AOK WHITEPAPER

AOK Group

V.1.0

目录

目录

1. 简介

1.1. 初期技术

美国Bellcore研究所(Bell Communications Research, Inc., Bellcore) 所属的暗号学者Stuart Haber和Scott Stornetta在1991年9月暗号日报上发表了'如何在数码文件上盖时间戳(How to timestamp a digital document)' 的论文。 他们在论文中首次记述了在数码文件上印上时间戳来证明信赖性的时间戳概念。 他们介绍了使用密码提示算法生成各文件的固有ID，每次文件变更时ID也会变更的 "Surety" 时间戳服务。另外，Surety通过呼叫被解析的由顾客印鉴组成的"通用寄存数据库"的方式，发明了所有顾客的"不可伪造"印鉴总账 。另外，他们每周都会在美国《纽约时报》的小广告栏目上刊登新分类的"Hash值"，完成了区块链技术的第一个事例。

接着1998年工程师 Wei Dai 开发了基于初期阶段的加密交易系统——电子分散总账系统的 "B-money" 最初的电子交易分散化解决方案。B-money提出了成为所有虚拟货币根源的基本概念。不通过中央化的机构，以P2P方式让参与者之间直接进行交易;引入分散总账概念，让所有参与者共享交易记录;向成功生成新区块的使用者提供补偿等，提出了目前虚拟货币中使用的重要概念，但未能实现。 因为不是以区块链技术为基础，而是结合盲文签名等加密技术的电子货币。 因此，在 Satoshi Nakamoto 的论文中提出可以参考的基本性的重要概念具有重要意义。

> The prospect of a world in which all text, audio, picture, and video documents ar e in digital form on easily modifiable media raises the issue of how to certify wh en a document was created or last changed. The problem is to time-stamp the d ata, not the medium. We propose computationally practical procedures for digit al time-stamping of such documents so that it is infeasible for a user either to b ack-date or to forward-date his document, even with the collusion of a time- sta mping service. Our procedures maintain complete privacy of the documents the mselves, and require no record-keeping by the time-stamping service.

Excerpts of How To Time-Stamp a Digital Document

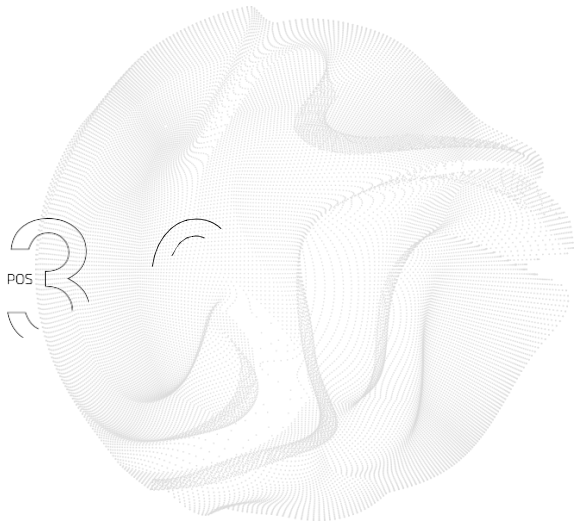
1. 简介

1.2. 试行及开发

区块链技术超越了体现“分散总账”基本概念的第一代Bitcoin，在总账中进化成了以添加合同功能的智能转换（Smart contract）功能为特征的Ethereum第二代。被称为第一代的代表性区块链——维特币是由协议制的管理结构构成的，系统升级很难。另外，由于是作业证明（PoW: Proof of Work）方式，所以与开采利益相关，还发生了被开采商的利害关系所左右，脱中央化概念受损的问题。

这是随着提供计算力量的业主们的力量增强而发生的事情。随着数据处理容量的增加，Ethereum的速度延迟成为了大问题，而传输手续费Gas Fee的增加引发了交易费用增加问题。

这种第一代和第二代主网都是以PoW方式产生块状的，从根本上来说，只能存在计算力和电力资源过度消费的问题。 因此，虽然试图从"Ethereum 2.0"转换为"PoS（Proof of Stake）"方式，但截至2020年11月，仍然未能得到解决。



1.3. 解决方案

AOK是弥补这种第一代、第二代区块链缺点的第3代主网，使用PoS 3.0方式的协议算法。

PoS 3.0拥有一种协议体制，即不参与以Wallet为线下状态的-不参与节点的-不给代币持有者提供积木补偿，提高通过节点参与的wallet中对拥有更多硬币的人获得积木补偿的概率。 这是现有的PoS方式，提高了将代币长时间停留的wallet获得补偿的概率，解决了由此产生的Coin-Age问题。

AOK通过这种方式不仅可以实现技术上的稳定性、效率性、分散化，还可以产生以AOK主网币为基轴货币的代币（Token），通过这些，个别项目构建了Eco-system，并根据个别Dapp的活跃程度，具有提高AOK主网币值价值的良性循环结构。

2. AOK MainNet

2.1. 发展概况

AOK 继承了最传统、链条安全性得到认可的 Bitcoin区块链技术，确保安全性，通过PoS 3.0 协议算法，改善 Bitcoin区块协议算法PoW方式的缺点，完善Bitcoin最大弱点慢处理速度，将目标区块时间从原来的20分钟缩短为1分钟，提高交易速度，保障快速传输速度，通过最改善的协议算法PoS3.0进行区块验证。

股权证的保密工作经多年试验已得到验证, AOK的PoS 3.0同时解决了CoinAge和区块补偿及区块链预计算问题。
PoS 3.0 协议强力推荐活性节点，使节点持续连接网络。该文件中提出了现有PoS协议算法中的保安问题及解决方案，并记述了进一步加强AOK保安的想法。

2. AOK Main-Net

2. PoS 3.0

1. 现有协议运算法则

区块链系统是参与网络的所有参与者分别拥有同样的数据，分散储存同样的数据，因此不存在原件和副本的区别，也不存在可以做出统一决策的中央。 在这种情况下，开发了可以进行合理、有效决策的多种算法。通过这种协议算法，分散总账可以实现数据的一贯性，这种协议体制包括工作证明方式（PoW; Proof of Work）和股份证明方式（PoS; Proof of Stake）、委托股权证明方式（DPoS:Delegated Proof of Stake）等。

在具有代表性的PoW比特币（Bitcoin）网络中，开采者将参与交易验证过程。 采矿者计算出Hash值后，发现区块并报告给网络，然后根据区块补偿进行开采。 这种PoW协议算法为了形成一定的区块，引入了动态难度的概念。 这是各节子的Hash power的增减，在开始区块竞争时实施，如果Hash power增加，则运算难度增加，相反，如果Hash power减少，运算难度就会降低。

即，为获得开采补偿而参与开采的计算力量少则难度降低，多则难度加大。 因此，随着密码货币的开采竞争越来越激烈，开采难度也在不断上升。 开采难度上升意味着投入的"Hash力量"的量也在增加，而始终相同的"Hash力量"意味着开采虚拟货币越来越难。 另外，如果开采难度加大，为了生成与以前相同的区块，需要更多的hashrate，为了达到和过去相同的水平，需要投入对开采装备的持续性能升级费用及庞大的电力费用等相当大的费用。 这必然带来资源浪费。

2.2.2. PoS 3.0 协议运算法则

维特币通过解决"Byzantine Generals Problem"，展示了Peer-to-Peer网络结构是防止伪造和变造的解决方案，此后很多虚拟货币都是以Bitcoin公开的开放源代码为基础制作的。AOK也继承了Bitcoin稳定的开放源代码，追加开发了必要的新一代功能。根据开放源代码规则，AOK同样是在本公司的Github频道上公开修改后的源代码的透明Public Open-Source Public区块链。

AOK引进的PoS 3.0协议算法具有避免过度的计算力量导致电力和装备费用浪费的优点。 AOK为了基本协议方式，以最新的Bitcoin代码为基础，引进PoS 3.0逻辑，实施合理、经济性的区块生成。一般的PoS协议逻辑由于CoinAge攻击及各种类型的攻击，具有多样的安全话题，所以AOK将改善的PoS 3.0作为协议逻辑。

2. AOK MainNet

PoS的创意最初在PeerCoin中体现，并再次从BlackCoin发展到PoS 2.0的概念，之后QTUM等一些虚拟货币平台发展为PoS 3.0算法。PoS的股权证据本质上可以转换为代币持有者之间的代币持有量的竞争，基于网络连接性和随机偶然性，概率上可以得到代币的补偿。得到补偿的几率取决于要持有多久的代币，如果得到补偿，那么相关股份在一定期间内就不参与验证，控制大量股份的节点。 这既解决了Bitcoin的能源浪费问题，又对网络安全提出了新的挑战课题。 AOK将实现对该协议优点的技术性体现，尊重现有的理论创始人，并完善潜在的改善点和缺点。AOK认为PoS 3.0是目前最安全、最进步的有效区块生成方式，决定体现PoS 3.0协议算法并制作完成。

2.3. Block Reward

对现有PoS系统的大部分证件的补偿，不幸的是以Coin Age为基础，从理论上讲，这是让节点得到暂时的支付，公平分配关心，并试图维持共同的利率。 另外，节点没有提供维持连接状态的奖励。 在分散系统中，信任从单一的实体转移到网络本身，因此节点的量越多，保安就越强。

AOK为了解决这个问题，作为PoS 3.0的解决方法，区块补偿是每个区块 4 AOK，维持一定的代币生成补偿，只有作为节点参与一定时间以上时才能作为区块补偿的对象参与。这种方式可以增加节点的参与，诱导其脱离中央化，并有稳定地维持安全网络和通货膨胀的效果。

4. Coin-Age Problem

1. 保安问题

股份证明是拥有很多相关代币的（拥有很多股份），因此验证区块有效性的概率会提高，证明拥有代币并获得相当于持有数量的区块补偿的概率会提高。由此，将引发更多人为了获得更多的区块补偿而展开的竞争。

Coin Age是长期放置代币，发现区块的概率会提高的理论，其本意是赋予持有代币的人动机，但只要等到补偿增加，其概率就会提高，因此不提倡节点们实际上继续连接网络。由于这些问题，长期中断网络连接并重新连接，有可能对网络发动51%的攻击。像这样连接的节点越少，就越容易获得大部分协议，为了有效进行这种攻击，可以事先计算出必要的币种数量。

2. AOK Main-Net

2.4.2. 对Stake grinding attack的防御

随着时间的增加，消除Coin Age区块补偿带来了安全性的改善。因此，固定的节点量减少与断裂节点成正比。 例如，如果只有1/4的网络在站台，补偿最多可望达到保有量的5倍。因为很多币种的记事本不够充分，所以对小规模持有者来说也是很大的好处，一般来说，记事本的占比不到20%。AOK认为这些奖励的增加将切实维持节点的竞争力，并认为对防止"Stake grinding attack"很有用。

Neucoin对这次攻击的概率进行了很好的分析。 Neucoin的主张是，即使使0用Bitcoin网络的所有哈兴力量，也不能进行攻击。但几分钟Roll-back无法确定新用户将连接到网络上的任何链条，Stake系统使用"Check pointing"基本上由中央控制，以供主开发者选择尝试此操作的链条。 当然这不是理想的解决方案。 清除Coin Age通常是安全的决定，它可以要求执行检验时间服务器的混合系统来计算漂移，使节点与一般的时间协议密切同步。基于区块链的其他随机参数的追加也是考虑事项。

2.4.3. 决解问题

Coin Age是根据未使用过的代币的数量和持有时间来计算的，这是从最初的PoS代币PeerCoin中引进的概念，是以未使用过的代币的数量和持有时间乘以的价钱制作网络中最古老的链子，然后该链被登记为区块的方式。

Coin Age在获得第一块区块补偿后重新设置，很难执行连续的双重支出，因此说明为拯救Coin Age而发动攻击是不可能的。

但是输入可能会被分割成大量的输出，这并不明确，而且可以给连续的双重支出攻击带来可能性，因为攻击者为了维持比网络更大的权重值，需要相当金额的资金，所以仍然是个难题。 理论上可以说非常合理。

从使用与AOK不同人气PoS方式的系统的复刻量可以看出，节点量相当少，这意味着在少数节点中占有更大比重，因为拥有大量代币的人可能会因为节点价值严重降低而不愿意执行这一攻击。 Coin Age依然是重要的攻击渠道，每时每刻在生成新的区域时都会发行代币，因此为了安全起见，必须尽可能多地连接节点，所以从PoS 2.0开始，这个概念就被删除了。 因此, AOK不受Coin Age的攻击。

2. AOK Main-Net

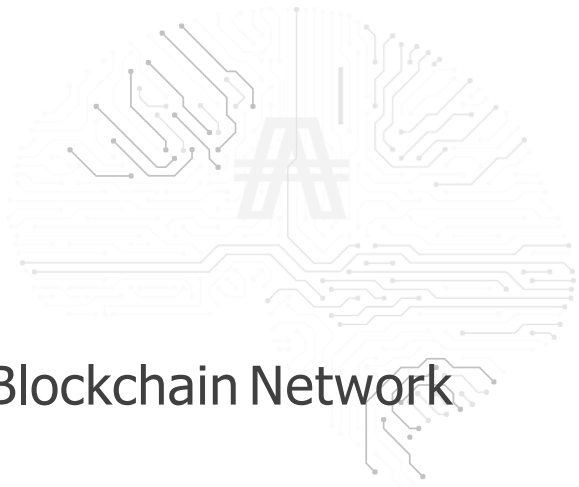
2.5. Multi signature Staking

协议中值得关注的追加事项是"Multisignature Staking"的体现。许多PoS算法的缺点是单个键支持Stake。 因此，使用被称为"2重Escrow"的单一Escrow系统和更安全的双重键账户，让账户参与网络安全变得更为重要。

另外，还有利用P2SH的方法。 P2SH(Pay To Script Hash)是指支付给脚本解示而不是公开键的概念，不是使用一个公开键，而是用脚本解示代替公开键解示，可以发送事务处理。 这种多重信号排查很重要的原因是，在单一密钥账户中，黑客会使用key logger识别密码，在解锁时钱包可能会受损。

PoS 3.0 证明的解决方法:用户可以在以地址著称的输出上设置区块签名键，发送标准事务处理后做Stake。

通过这个可以提交所有的输入，这样AOK对软件、投票及"Cold Stacking"都有很大的好处。 Cold Staking技术需要多台电脑，如果多重签名输入适合于Stacking，签名将分割在多个电脑之间。 因此，即使一个密钥受损，由于在本地网络或多个服务器上处于完全不一样的位置，所以事实上无法入侵账户，该技术已经在Black-Halo的最新发布上得到体现。



2. AOK Main-Net

2.6. Payment System

2.6.1. UTXO

AOK使用Bitcoin的结算系统UTXO。 UTXO是Unspent Trasaction Outputs的缩写，意味着未使用的交易输出值。Bitcoin与Ethereum的"账户余额模式"(Account Balance Model)不同，没有账户或余额，通过区块链记录的"不消耗的输出值"检查交易的有效性，确认代币的存在与否。

2.6.2. UTXO 动作结构

AOK 将从某人那里得到的金额保存为UTXO。 例如，从A和B分别得到2AOK和3AOK，拥有5Bitcoin，钱包里就不会存为5 AOK，而是分别存为2 AOK和3 AOK的UTXO。 然后将UTXO内的金额汇出时，会生成新的UTXO，现有UTXO将被销毁。即，在有3 AOK的UTXO中，将2 AOK汇给他人后，重新生成汇出2 AOK的AOK和剩余的1 AOK的UTXO。

2.7. Asset Function

2.7.1. 资产发行与交易

AOK的代币牌名不能重复，以该名称发行代币牌的第一位发行者将成为该项目的所有者。 发行者可以决定发行数量、Decimal（小数点位）和今后是否可以发行更多的相同代币，将代币合并到QT钱包中，并制作提供代币管理功能的新RPC呼叫，可以轻松发行新的资产代币，告知目前余额，也可以向其他用户传送资产。

2.7.2. 多种使用

AOK可发行代表企业、财团、个别项目、组合或合作伙伴的项目代币。

关于每个代币的规则根据相应代币发行者不同而有所不同，记录保管是在工作分散的AOK区块链上进行的，因此可以灵活运用多种参与结构，有效地使用。 通过AOK 主网币基础上的代币，用户可以在新的世界经济中进行更多的资产交易，其费用也会降低。 而且用户们使用AOK 代币，可以更有效率、更明目张胆地证明固有资产及其有效性。

2. AOK Main-Net

2.7.3. 资产发行条件

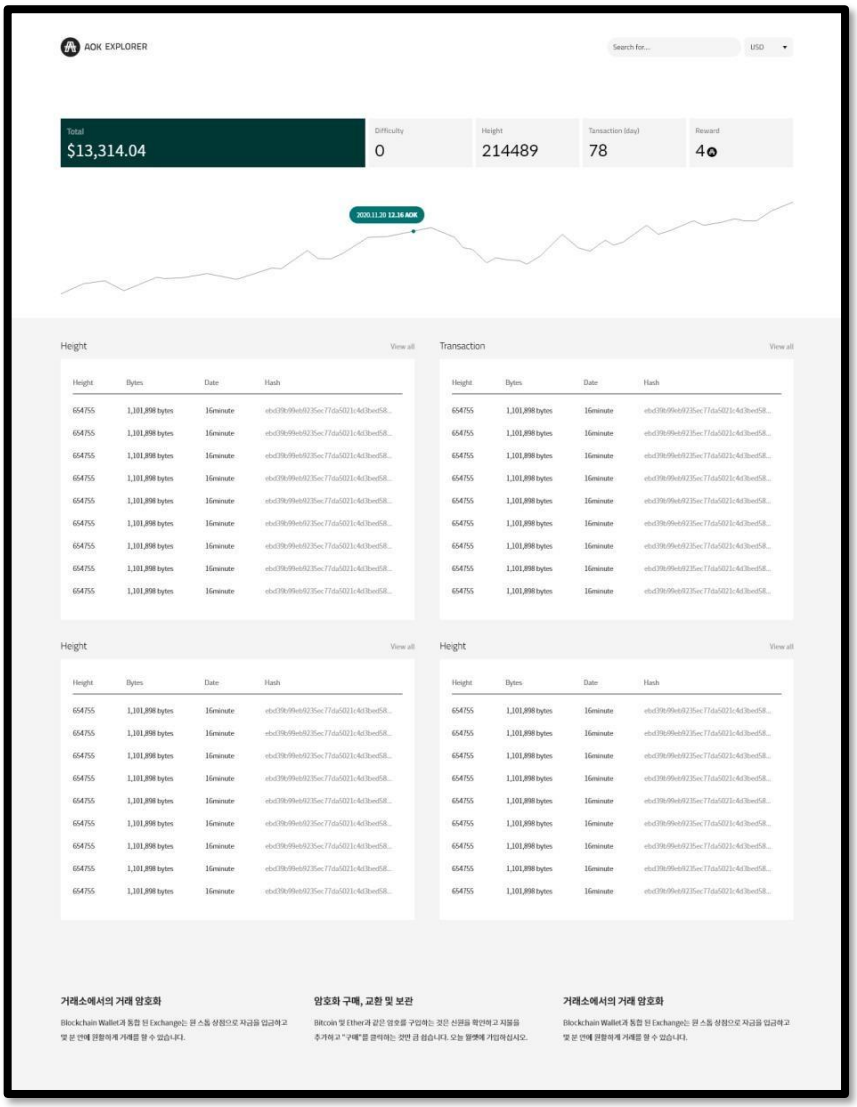
AOK是为了防止无差别的资产的生成而开发的，当想要以代币形式生成新资产时，必须将一定数量的AOK主网代码传送至特定地址的逻辑。 资产名称固有，资产单位或总量由资产发行人决定发行。 发行的代币可以使用与Ethereum ERC20代币类似的方式， AOK 主网网络可根据比特币方式的指令体系进行更直观的改变，而不是现有的ERC20代币的复杂使用方法。

而且，为了生成超过特定数量的代币，必须进行投票或认证，防止垃圾短信等资产形态的代币盲目泛滥。AOK的主网允许拥有更安全的固有资产，使得AOK的主网区块链生态系统得以进一步扩张，并可以开发多种目的和形态的DApp。

2.8. Transaction Fee

AOK 主网网络发生交易时，手续费至少从0.0001 AOK开始发生，根据网络的混乱程度可变性调整。在支付相关区块上使用的所有区块补偿的同时，还将支付给发现区块的持有节点。

3. AOK Explorer



3.1. Explorer Overview

AOK为了快速、稳定地搜索区块，提供独立模型的区块链探索器，并通过Github公开源代码。这台 AOK 区块链浏览器详细地提供着AOK 的区块、 AOK 地址、交易明细及使用 AOK 网络的副代币的记录。

3.2. Explorer Address

AOK Explorer 的连接地址如下。

https://explorer.aok.network

4. AOK Wallet

4.1. Wallet Overview

可存储、传送、管理 AOK 主网币及代币的 QT 钱包已开发完毕，并已向 Github 公开。

4.2. Windows / MacOS / Linux

4.2.1. Windows OS

AokChain-Windows.zip AokChain-Winows-Qt.zip

4.2.2. Apple Mac OS

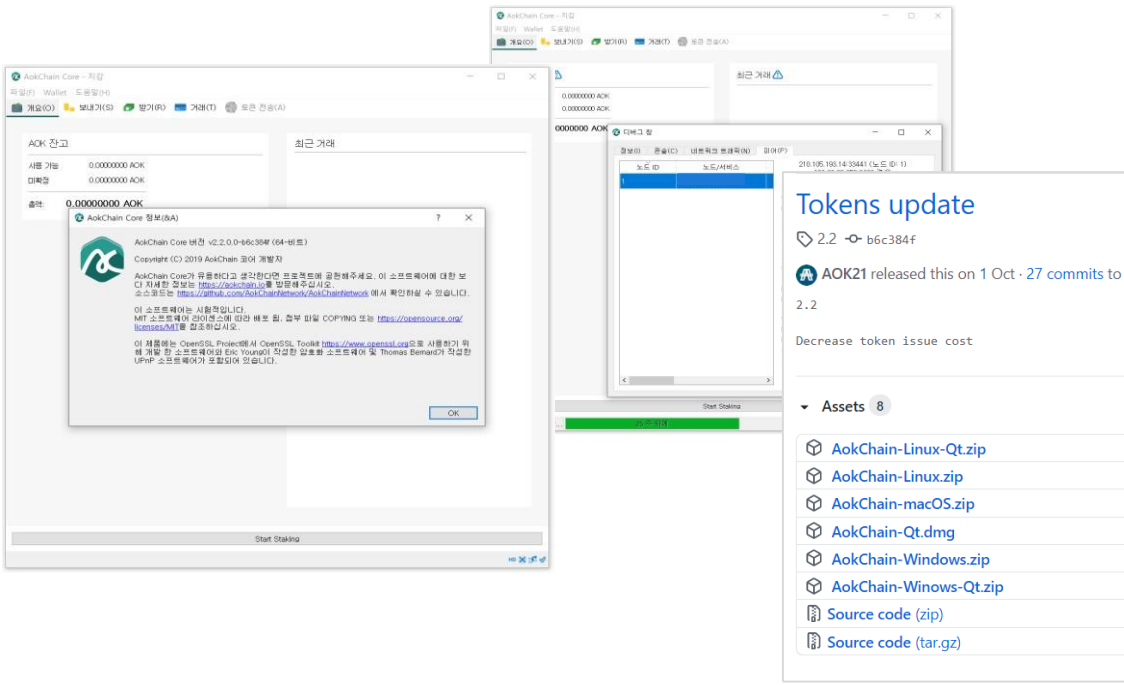
AokChain-macOS.zip AokChain-Qt.dmg

4.2.3. Linux AokChain-Linux-Qt.zip AokChain-Linux.zip

4.3. Wallet Address

接受AOK Wallet地址如下。

https://github.com/AokChain/AokChain/releases



4. AOK Wallet

4.4. QT Wallet Information

运行符合要安装的OS的Wallet程序。

4.4.1. Wallet 运行

运行Wallet时程序会自动启动Block Sync。 在节目的下端可以确认Sync的过程。

4.4.2. Wallet 表示画面说明

Spendable: 当前可发送的代币数量
Stake Weight: 用于权益质押的代币数量
Immature Stake: 权益质押后获得的区块补偿将反映在钱包里的代币数量
Unconfirmed: 传送后等待confirm的代币数量（至少需要1 confirm以上）

4.4.3. Wallet 设定密码

在Wallet 屏幕上端选择[设置>>钱包加密]来设置密码。 设定的wallet密码可以变更，但如果忘记密码，则无法复原。

4.4.4. 生成地址

如果运行Wallet，基本上可以生成一个地址，除此之外，还可以追加生成用户想要的地址。 在钱包左侧菜单中选择Receive，就能显示生成地址，还可以通过下端的新Address按钮生成新地址。

4.4.5. 代币转账

在Wallet左侧目录中选择发送目录，就会出现传送代币的画面。 输入收代币的对方的Wallet地址和代币的数量，然后选择下方的发送按钮。在钱包里设置密码时会出现密码输入窗口，输入密码后可以传送密码。

汇款手续费可在wallet上方的[设置>>选择>>>主]设定。如果选择下端收货人添加按钮，就会添加地址输入窗口，通过这些可以一次性进行大量交易。

4.4.6. 交易明细确认

交易菜单提供Wallet内所有交易明细，通过设定选项可以简单查询想要的交易明细。

4. AOK Wallet

4.4.7. 地址

交易菜单提供Wallet内所有交易明细，通过设定选项可以简单查询想要的交易明细。

4.4.8. Staking (PoS Mining)

如果Wallet中有代币，可以进行Pos Mining。

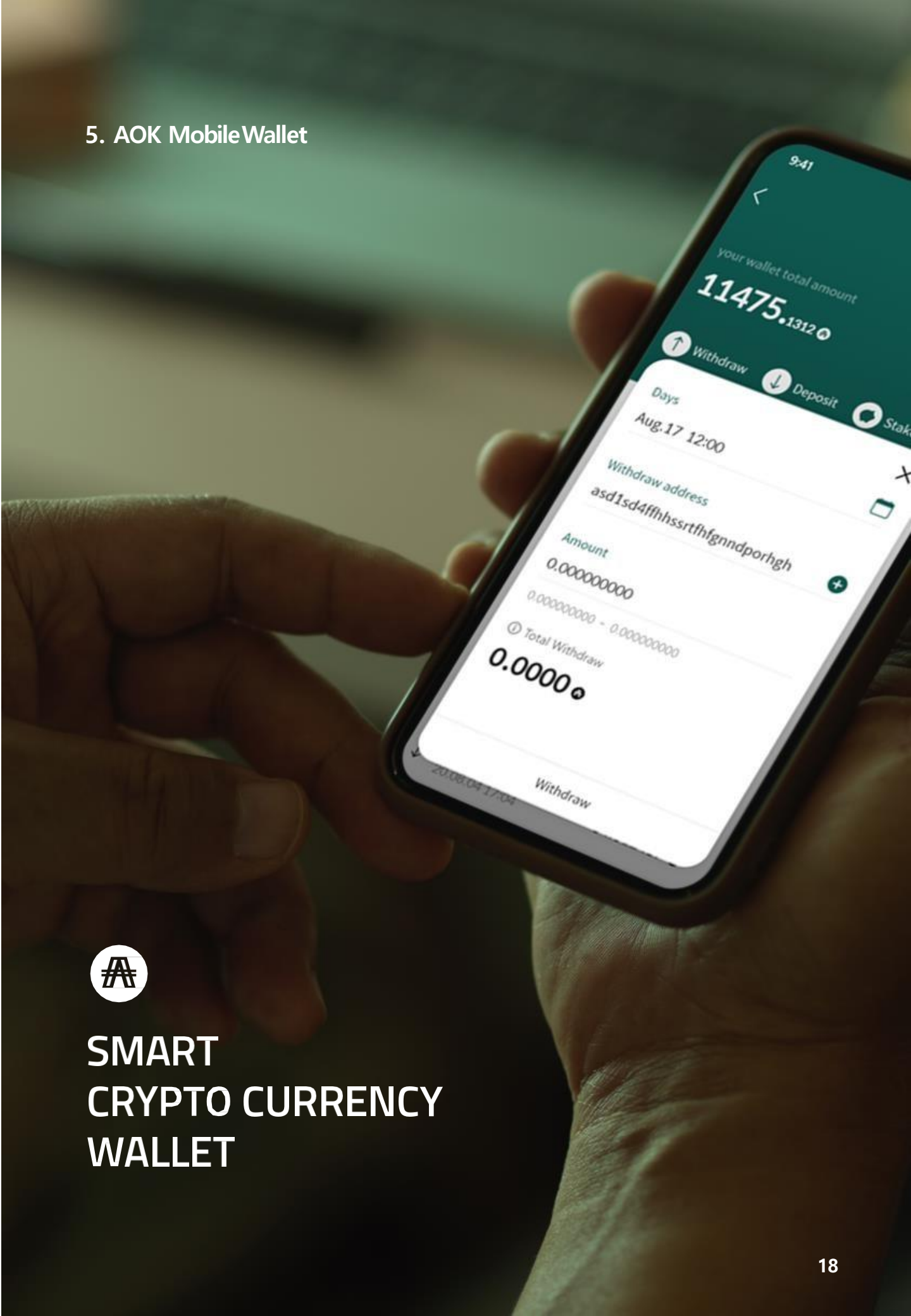
4.4.9. Backup

生成Backup文件，有事时可以恢复wallet。

4.4.10. Restore

在损失现有data的情况下，打开钱包就会生成新的wallet。 这种情况下，可以将上面制造的backup file移动到安装wallet的渠道，恢复wallet。

5. AOK Mobile Wallet



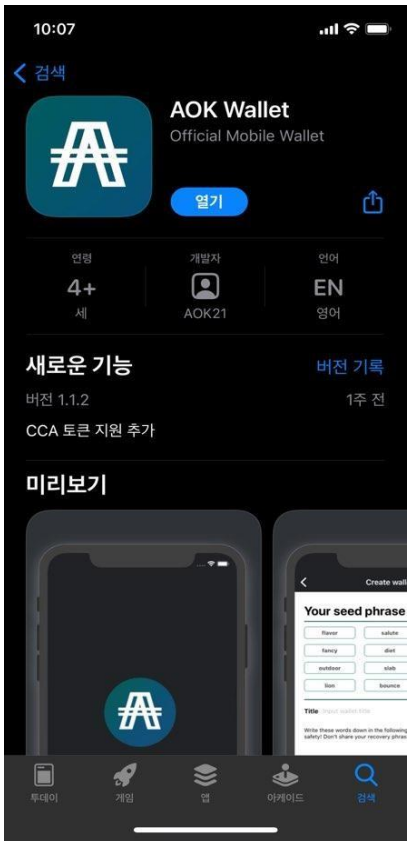
SMART CRYPTO CURRENCY WALLET

5.1. Mobile Wallet Overview

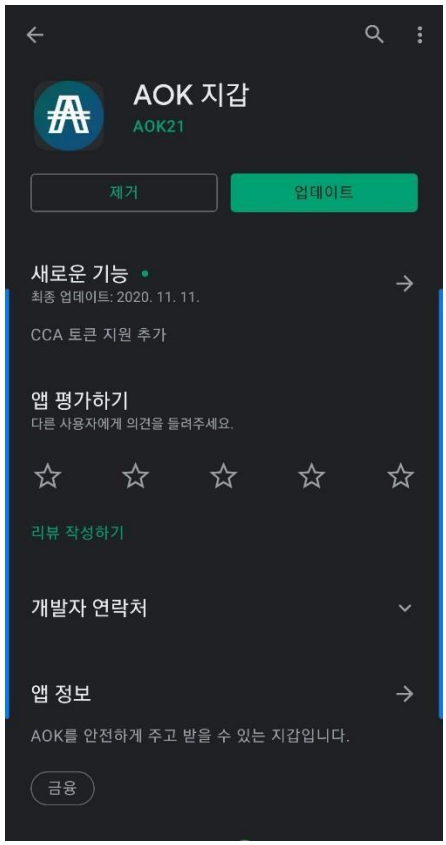
AOK将脱中央化的手机钱包正式提供给Android/iOS平台。 利用该应用程序，可以方便进行AOK币和代币的传送、保管和管理。

5.2. Android/iOS

AOK的手机应用软件是脱中央化的自然应用软件，分别支持Android和iOS。



App Store by iOS



Play Store by Android

6. AOK API

6.1. API Overview

AOK API是为构建和整合应用软件的定义及协议套装，是指在制作使用AOK网络的3rd party软件时，可以灵活使用的应用软件编程接口。

如果使用AOK的API，即使不直接运行软件记录，也可以轻松完成验证传输明细或确认余额的一系列过程。 AOK 的API采用URL方式，可方便使用，所有结果均以包含项目的JSON形式提供，使用率更高。

目前可使用的API种类

- /Info
- /height/int:height
- /block/string:hash
- /header/string:hash
- /range/int:height
- /balance/string:address
- /mempool/string:address
- /unspent/string:address
- /history/string:address
- /transaction/string:hash
- /mempool
- /fee
- /decode/string:raw
- /broadcast

6.2. API Address

AOK的API可以在以下地址确认。

https://api.aok.network/

7. Disclaimer 免责事项

7.1.

This white paper is intended to help you understand the AOK business. Investors are encouraged to purchase through exchanges or open sales channels at their own discretion.

本白皮书为帮助理解AOK事业，请投资者根据各自的判断，通过交易所或公开的销售渠道购买。

7.2.

AOK, we do not guarantee return on investment to the buyer.

AOK 不保障购买者投资收益。

7.3.

AOK, we do not guarantee the price after listing.

AOK上市后不保证价格。

7.4.

AOK, we do not promise repurchase at the specified price

AOK不承诺以指定价格重新购买。

7.5.

AOK, we do not operate branAOKs or sales agents.

AOK 不经营分店或营业代理。

7.6.

AOK investors should make their own judgment that they are not in violation of the blockchain policy of each country.

AOK投资者必须自行判断，不违反各国区块链政策。

7.7.

Despite technical efforts, AOK may incur investment losses depending on market conditions.

尽管在技术上做出了努力，但AOK根据市场情况可能会造成投资损失。

7.8.

Despite our efforts, market instability or risk of market collapse is possible.

尽管我们努力，市场仍存在不稳定或市场崩溃的危险。

7.9.

AOK main notice is to prioritize the presentation of the homepage.

AOK 主要公告优先于主页的预览。

7.10.

AOK Other policies are announced on the official website.

AOK 其他政策将在官方网站上公布。

7. Disclaimer 免责事项

7.11.

AOK is not a stock or any way of value guarantee.

AOK不是股票或保值的方法。

7.12.

AOK business model may change slightly depending on the agreement with the partner company.

AOK事业模式可根据与合作伙伴公司签订的协议内容进行部分变更。

7.13.

Purchase of AOK coin must be done by the buyer himself according to local law, AOK does not make any legal guarantee for purchase.

购买 AOK Coin 须由购买方依照当地法律自行进行，AOK 对购买不提供任何法律保证。

7.14.

Among the contents mentioned in this white paper, the business model may change its brand or target in the process.

本白皮书提及的内容中，事业模式在实施过程中可能会改变品牌或对象等。

8. References

1Stuart Haber & W. Scott Stornetta. (1991). How to time-stamp a digital document. Journal of Cryptology volume 3, pages99–111.

2Karamitsos, I. , Papadaki, M. & Barghuthi, N. (2018). Design of the Blockchain Smart Contract: A Use Case for Real Estate. Journal of Information Security, 9, 177-190.

3Bo Liu, Fan Qiu, Yanchuan Cao, Bin Chang, Yi Cui & Yuan Xue. (2011). Maximizing Resilient Throughput in Peer-to-Peer Network. Communications and Network, Vol. 3 No. 3, pp. 168-183.

4Ioanna Roussou, Emmanouil Stiakakis & Chaido Dritsaki. (2019). The Bitcoin's Network Effects Paradox—A Time Series Analysis. Theoretical Economics Letters, 9, 1981-2001.

5 Satoshi Nakamoto. (2008). Bitcoin: A peer-to-peer electronic cash system. bitcoin.org.

6Gao, X. (2015). Design and Implementation of Peer-to-Peer Service Routing Algorithm. Journal of Software Engineering and Applications, 8, 575-580.

7Lim, I.K., Kim, Y.H., Lee, J.G., Lee, J.P., Nam-Gung, H. & Lee, J.K. (2014). The Analysis and Countermeasures on Security Breach of Bitcoin. In: International Conference on Computational Science and Its Applications, Springer International Publishing, Berlin, 720-732.

8Sunny King & Scott Nadal. (2012). PeerCoin: http://peercoin.net/assets/paper/peercoinpaper. pdf.

9 Pavel Vasin. (2013). Proof of Stake 3.0: http://bravenewcoin.com/assets/Whitepapers/blackcoin-pos-protocol-v2-whitepaper.pdf.

10Kourosh Davarpanah, Dan Kaufman & Ophelie Pubellier. (2015). NeuCoin: the First Secure, Cost- efficient and Decentralized Cryptocurrency: http://www.neucoin.org/en/whitepaper/download.

11 https://www.blackhalo.info

12 https://www.ethereum.org

白皮书最初发生日期
2020.11.24

AOK Group