2018-3-25
March 25, 2018

安网 anwang
关注应用安全和隐私保护的区块链应用开发平台 v1.0
SAFE - A Blockchain Application Development Platform v1.0 Concerning Application Security and Privacy Protection

新加坡 SAFE 基金会出品
Singapore SAFE Foundation

目　　录

Contents

安网是企事业单位实施“区块链+”战略的最佳应用开发平台，本白皮书主要介绍安网的发展历史、研发团队、商业价值、系统架构和技术方案。本白皮书的技术方案在不断更新和迭代中，请上安网官网（anwang.com）获取最新白皮书。

SAFE is the most ideal platform for developing applications of enterprises and institutions implementing the “Blockchain+” strategy. This white paper details its development, R&D team, business value, system architecture and technical schemes which are in updating and iteration. The latest version is available at anwang.com.

1 前言

1. Introduction

安网（Anwang.com）是由新加坡 SAFE 基金会推出的、去中心化的、关注区块链应用安全和隐私保护的区块链应用开发平台。任何人可基于安网发行代币、开发区块链应用，而无需审核，安网通过 Sapp 应用开发协议提供了比智能合约更安全的区块链应用解决方案。

Launched by Singapore SAFE foundation, SAFE is a decentralized platform for Blockchain application development while concerning Blockchain application security and privacy protection. This platform enables people to issue tokens and develop Blockchain applications without review procedures, providing Blockchain application solutions that are more secure than smart contracts via Sapp application development protocols.

1.1 区块链发展史

1.1 History of Blockchain

比特币诞生于 2009 年，是第一个、也是最成功的一个区块链应用。区块链的核心技术——密码学和分布式系统却早已出现。

Bitcoin created in 2009 is the first and most successful Blockchain application, with its core technologies – cryptography and distributed system emerged earlier than Bitcoin.

1976 年，Bailey W. Diffie、Martin E. Hellman 两位密码学大师所发表《密码学的新方向》论文标志着密码学的发展进入了新时期。

In 1976, cryptography masters Bailey W. Diffie and Martin E. Hellman issued a paper *New Directions in Cryptography*, marking a new era for development of cryptography.

1979 年，Ralf Merkle 提出了 Merkle-Tree，Merkle-Tree 主要是用来快速验证分布式网络的数据完整性，比特币使用了 Merkle-Tree 进行数据完整性校验。

In 1979, Ralf Merkle proposed Merkle-Tree for rapid verification on data integrity of distributed networks, which is applied by Bitcoin.

1985 年，Koblitz 和 Miller 提出著名的椭圆曲线加密（ECC）算法，相比 RSA，ECC 更加安全，运算速度更快，对带宽要求更低，使得非对称加密进入了实用阶段。比特币采用 ECC 作为签名技术。

In 1985, Koblitz and Miller proposed the famous Elliptic Curve Cryptography (ECC) which, compared with RSA, is safer, faster in computation and easier on bandwidth request, and thus put asymmetric encryption in practical use. Bitcoin employed this for its signature technology.

美国国家安全局 NSA 于 1995 年发布了 SHA-1，SHA-1 和后来持续发布的 SHA-224，SHA-256，SHA-384，SHA-512，组成 SHA 算法大家族。比特币采用 SHA-256 作为哈希算法。

In 1995, National Security Agency (NSA) launched SHA-1 which formed the SHA Algorithm family later with SHA-224, SHA-256, SHA-384 and SHA-512. Bitcoin adopts

this SHA-256 for its Hash algorithm.

1997 年 Adam Back 在一篇论文中提出了 Hash Cash 算法来防止垃圾电子邮件，比特币所采用该技术作为 Proof-of-work（POW，工作量证明）算法。

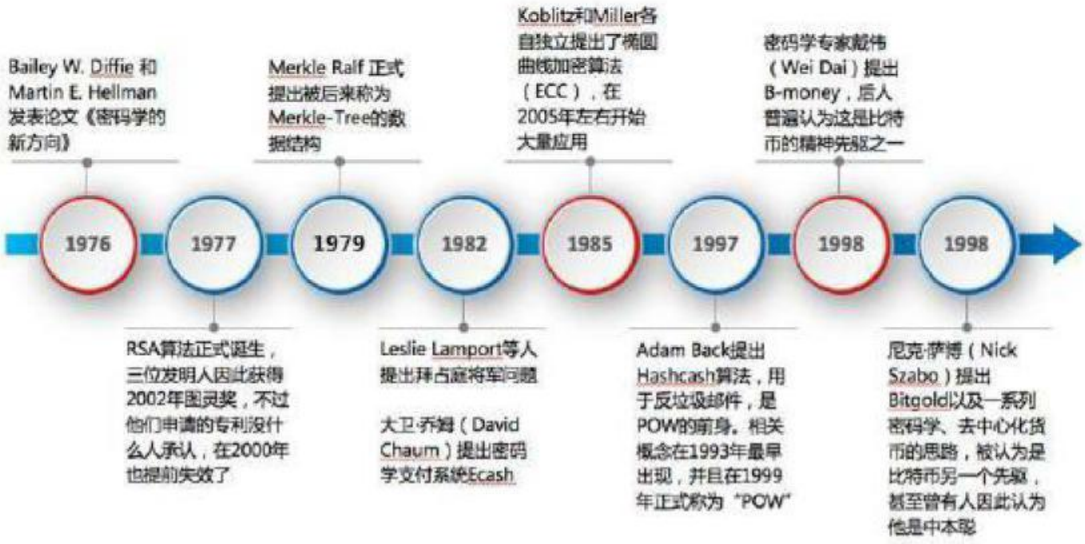
In 1997, Adam Back proposed Hash Cash algorithm in his paper to prevent spam. Bitcoin adopts this technology as Proof-of-work (POW) algorithm.

图灵奖获得者 Leslie Lamport 是分布式计算的先行者者，早在 1978 年开始了分布式计算研究，在 1982 年与另两人共同发表论文“拜占廷将军问题”，标志着分布式计算从研究进入了实用研究。

Turing Award winner Leslie Lamport as a pioneer in distributed computing started his research in this field early in 1978, and co-issued the paper *Byzantine Failures* with other two scholars in 1982, marking a transition of study on distributed computing to practical research.

P2P 协议开始出现，尤其是 2003 年出现的 BT，让 P2P 技术的发展进入快车道。

The emergence of P2P protocol, especially BT in 2003, accelerates P2P technology development.



Bailey W. Diffie 和 Martin E. Hellman 发表论文《密码学的新方向》	Bailey W. Diffie and Martin E. Hellman issued their paper *New Directions in Cryptography.*
Ralf Merkle 正式提出被后来称为 Merkle-Tree 的数据结构	Ralf Merkle formally proposed a data structure later named as Merkle-Tree.
Koblitz 和 Miller 各自独立提出了椭圆曲线加密算法（ECC），在 2005 年左右开始大量应用	Koblitz and Miller proposed Elliptic Curve Cryptography (ECC) respectively, which was applied widely since 2005.
密码学专家戴伟（WEI DAI）提出 B-money，后人普遍认为这是比特币的精神先驱之一	Cryptography master cryptography proposed B-money, which is widely considered as one of the spiritual pioneers of Bitcoin.
Rsa 算法正式诞生，三位发明人因此获得 2002 年图灵奖，不过他们申请的专利没什么人承认，在 2000 年也提前失效了	Rsa algorithm was created, and the three creators won Turing Awards in 2002. However their later patents were rarely recognized and went void in 2000.
Leslie Lamport 等人提出拜占庭将军问题 大卫·乔姆（David Chaum）提出密码学支付系统 Ecash	Leslie Lamport et al. proposed the issue of Byzantine Failures. David Chaum proposed Ecash - a cryptographic payment system.
Adam Back 提出 Hashcash 算法，用于反垃圾邮件，	Adam Back proposed Hashcash algorithm to prevent spam,

是 POW 的前身。相关概念在 1993 年最早出现，并且在 1999 年正式称为“pow”	who is the pioneer of POW. The related concept appeared early in 1993 and was named as “pow” in 1999.
尼克·萨博（NICK SZABO）提出 bitgold 以及一系列密码学、去中心化货币的思路，被认为是比特币的另一个先驱，甚至曾有人因此认为他是中本聪	Nick Szabo proposed bitgold as well as a series of ideas on cryptography and decentralized money, he was then recognized as another pioneer of BitCoin, and some even thought he was Satoshi Nakamoto.

至此，比特币所需要的密码学、分布式、POW 算法等等技术都已经准备就绪。2008 年 11 月，中本聪那篇著名的论文《比特币：点对点的电子现金系统》正式发布，2009 年 1 月，中本聪挖出了创始区块，包含着这句经典的话：“The Times 03/Jan/2009 Chancellor on brink of second bail out for banks.”，标志着区块链的第一个应用比特币正式诞生。

So far, there are mature technologies such as the cryptography, distributed system and POW algorithm required for Bitcoin. In Nov. 2008, Satoshi Nakamoto published his famous paper *Bitcoin: A Peer-to-Peer Electronic Cash System*. In Jan. 2009, he proposed the Genesis block with this famous quotation “The Times 03/Jan/2009 Chancellor on brink of second bail out for banks.”, marking the birth of the first Bitcoin application on Blockchain.

1.2 项目背景和意义

1.2 Project Background and Significance

安网项目背景和意义主要从应用安全性、资产发行的便捷性、隐私保护三方面来说明。

Background and significance of SAFE in this paper are expounded from three aspects, application security, convenience of asset issuance, and privacy protection.

1.2.1 应用安全性

1.2.1 Application Security

目前开源社区的主流区块链应用开发平台是 Ethereum、EOS，企事业单位级别、无代币的主流区块链应用开发平台是 Fabric，他们共同的特征是使用智能合约开发区块链应用，用编译工具把源代码编译成可执行代码嵌入到交易中，再用虚拟机来装载可执行代码验证执行结果。

At present, open source communities adopt Ethereum and EOS as their mainstream platforms for Blockchain application development. Enterprises and institutions without token use Fabric as their mainstream platform for Blockchain application development. Both of the above groups adopt smart contracts for Blockchain application development. They use compilers to compile source codes into executable codes, which are subsequently embedded in transaction and loaded into a virtual machine to verify execution results.

智能合约系统是一个很新的方向和课题，但目前的安全性堪忧。Fabric 和 EOS 的智能合约很少有人使用，还未爆出太多问题，但 Ethereum 的智能合约安全性问题已经非常突出。

Smart contract system as a new technology brings about much security concern. Smart contracts from Fabric and EOS are rarely used, so there is not much problem exposed. However, smart contracts of Ethereum are in a noticeable security problem.

2016 年 DAO 的智能合约被遭黑客盗走价值 5000 万美元的 ETH，Ethereum 官方团队为了保护投资者的利益，取消所有 DAO 交易，与区块链不可修改的理念冲突，导致了 ETH 和 ETC 的分叉；

In 2016, DAO’s smart contract suffered hackers who stole ETH worth 50 million US dollars. For the sake of its investors’ interests, Ethereum’s official team had no choice but to cancel all transactions on DAO, which was in conflict with the idea that Blockchain cannot be modified and thus resulted in the fork of ETH and ETC.

同年 7 月，同样基于以太坊的电子钱包服务商 Parity 被偷超过 3000 万美元，11 月 Parity 中大约有 1.5 亿美元的用户资金被冻结。

In July of the same year, Parity, an E-wallet service provider based on Ethereum, lost more than 30 million dollars due to cyber break-ins. In November, about 150 million dollars of user funds on Parity are frozen.

2018 年 2 月 24 日伦敦大学学院计算机科学家 Sergey 及其同事对将近 100 万份的以太坊智能合约样本进行了分析。结果发现约有 3.4 万份都是存在安全隐患的，涉及几百万美元，其中 2365 份属于著名项目。

On Feb. 24, 2018, the computer scientist of University College London Sergey together with co-workers analyzed nearly 1 million smart contract samples, and about 34,000 samples were found vulnerable, involving millions of US dollars, including 2365 samples for some famous projects.

目前 Ethereum 上发现的严重智能合约漏洞已经超过 20 多个，严重威胁着智能合约的资金安全。

At present, more than 20 serious smart contract vulnerabilities are found on Ethereum, a deadly threat to fund security of smart contracts.

一方面，链上智能合约是一种开创性的技术，值得进一步探索和优化，其安全性应该继续提升；另一方面，在智能合约成熟前，也可探索非智能合约形式的、更安全的应用开发模式。安网的应用开发协议，就是对更安全的应用开发模式的探索。

On the one hand, smart contracts on Blockchain adopt an innovative technology which needs further exploration, optimization and security promotion. On the other hand, as smart contract technology has not yet been refined, safer non-smart-contract application development modes can be explored. The application development protocol of the SAFE is a probe for a safer application development mode.

1.2.2 发行资产的便捷性

1.2.2 Convenience of Asset Issuance

资产发行是应用开发中的一个重要方面，每个应用几乎都会涉及到数字资产发行，如代币、积分、游戏装备、单据之类。Ethereum 智能合约的资产发行过程比较复杂，需要按照 ERC20 标准自行编写智能合约，虽然有些开源代码，但毕竟需要技术人员研发，有一定的门槛。

Asset issuance, especially digital asset issuance, as an important link in application development is widely adopted for almost all applications such as token, bonus points, game equipment and receipts. Issuing Ethereum smart contracts is a complex process including smart contract writing as per ERC20 standards, during which some open source codes are available, but some technicians at certain level are still required for research and development.

能否以更简单的方式发行数字资产，让没有区块链应用和智能合约开发能力的人员能点击几下鼠标、输入一些信息，就把数字资产发行出来？

Is there any simpler method for those incapable of developing Blockchain application and smart contract to issue digital assets just by clicking the mouse and entering some information?

1.2.3 隐私保护

1.2.3 Privacy Protection

区块链上的隐私保护主要针对金额和过往交易的问题。给定一个比特币地址，任何人都可以看到该地址的余额以及过往的交易细节，这无法满足用户的隐私保护需求。

The Blockchain privacy protection mainly targets the amount of money and previous

transactions. Given a Bitcoin address, anyone can view its corresponding balance and previous transactions in details, and this is a risk against privacy protection.

DNC（DarkNetSpace，项目名称暗网空间，后改名安网），由 SAFE 基金会创始人申屠青春先生于 2014 年 10 月发布，2017 年 7 月发布了第二个版本，并且改名为安网 2。DNC 以环签名和隐身地址的技术，隐藏了发送人和接收人，割裂了输入和输出的关联，使得区块链不可被分析，达到了隐私保护的目的。

DNC (a project previously named as DarkNetSpace) was launched by SAFE Foundation's founder Shentu Qingchun in Oct. 2014, and the second version was launched in July 2017 and renamed as DNC2. DNC adopts the ring signature and stealth address technology hiding the information of the sender and receiver, splitting up the connection between input and output, and leaving Blockchain analysis impossible.

CryptoNote 技术的系列币种，由于其区块链的不可分析，导致区块链应用和智能合约引入的难度剧增，因而把隐私保护这些特性当成可选项更为合适。

As for coins adopting CryptoNote technology, its Blockchain cannot be analyzed, leading to an increasingly difficult introduction of Blockchain application and smart contract. Therefore, it is better to make features such as privacy protection optional.

1.3 安网历史

1.3 History of SAFE

如上所述，安网空间（简称安网）的代币 DNC 早在 2014 年 10 月份就已经发布，是中国最早的关注个人隐私保护的数字货币。

As mentioned above, DarkNetSpace token (DNC) was launched early in Oct. 2014, which is the earliest digital currency in China focusing personal privacy protection.

2017 年 7 月，安网团队将安网 1 升级到安网 2（Anwang 2），DNC 升级到 DNC2。DNC2 相比 DNC，所需内存更少，更安全高效。主要特色：存币理财、私密通信（包括个人以及群组）、钱包直接挖矿、远程交易释放等等。

In July 2017, DNC team made upgrades from DNC to DNC2. DNC2 requires less memory, features higher security and efficiency, and provides functions like coin deposit and money management, private communication (including individuals and groups), direct mining via wallet and remote transaction release.

强隐私保护：如支持 TOR 网络、环签名、隐身地址、交易远程释放等，实现了真正的隐私保护：

Strong privacy protection: such as Tor network, ring signature, stealth address and remote transaction release, that realized privacy protection.

存币利息：DNC2 可锁定在区块链上，不到解锁时间不得动用，且可产生最高 5%的年利率，防止手欠卖出又能得到更多 DNC2。

Interest on coin deposit: DNC2 can be locked on the Blockchain, which cannot be moved until the unlocking time, with an annual interest rate tops at 5%, to avoid selling out upon bad decisions and gain more DNC2.

密聊：密聊是指加密聊天，DNC2 用公钥体系，用聊天对象的公钥加密，聊天对象必须用自己的私钥解密才能得到聊天内容，安全性极高。密聊包括了单密聊和群密聊，单密聊是指与一个对象地址进行聊天，群密聊是指与多个地址进行聊天，其他人员可以很容易加入到聊天中。

Encrypted chat: DNC2 adopts a public key infrastructure using the talker's public key to encrypt chat, and the content can be viewed only by entering the talker's private key for

decryption, which is very safe. Encrypted chats include individual encrypted chat and group encrypted chat. Individual encrypted chat means to chat with an individual at its address. Group encrypted chat means to chat with group at their addresses, and others can join the chat.

区块浏览：内置了区块浏览器，可以查看到所有区块和交易数据。

Block browse: with a built-in block browser, all blocks and transaction data are viewable.

内置挖矿：简化了挖矿功能，直接在钱包中就可以挖矿，无需安装其他挖矿软件。

Built-in mining: the mining function is simplified, so mining in wallet is available without installing other mining software.

网络监视：包含了网络监视功能，如交易内存池、节点列表之类的。方便查看网络。

Network monitoring: this function covers the transaction memory pool, node list, etc., to facilitate network viewing.

2018 年 1 月，SAFE 基金会决定分叉 DASH，合并投票链和安网 2，升级成安网 3，分叉币更名为 SAFE，全力打造更开放、具有更大生态圈的项目。

In Jan. 2018, SAFE foundation made the decision to release a fork Bitcoin named DASH, merge the ELT and DNC2 and upgrade it into SAFE. The fork Bitcoin was renamed as SAFE, to create a more open project with a bigger ecosphere.

SAFE 进展	SAFE progress

2018 年 1 月 20 日，SAFE 从 DASH 的区块高度 807085 分叉成功，安网 3 正式上线。截止至 3 月 30 日，项目进展如下：

On Jan. 20, 2018, the fork of SAFE succeeded at a Block height 807085 of DASH, and SAFE was launched officially. Up to March 30, the project progressed as follows:

安网已经有 2100 个主节点；

SAFE now has 2100 masternodes.

安网 SAFE 已经在 zb.com, coinegg.com, dragonex.im, hb.top, kex.com, oex.com, chaoex.com，btctrade,im，coolcoin.com 上线交易；

SAFE has its online transactions on zb.com, coinegg.com, dragonex.im, hb.top, kex.com, oex.com, chaoex.com, btctrade,im and coolcoin.com.

安网 SAFE 已上线矿池 vvpool.com，目前已经有稳定的算力；

vvpool.com, a mining pool launched on SAFE has steady Hash rate.

安网 SAFE 已上线币看钱包 bitkan.com 和比特派 bitpie.com；

bitkan.com and bitpie.com have been launched on SAFE.

1.4 安网应用

1.4 Application of SAFE

安网是一个区块链应用开发平台，开发者可基于安网开发各种应用，降低“区块链+”的门槛。应用开发协议，是实现安网上的区块链应用开发的标准和要求，如应用注册、权限设定、数据写入、数据查询等接口。以下是官方将基于安网应用开发协议开发的安网应用：

SAFE is an application development platform for Blockchain, based on which various apps can be developed to lower “Blockchain+” criteria. Application development protocol provides criteria and requirements on its Blockchain application development, such as application registration, settings of application rights, read-in of data and query of application data. The followings are official safe applications developed based on its application development protocol:

安资（资产管理与发行）：

Safe asset (asset management and issuance):

实现数字资产的发行、追加发行、转让、销毁、发糖果，领糖果等功能，其他应用在安网 3 上发行代币，拟建更宏大的生态圈。

It is for digital asset issuance, additional issuance, transfer, destruction, candy distribution and candy acquisition. Tokens for other applications are issued on SAFE, to plan a bigger ecosphere.

安付（即时支持、安全支付）：

Safe payment (real-time pay and safe pay):

实时支付和隐私支付。结合 DASH 的支付特点，结合原安网 2 的隐私支付技术，向更有效率的实时支付以及保护用户交易不可追踪的隐私支付方向发展。

Real-time payment and safe payment: realizing efficient real-time pay payment and untraceable privacy payment for transaction protection, based on payment featuring DASH and privacy payment technique of DNC2.

安投（安全投票）：

Safe vote (safe vote environment):

一种去中心化，公平，公开，公正的区块链投票系统，运用区块链技术手段解决投票过程中的公开、透明问题。

A decentralized, fair, open and just Blockchain voting system, adopting Blockchain technology to address problems concerning openness and transparency in voting

后续可能还会开发更多的官方应用，同时也支持第三方开发团队在其上自由开发第三方应用。

There may be more future official applications to be developed, as well as some applications developed by third parties.

1.5 SAFE 分配

1.5 Distribution of SAFE

（1）代币数量：4000 万枚，实际 SAFE 数量可能有所减少；

(1) Number of tokens: 40 million, the actual amount may be less.

（2）20%给原达世币持有者，约 800 万枚（根据分叉高度来计算的已产出 DASH 数量估算，准确数量大约 780 万枚左右）；

(2) 20% for the former holders of DASH: about 8 million (accurate to about 7.8 million, and the calculation is based on fork height);

（3）27.5%挖矿激励，约 1100 万枚（与 DASH 的产币数量和机制一致，其中 45%给矿工，45%给主节点，10%用于提案激励（SAFE 总金额的 2.75%，可能不会全部产出）；

(3) 27.5% as a mining incentive: about 11 million (consistent with DASH amount and its

mechanism, including 45% for miners, 45% is for builders of all nodes, and 10% for incentive) (2.75% of the total SAFE amount may not be generated totally)

（4）10%给团队，约 400 万枚

(4) 10% for the team: about 4 million

（5）15%用于市场推广，约 600 万枚

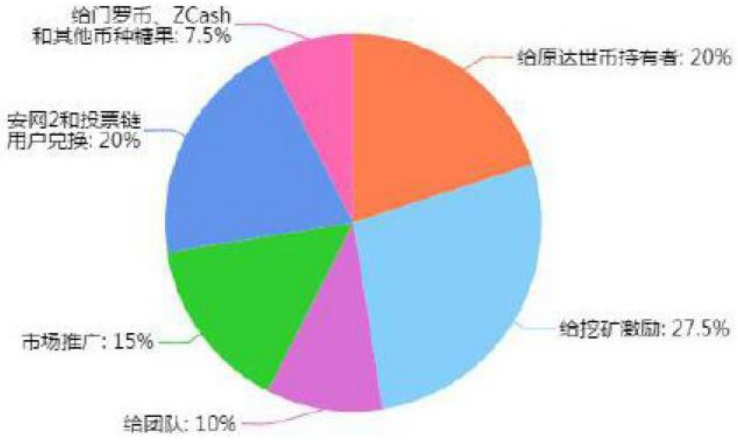
(5) 15% for market promotion: about 6 million

（6）20%用于安网 2 和投票链用户兑换，约 800 万枚

(6) 20% for conversion of DNC2 and ELT users: about 8 million

（7）7.5%给门罗币、ZCash 和其他币种分糖果，约 300 万枚（有可能会变更）

(7) 7.5% granted to the holders of Monero, ZCash and other cryptocurrencies as candies (tokens): about 3 million (subject to change)



给门罗币、Zcash 和其他币种糖果：7.5%	Holders of Monero, ZCash and other crypto currencies as candies (tokens): 7.5%
安网 2 和投票链用户兑换：20%	DNC2 and ELT users: 20%
市场推广：15%	Market promotion: 15%
给团队：10%	Team: 10%
给原达世币持有者：20%	Former holders of DASH: 20%
给挖矿激励：27.5%	Mining incentive: 27.5%

1.6 挖矿增益

1.6 Profits from Mining

1.6.1 主节点和矿工收益

1.6.1 Masternodes and Miner Profit

（1）使用 1000 个 SAFE 建立主节点，即可得到收益，收益占一个区块产币总量的 45%（目前是 1.67 个 SAFE），每 210240 块挖矿收益减少 7.14%，按照这个规则，之后主节点收益也将减少；矿工收益也一样。

(1) One can gain the profit by using 1000 SAFEs to establish the masternode. The profit accounts for 45% of the total Bitcoins generated in a block (1.67 SAFEs at present). The mining profit decreases by 7.14% every 210240 blocks. Accordingly, profit of the subsequent masternode will decrease, and so will the miner's profit.

（2）比如主节点总数为 2000 个，按照 1 天产生 576 个块，1 个主节点大约需要 3.47 天将会得到一次收益，每天收益大约为 0.48 个 SAFE（按照目前一次收益为 1.67 个 SAFE 计算）；

(2) Assuming that there are 2000 masternodes, if 576 blocks produced per day, it will need 3.47 days to gain profit from a masternode, with about 0.48 SAFE gained each day (based on 1.67 SAFEs gained each time currently).

1.6.2 活动增益

1.6.2 Profits from Activity

（1）从北京时间 2018 年 1 月 20 日 SAFE 成功分叉后第一个挖出来的区块开始计算（第 807026 个区块，以下计为第一个区块），后续的 103680 区块（近 6 个月）都有挖矿增益和主节点增益，以 SAFE 计（以下称增益）；

(1) Since Jan. 20, 2018, Beijing time, counted from the first block mined upon the successful fork of SAFE (the 807026th block, counted as the first block below), the subsequent 103680 blocks (of the recent 6 months) enjoy mining profit and masternode profit based on the amount of SAFEs (briefed as the profit below);

（2）按照每个区块的第一个交易，即 coinbase 交易的接收地址和金额，SAFE 官方将再发送相应的增益给相应接收地址，增益额度如下：

(2) According to the first transaction on each block, i.e., receiving address and amount and coinbase transaction, SAFE's official team will send the corresponding profit to the corresponding receiving address. The profits are as follows:

第1-17280区块	75%增益（是挖矿收益的75%）
第17281-34560区块	60%增益（是挖矿收益的60%）
第34561-51840区块	45%增益（是挖矿收益的45%）
第51841-69120区块	30%增益（是挖矿收益的30%）
第69121-86400区块	20%增益（是挖矿收益的20%）
第86401-103680区块	10%增益（是挖矿收益的10%）
超级块的受益者（即获得提案资助的人或者矿工）没有增益	

第 1-17280 区块	75%增益（是挖矿收益的 75%）
第 17281-34560 区块	60%增益（是挖矿收益的 60%）
第 34561-51840 区块	45%增益（是挖矿收益的 45%）
第 51841-69120 区块	30%增益（是挖矿收益的 30%）
第 69121-86400 区块	20%增益（是挖矿收益的 20%）
第 86401-103680 区块	10%增益（是挖矿收益的 10%）
超级块的受益者（即获得提案资助的人或者矿工）没有增益	

Blocks 1-17280	75% of the gain (75% of the Profit from Mining)
Blocks 17281-34560	60% of the gain (60% of the Profit from Mining)
Blocks 34561-51840	45% of the gain (45% of the Profit from Mining)
Blocks 51841-69120	30% of the gain (30% of the Profit from Mining)
Blocks 69121-86400	20% of the gain (20% of the Profit from Mining)
Blocks 86401-103680	10% of the gain (10% of the Profit from Mining)
Beneficiaries of superblocks (individuals or miners acquired the proposed financial support) gain none of this profit	

（3）SAFE 官方仅把增益发送到 coinbase 的两个接收地址。对于矿池地址而言，官方不知道该地址属于哪个矿池或矿工，因而矿池中的矿工，其增益都由矿池分配。而在 coinbase 交易中出现过的主节点地址将直接收到增益，无需别人分配；

(3) SAFE's official team will send the gains only to the two receiving addresses of coinbase.

As the official team is not clear which mining pool or miner the address belongs to, gains for mining pool address will be distributed by the mining pool, and masternode address once appeared coinbase transaction will receive gains directly rather than via a distribution.

SAFE 挖矿增益	SAFE Mining profit
每月额外赠送 10%-75%挖矿奖励	Monthly bonus 10%-75% mining bonus
1 月 20 日　7 月 19 日	Jan. 20　July 19
额外增益 持续半年 回报率高	Additional gain Lasting for half a year With high return rate
越早挖矿 增益越多	The earlier the Mining The more the gain

2 安网团队简介

2. SAFE's Team

安网团队由资深的比特币和区块链专家、技术研发团队和区块链运营人才组成，并且邀请了业内知名的技术专家和运营专家担任项目顾问，旨在打造一个有影响力、专注于区块链应用落地的项目。

SAFE has an elite team with many senior Bitcoin and Blockchain experts, technical R&D group and talented Blockchain operators, and is supported by well-known technical and operation experts in the industry serving as project consultants, and aiming to build up an influential project engaged in Blockchain application.

2.1 安网团队成员介绍

2.1 Team Members

2.1.1 负责人：申屠青春

2.1.1 Leader: Shentu Qingchun

银链科技 CEO、深圳金融标准委员会会员、深圳大学博士，高级工程师，深圳市高层次人才，深圳市政府采购评审专家。曾获 2008 年深圳科技创新奖、2009 年广东省科技进步三等奖，获得发明专利授权 4 项，获 2012 年深圳发明奖。2012 年创立银链科技，2013 年开始研究区块链。2016 年转向金融行业。曾发表 20 多篇区块链相关技术性文章，详见巴比特币专栏：http://www.8btc.com/author/14523

Shentu Qingchun is the CEO of Bankledger Technology, member of FPSB Shenzhen, doctor of Shenzhen University, senior engineer, high-level talent and government procurement review expert of Shenzhen. As the owner four patents, he is the winner of Shenzhen Technology Innovation Award 2008, third place in Guangdong Science and Technology Progress Award 2009, and Shenzhen Invention Award 2012. He found Bankledger Technology in 2012, started his research on Blockchain in 2013, expand business to finance, and published more than 20 articles about Blockchain Technology on http://www.8btc.com/author/14523

发表多篇学术文章，详见 arxiv.org 网站：

His academic articles are available at arxiv.org:

(1) Research on Anonymization and De-anonymizationin the Bitcoin System https://arxiv.org/abs/1510.07782

(2) A Blind-Shuffling Scheme for Bitcoin based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm https://arxiv.org/abs/1510.05833

(3) Transaction Remote Release (TRR): A New Anonymization Technology for Bitcoin https://arxiv.org/abs/1509.06160

2.1.2 研发总监：涂小强

2.1.2 R&D CEO: Tu Xiaoqiang

- 1984 年生，毕业于武汉大学计算机系；
- Born in 1984, and graduated from the Department of Computer Science, Wuhan University;
- 资深软件设计师和程序员，10 年 C++开发经验；IOS 开发工程师；
- Senior software designer and programmer; IOS development engineer, with 10-year experience in C++ development;
- 先后在富士康、东信网络、华阳信通任项目经理和部门经理，有金融科技研发背景；
- Former project manager and department manager of Foxconn, Donson Network and Huayang Xintong; Tu Xiaoqiang is experienced in financial technology research and development;
- 五年的区块链研发经验，熟悉各种区块链底层技术。2016 年任银链科技 CTO。
- With five-year experience in Blockchain research and development, Tu Xiaoqiang mastered various underlying technologies of Blockchain, and was appointed as CTO of Bankledger Technology in 2016.

2.1.3 运营总监：周婷

2.1.3 Bankledger COO: Zhou Ting

- 1985 年生，毕业于深圳大学英语系；
- Born in 1985, graduated from Shenzhen University and majored in English;
- 2013-2015 年任比特币国际交易所副总、算力吧运营总监，主要负责市场推广工作；
- Vice President of International Bitcoin Exchange and COO of the Hash Rate Department from 2013 to 2015, responsible for marketing;

- 2016 年任银链科技 COO；
- COO of Bankledger Technology in 2016
- 2018 年任 SAFE 基金会秘书长，全面负责 SAFE 海内外市场推广工作；
- Secretary General of SAFE Foundation in 2018, responsible for marketing at home and abroad;

2.1.4 产品总监：郭敏

2.1.4 Product Director: Guo Min

- 资深工程师，曾担任 SMG 算法工程师，盛大游戏资深工程师。具有多年产品研发管理经验；
- Senior engineer, former algorithm engineer of SMG, senior engineer of Shanda Games, with years of experience on product R&D and management;
- 曾经担任易诚互动区块链研发总监，负责公司区块链产品研发；
- Former R&D director of Interactive Technologies, responsible for Blockchain product R&D;
- 现任银链科技产品总监，负责安网 3 系列产品规划和设计。
- Product Director of Bankledger Technology, responsible for planning and design of SAFE product series.

2.1.5 其他成员

2.1.5 Other Members

2018 年初，安网团队总计 50 人：其中，软件工程师 40 人以上；运维，平面设计人员 2 人；推广，后勤 8 人。2018 年中期，安网团队可能会扩充到 70 人左右。

In early 2018, there are 50 team members including at least 40 software engineers, 2 for graphic design, operation and maintenance, and 8 for marketing and logistics. The team will grow to 70 members in mid 2018.

团队	Team
2018 年初安网有 50 人团队	In early 2018, there are 50 team members.
软件工程师 40 人以上；	at least 40 software engineers
运维，平面设计人员 2 人；	2 for graphic design, operation and maintenance
推广，后勤 8 人；	8 for marketing and logistics
2018 年安网团队可能会扩充到 70 人左右	The team will grow to 70 members in mid 2018.

2.2 安网顾问

2.2 Consultant Team

花松秀，比银集团董事兼创始人

Hua Songxiu, board member and founder of Bitbank;

姚远，汇币交易所 CEO

Yao Yuan, CEO of Currency Exchange;
李盈斐，比特大陆联合创始人
Li Yingfei, co-founder of Bitmain;
翟文杰，BW 联合创始人
Zhai Wenjie, co-founder of BW;
瞿佳炜，ZenithVentures 基金创始人
Qu Jiawei, founder of ZenithVentures;
耿军龙，比特世纪 CEO
Geng Junlong, CEO of BitCentury;
余芳，币看 CEO
Yu Fang, CEO of BitKan

2.3 以往开发经验

2.3 Development Experience

2012 年成立，原名嘉蓝天网，手机上网加速；	In 2012, the company was found with the original name of Jialannet, for accelerating mobile Internet speeds;
2013 年 6 月转向比特币和区块链；	In June 2013, it engaged in Bitcoin and Blockchain;
2014 年 10 月推出安网空间——中国第一个区块链隐私保护项目；	In Oct. 2014, Bankledger launched DNC - the first Blockchain privacy protection project in China.
2016 年 3 月更名为银链科技（bankledger.com）；	In March 2016, it was renamed as Bankledger.
2016 年 5 月获得天使投资，并且推动成立金链盟；	In May 2016, it acquired angel investment and founded FISCO (Financial Blockchain Shenzhen Consortium)
2016 年 9 月商业银行抵押品区块链上线；	In Sept. 2016, it launched Commercial Bank Collateral Blockchain online.
2016 年 11 月推出数字积分原型；	In Nov. 2016, it launched the digital integral prototype.
2016 年 12 月获得南京市政府 150 万资助；	In Dec. 2016, it received 1.5 million Yuan from Nanjing Municipal Government.
2017 年 3 月仓单质押融资区块链上线，获得 IBM 区块链黑客马拉松二等奖；	In March 2017, Bankledger released the warehouse receipt pledge financing Blockchain, which won the second prize in the IBM Blockchain Hackathon.
2017 年 4 月银链中间件上线	In April 2017, BMWare was set online.
2017 年 6 月开始投票链项目，7 月 1 日 ICO 成功，	In June 2017, ELT project was started; on July 1st, ICO

8 月上线交易所，9-10 月 ICO 清退；	succeeded; in August, the Exchange was launched online; and in Sept. and Oct., ICO was removed.
2017 年 11 月，投票链应用正式上线；	In Nov. 2017, ELT application was launched online officially.

安网团队在区块链应用上有深刻的商业认知、扎实的技术底蕴和丰富的开发实践经验：

The team has in-depth commercial perception on Blockchain, solid technical knowledge and rich experience on development.

申屠青春先生从 2013 年 6 月开始研究区块链和比特币，撰写了近 20 篇区块链技术文章，并且于 2017 年编著《区块链开发指南》一书，并由机械工业出版社出版；

Mr. Shentu Qingchun started his research on Blockchain and Bitcoin in June, 2013. He issued nearly 20 articles about Blockchain technology and had his book *Developer Guide for Blockchain* published at China Machine Press in 2017.

2014 年 10 月推出了主打区块链隐私保护的暗网空间项目，至今已近 3 年半时间；

Launched DarkNetSpace for Blockchain privacy protection in Oct. 2014;

2016 年 9 月发布银链联盟链（BLChain, BankLedger Consortium Blockchain）；

Released BLChain (BankLedger Consortium Blockchain) in Sept. 2016;

2016 年 9 月发布商业银行抵押品区块链；

Released the commercial bank collateral Blockchain in Sept. 2016;

2016 年 11 月发布数字积分区块链；

Released digital integral Blockchain in Nov. 2016;

2017 年 3 月发布仓单质押融资区块链；

Released the warehouse receipt pledge financing Blockchain in March 2017;

2017 年 4 月发布全球第一个区块链中间件产品——银链中间件（Bankledger Blockchain Middleware，BMWare）；

Released BMWare (Bankledger Blockchain) - the first middleware product of Blockchain in the world in April 2017;

2017 年 7 月，暗网空间正式更名为安网，并发布安网 2 钱包；

Renamed DarkNetSpace as DNC and Released DNC2 wallet in July 2017;

2017 年 12 月发布区块链投票产品——投票链（ElectionChain，ELT）；

Released ElectionChain (ELT) - a voting product on Blockchain in Dec. 2017;

2018 年 1 月分叉达世，安网 3 问世；

Released a fork Bitcoin named DASH and the SAFE in Jan. 2018;

由此可见，安网团队是一个在区块链行业耕耘近 5 年、开发过 7 个区块链项目、具有丰富的区块链开发和应用落地经验的资深团队。而安网将是安网团队后续 5 年中主打的一个最为重量级的区块链产品。

From the above, it’s easy to see that SAFE has a senior team experienced in Blockchain development and application with their seven Blockchain projects developed through five years of hard work. The team will focus on the SAFE in the coming five years as their most major Blockchain product.

2.4 联系方式

2.4 Contacts

项目官网：http://www.anwang.com；

Project website: http://www.anwang.com;

项目社区：http://www.anwang.org；

Project community: http://www.anwang.org;
中文电报群 telegram：https://t.me/safe_cn；
Chinese telegrams: https://t.me/safe_cn;
英文电报群 telegram：https://t.me/safe_anwang；
English telegrams: https://t.me/safe_anwang;
官方推特 twitter：https://twitter.com/safe_2018；
Official twitter: https://twitter.com/safe_2018;
官方 reddit：https://reddit.com/user/safe_2018；
Official reddit: https://reddit.com/user/safe_2018;
Facebook：https://www.facebook.com/anwang.safe/
Facebook: https://www.facebook.com/anwang.safe/
客服微信：elcoin666；
WeChat for customer service: elcoin666;

3 为什么分叉 DASH

3. Reason for Forking DASH

在本章节中，我们要说明如下几个问题：（1）为什么要升级安网 2（2）为什么要合并安网 2 和投票链？（3）为什么要分叉而不重开区块链？（4）为什么分叉 DASH 而不是 Bitcoin?

This section probes into reasons relating to the following questions: (1) why upgrade DNC2? (2) Why merge DNC2 and ELT? (3) Why fork instead of relaunch Blockchain? (4) Why fork DASH instead of Bitcoin?

为什么分叉 DASH	Reason for forking DASH
在本章节中，我们要说明如下几个问题：	This section probes into reason relating to questions below:
（1）为什么要升级安网 2	(1) Why upgrade DNC2?
（2）为什么要合并安网 2 和投票链？	(2) Why merge DNC2 and ELT?
（3）为什么要分叉而不重开区块链？	(3) Why fork instead of relaunch Blockchain?
（4）为什么分叉 DASH 而不是 Bitcoin?	(4) Why fork DASH instead of Bitcoin?

3.1 为什么要升级安网 2

3.1 Reason for Upgrading DNC2

安网空间 2 继承了安网空间 1 的隐私保护技术，在隐私保护方面进行了更深入的探索。

DNC2 continues using the privacy protection technology of DNC and probes into this technology.

随隐私保护而来的是在安网 2 区块链上开发应用的难度。因为安网区块链的不可分析性，使得引入智能合约、开发应用的难度也大大增加。这与我们旨在把区块链应用进一步落地的想法冲突，因而我们必须从 CryptoNote 底层区块链转向比特币类似的开放区块链，把 CryptoNote 技术当成可选项，这样就可以兼顾隐私保护技术的应用、智能合约和其他区块链应用的落地。

Requirement on privacy protection makes it difficult to develop applications on DNC2 Blockchain, because SAFE Blockchain is unanalyzable, making it harder to introduce smart contracts and develop applications. This is in conflict with our idea to further apply Blockchain applications. Therefore, we have to make transfer from CryptoNote's underlying Blockchain to open Blockchain similar to Bitcoin, regarding CryptoNote as optional, thus to realize privacy protection, smart contracts and Blockchain applications at the same time.

3.2 为什么要合并安网 2 和投票链

3.2 Reason for Merging DNC2 and ELT

投票链（ElectionChain）是安网团队于 2017 年 7 月份推出的一个 ICO 项目，代币名称 ELC。

ElectionChain is an ICO project launched by SAFE team in July 2017, with its token named as ELC.

投票链旨在研究和开发一个专门用于投票和选举、投票捐赠、投票竞猜、竞选演说和直播、竞选游戏等场景的应用。在投票链中，每个选民以真实或虚拟身份按照自己的意愿进行实名或隐私投票，能验证最终结果是否包含自己的选票。投票链用技术手段解决纸质选票、电子投票、网络投票的弊端，使得选举、决策、民意调查更加公开和透明，避免投票结果被外力干扰，让投票更可信。

ElectionChain is aimed to research and develop a Blockchain exclusive to voting for election, donation, quizzes, campaign speeches and live broadcast, and election games. In ElectionChain, each voter performs a real-name vote or anonymous vote with a real identity or virtual identity according to one's own wish, and the vote can be validated to see whether it is included in the final result. By technology, ElectionChain avoids disadvantages of paper ballots, electronic voting and network voting, making election, decision-making and public opinion poll more open and transparent, preventing man-made interference to election results, and making the vote more credible.

7 月 1 日，安网团队成功筹集了价值 2700BTC 的 BTC、ETH 和 DNC，9 月 4 日，中国央行叫停 ICO 项目之后，安网团队以 ICO 时的 ETH 价格全部退还了所有 ICO 资金，并回收了近 99.99%的 ELC 代币，同时也承诺免费赠送新的 ELT 代币给退还 ELC 的用户。2017 年 11 月份投票链 ELT 网络发布，ELT 未进行任何私募和 ICO，全部免费赠送给原 ELC 的用户。

On July 1st, the team raised BTC, ETH and DNC worth 2700BTC successfully. On Sept. 4, as the Central Bank stops the ICO project, the team returned all ICO funds at the ETH price of ICO, recalled nearly 99.99% ELC tokens, and promised to give new ELT tokens to users who had returned ELC. In Nov. 2017, when ELT website was launched, ELT gave it all to the original ELC users without any private placement and ICO.

一个团队运营两个不同方向的项目和代币，给安网团队带来不少麻烦，产品规划、技术研发、市场运营、用户关系维护都存在一些问题，征求了不少用户的意见之后，团队决定把两个项目合并。

Operating two projects and tokens of different orientations brings SAFE team with many troubles in product planning, technology R&D, market operation and user relationship maintenance. After listening to users' opinions, the team decided to merge the two projects.

合并策略很明显，安网主打底层技术应用平台的概念，而投票链是一个应用，投票完全可以在安网上发布，因而以安网为主打是一个好主意，而投票则成为安网上的一个具体应用，改名为安投。

As clear in the scheme for this merging, SAFE is mainly focused on the concept of underlying technology application platform, and ELT is an application, so a vote can be launched on SAFE. Thus, SAFE was set as the main platform supporting voting as one of its application, and then it was renamed as safe vote.

3.3 为什么要分叉而不重开区块链？

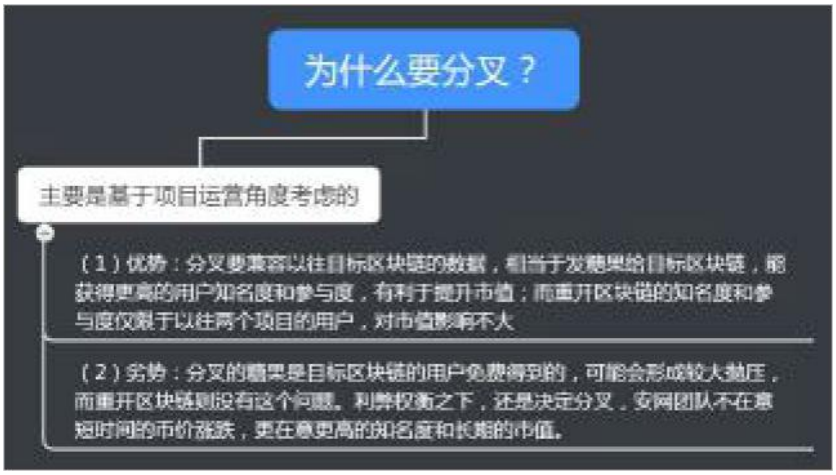
3.3 Reason for Forking Instead of Relaunching Blockchain

现在我们要升级安网 2，并且整合投票链到安网 3 中，一个技术路线的选择是基于现有优秀项目的代码来重开区块链，另一个技术路线是兼容现在优秀项目的数据来分叉。

Now we need to upgrade DNC2 and integrate ELT into SAFE. One of the technologies is selected based on existing excellent project codes to relaunch Blockchain, and the other technology shall match with existing excellent project data to fork.

为什么要分叉？主要是基于项目运营的角度来考虑的（1）优势：分叉要兼容以往目标区块链的数据，相当于发糖果给目标区块链，能获得更高的用户知名度和参与度，有利于提升市值；而重开区块链的知名度和参与度仅限于以往两个项目的用户，对市值影响不大（2）劣势：分叉的糖果是目标区块链的用户免费得到的，可能会形成较大抛压，而重开区块链则没有这个问题。利弊权衡之下，安网团队还是决定分叉，不在意短时间的币价涨跌，更在意更高的知名度和长期的市值。

The reason for forking is considered based on project operation in terms of its (1) advantage: the forking shall match with data of previous Blockchain data which means to distribute candies to the target Blockchain, to enhance user awareness, engagement and market value; while relaunching Blockchain will enhance awareness and engagement by users of only the two previous projects, which has little to do with market value; and (2) disadvantage: the forked candies to target users are gained for free, which may lead to great delivery pressure, while relaunching Blockchain will not cause such problem. From the above, the team, in spite of existing currency movements, decided to fork so as to enhance user awareness and long-term market value.



为什么要分叉	Reason for forking
主要是基于项目运营角度考虑的	Forking is considered based on project operation
1）优势：分叉要兼容以往目标区块链的数据，相当于发糖果给目标区块链，能获得更高的用户知名度和参与度，有利于提升市值；而重开区块链的知名度和参与度仅限于以往两个项目的用户，对市值影响不大	(1) Advantage: the forking shall match with data of previous Blockchain data which means to distribute candies to the target Blockchain, to enhance user awareness, engagement and market value; while relaunching Blockchain will enhance awareness and engagement by users of only the two previous projects, which has little to do with market value.
（2）劣势：分叉的糖果是目标区块链的用户免费得到的，可能会形成较大抛压，而重开区块链则没有这个问题。利弊权衡之下，安网团队还是决定分叉，不在意短时间的币价涨跌，更在意更高的知名度和长期的市值。	(2) Disadvantage: the forked candies to target users are gained for free, which may lead to great delivery pressure, while relaunching Blockchain will not cause such problem. From the above, the team, in spite of existing currency movements, decided to fork so as to enhance user awareness and long-term market value.

3.4 为什么分叉 DASH 而不是 Bitcoin？

3.4 Reason for Forking DASH Instead of Bitcoin

分叉 DASH 成为安网团队的首选，有两个主要原因：

Two reasons:

（1）DASH 和安网有相同的项目主题：即区块链上的隐私保护。

(1) DASH and SAFE share the same project subject: privacy protection on Blockchain.

（2）DASH 以比特币为基础，有不少技术创新点很吸引安网团队。比如添加了双层网络即主节点机制，并在此基础上建立了分布式社区的治理机制，有效解决了去中心化货币社区治理的问题。DASH 改进了比特币的支付，提供即时支付，使得 DASH 有挑战闪电网络的可能性。

(2) DASH based on Bitcoin features some innovations attracting the team, such as the double-layer network (masternode mechanism), and the distributed community governance mechanism established based on this network, which solves the problem of decentralized currency community governance in an effective way. DASH perfected Bitcoin payment by its in-time payment, making DASH challengeable and capable for the lightning network.

以下是 DASH 的创新点简要介绍：

The following is the innovation on DASH:

3.4.1 主节点（masternodes）网络

3.4.1 Masternode Network

除了针对 DASH 挖矿的传统工作证明（PoW）奖励之外，用户还可以运行和维护被称为主节点的特殊服务器。DASH 可以通过这种去中心化的方式来提供创新功能。

In addition to bonus to conventional PoW of DASH mining, users can run and maintain special servers called masternodes, a decentralized method via which DASH can provide innovative functions.

主节点提供以下服务：

This network provides the following services:

InstantSend 允许近乎即时的交易，InstantSend 交易四秒内确认。

InstantSend allows almost Instant Deal, with confirmation completed in 4 seconds.

PrivateSend 通过混淆区块链上的资金来源提供金融级别的隐私保护。

PrivateSend provides financial-level privacy protection by shuffling funding sources on

Blockchain.

治理和预算机制允许 Dash 的利益相关者确定项目的方向，并且投入 10％的挖矿奖励给项目和生态系统的发展。

The governance and budget mechanism allows Dash’s stakeholders to determine project orientation and inputs 10% mining bonus into development of projects and ecosystems.

主节点所有者必须拥有 1000 个 DASH，他们通过签名消息并广播到网络来证明。这些币可以在任何时候转移走，但转移将导致该主节点从主节点队列中被移走，并停止获得奖励。

Masternode owner must have 1000 DASHs, which is proved by signature message and broadcasting it in the network. These coins can be removed at any time. However, this will result in corresponding Masternode being removed from its list so there will be no more bonus for this.

DASH 的主节点有 4700 个，主节点网络很有价值；即有 60%的 DASH 币被抵押在主节点上未进入流通，这也是 DASH 价值提升的原因之一。

DASH has 4700 masternodes and the masternode network is valuable, which means 60% DASHs are mortgaged at the masternodes and out of the flow. This is one of the reasons why DASH value is enhanced.

主节点用户也可以获得提案的投票权。每一个主节点有一个投票权，投票权可以行使于预算提案或影响 DASH 的重要决定。

Users of masternodes can acquire voting rights for proposal. Each masternode has a voting right which can be used to influence important decisions such as a proposal for budgets.

主节点提供以下服务	Masternode Network provides the following services:
InstantSend 允许近乎即时的交易，InstantSend 交易四秒内确认。	InstantSend allows almost Instant Deal, with confirmation completed in 4 seconds.
PrivateSend 通过混淆区块链上的资金来源提供金融级别的隐私保护。	PrivateSend provides financial-level privacy protection by shuffling funding sources on Blockchain.
治理和预算机制允许 Dash 的利益相关者确定项目的方向，并且投入 10％的挖矿奖励给项目和生态系统的发展。	The governance and budget mechanism allows Dash’s stakeholders to determine project orientation and inputs 10% mining bonus into development of projects and ecosystems.

3.4.2 隐私支付（PrivateSend）

3.4.2 PrivateSend

PrivateSend 通过混淆资金来源为用户提供真正的财务隐私，用户钱包里的所有达世币都是由不同的“输入”组成的，我们可以把它看作是独立的、分开的币。PrivateSend 使用创新的流程将用户的输入与其他两个人的输入混合在一起，而不会让发送者的代币离开发送者的钱包。发送者始终保持对自己资金的控制。

PrivateSend realizes real financial privacy of users by shuffling funding sources. All DASHs in a user's wallet are made up of different “inputs” which can be regarded as independent and

separable coins. PrivateSend shuffles users' inputs by innovative process with the sender's token in the sender's wallet, so that the sender can control over its own money all the time.

3.4.3 即时支付（InstantTX）

3.4.3 InstantTX

DASH 通过交易锁定机制来实现即时支付。所谓交易锁定机制，首先通过交易锁定客户端请求的交易资产，通过选举算法在主节点排序靠前的 10%中选择 10 个主节点进行交易确认，选中主节点达成共识之后向全网广播，这时候所有的客户端将会遵守这些主节点达成的共识，锁定资金，避免了双花攻击。但是接受方在接收资金之后，需要在 6 个确认之后，方才可以动用这笔资产。

DASH realizes InstantTX by lock-in trade which locks the trade fund upon a client-side request, select 10 masternodes from the top 10% masternodes obtained based on the election algorithm for transaction confirmation, and then broadcast these masternodes in the network after a consensus that all client sides will obey for fund lock-in to avoid double spend attack. However, a party receiving the funds needs to make six confirmations before it can use the funds.

3.4.4 其它优点

3.4.4 Other Advantages

DASH 还包括了一些特点，包括（1）使用暗黑重力波作为难度调节算法；（2）采用软分叉机制，在发布新版本到网络但并不急于激活，只有 80%的网络参与者达成了共识，新功能才激活；（3）基于区块链的分布式治理机制，即是主节点分配 10%挖矿的收益和拥有对 DASH 的发展以及预算的投票权。

DASH features more advantages including (1) adopting dark gravity wave as the difficulty adjustment algorithm; (2) using soft fork mechanism for function activation of a new version issued in network upon a consensus by 80% network participants; (3) The distributed governance mechanism based on Blockchain enables the masternode allocate 10% of the income from mining and has the right to vote on DASH development and budget.

4 安网的商业价值

4. Commercial Value of SAFE

安网团队将打造好应用开发平台，并且围绕安付、安资、安投三大应用方向，结合第三方应用，构建一个庞大的安网生态圈。

The team will create a perfect application platform and build up a great ecosphere combining third-party application focused on safe payment, safe asset and safe vote.

4.1 应用开发

4.1 Application Development

区块链应用落地周期长，从业人才成本高，区块链难用，这些问题制约了区块链应用开发的快速落地。

Blockchain application takes long time for practical use due to limitations such as high cost on talents and difficult in Blockchain application.

安网拟简化区块链应用开发过程，并且提供一系列应用开发服务，目标用户是对区块链行业不了解、在区块链技术研发上有困难、但也想在区块链上进行应用开发及数字资产发行以获得用户信任的中小企业单位。他们只需确定区块链应用场景，发行出数字资产，专注于数字资产和现有业务的对接和应用即可。

SAFE plans to simplify Blockchain application development process, and provide a range of application development services to users especially middle and small-sized enterprises and organizations aimed to win users' trust by developing applications on Blockchain and releasing

digital assets while facing difficulties on this aspect due to little knowledge on Blockchain. All they need is to determine Blockchain application scenarios, issue digital assets and focus on connection between and application of digital assets and existing businesses.

安网能提供一整套区块链应用咨询、技术支持、协助或外包开发、代币真实应用落地服务，这将给团队带来赢利。

SAFE can provide a whole set of services like Blockchain application consulting, technical support, assistance or outsourced development and real application of tokens, which will benefit the team.

4.2 安付

4.2 Safe Payment

当安网用户量越来越多时，SAFE 就成了安网商圈内的一种通用凭证，安网用户愿意用 SAFE 来购买安网合作伙伴提供的商品和服务，安网商家愿意来接受顾客的 SAFE 支付，SAFE 的支付功能就体现出来了。

As SAFE users increasing, SAFE will become a 'general certificate' in the business circle of SAFE. With more and more SAFE users using SAFE to buy goods and services provided by SAFE's partners and more and more SAFE's sellers taking SAFE payment, this function works.

安付是安网的基础设施，安资、安投以及其他应用都会用到安付接口。安付要打通所有安网合作伙伴所提供的商品和服务使用 SAFE 及其在安网上发行的其他资产进行支付的通道；其次，则是打通基于安网发行的其它代币购买安网合作伙伴的商品和服务的通道。

Safe Payment is the infrastructure of SAFE, so safe assets, safe vote and other applications will use this interface. In light of this, Safe Payment needs to channel for payment functions for partners' goods and services using SAFE as well as other assets they released on SAFE, and also channel for purchasing partners' goods and services by using other Bitcoins released on SAFE.

安付的最大特点是即时支付和隐私支付，即时支付速度可比拟现有的第三方支付，解决了比特币的确认慢的问题；隐私支付的特点是隐藏发送人或接收人的真实地址，保护了个人隐私。安付在 DASH 的基础上新增了几种隐私支付模式如：转账备注、环签名发送、隐身收款、金额隐藏等，使得用户有更多隐私保护的选择。

Safe Payment features privacy payment and in-time payment with payment speed comparable to the existing third-party payment, which solved slow confirmation of Bitcoins. Privacy payment hides information of the sender and receiver, and thus protects personal privacy. Based on DASH, Safe Payment has more privacy-protection payment modes like transfer noting, ring signature, stealth collection and hidden amount, which strengthen user privacy protection.

4.3 安资

4.3 Safe Asset

有价值的、可转让的电子数据我们称为数字资产。安资，即基于安网的数字资产管理系统，可提供完善的数字资产发行、追加发行、转让和销毁功能，用户可以自行组合出许多种应用场景。其中有原本数字化资产，如加密货币、积分、点卡、预付卡、游戏装备、股票和股权等；也可以把物理资产数字化并且在安资中发行和转让，如法币、房产和土地、家具、各种单据，但前提是要有承兑机构。

Digital asset refers to valuable transferable electronic data. Safe Asset as a digital asset management system based on SAFE features perfect functions like digital asset issuing, additional issuance, transfer and destruction, based on which users can make their own portfolios according to different application scenarios, including original digital assets such as crypto-currency, bonus points, game cards, prepaid cards, game equipment, stock and equity, as well as physical assets

such as legal tender, house and land property, furniture and various receipts which, after being digitalized, can be issued and transferred via their special institutions.

安资的商业价值：

Business values:

（1）大大简化数字资产发行，只需在 APP 或 PC 钱包上点击几下，消耗一定数量的 SAFE，就可把资产发行出来，且安全可靠，没有编写智能合约的麻烦和大量风险；

(1) It greatly simplifies digital asset issuance by easy clicking on the APP or PC wallet, which only consumes certain amount of SAFE, to issue assets in a safe and reliable way, with no need to write smart contracts which often cause hassle and a lot of risk.

（2）在安资上发行的数字资产都有统一的图形化，SAFE 钱包支持、区块浏览器支持、支付接口对接、交易所接口对接，甚至是其他应用场景的对接，如竞猜、游戏、打赏、红包等；

(2) Digital assets issued on Safe Asset all have unified graphics, i.e. SAFE wallet and block browser supports, docking of payment interface, exchange interface and even other application scenarios such as quizzes, games, rewards and bonuses.

（3）和交易所合作，建立 SAFE 交易区，简化安资上的数字资产上交易所的流程，降低费用。

(3) By cooperating with exchanges, it establishes SAFE exchange zone, to simplify the process of transferring digital assets to exchanges and reduce costs.

每个数字资产发行方带来的众多用户都会成为安网用户以及 SAFE 的持有者，有利于建立庞大的安网生态圈。

The large number of users brought by each digital asset issuer will become SAFE users and SAFE owners, which is conducive to the establishment of a large network ecosystem.

安资的商业价值	Business values of Safe Asset
（1）大大简化数字资产发行，只需在 APP 或 PC 钱包上点击几下，消耗一定数量的 SAFE，就可把资产发行出来，且安全可靠，没有编写智能合约的麻烦和大量风险；	(1) It greatly simplifies digital asset issuance by easy clicking on the APP or PC wallet, which only consumes certain amount of SAFE, to issue assets in a safe and reliable way, with no need to write smart contracts which often cause hassle and a lot of risk.
（2）在安资上发行的数字资产都有统一的图形化，SAFE 钱包支持、区块浏览器支持、支付接口对接、交易所接口对接，甚至是其他应用场景的对接，如竞猜、游戏、打赏、红	(2) Digital assets issued on Safe Asset all have unified graphics, i.e. SAFE wallet and block browser supports, docking of payment interface, exchange interface and even other application scenarios such as quizzes, games, rewards and

包等；	bonuses.
（3）和交易所合作，建立 SAFE 交易区，简化安资上的数字资产上交易所的流程，降低费用。	(3) By cooperating with exchanges, it establishes SAFE exchange zone, to simplify the process of transferring digital assets to exchanges and reduce costs.

4.4 安投

4.4 Safe Vote

安投即投票链，投票链平移到安网 3 上之后的功能名称。安投旨在研究和开发一个专门用于投票、选举和彩票领域、能够支撑美国总统大选的区块链，并且支持投票捐赠、投票竞猜、竞选演说和直播、竞选游戏等娱乐化应用。在安投中，每个选民以真实或虚拟身份按照自己的意愿进行实名或隐私投票，能验证最终结果是否包含自己的选票。安投用技术手段解决纸质选票、电子投票、网络投票的弊端，使得选举、决策、民意调查更加公开和透明，避免投票结果被外力干扰，让投票更可信。

Safe Vote is a functional name of ElectionChain in SAFE. Safe Vote is aimed to research and develop a Blockchain exclusive to voting, election and lottery, which supports American Presidential Election as well as entertaining applications such as voting donation, voting quizzes, campaign speeches and live broadcast, and election games. In Safe Vote, each voter performs a real-name vote or anonymous vote with a real identity or virtual identity according to one's own wish, and the vote can be validated to see whether it is included in the final result. By technology, Safe Vote avoids disadvantages of paper ballots, electronic voting and network voting, making election, voting for decision-making and public opinion poll more open and transparent, preventing man-made interference to election results, and making the vote more credible.

4.4.1 应用场景

4.4.1 Application Scenarios

安投所支持的应用场景有选举、决策、民意调查、投票竞猜、彩票、捐款等，后期可能涉及竞选直播、竞选游戏之类的娱乐化应用。

Safe Vote supports election, decision-making, public opinion poll, voting quizzes, lottery, donation, as well as some related entertaining applications including election campaign live broadcast and campaign games.

投票和选举：全球所有选举和投票都可以在安投上进行，比如美国州长和总统选举、中国的人大代表投票、村委员会选举、上市公司股东投票，以及各种网络投票等；

Voting and election: all elections and voting around the world can be conducted on Safe Vote, such as U.S. governor and presidential election, NPC member election of the P. R. C., village committee member election, voting by shareholders of listed companies and various network voting activities;

决策：就某个决策或事项进行成员公投，如脱欧、动武、基建工程开工等；这种决策比较简单，是、否或不投是三种典型的态度。

Decision-making: public voting by members on certain decisions or matters such as Brexit, force use and commence of infrastructural projects. This method is simple for the voters to show their attitudes by choosing from yes, no or abstention.

民意调查：就某个主题向公民征求意见，一般以区块链问卷调查的方式进行，如总统支持率调查、对某项事情的看法等等；

Public opinion poll: seeking for opinions of citizens on certain themes such as presidential support rate and views towards something usually performed in the form of questionnaire survey on Blockchain;

投票竞猜：一般值得竞猜的主题应该是大众化的、重要的投票结果，如总统投票、脱欧等，人们可以进行竞猜哪个候选人或决策会最终胜出；

Voting quizzes: themes for voting quizzes are usually about popular and important matters such as presidential poll and Brexit. People can guess which candidate or decision will win at last;

投票捐款：人们可以在安投上对候选人进行捐款，区块链可记录下选民或非选民对候选人的捐款，使得款项更透明。

Voting donation: people can donate for candidates on Safe Vote. Blockchain can record the donation to a candidate by voters or non-voters, making the donation more transparent.

娱乐化投票：引入明星评选、竞选演说、直播和打赏、竞选游戏和其他娱乐性应用，使得投票链更有趣味性，而非政治化的项目。

Entertaining voting: with star selection, campaign speeches, live broadcast and rewards, campaign games and other entertaining applications introduced in, ElectionChain is a more interesting program, but a politicized one.

彩票：彩票的发行在中国只有获得许可的彩票机构才能进行，为避免与国家法律冲突，安投不会自行发行彩票，其中的彩票场景将与国内和国外的彩票机构合作进行。

Lottery: In China only approved lottery agencies are allowed for lottery issuance. To avoid conflict with national laws, Safe Vote will not issue lotteries by itself, and the lottery scenarios are realized by cooperating with lottery agencies at home and abroad.

4.4.2 商业价值分析

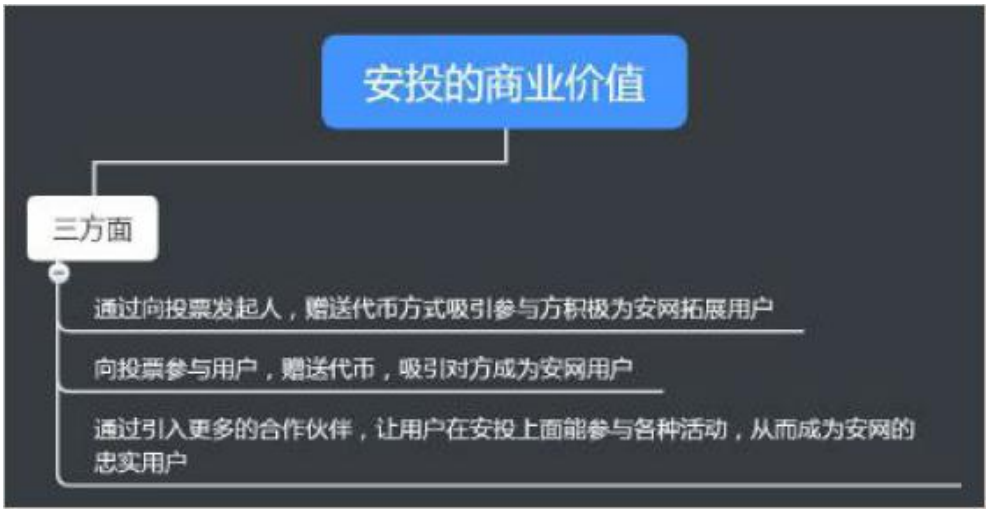
4.4.2 Analysis on Business Value

安投的应用场景众多，如果使用安投进行基层选举，一次居委会或村委会投票就能给安投带来上万用户，一次直播，可以带来潜在用户数十万，而针对明星的娱乐化投票带来的潜在用户可能有数百万。

Safe Vote applies to many scenarios. Once it is adopted for grassroots election, only one event of neighborhood or village committee voting will bring tens of thousands of users to Safe Vote. A live broadcast will bring it hundreds of thousands of potential users. As for entertainment voting for stars, the number may reach millions.

由此可见，安投的用户基数庞大，用户拓展更多是依托于安网 3 的合作伙伴来吸引用户。安投一是通过向投票发起人，赠送代币方式吸引参与方积极为安网拓展用户。二是向投票参与用户，赠送代币，吸引对方成为安网用户。三是通过引入更多的合作伙伴，让用户在安投上面能参与各种活动，从而成为安网的忠实用户。

Therefore, Safe Vote has a great number of users and develops users through SAFE partners attracting users. It develops SAFE users by encouraging participants to actively develop users for SAFE by offering tokens to voting initiators, offering tokens to user participants to make them SAFE users, and introducing more partners to provide users with more activities on Safe Vote and thus make them loyal users of SAFE.



按投的商业价值	Business Value of Safe Vote
三方面	Three aspects
通过向投票发起人，赠送代币方式吸引参与方积极为安网拓展用户	Encouraging participants to actively develop users for SAFE by offering tokens to voting initiators
向投票参与用户，赠送代币，吸引对方成为安网用户	Offering tokens to user participants to make them SAFE users
通过引入更多的合作伙伴，让用户在安投上面能参与各种活动，从而成为安网的忠实用户	Introducing more partners to provide users with more activities on Safe Vote and thus make them loyal users of SAFE

4.4.3 应用案例

4.4.3 Application Case

安投是 2017 年 11 月份推出的一个区块链投票系统，因而已经有不少应用案例。

Safe Vote as a Blockchain voting system launched in Nov. 2017 has many application cases.

2018 年 1 月 1 日至 1 月 9 日，广东惠州某学院在教育领域首创应用有别于微信投票等线上拉票方式，依托于去中心、公平、公开、公正的区块链投票系统——安投，活动期间，学院总计 15000 名学生当中，共有 8672 名学生踊跃参与投票，为主题为“给我心目中最优秀的老师发年终奖”进行评选，参与此次评选的有财经学院 44 名授课老师和 10 名班导，并最终评出了 3 名班导和 3 名授课老师作为“我心目中最优秀的老师”人选，他们不仅获得了相应的年终奖励，还获得了由安投提供的代币激励。

A college in Huizhou City, Guangdong Province first applied Safe Vote, a decentralized, fair, open and just Blockchain voting system, in education field, instead of other online voting apps such as WeChat. During the activity from Jan. 1, 2018 to Jan. 9, 2018, there were 8,672 students (15,000 in total) in the college participated in the voting themed as “Voting for Year-end Bonus for My Favorite Teachers” selected from 44 teachers and 10 instructors of the Institute of Finance and Economics. At last, 3 instructors and 3 teachers won the voting, in addition to their year-end bonuses, they were also rewarded with tokens offered by Safe Vote.

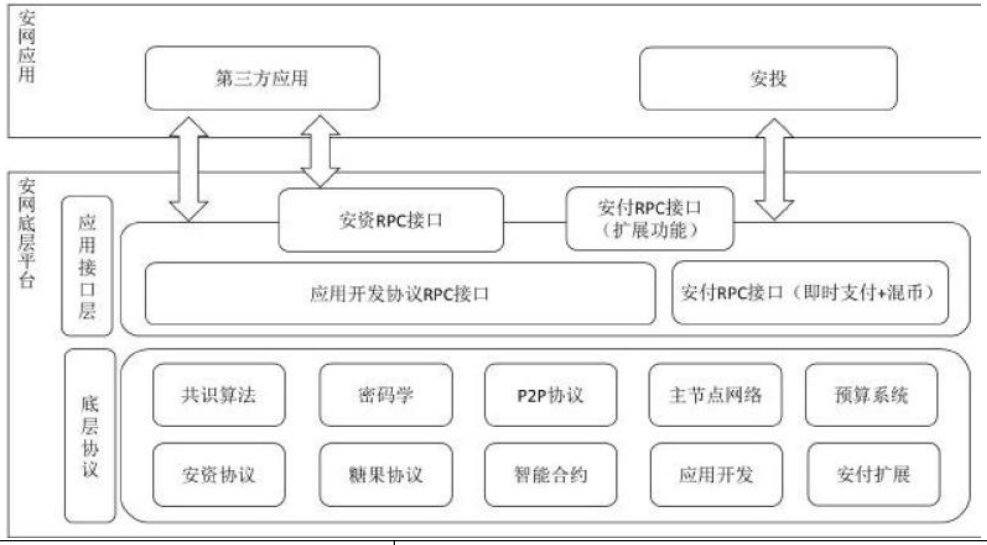
喜欢是海啸　爱就要投票	Show Your Favor　Vote for Your Favorite
投票链 支持为爱点赞	Vote Chian As long as you like, we support it.
给我的老师发年终奖 ——“惠经最优秀老师”评选	Voting for Year-end Bonus for My Favorite Teachers - Selecting“Best Teacher of Huizhou Economics and Polytechnic College”
活动截止到 2018 年 1 月 9 日 更多活动详情 请关注“深圳银链”微信公众号	Up to Jan. 9, 2018 For more information Please follow WeChat Official Account “Shenzhen Bankledger”
银链	Bankledger

5 安网的系统架构

5. System Architecture of SAFE

安网定位于关注应用安全和隐私保护的支付平台和应用开发平台，其系统架构图如下所示：

SAFE is a payment and application development platform focused on application security and privacy protection, and its system architecture is shown as follows:



安网应用	SAFE Applications
第三方应用	Third-party Application
按投	Safe Vote
安网底层平台	SAFE’s Underlying Platform
应用接口层	Application Interface Layer
安资 RPC 接口	Safe Asset RPC Interface
安付 RPC 接口（扩展功能）	Safe Payment RPC Interface (Extended Function)
应用开发协议 RPC 接口	Application Development Protocol RPC Interface
安付 RPC 接口（即时支付+混币）	Safe Payment RPC Interface (InstantTX + Coin Shuffle)
底层协议	Underlying Protocol
共识算法	Consensus Algorithm
安资协议	Safe Asset Protocol
密码学	Cryptography
糖果协议	Candy Protocol
P2P 协议	P2P Protocol
智能合约	Smart Contract
主节点网络	Masternode Network
应用开发	Application Development
预算系统	Budgeting System
安付扩展	Extended Function of Safe Payment

安网底层平台中，包括了底层协议和应用接口层，底层协议包括从 DASH 沿用过来的共识算法、密码学、P2P 协议、主节点网络、预算系统等；此外，还包括了安网独有的应用开发协议、安资协议、糖果协议、智能合约以及安付扩展功能等。

SAFE’s underlying platform includes the underlying protocol and application interface layer. The underlying protocol includes DASH’s consensus algorithm, cryptography, P2P protocol, masternode network and budgeting system, as well as SAFE’s exclusive application development protocol, safe asset protocol, candy protocol, smart contract and extended function of safe payment.

5.1 共识算法

5.1 Consensus Algorithm

安网的挖矿算法从 DASH 继承，未作修改。

SAFE’s mining algorithm is inherited from DASH without modification.

（1）使用 POW 工作量证明挖矿，X11 哈希算法，采用 11 次特定的 Hash 函数（blake、bmw、groestl、jh、keccak、skein、luffa、cubehash、shavite、simd、echo）；

(1) It uses POW for mining, X11 Hash algorithm, adopting 11 times specific Hash functions (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd and echo).

（2）挖矿可以是 CPU/GPU/ASIC，目前矿机以 ASIC 矿机为主；

(2) The mining maybe CPU/GPU/ASIC. At present, mining machines are mainly ASIC.

（3）矿工获得 45%的收益，主节点网络获得 45%收益，10%给予提案人；

(3) 45% revenue for the miner, 45% for masternode network and 10% for the proposer.

5.2 密码学算法

5.2 Cryptographic Algorithm

密码学算法从 DASH 和比特币继承而来，同时也将继承安网 2 的一些密码学算法，还将把一些新的加密算法引入，主要涉及：

The cryptographic algorithm is inherited from DASH, Bitcoin and DNC2, in addition to some new encryption algorithms introduced:

Merkle-Tree，安网使用 Merkle-Tree 生成区块中所有交易 ID 的根，以便进行数据完整性校验；

Merkle-Tree: SAFE uses roots of transaction IDs in the Merkle-Tree generation block to check data integrity.

椭圆曲线加密（ECC）算法，安网采用 secp256k1 曲线的 ECC 算法作为签名算法对交易进行签名；

Elliptic Curve Cryptography (ECC): SAFE uses ECC of secp256k1 curve as its signature algorithm to sign transactions.

哈希算法：安网采用 blake、bmw、groestl、jh、keccak、skein、luffa、cubehash、shavite、simd、echo 等哈希算法进行挖矿；

Hash algorithm: SAFE uses Hash algorithm for mining, such as blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd and echo.

环签名支付：安付拟采用环签名算法进行支付，以便隐藏发送人；

Payment by ring signature: Safe Payment plans to adopt ring signature for payment, so as to hide the sender.

隐身收款：安付拟采用隐身地址技术进行隐身收款，以便隐藏接收人；

Stealth collection: Safe Payment plans to adopt stealth address technology for stealth collection, so as to hide the receiver.

同态技术：安付拟采用同态加密技术对金额进行加密隐藏；

Homomorphic encryption: Safe Payment plans to adopt homomorphic encryption to encrypt and hide the amount.

5.3 主节点网络

5.3 Masternode Network

主节点网络是 DASH 最重要的基础设施，同样也被安网继承。一个主节点的建立需要抵押 1000 个 SAFE，得到 45%的全网挖矿收益，DASH 上线 4 年，主节点数量有 4700 个，安网上线两个月，至 3 月 25 日已有 1900 个主节点。

Masternode network is DASH's most important infrastructure inherited by SAFE. Creation of a masternode requires 1,000 SAFEs to be mortgaged, to obtain 45% mining revenue of the whole network. DASH has been launched online for 4 years and now has 4,700 masternodes, while SAFE

has been launched online for 2 months and has 1,900 masternodes up to March 25.

主节点承担了安网的即时支付、隐私支付、对提案项目投票等功能，还将承担更多的功能。我们希望安网中的主节点数量越多、分布越广泛、且比较稳定。因此从以下几个方面改进主节点建立：

Masternode functions on SAFE now include InstantTX, privacy payment and voting on proposed items in addition to many future functions. To make sure that there are as many wide-distributed stable masternodes as possible on SAFE, masternode establishment shall be modified at the following aspects:

（1）一键部署主节点工具，在工具设置好 VPS 服务器 IP 地址、密码，就能一键部署，使得部署更加方便、快速；目前支持阿里云，后续会支持更多 VPS 提供商；

(1) One-key masternode deployment tool: the convenient and fast one-key deployment will be available once the IP address and password of VPS server are set in the tool. The tool support Aliyun now, and will support more VPS providers later.

（2）升级主节点工具，升级主节点要求方便、快速，以满足安网快速的应用研发和升级；

(2) Masternode updating tool: Masternode updating shall be convenient and fast, to meet requirements for rapid application development and upgrades of SAFE.

（3）更改主节点机制，1000 个 SAFE 锁定 6 个月以上才能建立主节点；

(3) Masternode modifying mechanism: the masternode can be established only when 1000 SAFEs are locked for at least 6 months.

（4）后续将视情况提供主节点硬件盒子及配置工具，硬件盒子连接上网线，用工具配置完成后，即可成为主节点，不必购买 VPS 服务器，节省成本；

(4) Later, masternode hardware box and configuration tools will be available. Masternode can be established by connecting the hardware box with network cables before configuration by the tools. There is no need to buy VPS server, so the cost is low.

未来安网有望达到 1 万个主节点以上，有可能超越比特币成为全球最大的主节点网络。

SAFE is expected to have more than 10,000 masternodes surpassing Bitcoin and become the world's largest masternode network.

币种	Currency
全网节点	Whole Network Nodes
算力	Hash Rate
区块浏览器	Block Browser
日理论收益	Daily Theoretical Earnings
每全网节点	Per Whole Network Node
价格	Price
主节点教程	Masternode Tutorial
收益计算器	Income Calculator

5.4 预算系统

5.4 Budgeting System

预算系统是从 DASH 继承的一个很有特色的社区治理结构。安网每个区块的挖矿收益中，

有 10%（每月 7000 个 SAFE）未产生，而是要到月底通过“超级块”产生。

The budget system is a distinctive community governance structure inherited from DASH. In each block of SAFE, there is 10% mining earning (7000 SAFEs per month) generated by “superblocks” at the end of each month.

整个月中，任何人均可向安网提出预算申请，由主节点用户投票决定，任何提案只要获得至少 10%的网络主节点的同意，到月底将会创建一系列的“超级块”，向已批准的提案支付 SAFE，用于资助那些对安网社区发展有帮助的推广项目或研发项目。

During this month, anyone can apply to SAFE for budget, which will be determined after voting by masternode users. Any proposal needs to obtain the agreement of 10% of the masternodes, based on which a series of “superblocks” will be created at the end of the month, to pay the SAFE consumed by the approved proposal with a view to funding the promotional projects and research programs conducive to the development of SAFE communities.

5.5 应用开发协议

5.5 Application Development Protocol

安网提供了一套基于安网开发区块链应用的标准协议，这是成为应用开发平台的第一步。应用开发协议的设计目的：让想实施“区块链+”战略的企事业单位能非常容易地开发区块链应用。安付的扩展功能、安资、安投就是在安网应用开发协议上的应用范例。基于安网开发的应用，我们称之为 Safeapp，简称 Sapp。

SAFE provides a set of standard protocols for developing it Blockchain applications to make it an application development platform. These application development protocols are aimed to help enterprises and institutions to develop Blockchain applications so as to implement their “Blockchain+” strategies. The extended functions of Safe Payment, Safe Asset and Safe Investment are examples of applying development protocols on SAFE. Applications developed based on SAFE are called Safeapp (Sapp).

应用开发协议包括应用注册、应用权限设定、应用数据写入与更新、应用数据检索和查询等接口，因而 Sapp 应用开发的流程即：应用注册->权限设定->应用开发->应用部署->应用运行。

Application development protocols include application registration, settings of application rights, read-in and update of application data, and retrieval and query of application data. So Sapp application development processes are: application registration -> settings of rights -> application development -> application deployment -> application operation.

安网应用必须先在安网上进行 Sapp 应用注册，才能被全网接受和辨识。注册过程无需任何人审核，只要燃烧一定数量的 SAFE 且应用名称不冲突，注册交易就可被全网接受，注册通过。

SAFE application first must be registered as Sapp on SAFE so as to be accepted and identified. The registration need no review but consuming certain amount of SAFE with non-conflict application names. When the registration is passed, the registered transaction can be identified on SAFE.

应用权限设定，定义哪些用户可以访问哪些应用命令，这些应用命令由开发商自定义，但安网能帮助开发商来定义用户对应用命令的访问控制权限。某个用户要写入某一应用命令到区块链且把交易广播到全网时，所有节点和客户端都按照访问控制权限表检查其访问权限，无权限的操作交易将被拒绝。

Settings of application rights are used to define users allowed to access certain application commands. These application commands are customized by the developer, but SAFE can help

developers define users' access control rights to application commands. When a user writes an application command to the Blockchain and broadcasts a transaction to the entire network, all nodes and clients will check their access rights according to the table for access control rights, and unauthorized operation transactions will be rejected.

应用部署方法，除安付和安资外，其他应用都以 RPC 接口方式与安网对接，开发商仅在需要的节点部署 Sapp 即可，无需在全网部署。

Application deployment method: Except for Safe Payment and Safe Asset, other applications can connect to SAFE as RPC interfaces. Developers can deploy Sapp only on nodes they need.

数据检索是方便本地应用数据查询的方法，所有的安网 Sapp 的数据都将在安网节点中存贮，未部署相应 Sapp 的节点能辨别是哪个 ID 的 Sapp 数据，但是无法正确解析出具体 Sapp 数据。

Data retrieval is a convenient way to query local application data. All Sapp data on SAFE will be stored in its nodes. Nodes with no Sapp deployed on can identify ID of the Sapp app, but cannot properly parse the specific Sapp data.

安网应用开发协议使得在安网上开发 Sapp 更标准化和便捷化，且无需开发任何智能合约，很容易与区块链中间件结合，提供安网的中间件 API 和 SDK，进一步简化应用的开发。

SAFE's application development protocol enables more standardized and convenient development of applications on the platform, without developing any smart contracts, which is easy to be combined with Blockchain middleware, and provides SAFE's middleware API and SDK, further simplifying application development.

5.6 安资协议

5.6 Safe Asset Protocol

有价值、可转让的数据我们称之为资产，比如积分、数字货币、单据、征信、保险、贷款、数字人民币等等。安资协议，即安网资产管理协议，提供了数字资产发行、追加发行、转让、销毁、发糖果、领糖果、查询等多种操作，开发者可以自行组合出许多种应用场景，如数字货币发行和转让；提货单发行、转让与销毁；甚至可以同时发行积分和数字人民币几点，并且在一定汇率下进行兑换等。

Asset here refers to valuable transferable data such as bonus points, digital currency, receipts, credit, insurance, loan and digital RMB. Safe Asset protocol as SAFE's asset management protocol provides multiple operations such as digital asset issuance, additional issuance, transfer, destruction, candy distribution and candy acquisition and query, based on which users can make their own portfolios for different application scenarios, such as digital currency issuance and transfer; Bill of lading issuance, transfer and destruction; and even issue bonus points and digital RMB at the same time, and exchange them at certain exchange rates.

安网仅提供一个资产发行的平台，不对所发行资产进行背书与审核。资产发行方只要燃烧 500SAFE（按时间递减，最少 50SAFE）、资产名称不重名、几个点击操作即可发行出数字资产。安网钱包、区块链浏览器、交易所接口、支付接口都将自动支持，大大降低了开发商的数字资产发行成本和时间。

SAFE provides a platform for asset issuance without endorsement and audit on the issued assets. So asset issuer can issue a digital asset with a unique name by burning 500SAFE (at least 50SAFE, decreasing with time) with a few clicks. SAFE wallet, Blockchain browser, exchange interface and payment interface will provide automatic supports, greatly reducing developers' cost and time on digital asset issuance.

安网上的资产统一使用安网地址来接收和发送，需要消耗以 SAFE 计价的交易费。安网

团队还将在多个交易所开启 SAFE 交易区，安网上的代币将与 SAFE 形成交易对，方便安网生态的建立。

All SAFE assets are sent from and received at SAFE addresses, which consume transaction fees priced in SAFE. The team will launch SAFE exchange zones at multiple exchanges, and tokens on SAFE will form transaction pairs with SAFE to facilitate the establishment of the network ecosystem.

5.7 糖果协议

5.7 Candy Protocol

糖果协议是属于安资协议中一个很有特色的协议。主要思想是：在通过安资协议发行代币时，代币发行方需要把新发行代币的 0.1%~10%分给安网 SAFE 的持有者，具体比例由代币发行方指定。

Candy protocol is a special agreement in Safe Asset Protocol System, and its main philosophy is that token issuer needs to give 0.1%~10% of newly-issued tokens to the SAFE holders at a specific ratio designated by the issuer, when issuing tokens according to Safe Asset Protocol.

主要的技术思路：发行代币时，同时发送 0.1%~10%的新代币到一个糖果地址， SAFE 持有者在钱包中手动点击可领取的糖果，发出一个领取糖果的交易，即可把该糖果地址中属于自己的部分领取。糖果将在 1-6 个月内到期（由发行方定义），到期后将不能再领取；如果 SAFE 持有者没领取，则属于他的糖果就永远沉没，其他人也无法领取。

Its main technological idea is that during the issuance of the tokens, 0.1%~10% of them should be sent to a new candy address, facilitating the SAFE holders to take candies of their own just by clicking the wallet and making a candy-taking transaction. These candies can only be obtained between 1 and 6 months (the specific time is determined by the issuer). The candies which are not taken by the SAFE holders within the validity period will be unobtainable forever for anyone.

领取规则（1）以资产发行时的区块为快照计算糖果数量（2）SAFE 地址中必须有大于等于 1 的 SAFE 数量，否则不能领取（3）按照比例领取糖果，计算方法：你的糖果数量=全网该糖果的发放数量 * (本钱包 SAFE 数量/全网已生产出的 SAFE 数量)，如果可领取的糖果数量小于 0.01，则也不能领取（4）每种糖果仅允许一次性领取完毕，不可多次领取（5）糖果如果已经过期，不能领取。

Rules to obtain these candies:

1. The number of candies is calculated according to the block snapshot at the time when the asset is issued.
2. Only when the number of SAFEs in the SAFE address is no less than 1, the candies can be obtained.
3. The candies are taken in proportion by an Eq. – the number of your candies = the issuance volume of the candies in the whole network * (the number of SAFEs in the wallet / the number of SAFEs produced in the whole network), if the number of available candies is less than 0.01, the candies can’t be obtained.
4. Each kind of candies must be taken away at one time.
5. The candies can only be obtainable within the validity period.

5.8 智能合约

5.8 Smart Contract

智能合约目前面临较大的安全性风险，因而安网并未将智能合约作为首推应用，而是先用各种协议来安全地满足应用开发的需求，一些更为复杂的应用可能要用到智能合约，因而安网也将在后期引入智能合约。

Currently, smart contract is facing a great risk in security, so SAFE uses many other protocols to meet the requirements of application development, instead of taking smart contract as a primary application. However, some more complicated applications are likely to need smart contract, so SAFE will introduce smart contract later.

目前的技术路线是移植以太坊 EVM 到安网上，以太坊智能合约在自由社区的应用比较广泛，因而需要首先支持。EVM 在类比特币区块链上的移植已经有一些案例，安网将参考这些技术路线和自身对智能合约安全性的理解，制定一些智能合约的安全规则和权限访问体系，形成独有的智能合约虚拟机 SVM。

At present, the technical route is to apply EVM as a priority to SAFE, because EVM smart contract has a wider application in free community. There are already some cases revealing successful application of EVM to bitcoin-like Blockchain, SAFE will refer to these technical routes and knowledge on smart contract security, to formulate some security rules on smart contract and access permission system, thus forming a unique SVM – smart-contract virtual machine.

SVM 将在以下方面加强智能合约的安全性：

SVM will enhance the security of smart contract in the following aspects:

（1）智能合约代码必须开源，且在发布智能合约时需提供代码库地址和版本号、源代码的哈希，防止源代码与编译后的代码不一致；

(1) The code of smart contract must be open source code. Meanwhile, when smart contract is issued, the codebase address and version number, and Hash of source code must be provided to prevent the inconsistence between the source code and the code compiled.

（2）智能合约接口的访问控制，目前不少智能合约被攻击，原因在于任何人都可以访问智能合约的任何接口，因而在某些接口检查运行权限不严格的情况下，将被非法访问者获得更高权限；访问控制可设置只有许可的地址才能访问指定的智能合约接口，增强安全性。

(2) Access control on smart contract interface. Many smart contracts have currently been attacked. The reason behind this is that all interfaces are accessible to anyone. Therefore, in case of a loose check on some interfaces, the illegal visitors will obtain elevated permission; access control can make a setting only allowing authorized addresses to access to some designated smart contract interfaces, thus enhancing the security of smart contract.

（3）智能合约的冻结和解冻机制，一旦出现紧急事件，开发商可将智能合约冻结，同时也冻结了其中的资金，等待合适的处理措施出现后再解冻。具体机制等待智能合约引入的具体文档。

(3) Frozen smart contract and its thawing mechanism. In case of emergency, the developers can frozen smart contract and the asset in it, and thaw the smart contract when proper countermeasures are taken. The specific mechanism depends on the specific documents introduced by smart contract.

5.9 安付扩展

5.9 Extension of Safe Payment

目前 DASH 底层已经提供实时支付和隐私发送的功能，安付还将进一步拓展，主要有以下几个功能：

The DASH underlying technology has currently offered real-time payment and privacy sending. Meanwhile, Safe Payment will be further extended and have the following functions:

5.9.1 增加转账备注

5.9.1 Transfer note

每一笔转账交易都可以写一段备注进去，以便后续查看，这个备注将写到区块链上，可以是明文或加密的文本，也方便用户在区块链上作个人记录。

Every transfer transaction can be recorded by a note, to facilitate subsequent review, the note will be written on Blockchain in the form of cleartext or encrypted text, to facilitate users to make personal records on Blockchain.

5.9.2 环签名发送

5.9.2 Ring signature dispatch

环签名发送是安网 2 中的隐私支付功能之一，其特点：(1)签名者任意选取用户公钥参与签名，不必通知被选用户；(2)不可伪造：外部敌手不知道任何成员私钥，不能伪造合法签名；(3)无条件隐私：攻击者即便获得所有可能的签名者私钥，签名者被辨认的概率不超过 1/n，其中 n 为可能签名者个数。使用环签名技术，隐藏了发送者，相当于实现了一次混币。

Ring signature dispatch as one of PrivateSend functions in DNC2 includes the following features: (1) signers can select public key for any user to take part in the signature, with no need to inform the user; (2) unforgeability: any private key of any user is unavailable to outsiders, so forging a legal signature is impossible; (3) unconditioned privacy: even if attackers can obtain all possible private keys of signers, the possibility of recognizing the signers is less than 1/n, where n means the number of signers. The sender is hidden because of the ring signature technology, which is equivalent to carrying out a coin shuffle.

安网 3 将继承该技术，实现环签名发送。

SAFE will continue to carry forward this technology, and make efforts to realize ring signature dispatch.

5.9.3 隐身收款

5.9.3 Stealth collection

隐身地址同样是 CryptoNote 首先使用的隐私技术，源自椭圆曲线密钥交换协议（ECDH）。

接收者公开一个特殊地址称为隐身地址，发送者向该地址发送 SAFE，并且附带一个一次性公钥，敌手没法从公开地址中找到任何交易，但是接收者根据附带公钥计算出正确的接收地址和私钥，从而收到币。

Stealth address is the privacy technology initially used by CryptoNote, sourced from the ECDH. The receiver uncovers a special address called stealth address, the sender sends SAFE to this address, attached with a one-time public key, the rival is unable to find any transaction from this open address, but the receiver can get tokens by working out the correct receiving address and private key according to the attached public key.

环签名发送和隐身收款可以组成一个更隐私的交易。

The combination of ring signature dispatch and stealth collection can form a more private transaction.

5.9.4 金额隐藏

5.9.4 Hidden amount

同态加密是基于数学难题的计算复杂性理论的密码学技术。对经过同态加密的数据处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。

Homomorphic encryption is difficult math problem-based cryptography computing complicated theories. According to the data processing by homomorphic encryption, an output is gained and then decoded. The corresponding result is in great agreement with that of unencrypted raw data by the same method.

这种特性适用于金额隐藏，即 A 向 B 发送了金额 X，其他人看不到具体金额，但是（1）能够验证 X 的金额不会超过 A 所拥有的金额（2）B 可以解密出来金额且可以后续花费。

The feature is applicable to hidden amount. If A sends B the amount of X, which can't be seen by others, but (1) it is confirmed that the amount of X will not exceed that possessed by A; (2) B can decrypt the amount and can spend it.

5.10 P2P 协议

5.10 P2P protocol

安网的 P2P 协议延用比特币的 P2P 协议框架，在此基础上进行了一些扩展以适应后续的即时消息和去中心化存贮的需求，技术方案另行公布。

P2P protocol of SAFE continues to use P2P protocol framework of Bitcoin, based on which some extensions are made to apply to the subsequent requirements of instant message and decentralized storage. The relevant technical scheme will be announced separately.

6 安网的技术方案

6 Technical Scheme of SAFE

安网的技术方案包括分叉方案、应用开发体系技术方案、各个应用的技术方案等。这些技术方案有些已经成功实施，有些正在研发，有些还处于规划阶段，因而有可能有变动，请以最新的白皮书为准。安投在安网上的技术实现方案将另行公布。

Technical scheme for SAFE includes fork scheme, technical scheme on application development system and technical schemes on various applications. Some of them have already been successfully implemented, some are under research and development, and some are still being planned. Therefore, please refer to the latest white paper, lest these schemes might have some modifications. The technical implementation scheme of safe vote for SAFE will be announced separately.

6.1 分叉技术方案

6.1 Technical Scheme on Fork

6.1.1 分叉原理

6.1.1 Principles of fork

在区块高度 807085 进行分叉（即北京时间 2018 年 1 月 20 日上午 10：30 左右），由程序硬编码产生第 807085 个区块，该区块称为 SAFE 创世块。在这个区块里面，只有一个 coinbase 交易，输出 2100 万个 SAFE 到官方的钱包地址，没有矿工奖励。该区块的难度重置为 DASH 创世块难度、Nonce 为 0。矿工后续从区块高度 807086 开始挖，coinbase 输出恢复到原来 DASH 的奖励规则。

The fork was made at block height of 807085 around 10: 30 am, January 20, 2018, and then the 807085th block produced by hard-coded procedure is known as the creation block of SAFE, in which there is only one coinbase transaction, outputting 21 million SAFEs to the official wallet address, without mining bonus. The difficulty of this block is reset to that of DASH creation block, with Nonce being 0. Miners began to dig from the block height of 807086, thus, coinbase output is recovered to the original DASH rewarding rule.

6.1.2 相关参数

6.1.2 Relevant parameters

6.1.3 配置文件

6.1.3 Configuration files

·数据存放路径

Route to save data

Linux：/root/.safe

Windows:C:\Users\用户名\AppData\Roaming\Safe

·配置文件名

Names of configuration files

Linux:/root/.safe/safe.conf

Windows:C:\Users\用户名\AppData\Roaming\Safe\safe.conf

6.1.4 交易结构

6.1.4 Transaction structure

从区块高度 807085 开始，在交易结构的输出中，增加了两个字段：

There are two fields added in the output of transaction structure, starting from the block height of 807085:

（1）从区块高度 807085 开始 ，交易版本号(nVersion)为 101，以前 DASH 交易版本号为 1；

(1) From the block height of 807085, the transaction version or nVersion is changed into 101, while the previous DASH nVersion is 1;

（2）nUnlockHeight 字段，预留以后增加 SAFE 锁定功能，默认值为 0；

(2) After nUnlockHeight field is reserved, a new function to lock SAFE is added, with the default of 0.

（3）vReserve 字段，称为应用数据区，应用数据区最大长度为 3000 字节，最小为 4 个字节小写“safe”，以便于开发应用，比如：安资、安投、安付、智能合约等；

(3) vReserve field, known as application data area, has the maximum 3,000 bytes and the minimum 4 bytes of lower-case letter “safe”, to facilitate the application development, such as safe asset, safe vote, safe payment and smart contract.

6.1.5 区块难度和奖励

6.1.5 Block difficulty and bonus

（1）从区块高度 807085 开始，这个块的难度为 DASH 创世块的难度，后面区块的难度规则有变化，规则为：前 100 个区块采用 BTC 计算规则，再后 100 个区块采用 KGW 计算规则，200 个块完成后切换到 DGW 计算规则；因而前 200 个区块的产出会比较快，后续使用 DGW 难度调整算法后，会迅速维持在 2.5 分钟左右；

(1) From the block height of 807085, the block difficulty is equal to that of DASH creation block, while the difficulty of the subsequently-generated blocks has some changes as per the rules: the first 100 blocks adopt BTC computation rule, the second 100 blocks adopt KGW computation rule, after that, the computation rule is switch to DGW. Therefore, the first 200 blocks are generated fast. With adoption of DGW computation rule, the time of generating 200 blocks will keep around 2.5 minutes.

（2）因为降低了难度，为了保证 SAFE 的挖矿产出量与 DASH 一致，从区块高度 807086 开始，区块产量算法有所变化。DASH 的区块产量 2222222/(((Difficulty+2600)/9)^2)，最低 5 个 DASH，最高 25 个 DASH。而 SAFE 则改为最高最低都为 5 个 SAFE，以保证区块产量与 SAFE 官方公布的币数量基本一致。不过也导致后续的行为有些不同，DASH 在难度突降时，有可能会提高区块产量，而 SAFE 不会；

(2) Because of the reduction of the difficulty, the algorithm for block production changes from the block height of 807086, to ensure a same mining output by SAFE as that by DASH. The block production by DASH that is 5 at minimum and 25 at maximum is 2222222/(((Difficulty+2600)/9)^2), while the number of SAFEs for the block production is 5 at minimum and maximum, to ensure that the block production and the number of tokens are basically the same as the figures officially released. However, the subsequent activity may be impacted. As the difficulty is reduced, the block production may be increased by DASH, but it will remain the same by SAFE.

6.1.6 矿池

6.1.6 Mine pool

矿池需要配合修改如下：

The mine pool needs to be modified in the following aspects:

（1）从区块高度 807085 开始，交易版本号 101；生成区块时在 coinbase 输出结构中增加 vReserve、nUnlockHeight 两个字段；vReserver 大小为 4 个字节，内容为小写“safe”；nUnlockHeight 值为 0；

(1) From the block height of 807085, the nVersion is changed into 101; when the block is generated, the two fields of vReserve and nUnlockHeight are added into coinbase output structure; vReserver has 4 bytes constituted by a lower-case letter “safe”; the value of nUnlockHeight is 0.

（2）如果使用 DASH 的存放区块数据的目录，需要删除 DASH 有关文件；

(2) If the list for DASH block data storage is needed, the relevant DASH documents need to be deleted;

6.2 应用开发协议

6.2 Application Development Protocol

我们扩展了交易的输出结构（见 6.1.4），其中的应用数据区用于存贮应用数据，比如安付、安资、安投的数据，以及其他第三方应用写入的数据。

We have extended the output structure of transactions (see 6.1.4), with an application area to store application data including the data of safe payment, safe asset and safe vote, and other data written by the third party.

应用开发接口包括了应用注册、应用权限设定、应用数据写入等几种常用接口，定义了谁有权限写入数据、有权限写入什么数据的问题。

Application development interfaces include some common interfaces such as application registration, application permission setting and application data writing, defining who has the permission to write data and what kind of data can be written.

目前任何人都可以低成本写入任何数据到公有链如比特币和以太坊，造成区块链上垃圾数据泛滥，安网不希望应用开发接口被滥用，更不希望出现垃圾数据。

At present, anyone can write any data to the public chain like bitcoin and EVM at a low cost, leading to a flooding of rubbish data on Blockchain. SAFE hopes not to abuse the application development interfaces and not to generate rubbish data.

以下应用开发接口的调用都需要消耗 SAFE，因而通过 RPC 进行调用时，请确保提供 RPC 服务的 SAFE 节点开启了钱包功能，并且有足够的 SAFE 金额。

SAFE is needed for the calls of the following application development interfaces. Therefore, if the calls are made via RPC, please ensure the SAFE node providing RPC service opens the wallet function, and has enough SAFEs.

应用数据区中，应用头结构如下：

In the application data area, the structure of application head is as follows:

应用数据区 Application data area	说明 Statement
safe	安网应用标识，小写 SAFE sign in low case
版本号 Version	应用头版本号 Version of application head
应用 ID Application ID	系统分配的全网唯一应用 ID The only whole-network application ID distributed by system
应用命令 Application command	应用数据中的应用命令，由用户自定义 Application command in application data, defined by users

其中应用命令本应该是应用数据区的内容，但安网将之提前到应用头结构中，其目的是为了能让安网底层辨识应用命令，进行应用权限控制，保证应用接口的安全性。

Application command is supposed to be included in the application data area, but SAFE places it

in the application-head structure, to enable the SAFE underlying identification application command to conduct application permission control, thus ensuring the security of application interfaces.

6.2.1 应用注册

6.2.1 Application registration

应用注册是应用开发的前提，只有注册的应用才能被安网所辨识，安网节点和钱包才会把应用数据归类到正确的应用 ID 名下，方便后续的检索和查询；未注册的应用写入数据到应用数据区，将会被全网拒绝。

Application registration is the prerequisite of application development. Only registered applications can be identified by SAFE, and SAFE node and wallet can classify the application data into the correct application ID for subsequent retrieval and query; the data in the application area written by unregistered ones will be rejected by the whole network.

应用注册费用：注册应用时需要燃烧 500 枚 SAFE，该金额每过 17280 个区块（大约 1 个月时间）减少 5%，直到最低 50 枚，目的是让安网应用开发方更慎重地考虑是否开发安网应用，保证安网上的应用数据都是有价值的，避免垃圾数据加重安网的存贮负担。但在安网测试网络上，无需任何应用注册费用，以方便用户测试应用。

Application registration fee: 500 SAFEs are burnt for application registration. This figure reduces by 5% every 17,280 SAFEs until the figure reduces to 50, aiming to enable SAFE application developer to prudently consider whether the SAFE application should be developed, thus ensuring the application data is valuable, and preventing the rubbish data from burdening the SAFE storage. However, application registration fee is no needed on the network testing SAFE, to facilitate users to test applications.

应用注册时向安网全网广播一个应用注册的交易，声明该应用名称、开发商、网站、应用 LOGO 的 URL、应用封面图 URL、网址及简要介绍等，应用名称应该是全网唯一的。同时支付充足的应用注册费用到一个特定的黑洞地址以燃烧 SAFE，任何人都无法找回被燃烧的 SAFE。

During application registration, a transaction for application registration needs to be broadcasted to the whole network, elaborating the application name, developer, website, URL of application LOGO, URL of application cover, website address and a brief introduction. The application name must be different from all other names on the whole network. Then pay for corresponding registration fee to the given blackhole address to burn SAFEs. Nobody can retrieve the SAFEs burnt.

应用注册无需任何机构审核，只需燃烧足够 SAFE，并且保证应用名称是唯一的，即可获得应用 ID、交易 ID 和管理员地址。该应用注册交易被打包到区块被全网接受，即可在交易中写入应用数据。

Application registration does not require the review of any institute, just needs to burn enough SAFEs and ensures its name is unique on the whole network, then application ID, transaction ID and manager address can be obtained. Once the application registration transaction is sent to the block and accepted by the whole network, application data can be written in it.

其中应用 ID 在后续的应用数据写入中都要用到；交易 ID 用来检查交易详情；管理员地址则是 SAFE 钱包中的一个地址，默认情况是支付 SAFE 的那个地址，如果这样的地址有多个，则会自动选择第一个地址。

Application ID will be often used in the subsequent application data writing; transaction ID is to check the transaction details; manager address as an address in SAFE wallet is for receiving SAFEs

in case of default, if there are several manager addresses, the first address will be automatically selected.

6.2.2 应用命令设计

6.2.2 Design of application command

注册好应用，一定要先进行应用命令设计，相当于对安网应用的应用场景进行系统分析和需求提取。从技术原理上说，一个应用命令就像一个智能合约的函数，智能合约的函数谁都可以调用，因而智能合约需要在每个函数开头做权限控制，不让无关的用户来调用。

After application registration, design of application command needs to be done first, which is equivalent to systematically analyzing application scenarios for SAFE and spotting the demands. From technology point of view, one application command is like a smart contract function that can be called by anyone, so smart contract needs to do permission control on each function, so that unrelated users are unable to call these functions.

安网的应用开发体系规定：应用权限可细化到应用命令，即安网底层可控制哪些人可以调用哪些应用命令，其他人则不可以。而读取所有应用数据的权限是所有地址都具备的天然权限，不再另外提起。

According to the rules for SAFE application development system, application permission is elaborated to application command, i.e. SAFE underlying technology decides who can call the application commands and which kind of commands can be called. The permission to read all application data is the natural permission for all addresses, which will not be mentioned separately.

举例来说明应用命令设计过程。有一个在线电影票订购系统，商家发布电影票信息，买家下订单且付款，由商家发送电影票 ID，买家收到电影票 ID、买家去电影院出示 ID 看电影。这个应用涉及的应用命令设计如下所示：

Now we will take an example to describe the whole design process of application command. Sellers launch information on film tickets on an online movie ticket ordering system, to facilitate buyers to make an order and payment, they will send ticket ID to the buyers, then the buyers can go to cinema to watch movie by showing the ID. The application command design related to the application is shown as follows:

发起人 Initiator 应用命令 Application command	所有人 All people	商家 Seller	开发商 Developer
注册商家 Registered sellers	√		
商家审核结果 Review results on sellers			√
发布电影票信息 Launch information on movie tickets		√	
付款下订单 Make an order and payment	√		
发送电影票 ID Send ticket ID		√	

上表内只有打勾的框内才是正确的应用命令，如所有人都可以注册商家、开发商对要注册的商家进行审核并且发送审核结果、商家发布电影票信息等。只有明确地画出上述应用设计表，才能进行下一步操作。

The “√” in the table represents correct application commands. That is, all people can become a

seller after registration, developers are responsible to review these registered sellers and then send relevant results, after that, the sellers passed the review can launch information on movie tickets. Only when the table for application design is mapped out, can the next operation be done.

6.2.3 应用权限设定

6.2.3 Application permission setting

安网的应用权限体系是指某些公钥或地址对应用数据的写和更新权限，也涉及更细化的对某些应用数据中具体应用命令的写和更新的权限。经过上述的应用命令设计后，就可以很容易进行应用权限规则化。

SAFE application permission system is the permissions of writing and updating application data through some public keys or addresses, also refers to the permissions that detail the writing and update for specific application commands in some application data. With the above-mentioned design on application command, it is easy to regularize application permission.

应用权限设定接口必须由管理员地址来调用；管理员地址同时也是默认情况下唯一有权限写入应用数据的地址，而无需理会应用权限的规则。但一个应用的管理员不能去定义另一应用的权限。

The interface for application permission setting must be called by manager address that is the only authorized address to write application data in case of default, and is not restrained by the rules for application permission. However, the manager in charge of one application is not allowed to define the permission of another application.

通过该接口，管理员可增加、删除、更新某些公钥或地址的操作权限，如果地址为 0 则意味着指代所有公钥或地址，如果权限为 0 则指所有应用命令。下面举例说明：

Through this interface, the manager can add, delete or update the operation permission of some public keys or addresses. If the address is 0, it represents all public keys or addresses; if the permission is 0, it represents all application commands. See the following example:

上述的在线电影票订单系统，假设它的应用 ID 为 1001，有 5 个应用命令：1、注册商家 2、商家审核结果 3、发布电影票信息 4、付款下订单 5、发送电影票 ID；根据上述的应用命令设计表，应用命令的权限表如下所示：

Assuming that the application ID of the above-mentioned movie ticket ordering system is 1001, there will be 5 application commands needed: 1 registered sellers, 2 review results on the sellers, 3 Issuance of information on movie tickets, 4 make an order and payment, 5 send movie ticket; according to the above application command design table, the table for application command permission is shown as below:

发起地址 Address of initiator 命令号 Command code	所有地址 Addresses of all people	商家地址 Address of sellers	开发商地址 Addresses of developers
注册商家 1 Registered sellers	√		
商家审核结果 2 Review results on the sellers			√
发布电影票信息 3 Issuance of information on movie tickets		√	
付款下订单 4	√		

Make an order and payment			
发送电影票 ID 5 Send movie ticket		√	

三条权限规则：

Rules for three permissions:

（1）公钥 0 + 1、4，即所有地址都可注册商家、付款下订单；

(1) Public 0 + 1, 4. It means all addresses are available to make registration, order and payment;

（2）商家地址 +3、 5，即商家地址可发布电影票信息、发送电影票 ID；

(2) Seller address +3, 5. It means all seller addresses are available to issue information on movie tickets and send ticket ID;

（3）开发商地址+ 2，即开发商地址可公布商家审核结果，并且需要根据该商家地址设定商家+3、 5 权限；

(3) Developer address +2. It means review results on sellers can be released via developer addresses; according to the seller address, the permission of sellers +3, 5 can be set.

上述三条权限规则可一次性设定，也可分次设定。后续还可删除某些权限，如新增两条规则：商家地址-3、5；即取消了商家地址发布电影票信息和发送电影票 ID 的权限，成为普通用户地址。

The above three permissions can be set at a time or several times. Some permission can be deleted subsequently. For example, two rules can be added: seller address -3, 5; it means the seller address is changed into a common user address, because its permission to issue information on movie tickets and send ticket ID is cancelled.

通过管理员地址进行应用权限设定后，将发送一个权限设定交易到全网，该交易确认后，所有的节点和客户端都会按照该权限体系来限定公钥或地址对应用命令的写入权限，拒绝未授权的应用命令的交易。

As application permission is set via manager address, a permission setting transaction will be broadcasted to the whole network; once the transaction is confirmed, writing permission for application commands will be restrained by all nodes and clients via public keys or addresses as per the permission system, and the transactions related to unauthorized application commands will be rejected.

这套去中心化的应用权限设定系统是安网应用开发体系中一个独创性技术。

This set of decentralized application permission setting system is an ingenious technology in SAFE application development system.

6.2.4 应用数据写入

6.2.4 Application data writing

注册了应用后，就可向安网交易写入应用数据了，如果没有额外进行应用权限设定，默认情况下只有管理员地址具备写入权限。

After applications are registered, application data related to SAFE transactions can be written; if there is no additional application permission setting, only manager address has writing permission in case of default.

应用命令已经包含在应用开发接口中，因而不用在下述数据结构中出现，应用数据的结构设计如下：

Application commands have already been written at the application development interface, thus, will not appear in the following data structure, structural design of application data is as below:

序号	应用数据项	说明

No.	Application data item	Statement
1	版本号 Version No.	用于版本升级 Used for version update
2	与应用命令对应的自定义数据 Self-defined data corresponded to application command	自定义数据 Self-defined data

如果有加密需求，则可上述两个数据项中间再加两项：

If encryption is needed, another two items need to be added between the above data items.

2	加密算法 Encryption algorithm	无、AES 或 ECC None, AES or ECC
3	用接收方公钥加密的密钥 Secret key encrypted by public key of the receiver	如果是 AES 加密的话 If it is encrypted via AES

有些应用数据需要尽快确认，可选地调用安网中的即时支付功能，即可在 3-4 秒内确认。

It only takes 3 to 4 seconds to confirm some application data, in case of calling InstantTX function in SAFE.

整个应用数据区目前的限制是 3000 字节，除去应用头和应用数据项的部分数据占有，可写入的数据量很有限。

The current space in the entire application data area only accommodate 3,000 bytes, part of which is occupied by part of data of application head and application data items, so the remained space can only accommodate limited new data.

6.2.5 额外交易费

6.2.5 Extra transaction fee

当安网应用越来越多，某个应用的交易太频繁，存在很多垃圾数据，势必增加安网的负担，因而安网以增收应用数据额外交易费的方式来限制交易数量、无价值应用和数据，规则如下：

As SAFE application is widely applied, some application transaction so frequent that many rubbish data are generated, which certainly will burden the SAFE. Therefore, SAFE uses a way of requiring additional transaction fee to restrain the number of transactions, unvalued applications and data, with the rules shown as follows:

· 应用数据区只有 4 个字节（SAFE）数据，不收额外交易费；

· In case that the data in application data area only contains four bytes (SAFE), no additional transaction fee is required;

· 应用数据区每多 300 个字节增加 0.0001 个 SAFE，不足 300 字节以 300 字节计；

· That every 300 bytes are added into the application area will increase 0.0001 X SAFEs, and the added bytes of less than 300 shall be counted as 300.

· 应用数据区最大为 3000 个字节，因而额外交易费最多为 0.001 个 SAFE；

· The application data area can only accommodate 3,000 bytes at maximum, so the additional transaction fee is at maximum 0.001 X SAFE;

· 额外交易费的体现和正常交易费一样，由矿工挖矿获得；

· Like normal transaction fee, the additional transaction fee can be gained by mining.

6.3 安付

6.3 Safe Payment

安付是指基于安网平台上的转账功能，包括即时支持、混币、增加转账备注、环签名支付、隐身收款、金额隐藏等技术和支付方法。

Safe Payment is SAFE platform-based transfer function, including InstantTX, coin shuffle, transfer note, ring signature payment, stealth collection and hidden amount.

6.3.1 即时支付

6.3.1 InstantTX

安网 3 中的即时支付，只需 3 秒左右就能被全网确认，不用等待 6 个区块确认，从而提高支付速度，具体原理如下：

It just takes around three seconds to make the whole network confirm the transactions via InstantTX in SAFE with no need to get initial confirmation of six blocks, so that the payment time is shorten. The specific principles for this are as bellow:

（1）一个即时支付交易发送到网络后，达到安网 3 所有客户端；

(1) An InstantTX transaction is sent to the network and then reaches all clients of SAFE.

（2）主节点网络随机选定 10 个主节点，由他们投票确认该交易有效，如果 10 个交易都确认有效，则该交易被全网锁定；

(2) The masternode network randomly selects 10 masternodes to confirm through voting whether the transaction is effective, if all of the 10 nodes confirm the transaction is effective, it will be locked by the whole network;

（3）在后续等待产生下一区块的时间中，所有与锁定交易相冲突的交易将会被拒绝；

(3) During the period when the next block is going to be generated, all transactions in conflict with the locked transaction will be rejected;

（4）矿池把该锁定交易打包到区块并且广播到全网；

(4) Mine pool will package the locked transaction to the block and then make it known in the whole transaction.

6.3.2 混币

6.3.2 Coin shuffle

混币是隐私支付的前提条件，在隐私支付前必须将您钱包中的币和其他人进行混币，这个过程是在后台运行，没有任何干预。具体如下：

Coin shuffle is the prerequisite of PrivateSend, so the coin in your wallet must carry out coin shuffle with coins of other people before PrivateSend. The whole process is conducted at the

background, without any intervention. See the following steps:

（1）首先将钱包中的币分解成标准面额，这些面额是 0.01SAFE，0.1SAFE，1SAFE 和 10SAFE；

(1) First, the coins in the wallet need to be changed into standard denominations, including 0.01SAFE, 0.1SAFE, 1SAFE and 10SAFE;

（2）然后，当您想混合一定的面额，钱包把请求发送到网络上主节点，这些信息不会被追踪到您，因为都是一些不可识别的信息会发送到主节点；

(2) Then, when you want to mix a certain denomination, the wallet will send your request to the masternode of the network, nevertheless, you'll not be tracked, because the information sent to the masternode is unrecognizable;

（3）当另外两个人发送类似的信息，表明他们希望混合相同的面额，一个混币会话开始。主节点混合输入并指示所有三个用户的钱包支付相同面额给自己的不同地址。

(3) When another two people send similar information to express their desire to shuffle the same denomination, a Coin shuffle dialogue will start. The masternode will enter and direct the wallets of the three persons to pay for the coin with the same denomination to their own different addresses.

（4）为了充分混合资金，钱包必须多次重复这个过程，每一轮混币都使得搞清资金来源的难度大大增加；

(4) To fully shuffle the capital, the wallet must repeat this operation again and again, which makes the source of each round of Coin shuffle more difficult to be known.

（5）混币过程在后台进行，不需要任何人工干预。当你想进行转账时，你的资金已经被混淆了，不需要额外的等待；

(5) The coin shuffle is conducted at backstage, without any manual intervention. When you want to do transfer, your capital is mixed without any wait.

6.3.3 增加转账备注

6.3.3 Transfer note

本功能和以下的安付扩展功能，需要先在安网注册安付应用，应用命令包括增加转账备注、环签名发送、隐身收款、金额隐藏、环签名发送+隐身收款等。

For this function and the following safe payment extension function, you have to register a safe payment application in SAFE, with application commands including transfer note, ring signature dispatch, stealth collection, hidden amount, and ring signature dispatch + stealth collection.

转账备注可加密，可不加密，加密算法支持 AES 和 ECC，数据结构如下：

Whether the transfer note is encrypted or not is optional, encryption algorithm supports AES and ECC, with data structure as follows:

1	版本号 Version No.	用于版本升级 Used for version update
2	加密算法 Encryption algorithm	无、AES 或 ECC None, AES or ECC
3	用接收方公钥加密的密钥 Secret key encrypted by public key of the receiver	如果是 AES 加密的话 If it is encrypted via AES
4	转账备注 Transfer note	加密或非加密数据 Encrypted or unencrypted data

6.3.4 环签名发送

6.3.4 Ring signature dispatch

环签名它主要由下列算法组成，假定有 n 个用户。

Ring signature consists of the following algorithms, assuming that there are n users.

·密钥生成 KeyGen：输入安全参数 k ，为每个用户 u_i 生成公钥 P_i 和与之对应的私钥 d_i；

· Secret key KeyGen is generated: enter security parameter k, produce public key P_i and its corresponded private key d_i for each user u_i.

·签名 Sign：输入消息 m 、n 个用户公钥 L (P 1 ,P 2 ,...P n) 和一个成员的私钥 d s ，对消息 m 产生签名 R，其中 R 的某个参数根据一定规则呈环状；

· Sign: enter information m, n X public key for user L= ($P_1, P_2,...P_n$) and d_s - a private key of a member, the signature R is generated as per the information m, and some parameter of R is in ring shape as per certain rule.

· 验证 Verify：输入(m,R) ，输出合法与否。

· Verify whether the entered m and R and the output are legitimate or not.

环签名由于它的无条件匿名、自发性、群特性，因而应用较广。环签名根据不同的应用领域还发展出其他特殊属性如：关联性、门限特性、可否认性、可撤销匿名性等。

Ring signature has been widely applied because of its unconditional anonymity, spontaneity and clustering. It has also developed other special features such as connectivity, threshold, deniability and revocable anonymity, according to different application fields.

环签名的附加信息会以安网应用数据的方式写入到应用数据区，所有节点接收到该交易，都可以验证是否是其中的用户发送的交易，接收者无需额外处理，就能接收到金额。

Attached information of ring signature will be written into the application data area in the form of SAFE application data. All nodes receiving the transaction can verify whether the transaction is sent by one of node users. Receivers can receive the amount with no need to do anything.

环签名发送割裂了接收者和发送者的关联，有可能使得区块链应用受到某些限制，因而需要进一步研究对区块链应用的影响。

Ring signature sending breaks the connection between receivers and senders, and this is likely to limit the Blockchain application, so further research needs to be carried out for the impact on Blockchain application.

6.3.5 隐身收款

6.3.5 Stealth collection

隐身地址是重要的隐私保护技术，可以把实际交易与公开地址割裂开来，没法从公开地址中找到任何对应交易，但是收款人可以从这个地址收到币。有双密钥和单密钥两种情况：

Stealth address is an important privacy protection technology, which can break the connection between actual transaction and public address. Thus, although there are no corresponding transactions in public address, the payee can still get coins from this address. There are two situations for this, dual secret key and single secret key.

（1）双密钥的隐身地址

(1) Stealth address of dual secret key

双密钥隐身地址包含两个公钥，一个称浏览公钥，另一个称消费公钥，与之相对应的还有两个私钥，一个称浏览私钥，一个称消费私钥。浏览私钥用于查看交易、计算余额，消费私钥用于交易签名，即消费币。安网 2 的地址就是双密钥地址。

Stealth address of dual secret key contains two public keys, one is called public key for browse, the other is called public key for consumption, whilst there are two corresponding private keys, one is called private key for browse, the other is called private key for consumption. The former is used to check transactions and count balance, and the latter is used for transaction signature, i.e. consumption coin. The address of DNC2 is a dual secret key address.

其使用场景如下：

It can be used in the following scenarios:

· 用户 A 公布一个隐身地址 SA = (Q,R) ，该隐身地址包括两个椭圆曲线公钥 Q 和 R，Q = dG ， R = fG ，其中 Q,R 分别是浏览公钥和消费公钥，d, f 为 Q,R 对应的浏览私钥和消费私钥，G 为椭圆曲线的基点。

· User A announces a stealth address *SA* = (*Q,R*) containing two elliptical curve public keys Q and R, where Q equals dG and R equals fG. Q and R represent public key for browse and public key for consumption respectively, while d and f represent the private keys for browse and private key for consumption corresponded to Q and R. G is the base point of elliptical curve.

· 用户 B 向 A 支付币，生成一次性公钥对(P,e) ，计算 T = R + sG ，其中 T 是目的地址的公钥， R 是 A 的消费公钥， s = SHA256(eQ) 。在交易中公布公钥 P。

· User B pays coins to User A, which generates a pair of one-time public keys (P,e). It is calculated that T equals R + sG, where T is the public key of the destination address, R is User A's public key for consumption and s equals SHA256 (eQ). The public key P is announced during transaction.

· 用户 A 扫描每个交易，发现 P，计算可能的目的地址公钥 T' = R + sG ，其中 s = SHA256(dP) ，因为 SHA256(dP) = SHA256(eQ) 。

· User A spots P when he scans each transaction, then calculates that T', the possible public key for destination address, equals R + sG, where s equals SHA256(dP), because SHA256(dP) equals SHA256(eQ).

·· 如果用户 A 没有正确的浏览私钥 d ，计算出错误 s 和 T '，因而 T ≠ T '，不能计算出正确的目的地址。

·· If User A has no correct private key for browse d, he will get wrong s and T ', so T ≠ T ', from which the destination address cannot be calculated.

··如果用户 A 有正确的浏览私钥 d，无消费私钥 f ，计算出 T ' = R + sG ，且 T = T '，可以计算出 A 余额。

··If User A has a correct private key for browse d, but no private key for consumption f, it is calculated that T' equals R + sG and T equals T ', from which the balance of User A can be calculated.

·· 如果用户 A 有浏览私钥 d 和消费私钥 f ，则计算 T ' = (f + s)G ，且 T = T '。也能消费币，T 的私钥 l = (f + s) 。

··If User A has a correct private key for browse d and a private key for consumption f, it is calculated that T ' equals (f + s)G and T equals T', which can consume coins, l, the private key of T equals (f + s).

（2）单密钥的使用场景如下：

(2) Single private key can be used in the following scenarios

· 用户 A 公布隐身地址 Q = dG, d 为私钥，G 为椭圆曲线的基点。

· User A announces its stealth address Q = dG, where d is the private key and G is the base point of elliptical curve.

· 用户 B 向 A 支付币，生成一次性公钥对(P,e) ，计算 T = sG ，其中 T 是目的地址的公钥，s = SHA256(eQ) 。在交易中公布公钥 P。

· User B pays coins to A, which generates a pair of one-time public keys (P,e), it is calculated that T equals sG, where T is the public key of destination address, s equals SHA256(eQ). The public key P is announced during transaction.

· 用户 A 扫描每个交易，发现 P，计算可能的目的地址公钥 T'= sG，其中 s = SHA256(dP) ，因为 SHA256(dP) = SHA256(eQ)。

·User A spots P when he scans each transaction, then possibly calculates that T', the public key for destination address, equals sG, where s equals SHA256(dP), because SHA256(dP) equals SHA256(eQ).

·· 如果用户 A 没有正确的私钥 d ，计算出错误 s 和 T '，因而 T ≠ T '，不能计算出正确的目的地址。

·· If User A has no correct private key d, he will get wrong s and T ', so T is unequal to T ', from which the destination address cannot be calculated

·· 如果用户 A 有正确的私钥 d，计算出 T ' = sG，且 T = T ' ，计算出 A 余额。

·· If User A has a correct private key d, it can be calculated that T' equals sG and T equals T', so that the balance of User A can be calculated.

同样地，隐身地址割裂了接收者和发送者的关联，有可能使得智能合约和区块链应用有影响，因而其应用会被限制在一定范围内。

Likewise, stealth address splits the connection between receivers and senders, which may probably affect smart contract and Blockchain application. Therefore, stealth address will be applied within a limited range.

6.3.6 金额隐藏

6.3.6 Hidden amount

比特币侧链技术中，有一项技术称为私密交易，该特性仅允许交易的参与者（或他们指定的人）知道交易金额，其原理是使用佩德森承诺技术来隐藏金额。承诺场景让你把一段数据作为私密保存，但是要承诺它，使得你后来不能改变该数据。一个简单的承诺场景用哈希函数构建如下：

In the side-chain technology of bitcoin, there is a technology called private transaction, with a feature that only participants (the designated persons) of transaction know the specific transaction amount, because of a philosophy using Pederson Commitment Technology to hide account. Commitment scenario enables you to save a segment of data as privacy, but if the commitment is made, you cannot change the data later. A simple commitment scenario by HASH function is shown as follows:

承诺= SHA256（盲化因子||数据）

Commitment = SHA256 (blinding factor || data)

如果你仅告诉别人承诺，别人没法确定你承诺了什么数据（对哈希表的属性给定某些假设）。但你后来揭露了盲化因子和数据，别人可以运行该哈希函数来验证是否与你以前的承诺相匹配。盲化因子必须存在，否则别人可以试图猜测数据。如果你的数据比较少而简单，猜测成功可能性比较大。

If you only tell people commitment, they cannot confirm what data you promised (make some assumptions for properties of Hash table). However, you later uncover blinding factor and data, people can use this hash function to verify whether the commitment is matched with the previous one you made. Blinding factor must exist, or people may try to guess data. If your data is fewer and simpler, there might be a great possibility to guess your data successfully.

佩德森承诺与以上场景中的承诺类似，但是附加一个特性：承诺可以相加，多个承诺的总和等于数据总和的承诺（盲化因子的集合即盲化因子总和）：

Pederson commitment is similar to the commitment in the above scenario, but it has additional feature: commitments can be added together, the sum of several commitments equals

commitment of data aggregation (the aggregation of blinding factors is the total blinding fators)
C(BF1, data1) + C(BF2, data2) == C(BF1 + BF2, data1 + data2)
C(BF1, data1) - C(BF1, data1) == 0
换句话说，加法律和交换律适用于承诺。
In other words, addition law and commutative law are applicable to commitment.
利用该工具，我们替换比特币交易中的 8 字节整数金额为 32 字节佩德森承诺，如果一个交易的发起人认真选择他们的盲化因子,以便正确相加,然后网络还能通过承诺相加为 0 来验证该交易。
We capitalize in this method to replace 8-byte sum amount in bitcoin transaction with 32-byte Pederson commitment. If initiators of a transaction prudently select their blinding factors for correct addition, then the network can verify this transaction by a method that aggregation of commitments equals 0,
(In1 + In2 + In3 + plaintext_input_amount*H...) -
(Out1 + Out2 + Out3 + ... fees*H) == 0
以上公式需要交易费用，在实际交易中，这点没有问题。金额隐藏的原理基本如上所示，但是在实际应用中还需要考虑不少安全性，附加一些安全检查措施。
The above equation needs transaction fee. In actual transaction, it is no problem. The principle of hidden amount is basically as above, but the security needs to be considered in actual applications, in addition to some measures for security check
6.4 安资
6.4 Safe Asset
安资是基于安网应用开发协议开发的、整合在安网底层的一个典型应用，同样需要先注册安网应用，设定好权限，就可以基于它开发各种代币或数字资产。安资的技术方案包括发行、追加发行、转让、销毁、发糖果、领糖果等。
Safe asset is a typical application that is developed based on SAFE application development protocol and integrated as the underlying technology of SAFE. You first need to make registration for SAFE application, set up permissions, and then develop various tokens or digital assets based on safe asset. Its technical schemes include issuance, additional issuance, transfer, destruction, candy distribution and candy acquisition.
6.4.1 资产发行
6.4.1 Asset issuance
可发行数字资产，发行代币必须消耗 500 个 SAFE，每年减少 5%，直到不少于 50 个 SAFE，目的是防止在安网 3 上滥发代币。发行游戏装备类的数字资产不需要消耗 SAFE，因为这种数字资产只是在区块链上登记、转让等；
It can issue digital asset. Token issuance must consume 500 SAFEs, the figure reduces by 5% each year until it is no less than 50 SAFEs, to avoid overissuing tokens on SAFE. The digital asset to issue game equipment doesn’t consume any SAFE, because it just needs to check in and transfer on Blockchain.
数字资产信息有：资产名称（即简称，必须唯一）、资产简介、资产总量、初次发行总量、最小单位、是否可分、是否可追加发行、是否可以销毁；
Information on digital asset includes asset name (its short name, which must be different from others), asset introduction, total asset, initial issuance volume, minimum unit, whether it can be split, issued again later, or destroyed.
发行时，还可以设定是否给 SAFE 持有者分糖果，以及指定一个糖果比例和过期时间，称为

糖果协议。

During issuance, whether to give candies to SAFE holders can be set up, candy ratio and expiration time can be given, it is called candy protocol.

发行交易输出有两个，如下：

There are two outputs for transaction issuance, as shown below:

·输出一：

· Output 1:

输出金额：要消耗的 SAFE

Output amount: SAFE to be consumed

输出脚本：正常转账交易脚本，接收地址为黑洞地址

Output script: script for normal transfer transactions, receiving address is blackhole address

vReserve 字段：safe

vReserve field: safe.

· 输出二：

· Output 2:

输出金额：万分之一 SAFE

Output amount: 0.01% SAFE

输出脚本：正常转账交易脚本，接收地址为输入中某一个地址（消耗 SAFE 的地址）；

Output script: script for normal transfer transactions, receiving address is one of input addresses (address of consuming SAFE)

vReserve 字段：应用头 + 应用数据（资产发行）

vReserve field: application head + application data (asset issuance)

资产发行 Asset issued 应用数据 Application data	说 明 Statement
版本号 Version No.	2 字节 Two bytes
资产名称 Asset name	最大 20 个字节，1 个汉字可能占 3 个字节 Maximum 20 bytes, one Chinese character may take up three bytes
资产描述 Asset description	最大 300 个字节，1 个汉字可能占 3 个字节 Maximum 300 bytes, one Chinese character may take up three bytes
资产单位 Asset unit	最大 10 个字节，1 个汉字可能占 3 个字节 Maximum 10 bytes, one Chinese character may take up three bytes
资产总量 Total asset	如果为 0，代表总量不受限，可一直追加发行 If it is 0, it means the total amount is unlimited, and the coins can always be issued again
初次发行总量 Initial total issuance volume	第一次发行的数量 The volume at the first issuance
小数点位 Decimal places	最小 4 位，最大 10 位，例如：100000000，代表是 10 的负 8 次方； Minimum 4 decimal places and maximum 10 decimal places. For instance, 100000000 means negative eighth power of 10
是否可分	如果不可分，则小数点位必须是 0，发送资产时必须以整数发送

Whether it can be divided	If it is indivisible, the decimal places must be 0, and the asset must be sent in the form of integer.
是否可追加发行 Whether additional issuance is feasible	无此标识的，后续不能再追加发行 If there is no such a sign, additional issuance is unfeasible
是否可以销毁 Whether destruction can be done	有些资产可以销毁，有些不能，用户自行设置 Some assets can be destroyed, but some not. Users can set up by themselves
是否分发糖果 Whether candies can be distributed	是否给 SAFE 持有用户分发糖果 Whether candies can be given to SAFE holders
分发糖果比例 Ratio of distributing candies	拿出总量的 0.1%-10%来发给 SAFE 的持有用户 Give 0.1%-10% of the total amount to SAFE holders
糖果过期时间 Due day for candies	以区块数计的时间，1-6 个月之间，如用户设定 3 个月，则 3 个月后如果还未领取糖果，则作废。 1-6 months as per the number of blocks. If users set the time to 3 months, the candies not claimed are useless after 3 months
备注 Note	最大 500 个字节，1 个汉字可能占 3 个字节 Maximum 500 bytes, one Chinese character may occupy three bytes

发行时返回一个数字资产 ID，数字资产 ID 由上述资产信息生成 HASH，再把 HASH 值代入生成安网 3 钱包地址规则中而获得。

During issuance, return a digital asset ID, which is generated by substituting the HASH value calculated by the above asset information into the rules of generating SAFE wallet address.

·输出三：

· Output 3:

输出金额：万分之一 SAFE

Output amount: 0.01% SAFE

输出脚本：正常转账交易脚本，接收地址为糖果地址

Output script: script for normal transfer transactions, receiving address is the candy address

vReserve 字段：应用头 +应用数据（转账）

vReserve field: application head + application data (transfer)

转账应用数据 Application data for transfer	说 明 Statement
版本号 Version No.	2 字节 2 bytes
数字资产 ID Digital asset ID	为 0，即当前数字资产 If it is 0, that means it is current digital asset
数量 Amount	0.1%-10%数量 0.1%-10% of the amount
锁定时间 Locking time	以区块计的锁定时间，0 表示不锁定 Locking time by block, 0 means unlocked
备注	最大 500 个字节，1 个汉字可能占 3 个字节

Note	Maximum 500 bytes, one Chinese character may occupy three bytes

6.4.2 追加发行

6.4.2 Additional issuance

追加发行，数字资产必须在发行时已经指定了可追加发行标记，才能追加发行；追加发行时需要指定首次发行的交易 ID 和资产 ID，而且追加发行数量不得超过：资产总量-初次发行总量。

Additional issuance can be done only when the digital asset is given the sign of additional issuance during issuance; additional issuance needs to designate transaction ID and asset ID of initial issuance, whilst the additional issuance can't exceed: total asset – initial total issuance.

输出地址必须是发行时的输入地址之一，交易格式：

Output address must be one of the input addresses during issuance, with transaction format:

输出金额：万分之一 SAFE

Output amount: 0.01 SAFE

输出脚本：正常转账交易脚本，接收地址为糖果地址

Output script: script for normal transfer transactions, receiving address is the candy address

vReserve 字段：应用头 +应用数据（转账）

vReserve field: application head + application data (transfer)

转账应用数据 Application data for transfer	说 明 Statement
版本号 Version No.	2 字节 2 bytes
数字资产 ID Digital asset ID	要追加发行的资产 ID Asset ID for additional issuance
数量 Additional amount	追加发行的数量 Amount of additional issuance
锁定时间 Locking time	以区块计的锁定时间，区块数绝对值， 0 表示不锁定 Locking time by block, absolute value of blocks, 0 means unlocked
备注 Note	最大 500 个字节，1 个汉字可能占 3 个字节 Maximum 500 bytes, one Chinese character may occupy three bytes

6.4.3 转账

6.4.3 Transfer

转账代币或数字资产，通过安网地址来转账，转账时还有锁定选项，可以锁定一段时间之后才能花。交易格式如下：

Token for transfer or digital asset needs to be transferred via SAFE address, during which some options are locked for a period of time, and then can be spent. Transaction format is as below:

输出金额：万分之一 SAFE

Output amount: 0.01% SAFE

输出脚本：正常转账交易脚本

Output script: script for normal transfer transactions

vReserve 字段：应用头 +应用数据（转账）

vReserve field: application head + application data (transfer)

转账应用数据 Application data for	说 明 Statement

transfer	
版本号 Version No.	2 字节 2 bytes
数字资产 ID Digital asset ID	要发送的资产 ID ID of asset to be sent
数量 Amount	发送的数量 Amount of asset to be sent
锁定时间 Locking time	以区块计的锁定时间，0 表示不锁定 Locking time by block, , 0 means unlocked
备注 Note	最大 500 个字节，1 个汉字可能占 3 个字节 Maximum 500 bytes, one Chinese character may occupy three bytes

6.4.4 销毁

6.4.4 Destruction

销毁，有些数字资产可能需要用销毁，例如积分在兑换完成或者过期后，前提是，在发行代币或数字资产时必须指定可销毁标记，否则将无法销毁；而且只有拥有人才能销毁他自己的资产，该功能很危险，慎用。

Destruction: some digital asset might need to be destroyed, after some points are converted or expire, but the prerequisite for this is that the destruction sign is designated when tokens or digital asset is issued, or it can't be done; moreover, only owners of the digital assets can destroy their own asset. This function is dangerous and should be used with caution.

目前只能通过命令行、RPC 接口方式进行销毁，不提供任何操作界面，且只能销毁自己钱包内的资产。交易格式如下：

At present, the digital asset can only be destroyed by command line and RPC interface, no any operation interface for this. Additionally, only the asset in your own wallet can be destroyed. Transaction format is as below:

输出金额：万分之一 SAFE

Output amount: 0.01% SAFE

输出脚本：正常转账交易脚本，输出地址是黑洞地址

Output script: script for normal transfer transactions, output address is blackhole address

vReserve 字段：应用头 + 应用数据（转账）

vReserve field: application head + application data (transfer)

转账应用数据 Application data for transfer	说 明 Statement
版本号 Version No.	2 字节 2 bytes
数字资产 ID Digital asset ID	要发送的资产 ID ID of asset to be sent
数量 Additional amount	发送的数量 Amount of asset to be sent
锁定时间 Locking time	以区块计的锁定时间，0 表示不锁定 Locking time by block, , 0 means unlocked
备注 Note	最大 500 个字节，1 个汉字可能占 3 个字节 Maximum 500 bytes, one Chinese character may occupy three bytes

6.4.5 发放糖果

6.4.5 Candy distribution

资产发行时如果未发放糖果，也可以用该接口来发放，即使发放过糖果，但还想再次发放的，也可以调用该接口。该接口必须由资产发行地址来调用，交易格式如下：

If candies are not given during asset issuance, they can be distributed via this interface. If additional candies need to be distributed, this interface is also accessible. It can only be called by asset issuance address. Transaction format is as below:

输出金额：万分之一 SAFE

Output amount: 0.01% SAFE

输出脚本：正常转账交易脚本，输出地址为糖果地址

Output script: script for normal transfer transactions, output address is the candy address

vReserve 字段：应用头 + 应用数据（发放糖果）

vReserve field: application head + application data (candy distribution)

转账应用数据 Application data for transfer	说 明 Statement
版本号 Version No.	2 字节 2 bytes
数字资产 ID Digital asset ID	要发糖果的资产 ID ID of asset for candy distribution
分发资产比例 Ratio for asset distribution	拿出总量的 0.1%-10%来发给 SAFE 的持有用户，如果发送总量达不到上述比例，则不得发放。 Give 0.1%-10% of total amount to SAFE holders, if the total amount to be sent fails to reach the above ratio, it is unallowable to give candies.
糖果过期时间 Expiration time of candies	以区块数计的时间，1-6 个月之间，如用户设定 3 个月，则 3 个月后如果还未领取糖果，则作废。 As per time by blocks, 1-6 months. If users set up for 3 months, the candies failed to be taken within this period will be useless.
备注 Note	最大 500 个字节，1 个汉字可能占 3 个字节 Maximum 500 bytes, one Chinese character may occupy three bytes

6.4.6 领取糖果

6.4.6 Candy acquisition

与 6.4.1 和 6.4.5 中的糖果发放后，需要用户自行操作进行领取。领取糖果的交易格式如下：

After candies are distributed as per 6.4.1 and 6.4.5, customers need to take these candies themselves. The transaction format of taking candies is as below:

输入：发行交易 ID、输出项索引、黑洞地址的交易 ID 列表 HASH、领取地址的交易 ID 列表 HASH、对这些数据的签名；输入可能有多个，因为拥有 SAFE 的地址有多个；

Enter: transaction issuance ID, output item index, HASH for list of transaction ID at blackhole address, HASH for list of transaction ID taking address, signatures for these data; there may be several enters, because several addresses have SAFE;

输出：正常转账交易脚本，自己地址；

Output: script for normal transfer transaction, address per se.

金额：按照比例计算的资产；

Amount: asset calculated as per ratio;

领取规则：

Rules of taking these candies:

（1）领取范围：发行交易所在区块之前的拥有至少 1 个 SAFE 数量的地址才能领取糖果;

(1) Address accessible to take candies: candies can only be taken at the addresses that own at least one SAFE before blocks for transaction issuance generate;

（2） 领取比例为：本钱包 SAFE 数量/目前 SAFE 发行总量*资产糖果总额，如果计算出来的资产余额不足 0.0001 个，则不让领取；

(2) Ratio: the asset balance is less than 0.0001 SAFE according to the computation method - the number of SAFEs in the wallet / the current total issuance volume of SAFEs * total asset amount of candies, the candies can't be taken.

（3）领取时间如果过期，则不让领取；

(3) The candies are not available, if the time period defined is expired.

（4）在本地要维护一份糖果全网领取记录，根据区块中领取交易的记录生成每个资产的总领取记录，用来判断当前糖果是否还能领取，以及快速查找领取记录；

(4) A local record for taking candies needs to be filed in the network, according to the record, an overall record of taking candies by each asset is generated, to judge whether the candies can be taken again and fast search for records of taking candies;

（5）在本地要维护一份钱包地址领取糖果记录表，每个钱包地址领取过哪个资产，以及 SAFE、资产的数量；

(5) A local record chart of taking candies by each address is needed, to record which asset and how many SAFEs and assets are taken by each wallet address and.

7 安网的联合产品

7. Joint Products of SAFE

安网的联合产品有区块链中间件和数字货币支付平台。它们并非属于安网，但是与安网相结合，可以进一步加强安网的应用开发的便捷性和支付的便捷性。

Joint Products of SAFE include Blockchain middleware and digital currency payment platform. Although they do not belong to SAFE, their combination with SAFE can further enhance the convenience for SAFE application development and payment.

7.1 区块链中间件

7.1 Blockchain Middleware

区块链应用的区块链中间件产品，为想实施“区块链+”战略的金融机构和企事业单位提供专业的区块链基础设施服务，帮助客户快速搭建区块链应用所需的组件以及快速开发应用。
Blockchain middleware of Blockchain application provides financial institutions, enterprises and public institutions that want to implement “Blockchain +” with professional Blockchain infrastructure services, and offer customers components that are needed for fast building up Blockchain application and help them fast develop applications.

7.1.1 中间件意义

7.1.1 Significance of middleware

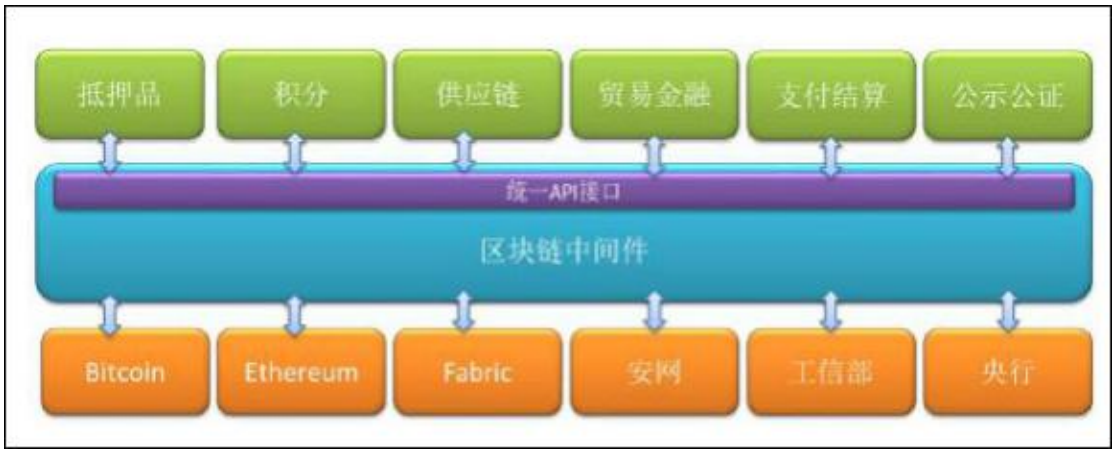
区块链技术必须与应用场景相结合才能真正体现出它的潜力。大量国内外金融机构和企事业单位正在研究区块链技术，以期与业务相结合、促进应用落地。但他们面临着不少问题，阻碍了应用落地的进程：
Blockchain technology must be combined with application scenario to show its potential. A large number of financial institutions, enterprises and public institutions are studying Blockchain technology, and hope to combine it with their businesses for its implement. However, they are now facing many problems, impeding its implementation.
（1）应用落地周期长。做区块链应用，得先掌握区块链技术和理念，再选取应用场景，选用区块链，熟悉该种区块链的开发技术，最后进行区块链应用开发和业务改造，整个落地周期较长。
(1) It takes long time to implement Blockchain technology. Before developing Blockchain applications, you need to master Blockchain technology and concepts, then select application scenarios and Blockchain, be familiar with this technology, and carry out Blockchain application development and business reform. It is a long process.
（2）从业人才成本高。区块链技术和应用对从业人才层次、技术积累和理念改变提出了较高的要求，难以在短时间内培养出金融和区块链的交叉人才，人才成本和成长成本很高。
(2) High talent cost. Blockchain technology and its application require talents in this industry to have a higher level in expertise, more experience in technologies and faster change in concept.
（3）区块链选用难。目前区块链底层技术平台如 Bitcoin、Ethereum、Fabric、Corda、Chain 等，其发展前景不确定，企事业单位在实施区块链应用时必须考虑选用的区块链能否长期存在、合规性、版权、运维等一系列问题。
(3) It is difficult to select Blockchain. Currently, its underlying technology platforms such as Bitcoin, Ethereum, Fabric, Corda and Chain have an uncertain prospect, enterprises and public institutions should consider a series of problems before carrying out Blockchain applications, for example, whether the selected Blockchain can exist for a long time and it is legalized, as well as its copyright and its operation and maintenance.
目前区块链底层技术平台（1）还不能完全满足应用需求（2）选用难（3）学习成本很高（4）有可能被替换（5）发展不可预测。这些不确定因素制约了区块链应用的发展和实践。
The current underlying technology platforms for Blockchain (1) can’t totally meet the application demands, (2) are difficult to be selected, (3) have a higher study cost, (4) are likely to be replaced, (5) have unexpected future. These uncertain factors limit the development and practice of Blockchain application.
因而，解决以上三个难点，就成了区块链应用的关键，区块链中间件应运而生。
Therefore, solving the above three difficulties become the key to Blockchain application. This is why the Blockchain middleware is generated.

7.1.2 区块链中间件

7.1.2 Blockchain middleware

结合中间件的概念，针对多种区块链底层技术平台，区块链中间件封装了多种异构的区块链，向区块链应用提供统一的 API 接口，使得客户随时切换区块链底层技术平台，无需考虑它们的编程语言、设计风格、适用场景、后续发展、存在风险和技术不确定性。

Combined with the concept of middleware, targeted to the multiple Blockchain underlying technology platforms, Blockchain middleware seals several heterogeneous Blockchains, and offers a unified API interface to Blockchain applications, thus enabling customers to switch Blockchain underlying technology platforms randomly, without considering their programming languages, design style, applicable scenarios, subsequent development, risks and technical uncertainty.



抵押品	Mortgage
积分	Membership points
供应链	Supply chain
贸易金融	Trading finance
支付结算	Payment settlement
公示公证	Announcement and notarization
统一 API 接口	Unified API interface
区块链中间件	Blockchain middleware
安网	SAFE
工信部	Ministry of Industry and Information Technology of the People's Republic of China
央行	Central bank

区块链中间件以区块链云服务方式运行于公网，客户只需前端和 JAVA 开发人员，使用 SDK 开发包，调用 API 函数，在 1-2 周内即可完成区块链应用原型开发，无需理解底层技术，大大降低中小型企事业单位实施“区块链+”的时间成本、人力成本和人员要求，更快地实施“区块链+”战略。

Blockchain middleware operates in the public network in the form of cloud services, customers along with front end and JAVA developers just use SDK development package, call API function to complete the prototype development of Blockchain application in one to two weeks, without need to understand underlying technologies, which greatly reduces the time cost, labor cost and personnel requirements for implementation of the “Blockchain +” strategy by small and medium-sized enterprises and public institutions, prompting its fast implementation.

区块链中间件在区块链应用和区块链底层技术平台之间架起一座桥梁，可以认为是区块链应

用的入口，意义重大。

Blockchain middleware acts as a bridge connecting Blockchain application and its underlying technology platform, also as an entrance of Blockchain application, and has a great significance.

7.1.3 安网与区块链中间件的结合

7.1.3 Combination of SAFE and Blockchain middleware

安网是一个典型的区块链底层技术平台，很方便地进行开发区块链应用以及发行各种数字资产，安网与区块链中间件的结合将起到很有意思的效果。

SAFE as a typical underlying technology platform for Blockchain facilitates the development of Blockchain applications and issuance of various digital assets. Combination of SAFE and Blockchain middleware will have a great effect in this regard.

一方面，区块链中间件可以使用安网公链，借助于安网的应用开发协议来实现资产管理、用户管理、区块链管理等接口功能；另一方面，也可从安网中引出一些特殊的功能和应用的 API 接口，如即时支付、隐私支付、信息记录，以及第三方开发的区块链应用，并且集成到 SDK 中去，进一步降低安网应用开发的难度，无需建立节点，只需使用 SDK 对接 API 即可。

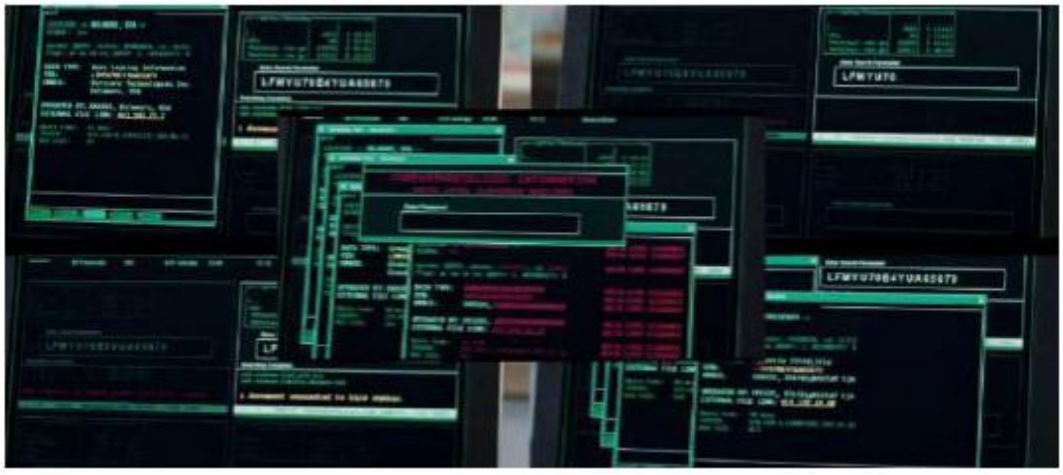
On one hand, Blockchain middleware can use SAFE public chain, and realize asset management, user management and Blockchain management with the help of SAFE application development protocol; on the other hand, it can create some special functions, API application interfaces such as InstantTX, PrivateSend and information record, and Blockchain applications developed by the third party, and can integrate these to SDK, thus further reducing the difficulty of developing applications for SAFE by just connecting SDK and API without building up nodes.

区块链中间件可屏蔽币的因素，需要消耗 SAFE 的接口和服务，都由中间件处理，用户无需关注币。这对于一些不喜欢币，只想做纯区块链应用的单位来说比较合适。

Blockchain middleware is able to shield coins and deal with the interfaces and services consuming SAFEs, enabling customers to put their attention out of coins, which suits for those who don’t like coins but just want to develop Blockchain applications.

7.2 数字货币支付平台

7.2 Payment Platform for Digital Currency



安网团队还正在研发一款中心化的、聚合类数字货币支付和应用落地系统（类支付宝），主要解决并提供：

SAFE team is developing a centralized, aggregated digital currency payment and application implementation system (similar to Alipay), aiming to:

（1）为数字货币寻找二级市场以外的消费场景，重新应用数字货币到其本质的货币属性上。

给各种数字货币提供真实的落地场景，避免“空气币”之称。
(1) Find consuming scenarios for digital currencies besides secondary markets, and restore the fundamental properties of digital currencies; provide real implementation scenarios for various digital currencies, to avoid being known as “air coins”.
（2）线上服务：平台提供线上各类商家入住，及对接消费者。为商家提供 SAFE 及其他数字货币的最便利支付通道。商家可自行选择结算数字货币或者法币。选择结算数字货币自行承担数字货币本身的涨跌性。选择结算法币则由平台来解决数字货币兑换，并用法币支付给商家。平台提供完善的结算/清算系统，结算方式按 T+X 方式。
(2) Provide online services: the platforms are available to various sellers and consumers, whilst they provide the sellers with most convenient payment channels for SAFE and other digital currencies, so that the sellers themselves can make settlement via digital currencies or legal currencies, but they have to bear the rise and fall of digital currencies per se if they use the former for settlement, while the platforms are in charge of the conversion of digital currencies if the latter is selected for settlement. Moreover, the platforms provide complete settlement/liquidation system, with payment means of T+X.
（3）线下服务：平台提供线下门户/商场支付的软件/硬件/二维码/APP 等设备及应用，并提供完善的结算/清算系统，按 T+X 方式结算给商家。商家获取方式同线上服务，自行选择数字货币或法币。
(3) Provide Offline services: the platforms provide offline portals/ payment software for shopping malls/ hardware /QR code / APP and other equipment and applications, as well as complete settlement/liquidation system for sellers with payment means of T+X. the sellers The way of acquiring the platform by sellers is the same as the online service, and they can select digital currencies or legal currencies.
（4）应用服务：提供公有的数字货币聚合支付 SDK 接口，提供三方应用的数字货币支付对接。如支付、红包、打赏、游戏等应用。
(4) Offer application services: provide SDK interface for integration payment of public digital currencies, and payment docking of digital currencies used by the three party, such as payment, red envelop, reward and games.
（5）解决方案服务：为有需企业提供完整的 TOB 数字货币支付/清算/结算解决方案服务。
(5) Provide solutions: offer enterprises complete TOB digital currency payment / settlement / liquidation solutions.
（6）上币方服务：因平台完善的支付/应用场景。平台对接各类数字货币发行商，以 SAFE 为中心开始拓展到各类数字货币。并提供完善的发行方展示系统。提高发行方数字货币的流通率/网络手续费消耗/数字货币整体估值等。
(6) Offer services of listed coins: because platforms have complete payment / application scenarios, they connect with various digital currency issuers, applicable to SAFE and extended to various digital currencies, provide complete issuer exhibition system, increase the flow rate of digital currencies issued by issuers / network commission expense / and overall estimated value of digital currencies.
实施过程，按照“支付平台 -> 个人手机 APP ->数字货币应用落地平台”的步骤来完成整个数字货币支付平台和应用落地平台的建设。首先支持安网的支付体系，同时可以使用 SAFE 支付本平台的手续费、上币费或补贴费。
Implementation process: the building of a complete digital currency payment platform and application implementation platform needs to be done according to steps of payment platform ->

APP on mobile phone -> digital currency application implementation platform. Meanwhile, SAFE can be used to pay commissions, expense for listed coins or subsidy.

数字货币支付平台是安网积累用户量的是一个绝好途径。

Digital currency payment platforms are great way to accumulate the number of users.

8 安网路线图

8 Time Schedule

安网的主要的推出路线图如下所示，有任何调整，我们将在官网上通知。

The time schedule of launching SAFE is shown as follows, if there is any adjustment, we will make an announcement on our website.

2018.1 分叉和稳定版本	Fork and stable version in Jan. 2018
2018.2.4 底层设计和开发	Design and development of underlying technology on Feb. 4, 2018
2018.5 发布 V1.1 版本：应用开发平台+安资+糖果协议	The release of V1.1 version in May 2018: application development platform + safe asset + candy protocol
2018.9 发布 V1.2 版本：安投新版本发布+安付部分扩展功能	Release V1.2 version in Sept. 2018: release new version on safe asset + some extensions of safe payment
2018.12 发布 V1.3 版本：智能合约	Release V1.3 version in Dec. 2018: smart contract

9 安网愿景

9 Vision of SAFE

安网空间 3（SAFE）结合 DASH 优点，融合了安网空间 2（DNC2）和投票链（ELT），陆续引入 Sapp 应用开发协议和安全智能合约，延伸出安付（即时支付、安全支付）、安资（资产发行和管理，基于安网 3 发行代币）、安投（安全投票，原投票链）等三大应用方向，旨在成为全球最大、最安全的数字货币支付和应用开发平台，联合区块链中间件和数字货币支付平台，大大简化企事业单位实施“区块链+”战略，从代币发行和支付落地、应用开发、隐私保护、区块链投票等多个维度来构建千万级用户量和社区生态。

SAFE has combined the advantages of DASH, integrating DNC2 and ELT, introducing Sapp application development protocol and safe smart contract, thus generating three application directions, that is, safe payment (InstantTX and safe payment), safe asset (asset issuance and management, SAFE-based token issuance) and safe voting (safe voting, the former ELT). SAFE is aimed to become the largest and safest digital currency payment and application development platform in the world, hopes to work with the Blockchain middleware and digital currency payment platform to greatly facilitate enterprises and public institutions to implement “Blockchain +” strategy, thus building ten millions of users and community ecology from aspects

of token issuance, payment implementation, application development, privacy protection and Blockchain voting.

任重道远，我们一路前行。

To this end, we still have a long way to go.