币销毁可以生成子币，但不允许凭空销毁母币。

b) 子币

拥有私钥可以销毁本账户上特定种类特定数量的子币，用处是当收到恶意帐号的小额子币攻击时，以及其他一些方面的需求，比如物权对应的物品已不存在，保持自己帐号的整洁。

5. 交易确认

a) 工作量证明

母币的交易验证和发行子币由全网通过分布式计算确认。

由于小型子币发行者并不会建立自己的验证服务器，子币的交易验证也可以通过全网工作量证明决定，但子币允许更快的中心化方式。

b) 发行者证明

子币发行人有权力通过私钥签名对自己发行的子币进行快速交易确认，子币的交易确认体系中，发行者具有高可信的确认权，一旦发行者认可交易，那么便可以认为交易有效，不用等待网络进行 6 次以上确认。发行者通过架设自己的确认服务器，可以达到和中心化相同的确认速度。但发行者确认本质上只是一次确认，如果网络不承认，依然会被推翻。

6. 挖矿

挖矿只能挖到母币，母币的数量将不进行数量限定。网络会按照恒定的速度不断产生母币，但由于母币具有了主动销毁的特性，整个网络会避免母币数量的泛滥，甚至相对紧缺，使得母币矿工具有持续的收益。同时由于母币紧缺，将维持较高价格，可以保证不被缺乏信用的闲人用来滥发子币。由于引入了二次发行机制，同样数量的母币在不同发行人的手里将意味着不同的价值，同样数量的母币可能被赋予极大的价值，也可能变的一文不值，母币将被作为整个网络的储备货币存在，由于子币具有高速交易的优势，普通人可以直接使用高信用帐号发行的子币作为货币，避免母币价格的持续走高，发行量和需求量不能适应导致的货币紧缺现象。

挖矿同样能挖到货币转移方愿意付出的手续费。手续费可以是用于交易的子币也可以是母币。如果是带数据类型的子币，不能作为手续费。

7. 授权和回收

出于安全考虑，子币发行帐号的私钥必须严格保密，所以需要尽量减少子币发行帐

号的使用，同时为了保证发行者验证的机制，voidcoin 体系定义了授权和回收指令，授权指令允许子币的最初发行者将特定子币的发行权和验证权授权给若干其他帐号拥有，网络接受后就会承认被授权者。

当出现安全问题，被授权帐号出现私钥泄漏等情况时，最初发行者可以使用权力回收指令收回上述两项权利，网络将不承认被授权者的发行验证权。

由于整个子币系统的安全性基于发行者私钥的保密性，该机制让最初发行者尽量少参与到网络互动中，以降低子币系统的安全风险。

8. 应用

a) 发行货币

只要获取足够数量的母币，任何人可以向网络宣布销毁母币，并多次发行任意数量的子币。国家央行可以直接接入该体系以子币的形式发行法币，并依据宏观调控不断调整货币发行数量，但发行数量和货币流向保证了绝对的透明度来接受公众监督。同样，如果对央行的服务器不满意，第三方支付公司也可以发行自己的子币，并声称和法币进行 1:1 挂钩，通过自己架设服务器提升交易性能，这样就直接和央行进行竞争，最终产生最佳的货币。

现实中使用的纸币系统同样可以接入到整个体系中，只要银行承诺纸币可以兑换为子币形式的法币。

b) 发行股票

现行的股票及债券市场将被完全颠覆，任何公司都可以直接通过子币的形式发行自己的股票，而不用通过交易市场进行上市。股票和货币本质变得完全一样，投资股票变成了简单的子币转移，交易和变现变的极为方便，并由于公司法币账户和股票发行数量都挂在同一个网络上，极其透明，避免了各种金融欺诈现象。

c) 会员认证

发行特定的会员卡变的极其简易，只需要生成子币并发送 1 个币到特定的账号上，就可以通过币的所有权轻易验证对方的身份，并且由于可以对交易进行跟踪，任何用其他人的卡或者会员转让都可以轻易发现。卡的价值和子币发行数量相关，高级会员卡可以使用数据子币。

d) 产品跟踪和反馈

厂家可以对自己生产的每一件商品赋予一个子币作为身份，并在发生实体交易时将子币转移到买家的账号上，这样就间接标识了物品的所有权，并通过批量下发给下层批发商，方便厂家对零售情况进行实时跟踪，以调整策略，传统厂家也将获得互联网公司级的数据追踪能力。如果使用数据子币，厂家还可以直接让用户发回简单的评价和建议，提高沟通力。

e) 物权和产权

物权和产权也变得极度透明，物权和产权转移也简单变成了标有特定数据子币的转移，绝对可信，成本极低。由于数据链的不可修改性，公证处、XX 管理局等机构将消失。

f) 公共身份认证

公民将在出生时用公钥向政府注册自己的公共身份帐号，用于各种公共事务。怀疑身份泄漏后，可以到政府重新进行更改。

g) 选举和投票

选举和投票也将变的极其方便，每个婴儿出生时将被赋予一个公共事务帐号，当政府需要公众进行投票时，政府在自己的帐号生成某种子币作为本届的选票，自动下发到达到年龄的公民公共事务账号中，参选人公布自己的接受投票帐号，做到低成本，透明进行选举。

h) 公共事务监管

央行每年增发的货币和流向都将被公开监管。

税收将被集中到特定的公开帐号，流向将被公开，流向未公开信息帐号的货币将引发公民质疑，政府必须公开一切货币流向方。

公务人员财产公开变的极为容易。

i) 设备

某种专用的身份认证或查询设备将变的非常重要，可以集成在智能手机或者某种专用硬件上。

j) 更多的玩法……

9. 与比特币相比

a) 解决财富不平均的问题

由于系统引入了子币概念，可以依靠信用放大母币的价值，使得 voidcoin 体系的价值可以被无限放大，有效避免早期囤积者占据大量母币，而占有整个体系过大财富比例的问题。

b) 解决增长速度和经济规模不匹配的问题

比特币固定的增长规则，在经济学上产生二个问题：一是和实体经济规模增长不匹配，导致价格波动剧烈，长期看不稳定；二是为保证不被早期用户占据过大比例，前期增长需要相当的时间达到相对可用数量，无法早期切入实体领域。

子币系统有效解决了这两个问题，子币可以随着经济增长而增发，而增发又是真正公开的，让信用真正变的可以相信。

c) 解决交易速度问题

比特币受限于数据块产生的速度，使得一次有效的交易至少要数十分钟才能得到确认，其本质是因为对其他用户的不信任，而引入子币体系，相当于引入了自由竞争的可信第三方，由发行者对自己发行的子币进行确认，解决确认速度问题；而这个确认又是公开在网络中的，对发行者权利进行了制约，并可以公开监管。

d) 解决比特币扩展性不好的问题

现有基于比特币的带标记功能的其他电子货币，比如彩色币、MasterCoin，都受

限于比特币的设计，只能强行利用某种方式标记在比特币数据链上，就像在 HTTP 上开发 FTP，而且有些实现方案还受限于初始块、拆分、小额等机制可能导致种种问题，实际上比特币本身并没有设计二次扩展性，用题头引用道德经的话来说，比特币只实现了从无到有的突破，并没有设计从有到万物的扩展，大大限制了比特币的适用范围。

e) 解决币种间的自由竞争问题

比特币和山寨币，山寨币和山寨币目前只能进行货币体系间的竞争，而不能在同一个体系内进行真正公平的竞争，可能仅仅因为发行时间晚，而导致劣币驱逐良币。voidcoin 目的就是打造一个自由竞争的平台，使得不同子币在同一个框架下真正做到自由竞争，大家要做的就是比运营、比信用。

f) 解决比特币不能对接实体法币的问题

由于子币由发行人生成，使其理念上可以和实体发币进行对接，只要发行方承诺子币和法币能互相兑换，这样法币本质上变成了 voidcoin 网络的线下交换途径。

g) 降低 51%攻击的风险

针对网络的 51%攻击将只会影响到母币体系，而蕴含更大价值的子币系统由于发行者的存在，攻击难度将大大提升。相对比特币系统，整个系统被攻击的风险被降低，安全性更好。

h) 降低小额攻击危害

由于引入了子币体系，整个体系更加容易产生小额攻击，系统引入了子币销毁功能，方便删除来自攻击者的小额无用子币。

i) 更海量的交易需求

部分应用方式将导致庞大的小额数据，尤其是使用选举功能时，需要下发数千万的选票，对整个网络将产生极大的考验。为了解决这个问题，voidcoin 计划采用双难度块链机制，凡是被发行者校验过的子币交易打包在一起，校验难度将被显著降低，并提高块链生成速度，而母币和没有发行者验证的子币交易，依然需要较高难度、较长时间的全网校验来保证安全性。

j) 更高的安全需求

由于一个子币体系完全由发行者的私钥保密决定安全性，导致对发行者的私钥保密要求大大提高，私钥泄漏将直接导致相关子币崩溃。体系引入了发行权和验证权的授权和回收机制，尽力保证最初发行帐号的安全。