验证器概述

简介

Fax 基于 Tendermint，它依赖于一组负责在区块链中提交新块的验证器。这些验证者通过广播投票参与共识协议，其中包含由每个验证者的私钥签名的加密签名。
验证人候选人可以绑定他们自己的 fax，并让代币持有者将 fax“委托”或质押给他们。Fax 网络将有 23 个验证者。验证人由收集最多质押 fax 的人的排名决定——质押最多的前 23 名验证人候选人将成为 Fax 验证人。
验证者将通过执行 Tendermint 共识协议获得 fax 作为区块规定和代币作为交易费用，并且委托人应该以自己的方式从目标验证者那里获得奖励。最初，交易费用将以 faxs 支付，但在未来，如果 Fax 生态系统中的任何代币被治理列入白名单，它将作为费用投标有效。请注意，验证者可以为其委托人收取的费用设置佣金，作为额外的激励。

硬件

当前不存在用于验证者密钥管理的合适的云解决方案。当云 SGX 变得更广泛可用时，这种情况可能会改变。出于这个原因，验证者必须设置一个受限制访问的物理操作。例如，一个很好的起点是在安全的数据中心共存。
验证者应该期望为他们的数据中心配备冗余电源、连接和存储备份。建议使用多个用于光纤、防火墙和交换的冗余网络盒，以及带有冗余硬盘驱动器和故障转移的小型服务器。
我们预计最初的网络要求会很低。当前的测试网需要最少的资源。随着网络的增长，带宽、CPU 和内存需求将会增加。建议使用大硬盘来存储完整的区块链历史。

建立一个网站¶

建立一个专门的验证者网站，并在我们的聊天中表明您打算成为验证者。这一点很重要，因为委托人将希望访问有关他们将 fax 委托给的实体的基本信息。

验证者指南（CLI）

Staking 是支持 PoS（Proof of Stake）共识机制的重要基础模块。它根据验证者接受的委托权益证明的总量确定每个选举周期内的区块生产者集合的数量，并根据投票权动态确定区块顺序。同时，它也为分发和治理模块的委托关系和验证者信息查询提供了必要的支持。
通过质押，您可以自由地创建验证人、更新验证人、将权益证明委托给受信任的验证人、取消您不再信任的验证人的委托以及将权益证明重新委托给其他验证人。

旋转机制

Fax 会在每个固定的块高度间隔从每个集合中重新选举块生成节点，称为周期。出块集合是固定的，在同一周期内，集合中出块节点的身份保持不变。在同一周期的倒数第二个区块高度间隔，Staking 将轮换下一个周期的区块生成节点集。fax 数最高的前 23 个节点将成为下一个周期的出块节点，而不是集合中 fax 数最高的前 23 个节点将被强制退出。fax 的个数只能是整数，轮换时比较集合支

持的节点数时不考虑小数部分。Fax 会在每个固定的区块高度间隔重新选举区块生成节点，称为循环。每 276 个区块（一个周期）更换一次出块人，在一个周期的第 275 个区块选出下一个出块人。此更改在下一个循环的第一个块中生效。fax 数最高的前 23 个节点将成为下一个周期的出块节点，不在集合中 fax 数最高的前 23 个节点内的节点将被强制退出。fax 的个数只能是整数，每次轮换比较集合支持的节点数时不考虑小数部分。fax 数最高的前 23 个节点将成为下一个周期的出块节点，不在集合中 fax 数最高的前 23 个节点内的节点将被强制退出。fax 的个数只能是整数，每次轮换比较集合支持的节点数时不考虑小数部分。fax 数最高的前 23 个节点将成为下一个周期的出块节点，不在集合中 fax 数最高的前 23 个节点内的节点将被强制退出。fax 的个数只能是整数，每次轮换比较集合支持的节点数时不考虑小数部分。

命令

Staking cli 命令包含以下 5 个用于 PoS 操作的命令。

- create-validator：创建验证器
- edit-validator：更新一个验证器
- deposit：存入代币
- add shares：添加以存入代币计算的股份
- withdraw：提现存入的代币

创建验证器

将节点升级为验证器并在验证器上设置描述。

exchaincli tx staking create-validator --pubkey=$(exchaind tendermint show-validator) --moniker="my nickname" --identity="logo|||http://mywebsite/pic/logo.jpg" --website="http://mywebsite" --details="my slogan" --from jack

- **Pubkey** 代表当前节点的 tendermint 公钥
- **Moniker** 表示验证者的别名
- **Identity** 指定验证者头像的地址
- **Website** 表示验证者的网站地址
- **Details** 表示验证者的详细描述
- **from** 指定操作者的账号，这里是 jack

更新验证器

运营商可以更新验证者的描述并调整佣金率。

exchaincli tx staking edit-validator --moniker="my new nickname" --identity="logo|||http://mynewwebsite/pic/newlogo.jpg" --website="http://mynewwebsite" --details="my new slogan" --from jack

- **moniker** 表示要更新的验证器的别名
- **identity** 指定要更新的验证者头像的地址
- **website** 表示要更新的验证者的网址

- **details** 表示要更新的验证器的详细描述
- **from** 指定运营商的账号，这里是 jack

存款

用户首先需要存入一定数量的 fax 才能使 Staking 账户成为委托人。

exchaincli tx staking deposit <amountToDeposit> --from <delegatorKeyName> --gas auto --gas-adjustment 1.5 --gas-prices <gasPrice>

添加股份

Fax 委托人可以通过以下命令向自己或其他验证人添加股份：

exchaincli tx staking add-shares fvaloper1qj5c07sm6jetjz8f509qtrxgh4psxkv3m2wy6x,fvaloper1hcngft7gfkhn8z8fnlajzh7agyt0az0vv9pllr,fvaloper1c5g4v00np7fjjnexkhh5yk0hc6mamf40u5vjrh,fvaloper1fh9tpkqka29n0mj307cu5cvp5ts0p4dl8uug6e --from <delegatorKeyName>

- 在上面的例子中，fvaloper1qj5c07sm6jetjz8f509qtrxgh4psxkv3m2wy6x,fvaloper1hcngft7gfkhn8z8fnlajzh7agyt0az0vv9pllr,fvaloper1c5g4v00np7fjjnexkhh5yk0hc6mamf40u5vjrh,fvaloper1fh9tpkqka29n0mj307cu5cvp5ts0p4dl8uug6e 是验证人的地址，所有存入的 fax 都将转换为股票并添加到上述验证人上。
- from 标志指定谁签署交易。

提现

当 Fax 用户提取存入的代币时，添加到验证者的份额将被移除。此代币提取过程需要 21 天。

- 允许提取的代币数量必须大于或等于 0.0001 ~ n（用户存入的代币总数）。
- 如果用户在某些验证人上添加了 Staking 权限，执行该命令后，Staking 权限的数量会自动更新。本质上，这个动作可以被认为是一种 re-vote 行为。
- 如果用户已经添加了股份，在执行撤消所有代币的命令后，可以认为是一种 unbond 行为。
- 如果用户没有添加股份，则执行该命令后新的代币不会转化为股份。
- 允许用户多次提取存入的代币。每次提取代币时，代币将被锁定 21 天，然后再发送回用户的账户。如果用户在 21 天内（最后一次提币后）再次提币，最后一次提币将被锁定 21 天，并与第二批提币一起退回用户账户。
- 从所有验证者中提取一定数量的 fax 和相应的份额。

exchaincli tx staking withdraw 10fax --from rose

- 在示例中，10 是要提取的存入 fax 的数量。
- 这里，“from”表示要提现的用户账户，在本例中为“rose”。

奖励

验证者将因表现良好而获得奖励。所有者可以使用以下命令提取奖励：
exchaincli tx distr withdraw-rewards <validator-addr> --from <validatorKeyName> --gas auto --gas-adjustment 1.5 --gas-prices <gasPrice>

验证者常见问题解答

此内容尚未在其最终版本下呈现。机制和价值观容易发生变化。

一般概念

什么是验证器？

Fax 基于 Tendermint，它依赖于一组负责在区块链中提交新块的验证器。这些验证者通过广播投票参与共识协议，其中包含由每个验证者的私钥签名的加密签名。验证者在区块链中提交新块并获得收入以换取他们的工作。他们还必须通过对提案进行投票来参与治理。验证者根据他们的总权益进行加权。

什么是“质押”？

Fax 区块链利用公共权益证明 (PoS) 机制。每个验证者的权重由质押 (fax) 和作为抵押品的代币数量决定。这些 fax 可以由验证者直接自行委托，也可以由其他 fax 持有者委托给他们。
create-validator 系统中的任何用户都可以通过发送交易来声明他们成为验证者的意图。从那里，他们可以成为验证人候选人。
验证者的权重（即投票权）决定了他们是否是活跃的验证者。最初，只有投票权最大的前 23 名验证人将成为活跃验证人。

什么是全节点？

全节点是一个完全验证区块链交易和区块的程序。它与只处理块头和一小部分交易的轻节点不同。运行全节点比轻节点需要更多资源，但对于成为验证者来说是必要的。在实践中，运行全节点仅意味着运行具有低网络延迟和无停机时间的软件的最新版本。
当然，即使用户不打算成为验证者，也可以并鼓励他们运行全节点。

成为验证

如何成为验证者？

网络中的任何参与者都可以通过发送交易来表明他们愿意成为验证者 create-validator，他们必须填写以下参数：

- **验证者 PubKey**：与此 Tendermint 关联的私钥 PubKey 用于签署预投票和预提交。
- **Validator's Address**：应用层地址。这是用于公开识别您的验证者的地址。与该地址关联的私钥用于委托、解绑、领取奖励和参与治理。
- **验证者的名字（绰号）**
- **验证者的网站（可选）**
- **验证者的描述（可选）**

创建验证者后，fax 持有者可以将 fax 委托给他们，从而有效地将权益添加到他们的池中。一个地址的总权益是委托人绑定的 fax 和指定自己的实体自绑定的 fax 的组合。
在所有发出信号的验证人候选人中，质押最高的 23 人被指定为验证人。如果验证者的总权益低于前 23 名，则该验证者将失去验证者特权：因此他们无法再参与共识并产生奖励。

有哪些不同类型的键？

简而言之，有两种类型的键：

- **Tendermint 密钥**：这是用于签署共识投票的唯一密钥。
  - 它与公钥相关联 fvalconspub（使用 获取此值）exchaind tendermint show-validator
  - 它是在使用 exchaind init 创建节点时生成的。
- **应用程序密钥**：此密钥由交易创建 exchaincli 并用于签署交易。应用程序密钥与前缀为 的公钥 fpub 和前缀为 f 的地址相关联。两者都是从 exchaincli keys add 生成的帐户密钥派生而来

注意：验证器的操作员密钥直接与应用程序密钥相关联，但仅出于此目的使用保留前缀：fvaloper 和 fvaloperpub.

验证者可以处于哪些不同的状态？

在使用事务创建验证器后 create-validator，它们可以处于三种状态：

- **Bonded**：验证者处于活跃状态并参与共识。验证者正在获得奖励，并且可能会在行为不端的情况下被削减。
- **jailed**：验证者行为不端并被监禁，即被暂停。如果监禁是由于离线时间过长造成的，验证者可以发送 `unjail` 交易以重新获得他的验证者全部权利。如果监禁是由于双重签名造成的，则验证者不能自己解除监禁。
- **unbonded**：验证者不活跃，因此无法签署区块。验证人不能被削减，也不会获得任何奖励。仍然可以将 fax 委托给该验证者。`unbonded` 立即取消对验证者的委托。

是否必须委派最少数量的 faxs 才能成为活跃（绑定）验证者？

最小值是 30000 fax

委托人将如何选择他们的验证人？

委托人可以根据自己的主观标准自由选择验证人。我们认为重要的一些标准是：

- **委托 fax 数量**：委托给验证者的 fax 总数。高投票权表明社区信任这个验证者，但这也意味着这个验证者可能是黑客更大的目标。更大的验证者也会减少网络的去中心化。
- **跟踪记录**：委托人可能会查看他们计划委托给的验证者的跟踪记录。这包括资历、过去对提案的投票、历史平均正常运行时间以及节点可能被入侵的频率。

除了这些标准之外，验证者还可以添加一个网站地址来完成和增强他们的简历。验证者需要以一种或另一种方式建立声誉以吸引委托人。例如，验证者最好让第三方审核他们的设置。但请注意，Fax 团队不会自行批准或进行任何审计。有关尽职调查的更多信息，请参阅此博客文章。

职责

验证者是否需要公开身份？

不，他们没有。每个委托人将根据自己的标准评估验证人。验证者在提名自己时将能够注册一个网站地址，以便他们可以在他们认为合适的时候宣传他们的操作。一些委托人可能更喜欢一个清楚地显示运营验证器的团队及其简历的网站，而其他人可能更喜欢具有积极记录的匿名验证器。

验证者的职责是什么？

验证者有两个主要职责：

- **能够持续运行正确版本的软件：**验证者需要确保他们的服务器始终在线并且他们的私钥不被泄露。
- **积极参与治理：**验证者需要对每个提案进行投票。

此外，验证者应该是社区的活跃成员。他们应该始终与生态系统的当前状态保持同步，以便他们可以轻松适应任何变化。

“参与治理”意味着什么？

Fax 上的验证人和委托人可以对更改操作参数（例如区块气体限制）、协调升级或对任何给定事项做出决定的提案进行投票。

验证者在治理系统中扮演着特殊的角色。例如，他们需要对每一个特别重要的提案进行投票，因为不投票的委托人将继承其验证人的投票。

质押意味着什么？

可以将质押 fax 视为验证活动的保证金。当验证人或委托人想要取回他们的部分或全部存款时，他们会发送一笔 unbonding 交易。然后，fax 将经历 **3 周**的解绑期，在此期间，它们可能会因验证者在解绑过程开始之前犯下的潜在不当行为而受到惩罚。

验证者和协会委托人获得区块奖励、费用，并有权参与治理。

验证者能否带着委托人的 fax 逃跑？

通过委托给验证者，用户委托投票权。验证者拥有的投票权越多，他们在共识和治理过程中的权重就越大。这并不意味着验证者拥有委托人的 fax 的保管权。**验证者绝不可能带着委托人的资金逃跑。**

即使委托的资金不能被他们的验证人窃取，如果他们的验证人行为不端，委托人仍然要承担责任。

多久会选择一个验证者来提议下一个区块？它会随着绑定 fax 的数量而增加吗？

被选中提议下一个区块的验证者称为**提议者**。每个提议者都是确定性地选择的，被选择的频率与验证者的投票权（即绑定的 fax 数量）成正比。例如，如果所有验证者的总抵押权益为 100 个 fax，而验证者的总权益为 10 个 fax，则该验证者将提议约 10% 的块。。

技术要求

硬件要求是什么？

验证者应该期望为一个或多个数据中心位置提供冗余电源、网络、防火墙、HSM 和服务器。

我们预计最初　　将需要适度水平的硬件规格，并且随着网络使用的增加，它们可能会增加。参与测试网是了解更多信息的最佳方式。

什么是软件要求？

除了运行 Fax 节点外，验证者还应开发监控、警报和管理解决方案。

什么是带宽要求？

与以太坊或比特币相比，Fax 网络具有非常高的吞吐量。

我们建议数据中心节点只连接到云中受信任的完整节点或其他社交上相互认识的验证者。这减轻了数据中心节点减轻拒绝服务攻击的负担。

最终，随着网络的使用越来越频繁，每天数 GB 的带宽是非常现实的。

运行验证器在物流方面意味着什么？

成功的验证器操作将需要多个高技能人员的努力和持续的操作关注。例如，这将比运行比特币矿工涉及更多。

如何处理密钥管理？

验证者应该期望运行支持 ed25519 密钥的 HSM。以下是潜在的选择：

- YubiHSM 2
- Ledger Nano S
- Ledger BOLOS SGX enclave
- Thales nShield support

Fax 团队不推荐一种解决方案高于另一种解决方案。鼓励社区加强改进 HSM 和密钥管理安全性的努力。

验证者在操作方面可以期待什么？

运行有效的操作是避免意外解除绑定或被削减的关键。这包括能够响应攻击、中断以及维护数据中心的安全性和隔离性。

维护要求是什么？

验证者应该期望执行定期软件更新以适应升级和错误修复。网络在其引导阶段的早期不可避免地会出现问题，需要高度警惕。

验证者如何保护自己免受拒绝服务攻击？

当攻击者将大量 Internet 流量发送到 IP 地址以阻止 IP 地址处的服务器连接到 Internet 时，就会发生拒绝服务攻击。

攻击者扫描网络，试图了解各种验证节点的 IP 地址，并通过大量流量使它们与通信断开连接。

减轻这些风险的一种推荐方法是让验证者在所谓的哨兵节点架构中仔细构建其网络拓扑。

验证器节点应该只连接到他们信任的完整节点，因为它们自己操作它们或由他们在社交上认识的其他验证器运行。验证器节点通常会在数据中心运行。大多数数据中心提供与主要云提供商网络的直接链接。验证者可以使用这些链接连接到云中的哨兵节点。这将拒绝服务的负担从验证者的节点直接转移到其哨兵节点，并且可能需要启动或激活新的哨兵节点以减轻对现有节点的攻击。

Sentry 节点可以快速启动或更改其 IP 地址。由于到哨兵节点的链接位于私有 IP 空间中，因此基于 Internet 的攻击无法直接干扰它们。这将确保验证者区块提案和投票始终能够传递到网络的其余部分。

预计验证者那部分的良好操作程序将完全减轻这些威胁。

有关哨兵节点架构的更多信息，请参阅此。