STEGOS

A Platform for Privacy Applications

Stegos AG

May 28, 2019
v1.0
https://stegos.com/docs/whitepaper

Contents

0.1 摘 •

多功能移动app和社交媒体平台可以 © 从前无法 Þ 接 w 来的几百万人 ý 能够使用在线的服务和社区。但是 他们却付出了用户 • 私作为代价。相反地是 区块 þ 和数字 ' 币平台可以为用户带来前所未有的 • 私保护 但是目前区块 þ 技术 Ø 相对 ƒ 慢 而且属于 D 源密 Æ 型 Ù 就使得区块 þ Ø 无法为普 用户提供服务。我们 • Ù 种方式可以把 • 私和可用性结合在单个的平台。

Stegos • 私平台 Stegos 将特殊的区块 þ 和 Á ¾ ¡ 结合 w 来 并且发 L 了 – 个 • 私、安全、 Ø 效以及环保的数字 ' 币。Stegos是完全可扩展化以及不可篡改的 Ù 就保 Á 了区块 þ 始终保持紧凑 而且不会损害信任。 Ù © Stegos成为了全球 – 个能够提供 d 了支付 l & 之外 Ø 有安全且 • 私的数据存储和 l 移的公 þ 。

Stegos将区块 þ 底层扩展 从而提供了能够打 • 私应用的平台 并且 Ù 些应用可以为社交聊天带来最小的延 ß 效果。我们提出的可信应用存储 TAC 以及 • 私应用商城可以 © 搭建和分发 • 私应用的 Ç 程变得很简单 同时也能够提供更 Ø 的用户安全性。最后不能不提地是 Stegos市场、聊天、以及红包功能是去中心化应用中最流 L 的功能 Ù 些可以 © 用户能在完全 • 私地情况下 Û L l & 和聊天。

Stegos的共 Æ 机制是 L 注权益 Á 明 gPoS 共 Æ 机制 它是基于可 Œ Á 的无偏分布 • 机性。gPoS机制可以 © 任何人 • « Ð L Stegos区块 þ 并且 Ç 维护网络可以 Z 取收益 甚至无很 Ø 的抵押。 Ù 可以 励更多的人参与 从而保 Á 移动用户有 ³ 够的激励来 Œ Á 网络。

0.2 反 ˆ

如果对于此白皮书有任何建 ® ÷ 发 ® 件至paper@stegos.com.

1. 介绍

1.1 我们ý应å掌握•私

每个人ý应å掌握自己的•私　同时也应å·得现代社会所有的服务和福利。但是现在的技术和商业模式并不能实现Ù点　或者ô压根不愿意　同时提供Ù两个服务。

Ç去10年　我们看到的全球社交媒体平台和多功能应用的崛w　其中ý会带有支付功能　例如微信和Facebook。•着移动互联网技术的快　发展　Ù可以©大约10亿人能够在线上Û L沟　、交易以及合作。但是Ù些平台的•私功能是个噩梦　你任何的L为ý可以«ý *　并且拿出你和别人的聊天或者l &°录　不º你是否想•分享Ù些信息。同时　用户数据会«•意地盗用　从而变成了广告商和Ñ客的目标。目前为制止Ù种滥用所作的努力是徒劳无功的　而且并没有什么意义　常是因为政府和监管机构不希望放弃控制　©用户对自己的网络L为　#。

从硬件Ò度来看　固态技术、智能手机以及物联网技术把生活Å Û了我们的口‹、手机和电脑。但是在保护我们•私的h b下　从恐怖主义　从Ñ客　从我们自己所　的缺乏#任Ò度来看　我们的•私早就«严Í破坏。在机场　甚至在w上　我们«ë以惊人的'率泄2我们的私人数据。

Ù种入侵©我们感到•私暴2在空气中　并且十分无助。很多人ý b临着更加令人毛¨悚然的结果　例如失去工作、自由甚至生命。

我们生活在一个史无前例的国家监Æ和G压新û自由甚至思想自由的时代。但是　其实你如何对待自己的D Ñ　无º是现Ñ Ø是数字'币　又或者是如何　Ç区块þ去Û L交易　Ù ý和别人无关。

Ù个‹势并没有«忽Æ。纵Â世界上各个国家　人们对他们的•私和数据是如何«利用以牟利h示不满。因此　我们　•更加安全和•私的　择　而且Ù只会在未来几个月以及几年Ì持续增•。

1.2 区块þ和•私

从另一个Ò度来看　区块þ和去中心化技术促Û了数字•私和安全†域的巨大Þ Ã。}然传统的数据分享和存储技术　在线云存储　®件　笔°本电脑等等　已经有了内置的安全性　但是Ù些技术很容易«攻破。一旦有人·得你的密码　并且Û入你的系统　£么你的数据就会永久暴2。

基于区块þ的私有的去中心化ã决方案会更好地保护你的私人信息　并且可以和你信任的人Û L共享。

但是　大众对于Ù种ã决方案的接受程度却不是很乐Â。目前的区块þ Ð L　度很慢　Ð l不够流畅　而且对环境也有影响　而且没有任何•私币真正地拥有它所ô的•私性能。对于D源匮乏的Y态硬件以及不友好接口的依V　最终会©Ù y技术Ü离普　用户　但是如果没有用户的参与　区块þ平台注定会　缩和Í新变得中心化。•着用户的使用习惯从桌b端到移动端　加密'币其实很¾ ß得上Ù个潮流。

ã 决方案很清晰　为了 ß 上 Ù 个潮流　区块 þ 平台必 { 学习例如微信和Facebook Ù 些平台的吸引力和可用性　同时 Ø • 保持很强的 • 私性、匿名性以及去中心化。

Stegos是 – 个将 Ù 些 † 域结合 w 来的区块 þ 。Stegos是为安全 l & 、数据 l 移以及　信的最好机制　因为和传统的 ® 件和在线　信服务于不同　它是完全去中心化的、加密安全的、同时也不会留下用户 « 份的 Û 丝 l ù 。因此　不会有人能看到你给　发　信息或者接收了　的信息　又或者确定任何人和Stegos建立联系。只有信息或者交易的接受者会知 S 发　的具体 Ñ •　而且没有任何东 • 可以将数据或交易与任何人的真实 « 份联系 w 来。

Stegos同时也是 – 个　M 于移动 ¾ 备的区块 þ　智能手机节点可以有完全的Œ Á 能力　并且无基于硬件的工作 Ï Á 明　Ù 意味着任何人 ý 可以　Ç 支持Stegos网络 · 得代币收益。　Ç 把数据 l 移和信息　信作为和 l & 相同的优先级　Stegos会是所有人 ý 想使用的区块 þ 。而且　专注于移动手机意味着所有人 ý 可以使用。

在我们现代社会　每个人 ý 应 å 有安全和 • 私的交易和　信。Stegos是 – 个并且仅有的区块 þ 平台　能够提供 Ù 些功能。

2. Stegos是什么?

2.1 简介

Stegos • 私平台 Stegos 将独特的区块þ和 Á ¾ ¡结合 并且发 L 了 – 个完全 • 私、安全、Ø效以及可持续环保的加密 ' 币。Stegos使用了*UTXO* 代币 模型以及*gPoS* (L 注权益 Á 明)共 Æ 机制 将现有的 • 私代币和最新的加密研究结合 从而创建完全的可拓展 scalable 以及可修剪 prunable 的 • 私区块þ和应用平台。

2.1.1 绝对的 • 私

由于Stegos中的ê球协® Snowball protocol ÷ Á D 件B Stegos中的支付和数据 l & 是不可þ接的、不可ý * 的、并且完全 • 私的。每个Stegos中的交易是ó l 到全新的、独特的秘密地址 从而无法发现接受者。ê球同时也© ý * Stegos交易历史变为不可能 因为单个交易 – 先会Æ合w来 才能在提交给区块Œ Á 者之前 形成 … 级 l & supertransaction 。所有Ù些ý会 Ç 安全、 • 私保护的方式Û L 同时确保Stegos代币是完全可替代。

2.1.2 支付和信息传

其他 • 私类代币- 例如Monero, Dash, ZCash和Grin - 只可以用于支付 而且对于可扩展性、 • 私性、安全性或者可用性来ô ý 存在缺w。Stegos就Ù些和其他 • 私币的î ˜ Û L 了提升和优化 同时可以用于支付和数据的发 并且是完全 • 私的。Stegos可信的应用存储器 TAC 可以©开发者很容易地搭建应用 并且能够匿名、 • 私并且Ø效地Û L 沟 。

2.1.3 可扩容性和数据压缩

Stegos是一个快 并且Ø度扩容的区块þ 而且和其他区块þ不同 它在不损失信任的前提下整体保持ƒ小。花 9 代币和数据消耗的细节ý可以 Ç 安全加密修剪的方式 从区块þ上安全移d。由于交易分片机制 Stegos区块þ具有很Ø的扩容性 Ù就©其成为世界上 – 个能够提供d了交易 l & 以外 Ø有安全以及 • 私数据存储和传 " 的公þ Ù也©Stegos可以在智能手机上Ð L 。

2.1.4 权益 Á 明**(PoS)**

Stegos是环保的 并且不会浪 9 电能去挖矿的区块þ。相反 Stegos使用了定制化的 L 注权益 Á 明 gPoS 机制 Ù是基于分布式系统理 º 和加密学的Û步。每个Stegos区块必 { 由一群Œ Á 者 validators ÛLŒÁ和确¤ 所有的Œ Á 者必 { • 将代币作为抵押。 Ç Ù 种方式 抵押代币的价值直接影响了Œ Á 者挖出区块 并且 · 得相关 l & 9 用的可能性。

2.1.5 移动应用

为了体现平台的实力 Stegos正在开发自己的原生多功能移动应用 o 件 并且将 ± 包、点对点以及群聊、应用存储器 TAC 、 • 私应用商城以及Stegos红包功能整合。 Ù 个应用将会是用户使用Stegos • 私平台的网关。

2.2 Ø ¤ • 私保护

最初的比特币白皮书只包含了很少 è 分的 • 私相关内容 它假 ¾ 尽管交易数 Ï 是公开的 但是也不可能将 Ù 些交易和任何真实的 « 份 þ 接 w 来。 Ù 个假 ¾ 已经 « 研究者、区块 þ 研究公司以及 Ñ 客多次 Á 明是 ï 的。例如ChainAnalysis Ù 类 o 件已经 Û L 了交易分析 可以 © 任何人很快地发现比特币和其他加密 ' 币使用者的 « 份。

大多数区块 þ y 目 ý ß • 了比特币的脚步 Û L 了完全 明的 ¾ ¡ 并且包含了可 Á 的地址和交易数 Ï 其中也包含了任何 ± 包的余 • 、发 和收到了多少 D Ñ 、以及每个接受和发 者的地址。但是所有 Ù 些信息 ý 成为了 Ñ 客可 Á 的目标。 • 着类似 2 弹(Bulletproofs)协 ® 和 ö 知 Æ Á 明 zk-SNARKs 技术的发展 我们再也没有理由去延续比特币的 ï 。区块 þ Ø ¤ 就应 å 是具有 • 私功能。

为了 ¾ 到 Ù 个目标 Stegos中的交易所是 ^ þ 接的, 不可 ý * 的, and 保密的:

- Stegos使用一次性支付地址 从而无法去 ¤ Á 交易的接收方。我们的一次性地址和Monero和ZCash的 • Ï 地址很相似。
- Stegos将个人的交易整合形成 … 级 l & 从而无法 ý * 交易 ° 录。为了 Ù 个目的 我们已经开发了增强版的ValueShuffle协 ® [7] Ù 是 – 个与保密交易兼容的代币混合协 ®。
- Stegos中的 l & Ñ • ý 是 Ç 佩德森承 ú [8]以及Bulletproofs 围 Á 明(range proofs) [4] Û L 保密。Œ Á 者的抵押和交易 9 用 d 外 因为对于区块Œ Á 而 Ù 是必 { • 可 Á 的。

我们称 Ù 种 • 私功能的组合为 ê 球 如果想了 ã 更多细节信息 ÷ 查看 D 件B 。

2.3 L 注权益 Á 明**(gPoS)** 共 Æ 机制

标准的权益 Á 明共 Æ © 很多持有小 • 抵押代币的用户感受不到激励。为了 ã 决 Ù 个 î ˜ Stegos使用了 L 注权益 Á 明 (gPoS) 其中每个Œ Á 者在Ð L 了一段时 ô 后 ý 有几率 · 得 • 机的Œ Á 者服务奖励 并且 Ù 无 º 他们抵押代币的数 Ï 。

为了提供 D Ñ 每个区块奖励的一 è 分会加入到服务奖励池 Ù 个 D Ñ 池会 渐增加 直到有人 b 得基于可Œ Á 分布 • 机性的加密彩票。

因为智能手机节点可以有完全的Œ Á 功能 任何人 ý 能 • « b 得代币奖励。

[0]名义上的最小 值将 © 用户无法使用系统 但是因为每个可用节点必 { • 提供Œ Á 服务来 Û L ¤ Á 从而不可能去对系统 Û L 欺 È 因为Œ Á 节点服务奖励的目标之一 就是能够最大化不同节点的数 Ï 。

2.4 分片 · 得扩容性

Stegos使用交易型分片来 Û L 扩容。不同的Stegos Œ Á 者会保持整体区块 þ 的状态　但是只会 Œ Á 即将 Û L 的交易　并且使用 è 分片的原子提交　atomic commits　　从而消 d 了双花的可能性。 Ù 种扩容的方式可以 © Stegos能够每秒在数百万个移动 ¾ 备中处理几千笔交易　© Stegos成为 – 个　并且是仅有能够整体在移动端 Ð L 的区块 þ 系统。

2.5 修剪和数据压缩

很多 y 目自称可以 ¾ 到成百上千或者甚至几百万的每秒 l & 数 •　tps　　但是很多有 y 目 ã Ê 它们 ¡ 划如何去维护 Ù 些累积的数据。比特币区块 þ } 然只有7-10的tps　但是现在数据已经大于200千兆字节。假 ¾ 比特币突然可以支持16,000tps　£ 么比特币区块 þ 的数据会每天增 • 350千兆字节[1]　也就是 ô 每年增 • 127百万兆字节。如果不　Ç 几个 … 级 ¡ 算机　Ù 个 Ï 级的数据是完全不可持续的　但是 Ù 和区块 þ 的去中心化理念是相反的。

Stegos是可压缩的区块 þ 。　Ç 安全的加密修剪　pruning　功能　消 9 的代币和 Ç 期的数据可以安全地从区块 þ 上移 d 。为了 © 消 9 Ç 的代币信息可以从区块 þ 上移 d　我们使用了中本聪在最初比特币白皮书 [1]上提到的技术。数据可以自动和快　地 « 移 d 。

2.6 快　数据传 “

和其他区块 þ 不同　Stegos不会 P 制用户只可以 Û L 支付。Stegos支持数据传 “　可以 © 用户的数据传 “ · 得和支付同样的安全性。数据是Stegos区块 þ 中的头等公民　Ù 是合乎 ; ‘ 的　因为一般来 ô　用户发　数据消息的 ‘ 率比支付 • 多的多。

2.7 Stegos移动应用

Stegos移动应用是Stegos生态系统中的一 è 分　并且是我们平台潜力的展现。 Ù 个应用会整合在 ± 包中　并且 Ù 个 ± 包拥有安全的环境可以 Ð L • 私应用。　Ç Ù 种方式　Stegos能够提供现在中心化多功能应用的所有功能　例如微信等等　但是却是　Ç 完全 • 私和去中心化的方式。

Stegos快　信息传 “ 功能包含点对点聊天和群聊　同时 Ø 有支付和红包功能。在微信中　红包功能 ^ 常 W 名　它可以 © 任何人给个人或者群聊中发红包　或者创建定制化的代币空投　从而任何人 ý 可以扫描二维码去 † 取。

Stegos应用同时也可以 © 用户简单且直接地控制自己的抵押代币　© 所有人 ý 可以简单地参与到网络维护中来。

每个人 ý 应 å 有 • 私　而且每个人 ý 应 å 因为 ! 献了更加 • 私的世界而 · 得奖励。Stegos不仅

[1]https://hackernoon.com/if-we-lived-in-a-bitcoin-future-how-big-would-the-blockchain-have-to-be-bd07b282416f

只© 你的 " 产和 • 私安全　而且会因为你支持网络建¾ 而给你奖励　甚至你可以使用手机来Û L 参与。

2.8 • 私应用

Stegos致力于满 ³ 人们　渐增 • 的 • 私　求　而且不会牺牲可用性或者可¿ î 性。研究显示数百万用户ý 对现有的例如Facebook和微信平台不满意　但是却没有很好的替代方案可以© 用户去择。为了满 ³ Ù 个　求　Stegos的¾ ¡ 可以满 ³ • 私应用的爆发　　Ç Stegos聊天　用户的聊天内容会很安全且 • 私。

2.8.1 可信应用容器**(TAC)**

可用性和可¿ î 性不仅是用户的　求。开发者如果想 • 去新平台Û L 开发　也很关注Ù 方 b 。开发原生的移动应用很困¾　并且很容易出　　而且开发安全移动应用也很¾　区块þ 的介入会© 整体更加困¾ 。Stegos的目标使开发移动 • 私应用程序变得简单和低è 槛　同时保护用户免受恶意或写得不好的应用程序的侵害。

Stegos 可信应用容器 (TAC)是一个原生的移动应用和一个è 署 • 私应用的容器。Ù 些应用可以Ç 类似Javascript、HTML以及CSS Ù 样的技术来完成　并且可以按照类似沙盒中的插件 Ù 样Ð L　拥有对用户 ± 包和外è 环境的严格控制。

2.8.2 应用商城

用户　• 能够简单寻找和安Å 应用的方式。Stegos • 私应用商城会提供þ 上寻找和安Å • 私应用的机制　并且在TAC中开发和Ð L　同时也可以Ä 估它们的可用性。

2.9 私人市场

私人 l & 不仅是 P 于代币支付。} 然代币 l & 对于很多用户来ô 是 ^ 常Í • 的　例如汇款　　大多数交易包含了对某几种商品或者服务的支付。　Ç 将私人支付、快　信息传 " 、聊天以及TAC Û L 整合　Stegos会开发私人交易市场　其中很多东 • ý 能够匿名和 • 私地Û L 售卖。

Stegos会发布一个单独的移动 o 件作为Ù 个市场的界 b 。

2.10 提Ø 应用的激励方式

去中心化网络可以从用户中 · 得巨大的力Ï 。因此　为了激励大Ä 模应用　Stegos会包含各种激励措施　旨在吸引各类不同的用户群体。

d 了标准的抵押支付会按他们的抵押比例奖励Œ Á 者　Œ Á 者服务奖励是独特的Stegos功能

会因为Œ Á者保持在线并且支持网络就给予他们奖励。每个区块奖励的1/3会加入到服务奖励池中 [2]然后会每几千个区块就Û L分发。Œ Á者会Ð L基于可Œ Á分布 • 机性的加密彩票 从而择单个Œ Á者来 · 得奖励。所有用户 Ç Stegos应用ý可以看到当前的服务奖池数Ï 。

红包[3] 是 ^ 常有名的微信功能 Ù也是基于中文"红包"。红包功能的引入会 © 几百万用户加入微信 同时他们Ø • 交出自己的ö L卡信息。Stegos想 • 在不侵犯用户 • 私的前提下 复制Ù个 ^ 常W名的功能。

正如微信中红包功能£样 Stegos红包会有不同的 y 可以是公开的 也可以是私下的 而且红包数 • 可以是固定或者 • 机的。最简单的方式 红包可以 Ç Stegos聊天功能 发 固定数Ï的代币给别人 或者是给群聊 其中的代币数Ï是未知的 只有你打开红包才会知S 。

私聊群的红包同样可以是 • 机的 群Ì每个人ý会 · 得 • 机的数 • 。

Stegos同时也会 © 用户在Stegos • 私平台内的Stegos本 « 、单个的 • 私应用和私人市场中创建公开的红包 Ù个功能可以 © 用户传播代币 并且提Ø知名度。公开红包和空投类似 但是可以 励更多用户积极参与。

任何人可以创建公开红包 并且放入一定数Ï的代币。然后 他们 • 将相应的二维码或者URL þ接发 给目标人群 每次打开红包ý会 · 得一定数Ï的代币奖励 直到红包« †完或者经Ç一天后 Ù时候所有没有†取的代币会添加到Œ Á者服务奖励池。

关于使用Stegos红包的è署信息 ÷查看4.3.2 è分。

[2]以及£些红包Ç期未使用的代币.

[3]https://en.m.wikipedia.org/wiki/Red_envelope#Digital_red_envelopes

3. • 私应用平台

Stegos • 私平台会基于我们的快 信息传 " 功能(Section 4.6) 并且使得开发移动 • 私拥有变得 ^ 常容易。Stegos移动应用是整个平台的窗口 它会将可信应用存储器 TAC 和点对点以及群聊 Ø 有 • 私应用商城和红包功能整合 w 来。

3.1 可信应用容器

可信应用容器 TAC 是一个沙盒和 Z 拟机 VM),并且可以 Ð L Ç HTML, CSS和JavaScript í 编写的内置应用。Ù 个技术底层和微信小程序很类似[1]。

TAC会 2 止应用程序对主机 成破坏 同时也 © 区块 þ 从 Ð L 应用中完全抽 a 出来 而不是提供接口 API 来发 信息并且 Û 入 ± 包。TAC严格控制对外 è 世界的 ¿ î 并确保消 9 代币 • 用户确 ¤ 。

Stegos会提供搭建 • 私应用的 o 件开发包 SDK 以及相关文件。

3.2 « 份信息

每个Stegos ± 包 ý 带有公 ¥ 地址 。Stegos使用 • Ï 地址 从而对公 ¥ 的支付 « 两个 • 机值掩盖 Ù 样就无法 Ç 分析区块 þ 去发现 l & 人的 « 份。只有发 方和接收方才有权 Û L 任何信息交换。Ù 意味着用户不必太 Ç 保护自己的公 ¥ 将Stegos公 ¥ 发布在网站或者甚至把它 4 在 W 上的广告牌上 Ù ý 是完全安全的。

Stegos使用了未花 9 交易 UTXO 模型 其中每个UTXO ý 可以理 ã 为一个代币。在Stegos中没有任何单独的 « 份概念 尽管 ± 包地址可以用作标 Æ 符或化 « 用于发 信息或在Stegos私人市场或其他 • 私应用程序上建立声 ‰ 或社会 Ä 分。

Stegos用户能够将 ± 包地址导出作为二维码。

3.3 • 私应用商城

用户有着不同的 • 私 求 有时候甚至用户下 } 的app ý 会 b 临 • 私泄 2 Î i 。用户 • 有 • 私地浏 È 和 Û 入app应用的方式 } 然他们 ¤ 为自己下 } 和安 Å 的app是 • 私和安全的。为了 ¾ 成 Ù 个目标 Stegos è 署了 þ 上 • 私app商场 其中 Ù 些应用的细节 ý 存储在Stegos区块 þ 上。

Ù 些app本 « 应 å 是 þ 下存储 并且不会影响到Stegos区块 þ 而且 • 上线Stegos • 私应用商城 每个 • 私应用 ý 必 { 创建声明 其中包括app的描 ð 下 } URL þ 接 以及应用程序包的哈希 Ù 个声明会存储在Stegos区块 þ 上。App中包含了标签 可以 © 用户 Ç 类别在app商城 Ì b 搜索。

[1] https://walkthechat.com/wechat-mini-programs-simple-introduction/

App会 Ç Stegos商城下 } 一旦下 } 成功 TAC会 Œ Á 应用程序包的签名 以及哈希是否符合声明中的信息。TAC会在本地安 Å 应用程序包 并且 © Ù 个应用在Stegos移动应用中可用。用户 • 时 ý 可以删 d Ù 些应用。

3.4 聊天

无 º 在 Ù 些 l & 中区块 þ 是如何模糊用户信息 用户仍然 • 找到对方 Ù 就有暴 2 个人信息的 Î i Ù 些 成比代币更大的影响。例如 MimbleWimble • 用户提前 Û L 信 从而可以分享在交易 Ç 程中确定 « 份信息所 • 的因素。但是每个交易 ý • 用户 ô 的一些初始 信 从而确定交易的参数。如果 Ù 个 信能 « 截 · £ 么恶意的第三方 ý 会开始对交易 ° 录去匿名化。

现在的平台 ý 会把 Ù 个 î ˜ 留给用户去 ã 决 大大 M 低了它们的吸引力和有效性。 } 然 Ù 些信息泄 2 无法完全满 ³ 但是在Stegos平台 我们相信 Ù 是我们的 # 任去给用户尽可能多的工具去保护他们的 • 私。每个能 Ç Ù 种方式保护的平台 ý 会提 Ø 平台用户的 • 私性能。

最终 Stegos会 è 署完全私人的 信 并且将其和Stegos应用整合 它会包含类似标准 信应用 其中所有用户 ý 对它很熟悉。用户使用公 ¥ 作为 « 份 ¤ Á (Section 3.2) 在不泄 2 任何与其他用户交易信息的情况下展示出来。信息会 Ç 快 信息总线(Section 4.6) Û L 传 从而确保信息是几乎即时收到。

用户可以 Ç 私聊发 二维码 从而启动STG l & 同时也可能创建聊天群 并且 Ç 二维码 € ÷ 用户 Û 群。

接下来的章节 我会更 æ 细地介绍Stegos功能。

4. Stegos æ 细 ã û

4.1 共 Æ 机制

Stegos共 Æ 协 ® 是基于*Albatross* [23] Ù 是 Ç 拜占庭机制BFT [9]的全新区块 þ 共 Æ 算法 而且在 · 得及时交易确 ¤ 的同时 Ø 有很强的一致性。Stegos共 Æ 协 ® 是安全的 并且和理 º 上 · 得单 þ PoS共 Æ 机制的最大值。

4.1.1 投机拜占庭容

投机拜占庭容 SBFT 算法有两种共 Æ 模式

1. the 乐 Â 模式, l & 度很完美 但是只有很少的安全 “ 假 ¾ 所有的节点 ý Ð L 良好。
2. the 悲 Â 模式, 唯一的目标是在有欺 È 节点的情况下 系统也能 z 利 Ð L 。

乐 Â 模式可以 © Stegos共 Æ 协 ® 能够和中心化系统类似的 度。节点会 Œ Á 每次状态更新 当有无效更新检测出来的时候 共 Æ 就会切换到悲 Â 模式。无效的更新就会 « 丢弃 然后共 Æ 回到乐 Â 模式。

4.1.2 Œ Á 节点

Stegos是公开 & 本 因此每个人 ý 可以加入网络 成为 Œ Á 节点 同时 Ç 维护区块 þ · 得奖励。和标准的PoS共 Æ 相比 Stegos使用 L 注权益 Á 明 gPoS 共 Æ 来更好地激励散户参与。节点 • Û L 绩效绑定 抵押 从而可以 Û L Œ Á 服务。 Ç 给出经济方 b 的抵押 • 求 Œ Á 节点 ý 提供绩效绑定 从而 2 止女巫攻击。 定的代币可以像普 代币 £ 样 Û L 权益抵押。

给出绩效绑定的 Œ Á 节点能够 « • 机 择 去作为活 Ã Œ Á 节点参与确定共 Æ 。每个活 Ã 的 Œ Á 节点 ý 会 Ç 可 Œ Á 的分布式 • 机方法去创建区块 同时 Ø 会从交易手续 9 中 · 得奖励。其他活 Ã Œ Á 节点会 Á Á 并且同时签署创建的区块 从而可以 · 得 Œ Á 节点服务奖励(Section 4.3.1)。

4.1.3 区块

Stegos有两种类似的区块

- 核心区块 核心区块是用来改变 Œ Á 节点列 h 并且作为Stegos区块 þ 上的检查点。核心区块只包含了活 Ã Œ Á 节点的 « 份信息 以及用来 择它们的 • 机助 º Í 。核心区块是 Ç 实用性拜占庭 Á 明 pBFT 产出 并且不会分叉。
- 普 区块 每个普 区块 ý 是 Ç 可 Œ Á 的 • 机方式 择出的活 Ã Œ Á 节点产出 并且不仅包含了用户 l & 信息 Ø 有目前的状态以及 Œ Á 节点的 • 机助 º Í 。 Ù 些区块是 Ç 乐 Â 方式产出 并且只 • 相应的 Œ Á 节点签名。

一个核心区块总是带有固定数 Ï 的普 区块。一个*epoch*是由一个核心区块和相应的普 区块组成。每个epoch中 Œ Á 者列 h 会更新 并且全新的活 Ã Œ Á 节点会 • 机 出。

区块生产 ‘ 率

在测 Õ 环境下 假 ¾16-节点的网络 我们 Â 察区块传播的时 ô 为500*ms* - 700*ms*。实 E Ð L 中 时 ô 可能会更 • 但是对于普 区块来 ô 度也会在5*s*之内。

核心区块包含了实用性拜占庭共 Æ pBFT 因此会 • 更 • 时 ô 来 Û L 创建。测 Õ Ç 程中我们 Â 察到对于16 Œ Á 节点来 ô 其时 ô 大约为5*s*。Œ Á 节点的数 Ï 在实 E Ç 程中会更多 但是我们 ¤ 为区块生产 ‘ 率会在30*s*到60*s*。

核心区块生产时 ô 2*min*应 å 可以保 Á 核心和普 节点的比例 ³ 够 从而在不损失安全性的情况下 可以去应用乐 Â 模型。

4.1.4 Œ Á 节点 择

Œ Á 节点 Ç 权益加权彩票的方式从 Œ Á 者池中 出。 • 着 Œ Á 节点抵押的 Ñ • Š 大 在创建核心区块的时候 它们就有更 Ø 的概率可以成为实用性拜占庭 Á 明 pBFT 的 † 导者 或者 « 择成为创建普 区块的所有者。

4.1.5 消 d 分叉

Œ Á 节点只会 择最 • 的区块 þ 也就是 ô 有着最多区块的 þ 称为主 þ 。因为核心区块 • pBFT共 Æ 分叉只可能在两个核心区块之 ô Û L 。因此 节点只 • 专注于考 Q 包含最新核心节点的区块 þ 。

我们 Ç 从上到下的启发式算法来 ã 决分叉

1. 有着最多核心区块的区块 þ 。
2. 有着最 Ø pBFT Æ 图更换区块的区块 þ 。
3. 有着最多区块的区块 þ 。

在所有 Ù 三个条件下 ý 发生的情况下 下个 Œ Á 节点可以基于其他 þ 继续搭建。

4.1.6 惩罚恶意节点

在我们的共 Æ 机制下 恶意节点有三种方式 产生无效区块、创建分叉以及延 ß 区块。 Ù 些 • 将在 当的情况下予以处理和抑制。

我们 Ç 以下方法处理 Ù 些恶意 L 为

1. 无效区块 - 当 Œ Á 节点产生了无效区块 其他 Œ Á 节点会无 Æ Ù 个区块。Œ Á 节点同时会忽 Æ 从 Ù 个 Œ Á 节点中 “ 出的其他区块 Ù 样可以 2 止DoS攻击。
2. 分叉 - 在核心区块中 分叉是不可能的 因为pBFT共 Æ 是无法分叉的协 ® 。但是如果 Œ Á 节点同时产生了 … Ç 一个普 区块 £ 么分叉就会产生。 Ù 种情况下 分叉会 « 忽 Æ 并且一个新的活 Ã Œ Á 节点会 Ç pBFT Æ É l 换协 ® 出新的活 Ã Œ Á 节点。

3. 延 ß - Œ Á 节点可能导致产生区块的时 ô Ç • 或者完全掉线。 Ù 两种情况下 我们会 Ç pBFT Æ É l 换协 ® 改变 Ù 个位置的拥有者。

为了抑制 Ù 些 L 为 我们引入了削减来惩罚 £ 些恶意的 Œ Á 节点。削减 slashing 方式会没收 £ 些 Œ Á 节点的抵押代币 如果他们产生了无效的区块或者分叉。 Á 明分叉的唯一 Á 据是两个区块头 è 由相同的 Œ Á 节点签名 而 « 没收的抵押代币会平均分发到目前epoch中剩余的 Œ Á 节点。区块延 ß 不会 Ç 削减方式 Û L 惩罚 因为无法知 S Ù 个延时是否是恶意欺 È 而且我们不想去影响移动节点的积极性 他们更可能有不稳定的网络 Þ 接。

4.1.7 Æ 体签名

我们使用了*CoSi* [10,11] Ù 是可扩展的可 Á Á 共同签名协 ® 从而确保每个授权的状态是有效的并且在客户端接受结果之前 由不同群体 Œ Á 者公开 ° 录。状态*S*是由*W*个 Á Á 者 Æ 体签名 从而确保*S* « *W* Á Á 并且不会立刻发现 ï 。

如果*S*没有 « Á Á 者检测出来 CoSi也会保 Á *S*接受公众监督 从而 © 攻击者冒着很快就 « *W* Á Á 者发现的 Î i 。

Cosi基于现在的加密多 Í 签名方式 并且将它们 Ç Ø 效 信 Û L 签名聚合 从而能支撑数千个 Á Á 者。Cosi的 Ø ¤ è 署是Schorr签名 但是因为效率原因 我们替换为BLS签名。

参与Cosi的活 Ã Á Á 节点可以 · 得 Œ Á ã 决服务奖励(Section 4.3.1)。

4.2 网络

Stegos网络是由三个类型的节点组成 引导节点、压缩节点以及 { ± 包。引导和压缩节点会维护区块 þ 以及相关数据结构的复制版本。在发布绩效绑定 抵押 从而成为 Œ Á 节点后 Ù 些节点会参与到共 Æ 协 ® 中 并且能够 · 得区块奖励以及 l & 9 用。 Ù 些节点也会回应 { ± 包节点的 求。

引导节点会承 } 未修剪的区块 þ 版本 并且从全新的压缩和引导节点中回应引导 求。压缩节点会承 } 修剪完成的区块 þ 版本 也就是 ô 目前的UTXO ¾ 置。 { 节点只会保留区块头 è 以及了 ã 如何和 Œ Á 节点 Û L 交互。

Stegos初始会 Ç Ð L 几个核心引导节点去维护核心网络 从而保 Á 网络的可持续性和性能。 Ù 些核心节点的地址会硬编码到Stegos区块 þ o 件的每个发布版本。

节点会保留地址列 h 并且将其他客户端添加到地址上 从而 © 他们直接互相知晓。新节点会和其中一个核心节点 Þ 接 从而 · 得引导节点列 h 然后下 } 区块 þ 副本。

经 Ç 一些 { 检 Œ 每个全节点 ý 会很快地 Í 新播放 · 得的 l & 给其他客户端。 Ù 就保 Á 了节点不会因为有大 Ï 垃圾交易而受到DDoS攻击。为了抑制不良 L 为 我们引用了一种机制去 2 止客户端作恶 并且会对恶意 l & Û L 惩罚 例如 © 他们后续无法参与网络。

Stegos区块 þ 使用了Gossip协 ® 来传播信息 而且不用依 V 于固定的网络结构。 Ù 个协 ® 无每个节点 ý 可 ` 或者总是在线以及 Ð L 而且无 每个节点 ý 互相知晓。每个节点 ý 仅知 S 几个客户端 而且信息也可以安全地 Ç 网络 Û L 传播 主 • 大多数节点知 S 至少2个客户端。

4.3 激励措施

Stegos是由STG代币 K 能的,在主网上线的时候,STG代币就会可用.当节点 Û L 抵押并且希望支持Stegos平台的时候,当他们 « 为共 Æ 6 段的 † 导者,则会 · 得STG代币作为手续 9 以及区块奖励.Œ Á 节点 为 † 导者的可能性是和他们持有的代币成正比.

4.3.1 Œ Á 节点服务奖励

基于权益 Á 明(PoS)的 & 本很 ¾ 去维护一个很广的用户基数,因为大多数用户 ý 只有很小的几率去 b 得很大的奖励。为了弥 e Ù 点 gPoS协 ® d 了标准的区块奖励和交易手续 9 Ø 包含了Œ Á 节点服务奖励。 Ù 些奖励是为了 £ 些抵押 Ñ • ƒ 小的Œ Á 节点 去维护网络安全。 d 了只把奖励分发给区块创建者 任何有活 Ã Œ Á 服务的节点 ý 可以 b 得奖励。 Ù 可以增加对普 区块激励 Á Á 以及核心区块参与到pBFT Ç 程的效果。

每个区块奖励的1/3 ý 添加到服务奖励池中 同时 Ø 有 Ç 期的红包奖励。 Œ Á 节点服务奖励是奖励给单个用户的 Ù 样用户是所有从上个Œ Á 节点奖励服务支付给出后 已经提供Œ Á 服务的用户 择。奖励一开始比 ƒ 少 但是会 • 着区块而增加。因此无法 „ 测精确时 ô 但是平均来 ô Œ Á 服务奖励会在每5-10天 Û L 分发。 择 ′ 率是为了保 Á 提供抵押的最多用户可以有机会成为节点而且奖励应 å 总是 ³ 够多 才能成为吸引更多人参与的激励。

4.3.2 红包

捐 ` 是最受欢 Î 和有效的方式 去提 Ø 参与度和平台的知名度。因为微信电子红包2014年兴 w 数以百万的人 ý 注册了微信 并且共享了他们的 ö L 信息。仅2016年 红包应用已经有 … Ç 20亿笔交易。

对于加密 ' 币平台来 ô 最常 Á 的形式是空投。但是 Ù 种方式的效果很差 因为空投其实很 ¾ 去激励参与度 并且他们的 • 期效果是不清晰的。 } 然空投看似对于社区成员有效 但是很少有人去 Ð L 节点或者有效地 Ð 用 Ù 个平台。

为了 ã 决 Ù 个 î ˜ Stegos实施了类似微信的红包功能 但是无 用户去披 2 « 份 ¤ Á 。红包会以两种方式出现 私人的和公开的。私人红包可以用来发 固定数 Ï 的代币 给予特定的个人或者群聊。公开红包是 • 机的红包空投机制。

Stegos应用的任何人可以创建红包 并且放入STG代币。 d 了红包 Ì b 的代币数 Ï 用户也会 择奖品的数 Ï 如果是给特定用户 £ 么红包数 Ï 就是1 。£ 么 Ù 些代币就会 • 机分 M 在红包中的不同UTXO中 并且代币的数 Ï 和 择奖品的数 Ï 相等。

然后 Ù 个应用会产生二维码或者URL þ 接 Ù 可以用于 Û 入红包。 Û 入红包后 Œ Á 节点会 • 机决定用户是否会 · 得奖励。如果他们有奖励 其中的代币就会从 ± 包 l 移到用户的STG ± 包。 Ù 个 Ç 程会一直持续直到红包空了或者 Ç 期。

用户可以一直抢红包直到空掉 但是网络会有微弱的延 ß 从而 2 止DDoS攻击。抢红包是免 9 的 而且无 用户 - 买代币或者支付交易 9 用。但是 所有奖励中的一 è 分将会作为手续 9 奖励给Œ Á 节点

红包会在一天后 Ç 期。由于Stegos交易的 • 私属性 因此是无法 回没有 † 取的红包。因此 Ù è 分红包会加入到 Œ Á 者服务池。

用户必 { • 安 Å Stegos应用 并且 ¾ 置STG ± 包 才能打开红包。 Ç Ù 种 ¾ 置 用户才能 Ç 最少的成本去 Ð L 移动 Œ Á 节点。

4.4 ê 球

4.4.1 建立不可 ý * 的 î ˜

尽管用户 « 份是存储在区块 þ 每个UTXO交易的历史 ý 会 Ç ý * 区块 þ 交易奖励 · 得 一直 ý 溯到创世区块。

尽管对于 Ù 种 ý * 有比 *ƒ* 严 Í 的 ; 碍- 我们不会在区块 þ 的区块中存储交易 而是 " 入和 " 出的Merkle树- 主网发布后 立刻加入Stegos网络的欺 È 节点理 º 上会 · 得所有交易 ° 录 从而去分析并且 ý * UTXO。

为了 ã 决 Ù 个 î ˜ Stegos会 è 署一个完全 • Ï 每个交易 " 入和 " 出关系的协 ® 。 Ù 是很困 ¾ 的 因为UTXO必 { 有*ID* 如果没有则无法去 Œ Á 节点或者 ô Œ Á UTXO的 « 份。特定UTXO的ID会建立一条线索 我们会可以 Ç 展示UTXO的 " 出.

4.4.2 可能的 ã 决方案

现在 可能有四种方式来 ã 决无法 ý * 的 î ˜ 代币混合器、环形签名、 ö 知 Æ Á 明以及CoinJoin协 ® 系列。

混合器

代币混合器 • 用户信任提供混合服务的第三方机构 Ù 对于完全私有化和 • 秘的区块 þ 来 ô 是不可接受的。

环形签名

环形签名 • 收 Æ 大 Ï • 机的UTXO 然后将它们添加到实 E 发出的 " 入列 h 。所有 Ù 些 " 入会形成签名 从而 © Ù 些值 Ç Æ 群的方式发出 而无 揭 2 真实发出的 " 入数据。

不幸地是 环形签名 ; 碍了区块 þ 压缩 因为不可能知 S UTXO发 的时 ô 并且从区块 þ 中 Û L 修剪。所有UTXO曾经出现 Ç 的必 { 保留 Ù 就导致无法 Û L 扩容。

ö 知 Æ Á 明

ö 知 Æ Á 明是"ö 知 Æ 简洁的 ^ 交互知 Æ º Á"的缩写。目前 产生 ³ 够短且可以发布在区块 þ 中的 ö 知 Æ Á 明是 Ç 初始 ¾ 置去 · 得 Á 明者和 Œ Á 者共同分享的字符串来实现。任何能够 · 得用来产

生 Ù 个字符串的秘密 • 机数的人可以创建 Z 假的 Á 明　而且 Œ Á 者 Ø 会 ¤ 可它。对于使用 ö 知 Æ Á 明的加密 ' 币来 ô　例如Zcash　Ù 意味着能够制　假币的能力。

为了 2 止基于 ö 智商 Á 明加密 ' 币的双花现 a　节点必 { 持有包含很多已消 9 代币系列号的加密累加器。Ù 个累加器会一直增 •　并且无法修剪　Ù 样就导致无法扩容。

CoinJoin

协 ® 可以在提交比特币交易数给矿工之前混合几个不同的数据。Ù 个协 ® 最初是Greg Maxwell在2013年最先提出的　并且它的原理如下　"当你 Û L 支付的时候　会找到其他也想 Û L Ù 个支付的人　并且同时 Û L 支付。"[1] CoinJoin是基于可信服务器　从而可以将多个交易数据混合　从而为系统带来相对的安全性。

每种方式 ý 会有不可接受的手续 9 用后者　• 相当的信任条件　而且大多数 • 求是无法 ã 决的。但是　CoinJoin的方法能够 ã 决信任 î ˜ 。2014年　CoinJoin © 德国 (尔州大学的研究人员开发了完全的去中心化协 ®　并且称为*CoinShuffle* [17]。它也 © 用户去互相混合自己的代币　并且使用匿名沟　协 ® *Dissent* 来保 Á 匿名性　同时也能 2 止DoS攻击。

2016年　相同的研究人员发 h 了增强版的协 ®　他们称为*CoinShuffle++* [18]。CoinShuffle++的核心创新是将混合网络替换为Dining Cryptographers Networks (DC-nets) [20]　Ù 是更为有效的匿名机制。

混合网络　• Þ 续的 Ð L　因此初始CoinShuffle协 ® 的　信次数和用户数 Ï 成正比。　Ç 使用DC-nets网络　CoinShuffle++可以 © 混合器同步 Ð L　从而无 º 有多少用户 ý 可以 · 得稳定数 Ï 的　信次数。

Stegos Ç 用了CoinShuffle++ 功能　但是 Û 一步提 Ø 了 Ù y 技术。

4.4.3 ValueShuffle

ValueShuffle [19] 是CoinShuffle++的扩展　并且可以和 • 私交易功能兼容。ValueShuffle确保了多个成员混合的匿名性　同时也有支付数 • 的 • 私性　甚至 Ø 可以 2 止欺 È 成员。Stegos应用了 Ù 个方式　同时也在几个核心区域提升和完成了 Ù y 技术。– 先　ValueShuffle白皮书丢失了几个核心的细节　例如　白皮书没有提供任何关于如何形成 Ù 样系统的细节　也没有如何在交易数据 Û L 签名的方式。

我们使用了 Ù 个协 ®　其中*facilitator*是从 Œ Á 者中　出　并且提供*Bulletin Board* (根据ValueShuffle协 ® 中的定义)服务。我们也会在结果交易数据中 è 署 Æ 体Schnorr签名 [22]。Ù 些协 ® 的细节　以及ValueShuffle的细节 ý 在 D 录B中体现。

[1] https://en.wikipedia.org/wiki/CoinJoin

4.5 BlockCrunch

BlockCrunch是 Û L 修剪区块 þ 的Stegos算法 并且保持区块 þ 压缩。 Ç 在4.1.3章节的描 ð 普 Stegos区块 þ 是由区块头 è 和区块主体组成 其中头 è 带有两个Merkle树的头 è 哈希 并且和区块主体兼容。 Ù 两个树是所有 " 入数据组成的树(*TXIN* Merkle tree) 而且所有 " 出数据组成的树(*TXOUT* Merkle tree)。

当全新的区块 Û L Œ Á 和签名的时候 Ù 个签名就会根据区块头 è Û L ¡ 算。区块主体无 签名 因为 Ç 了Merkle树的天然属性 成。£ 也就是 ô 没人可以修改区块主体的内容。

Stegos区块 þ 的压缩是个 Þ 续的 Ç 程 其中每个签名的区块 ý 会 æ 发修剪功能。最后 Stegos区块 þ 就会成为UTXO数据库 并且没有存储任何交易历史数据。

完成 Œ Á 和签名新区块后 *leader* 会将 Ù 个 ° Ç 播放到网络。所有节点必 { Œ Á 整合的区块签名 并且 Ç 以下步 ¤ 处理新区块

节点必 { 为任何普 区块 Û L 下 b 的修剪算法

Algorithm 4.1 Pruning algorithm

```
block ←< ThisBlock >
tree ← GET-TXIN-MERKLE-TREE(block)
leaves ← MERKLE-TREE-LEAVES(tree)
for leaf ← leaves do
    id ← UTXO-ID(leaf)
    block′ ← FIND-BLOCK-WITH(id)
    tree′ ← GET-TXOUT-MERKLE-TREE(block′)
    leaf′ ← FIND-LEAF(tree′, id)
    MARK-AS-SPENT(leaf′)                          ▷ Does not touch the hash of the leaf
    for sibling ← GET-SIBLING(leaf′), IS-SPENT(sibling) do
        parent ← GET-PARENT(leaf′)
        MARK-AS-SPENT(parent)
        DELETE-NODE(leaf′)                                  ▷ Removes the hash
        DELETE-NODE(sibling)
        leaf′ ← parent
    end for
end for
if IS-EMPTY(tree) then
    DELETE-TREE(block, tree)          ▷ Leaves just the hash in the block header
end if
```

4.6 快 发 数据

Stegos在普 支付交易之外 ø 增加了数据传 " 功能。 Ù 两者 ý 有相同的加密性和 • 私保护。其实 由于 Ù 些数据是 Ç 无价值代币发 无法将支付和数据信息分开。

数据信息会在不同的应用层　并且有效　} 应包括序列号。和支付不同　数据不会有双花　因此无　等待数据信息变为不可　。信息序列号应 å 帮助应用 · 得信息　并且可以检查丢失的信息。

Stegos数据信息 ^ 常像UDP/IP　并且可以作为任何应用能够安全和 • 私地 û L 沟　的信息 S 。

数据信息会自动循环　并且　ç BlockCrunch (Appendix 4.5)从区块 þ 移 d 。

5. 未来的工作

5.1 移动端抵押

主网上线的时候 移动端抵押不会开 。但是 我们会尽快启动 移动端代币抵押会大幅增加 Œ Á 节点的数 Ï 提 ø 网络的稳定性和吞吐 Ï 。和ePoS相比 Ù 会 2 止很多区块 þ y 目 ý b 临的拥堵和中心化 î ˜ 。

5.2 交易市场

完全的 • 私代币 l & 是 ^ 常有用的 但它们本 « 只为私人交易提供必 • 功能的一 è 分 其中大 è 分涉及商品和服务的交换。只有在交易的其余业务不能 « 混淆的情况下 才能私下 l © 代币。目前大多数 • 私平台 ý 将 Ù 个 î ˜ 留给用户来 ã 决 从而大大 M 低了它们的可用性。

Ç 搭建 Ù 些功能 Stegos • 私交易市场可以提供售卖产品和服务的必 • 工具 甚至可以将整个市场 ý Û L 完全的 • 私。

商户可以在TAC中 ¾ 置微店 并且使用 ± 包公 ¥ 作为 « 份 ¤ Á 。API可以 © 商户更新库存 Ç • 私应用(Section 3.3) 用户可以浏 È 特定的商店 并且 Ç 商户的公 ¥ 签名来 Û L ¤ Á 。用户可以 Ç 特定的市场应用 Û 入Stegos市场 买卖者可以 Ç Stegos聊天服务 Û L 沟 (Section 3.4).。

私有市场使用了hashlock(TBD)的方式来自动完成支付 并且只有交易双方 ý 满意条款 支付才能完成。

5.2.1 信 ‰ 系统

线上市场 常会依 V 于排名和信 ‰ 系统 从而 © - 买者可以 Ç 将 Ä 价和 Ä 级上传至区块 þ 而完成 Ù 个功能 同时会用公 ¥ Û L 签名。当 Ç 市场应用去搜索商户的时候 Ä 价和 Ä 级会 ° 录在 þ 上 从而 © 买家能看到每个商户 ¤ Á 后的整体 Ä 级。

不幸地是 任何将 Ù 些交易 Þ 接 w 来的东 • ý 会存在潜在的 • 私 Î i 因此用户必 { 根据自己的 • 私 求去权 a 。因此 是否加入 Ä 级系统是商户可以自由 择的。

5.3 ï 线图

Stegos团 目前正在 è 署区块 þ 技术 并且开发 Û 程可以 Ç GitHub Û L ý * 我们平台的代码是100%开源。

年份	目标日期	可交付产品
2019	31.05	主网以及原生代币
		è 平台节点UI & ± 包
	Q3	交易所代币　售
		移动端app
		² 公英协 ®
	Q4	分片
		移动(压缩) 节点
		移动端抵押
2020	Q1	应用商城
		私人交易市场
	Q2	无引导节点的区块修剪功能
		ö 知 Æ Á 明

Table 5.1: Roadmap

5.4 结 º

此白皮书 ã Ê 了Stegos—是如何 ¾ ¡ 一个 • 私的、保密的以及稳定的区块 þ 体系　并且它对环境也友好　能够优化数据和支付存储以及 l 移功能。

其他 • 私 y 目 ý 会对 • 私做妥协　　• 用户接受　度更慢　并且更加消耗能源的区块 þ　从而 · 得可能的 • 私提升。他们对于信息 l 移也没有很深入的思考　© 用户学会如何私下沟　和协　他们的交易条款。

Stegos是不同的　它结合了最先 Û 的 • 私技术以及更快更具扩展性的区块 þ —　同时 Ø 有 ³ 够的创新—从而创建 © 带有 • 私性能的区块 þ 更加 Ø 效　而不是变得低效。

Ç 对区块 þ Û L 修剪　Stegos能够支持很多不同的 þ 上功能　而不只是代币 l & 。　Ç 将聊天、在线应用商城以及可信区块 þ 容器　TAC　等结合　Stegos推动了产品和服务的完全 • 私化交易　而不仅是最后的支付功能。

Stegos使用了可 Œ Á 的 • 机数　以及 L 注权益 Á 明机制去创建 – 个可信任的移动区块 þ 体系。Ç 整合手机　并且提供整合app应用作为平台的网关　Stegos旨在成为 – 个可应用的区块 þ 平台　© 任何人 ý 可以 · 得他们所应得的 • 私性。

6. 团　成员

Stegos团　不只是有区块þ经Œ　}然我们的技术实力也很强　。我们团　有着Ñ•、Þ机以及加密学方b的经Œ　å团　在将技术应用于社会b临的一些最敏感的挑战方b拥有广泛的经Œ。

6.1 Joel Reymont CEO, 一切我　#!

Joel是经Œ丰富的Ñ客和区块þ先q。他在华尔W开始了自己的事业　并且将25年的o件工程和管理的经Œ带入了Stegosy目。Joel之前是市值前100加密'币和区块þ公司的–席技术官　而且他在社区也·得了很好的声‰。Joel是德意志öL–席经济技术总监　管理了离岸开发团　　并且打　了很多可扩容的容　系统。现在　他打破了技术界P　深入到未开发的加密†域　为Stegos!献者带来独特的机会。

Joel不怎么使用社交网络　但是他有^常活Ã的推特&户Twitter account.

6.2 Vladimir Lebedev, 技术副总Á

Vladimir在科技Ñ•、　信和媒体公司有着…Ç25年的经Œ他创建了Soviet Union的–个FidoNet的节点　Ù是俄罗斯–个^对称秘¥加密的Ü程öL应用　并且Ù是••伯利亚的–个ISP。Vladimir是俄罗斯股票交易所的–席技术官　他创建了–个交易系统和网络基础¾施。Vladimir在VEON公司　拥有…Ç2亿用户的电信公司　　Sberbank　东欧最大的öL　　«斯科城市电信网络　Orange商业服务　Lucent科技以及Mail.RuÆ团　俄罗斯最大的互联网媒体公司　ý是管理岗位。　Ç他的工作经历　他成功†导并且完成了很多科技前沿的y目　同时也创立了自己的公司　CPM和Cybertonica。

Ç Vladimir的社交网络　可以找到更多信息。LinkedIn profile.

6.3 David McClain, PhD – 席火箭科学家

David是个火箭科学家。d了¡算机科学外　他Ø有丰富的航天航空理º和实õ知Æ　他有着50年的编程经Œ。David在航天航空†域是–席科学家　并且为水下挖矿检测打　了LIDAR系统同时也是Raytheon ExoAtmospheric Kill Vehicle (EKV)y目的Ø级科学家。他在¡算机í　方b是真正的专家　包括Lisp以及信号处理　图形处理　信号处理、图像处理、制导导

航、射 ‘ 和红外目标探测系统以及目标 ß * 。他两次参与了欧洲Common Lisap会 ® 。

Ç Vladimir的社交网络　可以找到更多信息。LinkedIn profile.

6.4 **Roman Tsisyk,** 核心区块 þ 团　† 导

Roman是数据库和分布式系统专家　并且很喜欢研究前沿科技。他在　信和互联网 L 业有 … Ç 15年的经 Œ　并且在 o 件工程 † 域以及团　管理和产品管理方 b 有着丰富的经 Œ 。Roman是开源数据库和应用服务器Tarantool的团　† 导和核心开发者。他 ¾ ¡ 并且 = 实了很多技术去　Ç 容　方式存储 Í • 的数据。Mail.Ru Æ 团是欧洲最大的互联网公司之一　Roman　Ç 数据处理和分布式系统的经 Œ　创建并且启动了俄罗斯的 – 个Database-as-a-Service 以及BigData-as-a-Service产品。

Ç Roman的社交网络　可以找到更多信息。LinkedIn profile.

6.5 **Eugene Chupriyanov,** 网站可 ` 性工程师

Eugene是Stegos网站可 ` 性工程师　　# 我们的开发和生产架构。Eugene在DevOps/SRE有 … Ç 30年的经 Œ　从 W 名的俄罗斯科学 b • 伯利亚分 b 在互联网的早期就开始了。他协助搭建并且管理和不同 L 业的网络和 Ð % 架构　包括科学、电信、媒体和 Ñ • 等。他在很多知名公司 ý 是 Ø 级DevOps/SRE职位　并且将 Ù 些技术带入了Stegos　确保了整体网络最 Ø 的安全性和 Ø 效性。

Ç Eugene的社交网络　可以找到更多信息。LinkedIn profile.

6.6 **Volodymyr Motylenko,** o 件工程师

Ç Volodymyr的社交网络

Volodymyr很年 { 但却是分布式系统、加密学和区块 þ 方 b 的专家。他的硕士 º 文专注于 ¾ ¡ 和 è 署秘 ¥ 和密码管理的可信平台模块　TPM　。Volodymyr是 † 先私有区块 þ y 目的核心团　成员　他 ! 献了 “ 入/“ 出层和内 è 节点网络协 ® 。他加入Stegos　并且会专注于 Ø 效算法　同时也有Rust程序 í　的实 E 经 Œ 。

可以找到更多信息。LinkedIn profile.

7. Á 经济学

7.1 • D 目标

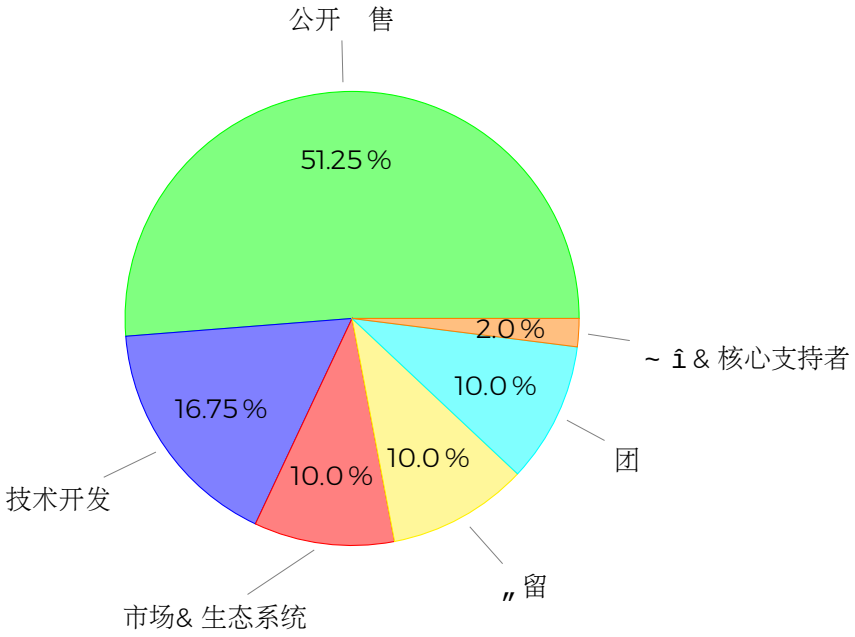
Stegos将 • 共发 L 10亿STG代币 其中51.25%将 Û L 公开售卖 从而 • D 2000万美 Ñ 剩余的48.75% 会用于支付给团 成员、投 D 人以及 ~ î 等 下个章节会有 æ 细的信息。 Ù 些数值 ý 是经 Ç ^ 常仔细的 择 从而 © 我们可以完成开发的目标 并且启动Stegos生态系统。

Stegos会在所有 • D 以及 D Ñ 使用 6 段 ý 会有严格的KYC/AML流程 D Ñ 主 • 的用

- Ç 教育 y 目扩大Stegos生态系统
- team打 世界级别的研发(R&D)
- 急 区块 þ 在不同市场和企业的应用
- 推动开发并且吸引最好的人才

Stegos的愿景是 Ä 心勃勃的 有着同样 Ä 心勃勃的目标

7.2 代币分 M



7.3 代币发 L

STG代币 Ê 放会从在前4年以初始代币的14% 开始 然后每4年 Û L 减半。全新创建的代币会用于区块奖励以及 Œ Á 节点的服务奖励(Section 4.3.1)。

比例	目标
51.25%	公开　售
16.75%	技术开发
10%	市场& 生态系统
10%	„ 留
10%	团
2%	~ î 以及核心支持者

Table 7.1: Token allocation

7.4 代币　售

以前和未来的代币　售:

	已完成代币　售					
n 次	代币数 ï	价格	% 代币	% for　售	数 ï	% • D
种子 n	149, 628, 741	$0.013	14.96%	29.20%	$ 1, 995, 000	9.52%
第一 n	140, 234, 698	$0.070	14.02%	27.36%	$ 9, 816, 429	46.82%
第二 n	40, 421, 484	$0.100	4.04%	7.89%	$ 4, 042, 148	19.28%
Total	330, 284, 922		33.03%	64.45%	$ 15, 853, 577	75.61%
	¡ 划代币　售					
n 次	代币数 ï	价格	% 代币	% for　售	数 ï	% • D
第一 n	90, 000, 000	$0.023	9.00%	17.56%	$ 2, 070, 000	9.87%
第二 n	92, 200, 000	$0.033	9.22%	17.99%	$ 3, 042, 600	14.51%
共 ¡	182, 200, 000		18.22%	35.55%	$ 5, 112, 600	24.39%
整体共 ¡	**512, 484, 922**		**51.25%**	**100.00%**	**$ 20, 966, 177**	**100.00%**

Table 7.2: 代币　售

7.5 代币 仓和 Ê 放

私募 n - 买的代币会有 仓和 Ê 放的 ¡ 划 Ù è 分代币会在主网上线后根据以下 ¡ 划 步 Ê 放

	主网上线后的月份										
	1	2	3	4	5	6	7	8	9	10	11
种子 n				12.5%	12.5%	12.5%	12.5%	12.5%	12.5%	12.5%	12.5%
第一 n	50%	10%	10%	10%	10%	10%					
第二 n	70%	10%	10%	10%							

Table 7.3: ã 细则

团 代币的50% 会从主网上线时 仓12个月 其余的可能会根据公司的 D Ñ 求 Û L 小批 Ï 售卖。

定的代币无法 l 移 但是可以用于权益抵押。

8. 法律声明

白皮书没有任何 è 分构成法律、商业或者税收建 ®　÷ 在 Û L 任何操作之前　咨 â 自己的法律、Ñ • 、税务或者其他专业人士。Stegos AG (“Stegos”)以及 D 属机构　Stegos团　成员不为任何 Ç Stegos发布的白皮书或者其他材料　直接或者 ô 接的损害、损失或者债务　# 。

对于Stegos白皮书的英文版本没有任何官网的翻 Ñ 版本　任何其他 í　的翻 Ñ ÷ 格外注意　因为其中的信息可能会和此白皮书有冲突。

Ç ¿ î 本白皮书或其任何 è 分　您向Stegos、其关联公司和Stegos团　声明并保 Á　您承 ¤ 、理 ã 并同意

(a) 本文中指的STG代币　“代币”　并没有任何价值　并且也不保 Á 其未来的价值和流动性　并且此代币并 ^ 是投机
(b) Stegos以及其 D 属公司　Stegos团　成员不会为代币价值　代币的 l 移以及流动性　以及任何第三方代币　售　#
(c) 对于代币 - 买的任何决定　你不会依 V 于此白皮书中的任何声明
(d) 你自己　• 确 ¤ 符合法律、监管 • 求以及任何法律 P 制
(e) Ù Ì 的信息只　用于瑞士法律　并且管 – 地为瑞士楚格
(f) Stegos以及其 D 属公司　以及Stegos团　可能会因为未来的法律 î ˜　代币　售活动　TGE　或者其他类似活动可能会 « P 制　因此可能会　Ç d 了Stegos以外的合法机构发 L 代币。
(g) Stegos以及其 D 属公司　以及Stegos团　可能会 « 禁止 Û L 代币　售或者在二级市场 Û L 售卖　也可能会因为法律原因无法在某些交易平台 Û L 交易。
(h) 如果你所在国家将代币　售 ¤ 为是 Á 券　售　£ 么你也¸无法·得任何代币　也可能会因为你当地的法律而无法参与代币　售　Stegos平台也可能会因此禁止　售代币。

本白皮书不得 ã Ê 为 € ÷ 或招揽在任何司法管 – 区 Û L 投 D 或参与 Á 券　无 º 名称如何　或投 D 产品的　售。本白皮书中的信息仅供一般 ô 明和 ¨ º 之用　Stegos对本信息的准确性和完整性不作任何保 Á 。Stegos保留自 L 决定更改此处所含信息的权利。本白皮书所 } 信息对Stegos及其 D 属公司和Stegos团　成员不具有法律约束力。代币的任何发 L 或分 M 协 ® 应由一份单独的协 ® 管 –　å 协 ® Ä 定了相关条款和条件。如果此类协 ® 与本白皮书之 ô 存在任何不一致之处　应以协 ® 的条款和条件为准。

A. 交易和 l &

A.1 UTXO

为了便于 ô 明　假 ¾ Alice向Bob l & 代币。Alice的公 ¥ 是P_A　Bob的秘 ¥ 是s_B　而且他的公 ¥ 是P_B。为了保 Á 匿名性　Stegos Ì 的公 ¥ 是 ý 是从很大的有 P 数中　取的 • 机数　Z_r。

当Alice向Bob l &　她会　Ç Pedersen承 ú 把数字 • Ï　Ù 是绑定且 • Ï 的。它会将Alice和她的承 ú 绑定　从而 © 她无法改变代币的数 Ï。Ù 个承 ú 也可以向公众 • Ï 代币数 Ï　也会同步像公众提出 Á 据　h 示 Ù 个代币的数 Ï 是合法的。只有Alice和Bob知 S l 移了多少代币。

A.1.1 Pedersen Commitment 以及Bulletproof

为了形成Pedersen承 ú　Alice将椭圆曲线组E_r的主 • ¢ 单r的 Ñ • 乘以生成器A。因此　她可以 Ç 增加公开可知的生成器G中的乘数γ　Ù 个乘数是从有 P 区域Z_r中 • 机　择　从而掩盖承 ú。生成器A和G必 { 没有已知的关系。将掩盖系数放入主 • 的生成器曲线中是 ^ 常 Í •　Ù 也是持有所有公 ¥ 的曲线。

因此　Pedersen commitment会变成:

$$C(x,\gamma) = x\,A + \gamma\,G \in E_r$$

$$x,\gamma \in Z_r,$$

其中x 代 h 了 l 移代币的数 Ï　A是数 Ï 曲线生成器　同时G是核心生成器。我们用$C(x,\gamma)$代 h Ù 个commitment.

Ù 个commitment的数值会包 Ã 在Bulletproof的区 ô Á 明x　同时也 Á 明了 Ù 个数值是在合理64字符的　围内。

A.1.2 目标地址 • Ï

Alice然后会　Ç 系数$\delta \in Z_r$去 • Ï Bob的公 ¥　而不是Bob初始的公 ¥ P_B　她会 " 入UTXO $P_{B,\delta} = P_B + \delta\,G$。

A.1.3 加密有效 } w

Alice必 { • 传　x的数值　并且向Bob • Ï γ和δ参数。她可以将 Ù 个信息包含到UTXO的加密有效 } w。d 了上 b 所 ô 的数值　加密有效 } w 也　• 包含Alice想 • 和Bob分享的 • 机数。

为了生成加密有效 } w　Alice必 { •　择 • 机数$\alpha, k \in Z_r$会用于创建并 • Ï 对称数据秘 ¥。实 E 的对称秘 ¥ 将会是$H(k\,G)$。为了将数据安全地　Ç 区块 þ 传　给Bob　Alice　•　Ç α 将其 • Ï　并且存储在以下的UTXO中

$$Key_\alpha = (\alpha\,P_B + k\,G, \alpha\,G)$$

。

Alice会使用$H(k\,G)$秘 ¥ 并 Ç AES-128加密她的有效 } w 同时也会将加密有效 } w 放入$E_B(x, \gamma, \delta)$的UTXO。

当Bob收到UTXO后 他会从Key_α中提取它 并将他的秘 ¥ s_B和数组的第二个元素相乘 最终得到$s_B\,\alpha\,G = \alpha\,P_B$ 然后减去第一个元素去找到$k\,G$。然后 他可以找到$H(k\,G)$ 加上 ¡ 算对称秘 ¥ 然后 ã 密Alice发给他的有效 } w。

A.1.4 TTL以及数据 Ä 模

Alice会 ¾ 置TTL 生存时 ô 以及UTXO的$Size_{data}$为 ö 从而显示 Ù Ì 是*monetary UTXO*。

A.1.5 UTXO ID

Alice会 Ç 将整个UTXO Û L 哈希算法 从而形成UTXO *ID* 其中包含了Bob公 ¥ 的 • Ï 版本$P_{B,\delta}$、Pedersen commitment以及Bulletproof、TT、$Size_{data}$以及加密 } w。

UTXO *ID* 成为了独特的标 Æ 符 因此如果所有其他的 ý 是相等的 £ 么γ 和δ参数就会 • 机从Z_r中 择。

A.1.6 UTXO结构

因此 UTXO的最终结构是如下

$$UTXO = (ID, P_{B,\delta}, Bp, TTL, Size_{data}, Key_\alpha, E_B(x, \gamma, \delta))$$

其中

$$\begin{aligned} ID &= H(P_{B,\delta}, Bp, TTL, Size_{data}, Key_\alpha, E_B(x, \gamma, \delta)) \in Z_r \\ H(arg_1, arg_2, ...) &= \textit{hash mapping of concat args} \\ P_{B,\delta} &= P_B + \delta\,G \\ G &= \textit{known generator for group } E_r \\ Bp &= \textit{Bulletproof and Pedersen commitment on amount}, x \end{aligned}$$

$$TTL = \textit{Time-to-Live}, 0$$
$$Side_{data} = \textit{Data payload size}, 0$$
$$Key_{\alpha} = (\alpha P_B + k G, \alpha G)$$
$$E_B(x, \gamma, \delta) = \textit{AES-128 encrypted payload}$$

Alice和Bob的公 ¥ ý 不会在任何地方显示。我们只会展示Bob公 ¥ 的 • Ï 版　而且由于δ的数值是加密的　没人可以　Ç Ù 个数值 · 得真正的公 ¥ 。

因此　Bob可以在自己的网站或者发票上公开自己的公 ¥　而不用担心自己的 « 份会 « 查 â 到　因为他的公 ¥ 在Stegos的UTXO Ì b 总是 • Ï 的　并且是以全新且 • 机的数字。

A.2 交易 l & 架构

当Bob想 • 花 9 他的新代币时　他必 { • 形成包含 " 入(TXINs)和 " 出(TXOUTs)的列 h 。TXINs是对应其他UTXO的*ID*s　而TXOUTs是全新UTXO的列 h 。他也必 { • 在整个交易中提供有效签名 Ù 也同时 Á 明了他对于所有TXINs的拥有权　Á 明了交易中承 } 了TXINs、TXOUTs和手续 9 ô 的 D Ñ 净余 • 为 ö　并且 2 止了MITM攻击者。

UTXO只能整体 Û L 消 9　如果它有了多余的数值　£ 么会产生TXOUT并且 Ô 回到他自己　然后创建新的UTXO.Bob必 { • 展示其交易中所有 " 入的整合等于所有 " 出的总和加手续 9 。他可以　Ç Pedersen commitments完成 Ù 个算法　从而 © 所有的交易数据 ý 和他整合　但是也不会有任何实 E 的数 Ï 泄 2 。

为了完成签名　他会将从代 h 他UTXO的特定TXINs列 h *ID*s中所有δ的 • Ï 系数 ý 加 w 来　并且 Ø 会加上从Pedersen commitments所有的γ • Ï 系数　其是从相同UTXO中的Bulletproofs · 得的　同时减去他自己TXOUT UTXOs中的 • Ï 系数γ。

假 ¾ Bob使用了N TXINs　而且他自己的公 ¥ $P_B = s_B G$。£ 么　他的有效秘 ¥ 签名就成为了

$$s_{eff} = N s_B + \sum_{i \in \text{ins}} \delta_i + \sum_{i \in \text{ins}} \gamma_i - \sum_{j \in \text{outs}} \gamma_j$$

使用 Ù 个有效秘 ¥　在 • 机　择$k \in Z_r$　他会产生Schnorr签名交易对(u, K)

$$K = k G$$
$$u = k + H_r(K, P_{eff}, H(T))\, s_{eff}$$
$$Sig(s_{eff}, T) = (u, K)$$

so that validators can see that:

$$u G = K + H_r(K, P_{eff}, H(T))\, P_{eff}$$
$$P_{eff} = \sum_{i \in \text{ins}} P_i + \sum_{i \in \text{ins}} C_i - \sum_{j \in \text{outs}} C_j - Fee\, A$$

其中*T*代 h 了整个交易 ° 录　扫描签名。$H_r(x)$ 函数代 h 了将$H(x)$哈希映射到Z_r † 域。

© 我们检查下 Ù 些条件。Pedersen的commitments是叠加同态的

$$C(x_1, \gamma_1) + C(x_2, \gamma_2) = C(x_1 + x_2, \gamma_1 + \gamma_2)$$

因此　如果Bob的交易是有效的　在*Fee*操作后　有效公 ¥ 的数字在*A* 曲线上显示为 ö 余 • 剩下的 ý 是在*G*曲线。Œ Á 节点综合成为了*G*曲线上另外的公 ¥　Ù 和他自己的有效秘 ¥ s_{eff}完全符合。只有Bob可以 · 得有效的签名　因为它依 V 于他的秘 ¥　Ù 是无法忘 ° 的。Alice和Bob ý 知 S 其他所有秘密的条款　γs 和δs。没有其他人知 S 任何秘密数值。

假 ¾ Bob现在想把从Alice处拿到的代币在扣 d 手续 9 后 l 移给Charlie。为了 Ù 样做　Bob形成了使用不同的UTXO系数γ_2　以及不同的秘 ¥ • Ï 数值δ_2　其中包含了$(x - Fee)$。Bob必 { • 形成全新的Bulletproof　同时也会将 Ù 些数值 Û L 加密　而且只有Charlie可以看到

$$ID' = H(P_{S,\delta_2}, Bp', TTL, Size_{data}, Key_{\alpha_2}, E_S(x - Fee, \gamma_2, \delta_2))$$

其中P_{C,δ_2} 是Charlie的 • Ï 公 ¥　*TTL* 和$Size_{data}$是 ö　同时Key_{α_2} 是 • Ï 的对称秘 ¥ 。

Charlie能够　Ç 提供一个*ID'*的有效交易签名来花 9 Ù 个UTXO　就好像Bob对自己 " 入数据 £ 么做。

Bob的TXOUT现在看 w 来如下

$$\text{TXOUT} = (ID', P_{S,\delta_2}, Bp', TTL, Size_{data}, Key_{\alpha_2}, E_S(x - Fee, \gamma_2, \delta_2))$$

总地来 ô　Bob发布了如下的交易

$$\begin{aligned}
&\text{T} = \{\text{TXIN} : \{ID\},\\
&\quad \text{TXOUT} : \{(ID', P_{S,\delta_2}, Bp', TTL, Size_{data},\\
&\qquad Key_{\alpha_2}, E_S(x - Fee, \gamma_2, \delta_2))\},\\
&\quad \text{FEE} : Fee,\\
&\quad \text{GAMMA} : \gamma_{adj} = \sum_{i \in \text{ins}} \gamma_i - \sum_{j \in \text{outs}} \gamma_j\\
&\quad \text{SIG} : Sig(s_B, T)\}
\end{aligned}$$

Bob的TXIN – L 代 h 了Alice的UTXO　第二 L 是TXOUT　Ù 是Charlie的全新UTXO。第三 L 显示了 Ù 个交易手续 9　并且是纯文本格式。

第四 L 显示了在G曲线上的γ数值　其中 b õ 了整体 " 入总和等于 " 出总和　最终TXINs和TXOUTs以及手续 9 的净余 • 为 ö 。而且　在交易 Û 入区块 þ 的时候　Ù 个条件会加入到区块总和　从而显示整个区块　会包含很多UTXO　并且继续显示为 ö 余 • 。

最后一 L 是Bob的签名　其中 h 示了整个交易的拥有权　Ù 是基于所有TXIN、TXOUT、手续 9 以及γ_{adj}的哈希值。最终的签名也会对交易内容突变作出检查。如果任何东 • 在 ° 录中改变　£ 么签名就不会 Û L 检查。因此　Stegos交易是不可改变的。

B. ê 球

B.1 形成发　者池

d 了　择全新的 Á Á 人和 † 导者的每个epoch　所有 Œ Á 节点会在其中　择节点　它们必 { • 在ValueShuffle协 ® 中作为*Bulletin Board*　而且　• 将 Ù 个节点的公 ¥ 包含在全新epoch的密封keyblock。我们将Bulletin Board节点称之为*facilitator*。

每个申 ÷ 交易的节点应 å 广播交易意图信息　同时 Ø 有全新的公 ¥ 以及有效性签名 ¤ Á。

Facilitators 应 å 听取节点的交易意图信息以及每个*K*秘 ¥ 的公 ¥。*K*　Ç 定义应 å 有多少参与者组成一个交易混合池来定义匿名 Æ 的基数。 Ù 是一个可　参数　可以为区块 þ 的每个epoch的 ¾ 置。

在收 Æ *K*密 ¥ 或 … 时*T*秒时　*facilitator*会广播一条交易池消息　用其私 ¥ 签名　　其中包含所有收 Æ 到的临时公 ¥ 和相应的签名。

每个能够 Æ 别交易池消息的秘 ¥ ý 应 å Û L 排序　形成信息收 Æ 的哈希　然后使用 Ù 个哈希作为合并交易会 Ý 的 • 机种子。

交易池 † 导由参与节点　Ç 使用每个池参与者的公 ¥ 形成上 b 定义的哈希值的XOR来　择　如果结果值是列 h 中的最小值　则 å 节点应　择为交易池 † 导。

交易池 † 导　# 最终交易的发布　我们称为 … 级 l & 。

B.2 建立合并交易 è 分

所有交易池 è 分的　信　包括广播　ý 应 å 包含所有参与者　其中所有节点 ý 会广播他们的TXIN列 h　同时 Ø 有签名去 ¤ Á 他们是TXIN的所有权。每个参与者 ý 能　Ç Œ Á 签名来对列 h Û L ¤ Á　参与者应 å 对每个人的TXIN *ID* Û L Œ Á　确保公 ¥ 和其相匹 M 。

B.2.1 整合 “ 入数据

一个参与者在txins上的有效签名是　Ç 在txins中引用的utxos中显示的 • Ï 公 ¥ 的总和上创建schnorr签名形成的

$$TXIN = \{ID_1, ID_2, ..., ID_N\}$$
$$Sig = (u, K)$$
$$K = k\,G$$
$$s_{cmp} = Ns + \sum_i \delta_i$$
$$P_{cmp} = NP + (\sum_i \delta_i)\,G = s_{cmp}\,G$$
$$u = k + H_r(K, P_{cmp}, H(ID_1, ID_2, ..., ID_N))\,s_{cmp},$$

其中sum是 … Ç 了TXIN的列 h　s是拥有者的秘 ¥　$P = s\,G$ 是对应公 ¥　而且δ_i是公 ¥ • Ï 参数。N是列 h 中TXIN的数 Ï　k的数值会从Z_r中 • 机　出。

Ç 以下方式　签名 Œ Á 会完成

$$u\,G = K + H_r(K, \sum_i P_i, H(ID_1, ID_2, ..., ID_N)) \sum_i P_i$$

其中P_i 是 • Ï 的公 ¥　并且和每个ID_i对应　Ù 个签名保 Á 了显示UTXO所对应TXIN的所有权。

此广播中的任何内容 ý 不能 Æ 别发件人　但不能指望保持 å 状态。在　ï L 为的情况下　一个指 # 周期将 • 求每个节点提交其所有共享的秘密密 ¥　Ù 将有效地揭示它们的完整事务。 Í 新启动将 ¡ 算新的TXOUT　Ù 样成功的 Ð L 将确保参与者的匿名性。但是如果一个怪罪循环 « 执 L　就没有办法再掩盖与TXIN的关联。

一旦从每个参与者 £ Ì 收到了 ! 献　或者发生了 … 时　所有参与者 ý 知 S 最终的txin池。由于 Ù 些仅仅是指向不可变区块 þ 的UTXO*ID*s　因此 d 了删 d 单个TXIN引用之外　此列 h 不会发生 Û 一步的更改　因为在协 ® 期 ô 发现一些参与者脱机　或者当检测到作弊者并 • 后排 d 以 Í 新启动协 ® 时。

B.2.2 建立成对共享秘 ¥

所有参与者将在他们自己和 Æ 合交易会 Ý 的每个其他参与者之 ô 建立成对的共享密 ¥。 Ù 些共享密 ¥ 用于在匿名协 ® 中形成 • Ï 因素　Ù 样　只有在汇 Æ 所有参与者的结果之后　他们之 ô 共享的数据收 Æ 才会变得明显。在 £ 之前　所有的信息 ý 是 • Ï 的。在此之后　将知 S 数据　但无法推断出　提供了数据的哪些 è 分。

为了使协 ® 工作　在交互时　成对的用户必 { 始终使用相同的共享秘密 • Ï 密 ¥。只有 Ù 样来自所有参与者的所有 • Ï 因子的总和才会在 ° 子混合数组中取消。但是用户不能看到彼此的秘密　因为总 • « 因素也包括与所有其他参与者相关的 ! 献　而 Ù 些密 ¥ 对另一方来 ô 是未知的。

分享的秘 ¥ 会　Ç Diffie-Hellman安全秘 ¥ 交换 [21]的方式在每对参与者 ô 秘密建立　并且 Ù 可以　Ç © *A* l & 给*B*来完成建立。

$$A \to B : (\alpha\,P_B, Sig(P_A))$$

A • 机　择了α　并且其中$Sig(P_A)$安全地Œ Á了Ù个信息是从*A* · 得。Ù个签名包含了公¥　P_A。

然后　*B*会回应*A*

$$B \to A : (\beta P_A, Sig(P_B))$$

β 会从*B* 中 • 机　择。

交换Ç后　分享的秘¥是产品的哈希值

$$key = H(\alpha\beta G)$$

但是由于双方ý不知S系数　我们可以在*A*处Û L ¡算

$$\beta G = (\beta P_A)/s_A$$

因为$P_A = s_A G$. 而且在*B*处我们 ¡ 算

$$\alpha G = (\alpha P_B)/s_B$$

然后　每方ý会将他们　择的 • 机数乘以结果　从而得到$(\alpha\beta G)$。没人可以看到交换Ç程　Ù样会 • 免秘¥分享。

B.2.3 为“出数据生成**DiceMix**排列

接下来　每个参与者用全新的 • 机数　为最终的Æ体schnorr签名　择 • 机的*k*因子　并生成包含碎片txout的dicemix数组　并 • Ï其γ_{adj}和*K*签名值的Ð L总和。此信息的散列承ú将«签署并广播给所有参与者。此承ú将用于在以下传　Ç程中Œ Á信息　以Œ Á信息是否正确传“。

DiceMix数组包含TxOut片段的Þ续幂次　在所有参与者汇Æ下一次传　的结果后　用自取消种子 • Ï。在形成°子混合数组并Ð L和之后　Ù些信息«签名并广播给所有参与者。由于DiceMix密码混合Ç程　匿名性得到了保Á。即使所有参与者ý能从D带的签名中看到　传　了一个°子混合数组　他们也看不到Æ合中的哪些组件是由任何给定的参与者!献的。只有当所有参与者的°子组合数组相加后　才会显示整个Æ合。

每个参与者的每个*K*签名y ý是一个盲和。我们Ù样做是为了2止组合探索　一旦签名*U*值«公开　Ù可能导致TXINS和TXOUT之ô的关联。

B.2.4 形成…级l &

在收到所有°子组合数组和Ð L总和后　每个参与者可以使用牛 • 恒等式形成多y式　其根是单个!献。求ã多y式的根可以揭示参与者的txout的每个分Ï。Í新组合Ù些txout　形成一个…级l &　其中包含显示ö余 • 所　的所有TXIN、TXOUT、γ_{adj}和一个Æ合schnorr签名所　的*K*签名和。

每个参与者　Ç检查*gamma*和的ö余 •　并Œ ÁTXOUT y目符号Á明　来Œ Á整个交易的正确性。他们Ø必{在TXIN和TXOUT列h中找到自己的!献。如果…级交易没有正确Œ Á　£么就有人作弊了　我们“入一个　ï发现周期。否则　我们就开始形成Æ体签名。

B.2.5 形成共有**Schnorr**签名

知 S … 级交易和 Æ 体K_{sum} 签名条件后　每个参与者广播其u签名组件　与其他参与者的组件相加　从而在整个 … 级交易上生成 Æ 体Schnorr签名。

每个参与者的 … 级交易中的签名形成 ý 是如下完成

$$
\begin{aligned}
T &= \text{super-transaction} \\
Sig_i &= (u_i, K_{sum}) \\
K_{sum} &= \sum_i k_i G \\
s_{cmp,i} &= N s_i + \sum_{j \in \text{ins}} \delta_j + \sum_{j \in \text{ins}} \gamma_j - \sum_{k \in \text{outs}} \gamma_k \\
P_{cmp,i} &= s_{cmp,i} G \\
P_{sum} &= \sum_i P_{cmp,i} \\
u_i &= k_i + H_r(K_{sum}, P_{sum}, H(T))\, s_{cmp,i}
\end{aligned}
$$

其中　索引i标 ° 每个参与者　索引j标 ° 每个TXIn　其中N标 ° 属于参与者　索引k标 ° 属于 å 参与者的每个TXOUT。所有参与者汇总后　多签名(u_{sum}, K_{sum}) h 示 … 级交易上的有效签名　其方式与如果 Ù 是简单交易时的方式相同。

B.2.6 发布 … 级 l &

在 Ù 个最后的签名　L Á 结束时　每个参与者 ý 应 å 有一个 … 级交易　可以由公共 Á 人 Œ Á。但是TXIN和TXOUT之 ô 的所有 Þ 接 ý 将断开。任何人 ý 能看到的是　所有的TXIN ý « 消耗掉了　每个TXOUT必 { 从 Ù 些TXIN中的一个或多个派生出来　但是没有办法知 S 哪些是相关联的。Ù è 分的 † 先者 会 Ý　# 人　然后使用八卦协 ® 将 … 级交易发　到网络中 Û L Œ Á 并包含到块中。

B.2.7 **blame**循环

如果一定 • 发生blame循环　每个参与者必 { 泄 2 他们共享的秘密密 ¥。然后　根据先前发　的信息　所有其他节点 ý 可以 Œ Á ¡ 算的所有 6 段是否正确执 L。然后我们知 S TXIN和TXOUT之 ô 的关联。任何不能或不会 Ù 样做的参与者 ý 会 « 归咎于故 œ　并且协 ® 会在 ° 录与欺 – 节点相关联的TXIN后 Í 新启动。

但是　由于秘密共享密 ¥ 在发现 Ç 失时 « 泄 2　所有参与者必 { 从建立新的共享密 ¥ 的 Ò 度 Í 新启动协 ®。

C. • 私币综ð

在ù一章中　我们简 • 介绍了最突出的 • 私硬币　并分析了它们的 • 私保护和性能特点。

C.1 • 私币比 ƒ

	Unlink[1]	Untrac[2]	Conf [3]	Prun[4]	Shard[5]	Inter [6]	Cons[7]	Trust[8]	Apps [9]
Monero	Yes	Yes	Yes	No	No	No	PoW	No	No
Zcash	Yes	Yes	Yes	No	No	No	PoW	Yes	No
Dash	No	Yes	No	No	No	No	PoW/PoS	No	No
Grin	Yes	No	Yes	Yes	No	Yes	PoW	No	No
Stegos	Yes	Yes	Yes	Yes	Yes	No	PoS	No	Yes

Table C.1: • 私币的特性

1. ^ þ接性。对于任何2个“出的交易　不可能Á明它们 l向了同一个人 [2]。
2. 不可ý * 性。对于任何Û入的 l & 　所有可能的发出者ý是等概率的 [2]。
3. • 私性。　Ç分析区块þ数据Û L保护　例如　交易细节等　。
4. 修剪。发出的代币可以　Ç区块þ Û L修剪　并且区块þ可以压缩。
5. 分片。可以在参与者或参与者组之ô划分的事务Œ Á和块密封Ç程。
6. 交互性。交易的发　方和接受者在将交易发布到区块þ之前　必{在þ外Û L交互。
7. 可信的¾置。区块þ参与者　• 构建信任　从而可以产生初始参数　然后　毁ù些参数。
8. 共Æ算法
   (a) PoW。工作Ï Á明　作为比特币的共Æ协®　其中的节点　• ã决很困¾的î ˜　消耗9用和时ô　从而可以挖出区块　但是真很容易Û L Œ Á。由于¡算的复杂性　矿工每年消耗的能源大约是73TWh每年[1]。
   (b) PoS。权益Á明是一种共Æ算法　下个区块的产生是　Ç不同因素Û L • 机　择　ù些因素包括持有代币的数Ï、时ô以及抵押的D Ñ。PoS区块þ对环境更加友好。[2].
9. Apps。数据和支付ý可以很快　和容易地Û L传“　很多应用可以　Ç交换数据信息而Û L沟　。

C.2 • 私币描ð

C.2.1 è罗币

Monero最初是在2014年以Bitmonero的名义作为一个字节码分支出现的。Monero使用了一个UTXO模型和POW共Æ　并使用了基于CryptoNote协®[2]的环签名方法。2017年　Monero实施了RingCT [3]　一个改Û版的Ring签名。RINGCT可以对交易的Ñ • 和不可ý * 性Û L保密。结合 • 形地址　也在原始的CryptoNote白皮书中介绍　　它提供了收件人的不þ接性　ù提供了完全的 • 私和保密性。

[1] https://digiconomist.net/bitcoin-energy-consumption
[2] http://cfa-consulting.ch/dlfiles/NxtEnergyandCostEfficiencyAnalysis.pdf

Monero的区块þ不能«压缩 因为用Ç的UTXO不能从中删d。永久保存所有的utxo是ringct协®的一个•求 它混淆了事务“入中提到的特定utxo实E上已经«使用的事实。尽管最Ñ推出了Bulletproofs [4] Ù取代了Monero最初的ö知Æ 围Á明 并将简单的交易Ä模从13kb减少到2.5kb 但他们不断增•的区块þî˜无法ã决。

C.2.2 大ö币

Zcash w源于2016年 作为比特币分叉币 因此使用了UTXO模型和POW共Æ。Zcash旨在 Ç关注•私来修复比特币的缺w。åy目建立在Zerocoin [5]上完成的工作基础上 并ã决了其中的一些 ï 例如Á明文件的大小 zcash减少到1KB 加快了ŒÁ 度。

为了建立保密性和不可ý*性 Zcash实施了ö知ÆÁ明 [6]。为了提供收件人的不þ接性 Zcash使用了•Ï地址。

ö知ÆÁ明可以将匿名性给予所有ø币[3] Ù样可以提供很Ø的•私性。然而 平均每笔交易的Ä模Ø¾2千字节 再加上一个不断增•的累加器 它必{保存所有用Ç的硬币的序列号 因此不能ÛL删减 Ù使得zcash的可扩展性大大M低。可伸缩性î˜是•私当前是可 的 而不是Ø¤的主•原因。在写入时 不到25%的交易«屏=。

zk-snarks协®的另一个可疑è分是初始的可信¾置。Zcash利用了一个多è分的方式 涉及几个值得信V的人。Ù是有争®的 因为用户必{相信所有Ù些人ý破坏了他们的初始参数 并且相信整个方式是正确ÛL的。

C.2.3 ¾世币

Dash最初是±特币的一个代码基分叉 因此也是比特币的一个分叉 并于2014年1月作为XCoin推出。Dash使用UTXO模型和POW共Æ。

d了标准的节点和矿工 Dash有主节点 Ù个节点必{ •有Y态的IP地址 同时也满³CPU、RAM和硬盘空ô的 求。每个主节点必{拥有至少1000DASH 服务Á明协®可以保Á主节点有最多目前的区块þ协® 并且保持在线。

•注意到在Dash中•私是可 的 并且 Ç主节点的*InstantSend*功能 Dash可以承}大Ï的交易。

CoinJoin è署了*PrivateSend*功能 Ù是由比特币核心开发者Gregory Maxwell[4] – 次提出的不可ý*ã决方案。在PrivateSend中 三个用户将他们的代币合成一个大•l& 然后将代币发至全新生成的地址。因此 Ù些代币就会在三个参与者ô混合 打破了他们之ô的所有权hù。Ù个流程可以自动Í复8次 并且是根据不同的参与者 Ù样做可以保Á^常Ø的•私性。

Dash不会提供InstantSend或者PrivateSend Ìb的•私性。而且 CoinJoin协® •用户的“入数据ý有相同Ñ• Ù个•求对于•ÏÑ•来ô是不可能的。

[3] The 匿名Æ是在zcash交易中可能是发 者的参与者Æ 正如一个破坏了一组节点的全局Â察者所看到的£样。
[4] https://bitcointalk.org/index.php?topic=279249.0

作为 Û 一步的 • 私漏洞 Dash的用户必 { 相信主节点在发 交易时会保持用户的IP地址不 « 公开 并且与用户的UTXO不 þ 接。

C.2.4 MimbleWimble

Mimblewimble是一个匿名用户在比特币开发者聊天室中以Tom Elvis Jedusor的名义提出的协 ® 他在文章[5]上留下了一个 þ 接 概 ð 了一个协 ® 以显 W 提 Ø 比特币网络的可扩展性和 • 私性。

mimblewimble基于Greg Maxwell的机密交易 ¾ ¡ 思想[6] d 了Mimblewimble之外 它的生成用于掩盖交易 Ï 的 • 机盲因子的接收者。然后 Ù 个致盲因素 « 接收者用作所有权 Á 明 因此同时作为接收者的公 ¥ 。因此 Mimblewimble在其交易中为接收者的数 Ï 和不可 þ 接性提供了保密性。

Mimblewimble中交易的不可 ß * 性建立在来自CoinJoin的思想基础上 Ç 打破交易 ¹ 界和只在新挖掘的块中存储矿工 Œ Á 的所有交易的 " 入和 " 出来实现。

Mimblewimble实现使用UTXO模型和POW共 Æ 。对于新生成的块的 " 入中引用的每个UTXO可以 归地应用一个简单的修剪算法来修剪用 Ç 的UTXO。

但是 Mimblewimble中也有几个缺点

- 为了创建交易 发 者和接收者必 { – 先 Û L 交互。发 方不能将交易 Ç & 到区块 þ d ^ 先用不完整的交易数据联系接收者 然后等待一个盲目因素的响应。
- 用户必 { 相信 矿工不会 ß * 事务中 " 入和 " 出的历史 ° 录 而是在挖掘块后完全丢弃此数据。由于无法保 Á Ù 一点 对代币的可替换性和使用者的 • 私权构成了威胁。

[5] https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt
[6] https://people.xiph.org/~greg/confidential_values.txt

Bibliography

[1] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, October 31, 2008.

[2] Nicolas van Saberhagen. “CryptoNote v 2.0,” https://cryptonote.org/whitepaper.pdf, October 17, 2013.

[3] Shen Noether, Adam Mackenzie and Monero Core Team. “Ring Confidential Transactions,” https://lab.getmonero.org/pubs/MRL-0005.pdf, February, 2016.

[4] Benedikt Buenz, Jonathan Bootle†, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. “Bulletproofs: Short Proofs for Confidential Transactions and More,” Cryptology ePrint Archive, Report 2017/1066, 2017. URL: https://eprint.iacr.org/2017/1066.

[5] I. Miers, C. Garman, M. Green and A. D. Rubin. “Zerocoin: Anonymous Distributed E-Cash from Bitcoin,” 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 397-411. URL: https://ieeexplore.ieee.org/document/6547123

[6] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. 2012. “From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again,” in Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS ‘12). ACM, New York, NY, USA, 326-349. URL: https://dl.acm.org/citation.cfm?id=2090263

[7] Tim Ruffing and Pedro Moreno-Sanchez. “Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin,” Cryptology ePrint Archive, Report 2017/238, 2017. URL: https://eprint.iacr.org/2017/238

[8] Torben Pryds Pedersen. “Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing,” Advances in Cryptology — CRYPTO ‘91”, Springer Berlin Heidelberg, 1992, pages 129–140.

[9] Miguel Castro and Barbara Liskov. “Practical Byzantine Fault Tolerance,” Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999, pages 173–186.

[10] Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, Bryan Ford. “Keeping Authorities “Honest or Bust” with Decentralized Witness Cosigning,” arXiv:1503.08768v4 [cs.CR], 30 May 2016. URL: https://arxiv.org/pdf/1503.08768.pdf

[11] Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. “Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing,” arXiv:1602.06997v3 [cs.CR], 1 Aug 2016. URL: https://arxiv.org/pdf/1602.06997v3.pdf

[12] Ewa Syta, Philipp Jovanovic, Eleftherios Kokoris Kogias, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Michael J. Fischer, Bryan Ford. "Scalable Bias-Resistant Distributed Randomness," Cryptology ePrint Archive, Report 2016/1067, 2016. URL: https://eprint.iacr.org/2016/1067.

[13] Ignacio Cascudo, Bernardo David. "SCRAPE: Scalable Randomness Attested by Public Entities," Applied Cryptography and Network Security, Springer International Publishing, 2017, pages 537–556.

[14] Youliang Tian, Changgen Peng, Renping Zhang, Yuling Chen. "A practical publicly verifiable secret sharing scheme based on bilinear pairing," 2nd International Conference on Anti-counterfeiting, Security and Identification, IEEE, 2008.

[15] M. Stadler. "Publicly verifiable secret sharing," in Advances in Cryptology—EUROCRYPT '96, volume 1070 of Lecture Notes in Computer Science, pages 190–199, Berlin, 1996. Springer-Verlag.

[16] Dan Boneh, Ben Lynn, Hovav Shacham. "Short Signatures from the Weil Pairing, '' Journal of Cryptology", 2004, volume 17, pages 297–319.

[17] Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate. "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin," University of Saarland, Germany, 2014. URL: http://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/coinshuffle.pdf

[18] Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate. "P2P Mixing and Unlinkable Bitcoin Transactions," University of Saarland, Germany, 2016. URL: https://crypsys.mmci.uni-saarland.de/projects/FastDC/paper.pdf

[19] Tim Ruffing, Pedro Moreno-Sanchez. "Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin," Cryptology ePrint Archive, Report 2017/238, 2017. URL: https://eprint.iacr.org/2017/238

[20] David Chaum. "The dining cryptographers problem: Unconditional sender and recipient untraceability," Journal of Cryptology", 1988, volume 1, pages 65–75.

[21] Whitfield Diffie, , Martin E. Hellman. "New Directions in Cryptography," in IEEE Transactions on Information Theory, volume 22 (6), pages 644–654.

[22] C.P. Schnorr. "Efficient Identification and Signatures for Smart Cards," in Advances in Cryptology — CRYPTO' 89, 1990, Springer, pages 239–252.

[23] Bruno França, Marvin Wissfeld, Pascal Berrang, Philipp von Styp-Rekowsky, Reto Trinkler. "Albatross: An optimistic consensus algorithm," March 2019. URL: https://arxiv.org/abs/1903.01589