ScaleBit

Babylon区块链介绍

Jason

大纲

- POW & POS
- Babylon概述
- Babylon技术方案解析

PoS链的问题

- PoS 区块链的安全性则由持有权益的验证人来保障。验证人将质押权益作为“押金”，当验证人违反协议时，验证人的权益“押金”可被罚减（slash）。
- 保障区块链安全的质押权益的总市值越大，攻击该链的成本越高，这条链的经济安全性就越强。
- 对于小型区块链或初创PoS链，吸引资本不太容易，且为了吸引资本质押，往往采用高通胀的质押收益，不利于长期发展。
- PoS链存在一种叫“长程攻击”的风险，导致质押者解锁缓慢。

Bitcoin链的优势

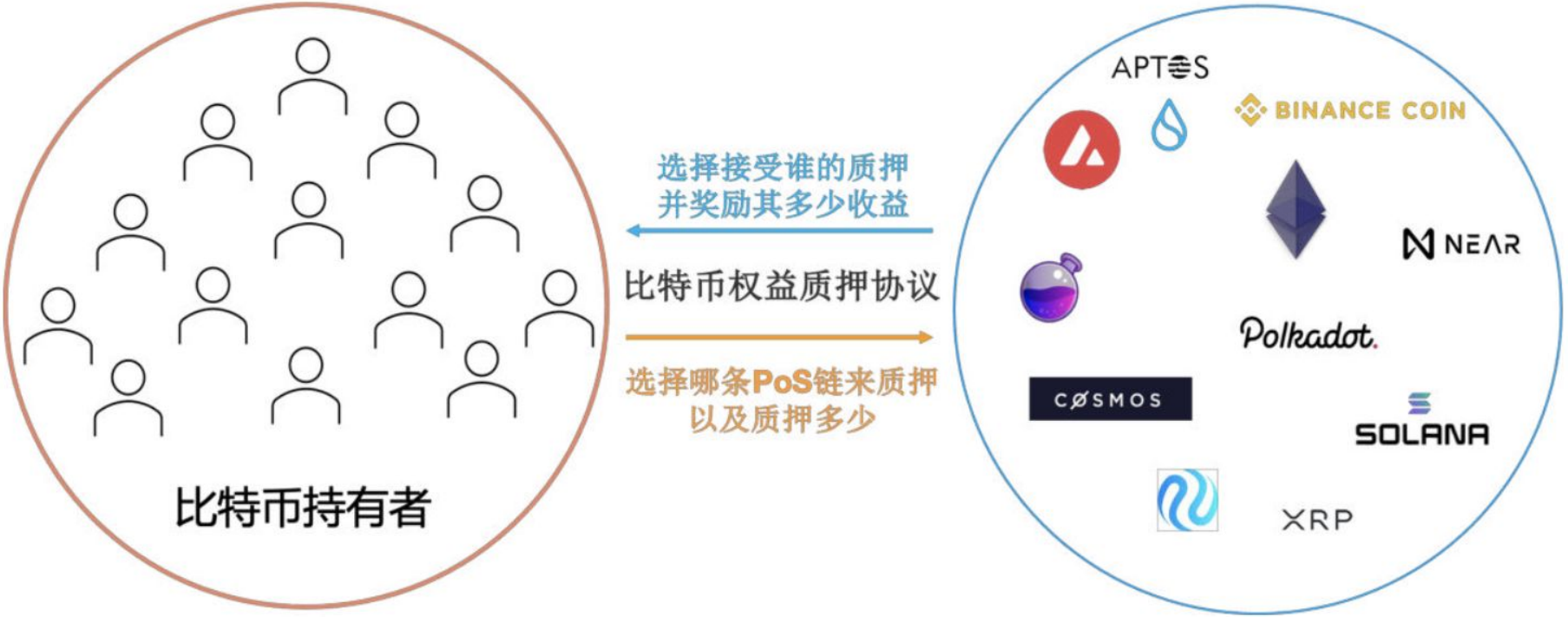
- 采用PoW共识算法，一般认为PoW会比PoS更安全。
- 比特币的认可度高、更稳定、市值高、闲置率也高，可以用来做PoS链质押，为持有者增加收益。

Babylon概述

- 一套比特币权益质押协议，该协议让比特币持有者能够在无需信任任何第三方的情况下质押比特币；
- 此质押“无需”将比特币跨链桥接到 PoS 链，就能为该 PoS 链提供“全面”可罚减（slashable）质押权益的安全保证。
- 该协议支持质押权益的快速解绑（fast stake unbonding），从而帮助比特币所有者最大程度地释放流动性。

比特币权益质押

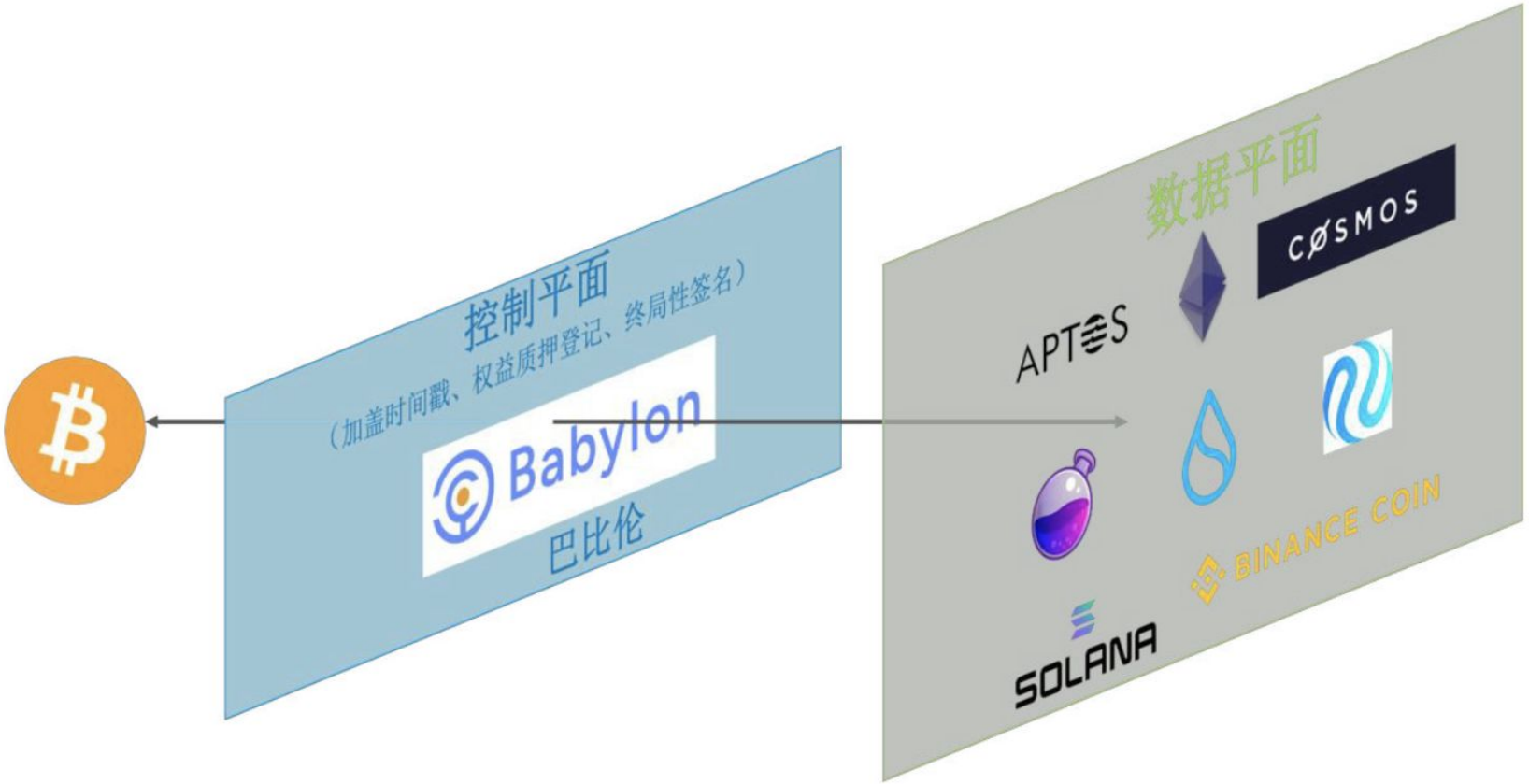
- 既然比特币性质优越，何不将其质押、发挥其能，助力保证 PoS 链的安全？



Babylon概述

- 一套比特币权益质押协议，该协议让比特币持有者能够在无需信任任何第三方的情况下质押比特币；
- 此质押“无需”将比特币跨链桥接到 PoS 链，就能为该 PoS 链提供“全面”可罚减（slashable）质押权益的安全保证。
- 该协议支持质押权益的快速解绑（fast stake unbonding），从而帮助比特币所有者最大程度地释放流动性。

Babylon系统架构



Babylon测试网现状

图 5：基于比特币的时间戳测试网与 31 条基于 IBC 的区块链

巴比伦比特币权益质押协议:安全性质

- Babylon比特币权益质押协议，该协议与现有的PoS链结合使用，具备3个重要的安全性质：
  1. **全面可罚减的 PoS 安全性**。一旦区块链完好性遭破坏（safety violatio）（如链分叉—译者注），则所质押比特币的三分之一必定会被罚减。只要所质押比特币的三分之二诚实地遵守PoS 协议，PoS 链就能保持良好的活性。
  2. **质押者的安全性**。只要诚实地遵守 PoS 协议，每一位比特币质押者都可以到期提取或提前解 绑其质押的比特币。
  3. **质押者的流动性**。所质押比特币的解绑保证安全，并且无需社区共识、快速解除绑定。

  性质 1 意味着，违反协议就会被罚减;性质 2 意味着，只有被罚减者才违反了协议。性质 1与 性质 2 结 合起 来 ， 反 映了 PoS 安 全性 的 金 科 玉 臬：全面 可罚 减 性。

两种质押方式

- 我们考虑两种基本的比特币权益质押方法，这两种方法各自有其挑战：
  1. **桥接到 PoS 链**。比特币权益质押的一种方法是首先将比特币从比特币链连接到消费者PoS 链，并在那里执行罚减规则。虽然这种方法能够为 PoS 链提供可罚减的安全性（性质 1），但从根本上却受限于桥接方案本身的安全性。即便是最完美的比特币桥也依赖于对目标链质押者的信任。因此，通过桥接解决方案，不可能实现性质 2，即无需信任任何第三方的权益质押。
  2. 从比特币链进行**远程权益质押**。即当质押者违反 PoS 链协议时，在比特币链上将该违反协议者所质押的比特币进行罚减。此方案能实现安全性质2，但因为比特币不支持智能合约而不能实现性质1。

Babylon的比特币权益质押协议**遵循远程权益质押**方法，但通过结合先进的**加密技术、共识协议创新**和**比特币脚本语言**的最优化使用，克服了比特币链缺少智能合约的挑战。

比特币质押者的行程

爱丽丝(Alice)有一枚比特币，她想将它质押在 PoS 链上。首先，她通过发送权益质押交易到比特币链来进入一个权益质押合约。该交易是一笔将她的比特币锁定到自我托管的金库的比特币交易。被锁定的比特币只能用爱丽丝的私钥通过**下述两种途径之一解锁**:

(1)**爱丽丝发起"解绑交易**(unbonding transaction)"，则比特币将在三日内解锁并返还给爱丽丝。

(2)**爱丽丝发起"罚减交易**(slashing transaction)"，将比特币发送至销毁地址。

一旦该权益质押交易进入比特币链，爱丽丝就可以开始用她的密钥签署区块以验证 PoS 链。在她的验证职责期间，有两种可能的路径。

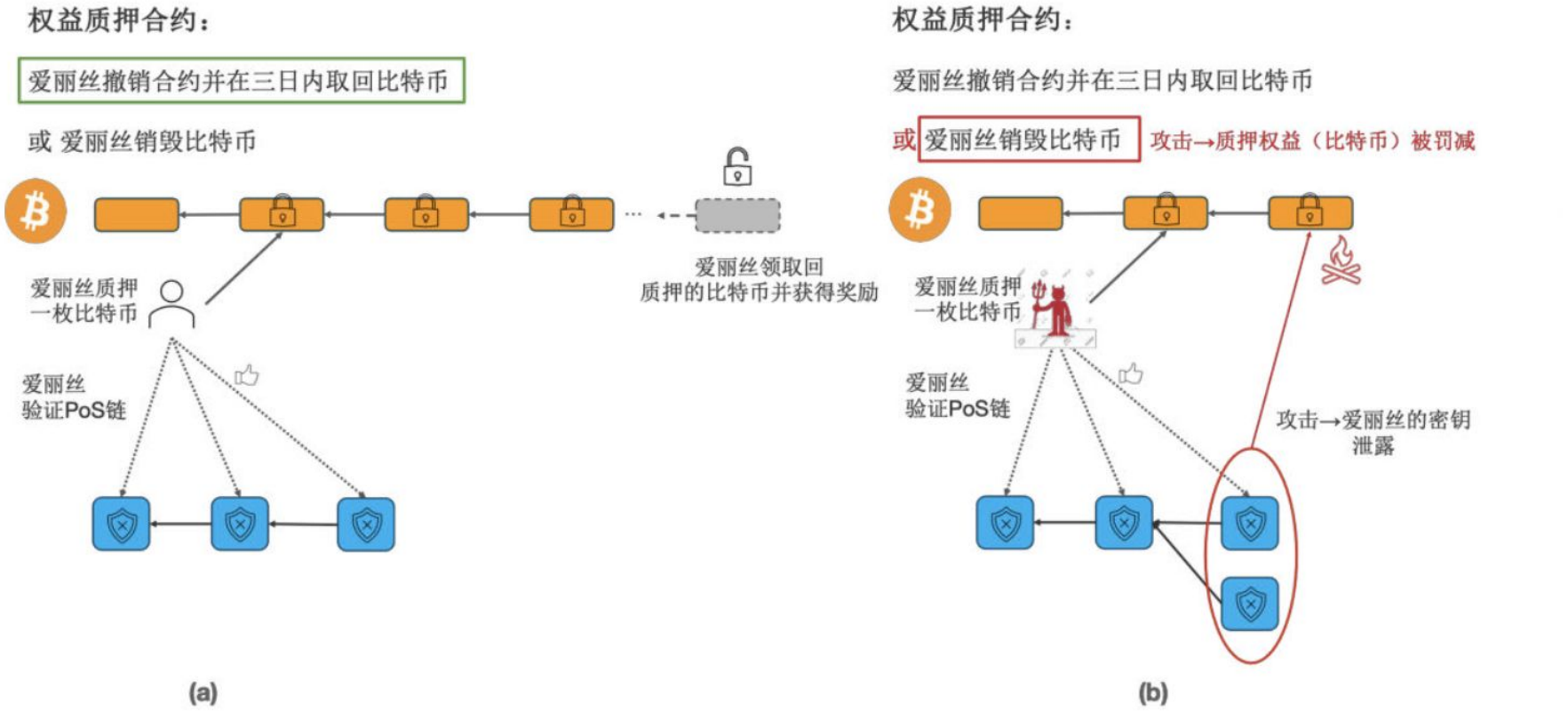


图 2：比特币质押者的行程：（a）快乐路径：爱丽丝质押比特币，验证 PoS 链，发起解绑请求，并在 3 日内解除质押；（b）不幸路径：爱丽丝质押比特币，攻击 PoS 链，然后，其比特币被销毁。

权益质押合约:通过比特币盟约模拟(Bitcoin covenant emulation)来实现

每个 UTXO 交易花费的款项均来自 UTXO集合，比特币脚本语言提供了少量操作码(opcode)，以详细规定款项的使用条件。一份权益质押合约有四种交易:

- 权益质押交易，其中，质押者输入的是其比特币地址，输出(output)的花费可使用下述二种方式之一:
  - **解绑交易。该交易允许质押者在对应锁定时间(测量解绑时间)结束后再花费该输出(对应锁定时间可由操作码 OP_CHECKSEQUENCEVERIFY[10]执行)。**
  - **罚减交易。该交易可将质押者的输出直接花费到销毁地址里(该地址的UTXO 无法被花费)**
- 解除权益质押交易。该交易可以在对应时间锁(timelock)到期后，才花费解绑交易的输出。

权益质押合约是“比特币盟约(Bitcoin Covenant) [25,26]”的一个例子，比特币盟约对如何花费交易的输出(the output of a transaction)有约束。该等盟约可通过OP_CHECKTEMPLATEWERIFY[8]执行。目前比特币暂不支持盟约，但有多种模拟方式。**Babylon的创新之一是比特币盟约模拟的新型方式，它几乎无需信任任何第三方。**

自动罚减质押的比特币—通过可问责断定（accountable assertions）与终局性小工具（finality gadget）

在比特币上罚减，就是直接发送作恶质押者的私钥，由下面两点来获得作恶者的私钥：

- 第一点是**可提取的一次性签名（extractable one-time signature）**。该签名保证了：如果签名者用同一组私钥签署两条消息，则其**私钥可以通过这两个签名提取出来并导致该私钥泄露**。EOTS 已被一些论文提议作为惩罚双关攻击（equivocation）的通用方法。
- 另外一点不改变基本共识协议本身的签名方案，而是在基础共识协议用可提取的一次性签名确定一个区块后，**加入一轮新的由 EOTS 签名的投票**。这轮额外签名可称为“**终局性小工具**”—一种 EOTS 终局性小工具。

该基于终局性小工具的解决方案，具有一个非常重要的 优势，即“模块化特性（modular nature）”：它可以在所有拜占庭容 错（BFT）共识协议上使用，且无需更改基础共识协议本身。这使得该项技术的应用**不局限于特定的 PoS 链**。

快速解绑质押的比特币—通过基于比特币的时间戳（Bitcoin timestamping）

在有着原生权益质押（native staking）的 PoS 链中，因为区块链需要社区共识来抵御远程攻击，所以质押权益的解绑耗时很长（比如，在 Cosmos 中心（Cosmos Hub）解除质押权益的绑定需要三周）。

为了避免长程攻击并实现质押通证的快速解绑，PoS 链应当与比特币链紧密同步。这可以通过一种称为“**基于比特币的时间戳**（Bitcoin timestamping）”的技术来实现，**将 PoS 区块的哈希值和参与其投票的质押者集合的信息记录在比特币上**。

参考

https://babylonchain.io/
docs.babylonchain.io/papers/btc_staking_litepaper(CN).pdf

Thanks

Contact us:

- Twitter: @scalebit_
- Email: contact@scalebit.xyz

ScaleBit

More information : www.scalebit.xyz