2019-1-9

安网 SAFE：

关注应用安全和隐私保护的区块链应用开发平台 v1.2

CRYP2NOVA

新加坡 SAFE 基金会出品

Archived copy · cryp2nova.com

目录

1 前言.....5
1.1 区块链发展史.....5
1.2 项目背景和意义.....7
1.2.1 应用和资产安全性.....7
1.2.2 发行资产的便捷性.....8
1.2.3 隐私保护.....9
1.3 安网历史.....9
1.4 安网应用.....11
1.5SAFE 分配.....12
1.6 挖矿增益.....12
1.6.1 主节点和矿工收益.....13
1.6.2 活动增益.....13
1.6.3 增益活动执行情况.....14
2 以往开发经验.....14
3 安网的商业价值.....15
3.1 应用开发.....15
3.2 安付.....16
3.3 安资.....16
4 安网的系统架构.....17
4.1 共识算法 SafePOS.....18
4.2 密码学算法.....20

Archived copy · cryp2nova.com

4.3 主节点网络 20
4.4 预算系统 21
4.5 应用开发协议 22
4.6 安资协议 23
4.6 糖果协议 24
4.7 安码/智能合约 24
4.8 安付扩展 25
4.8.1 增加转账备注 25
4.8.2 环签名发送 26
4.8.3 隐身收款 26
4.8.3 金额隐藏 26
4.9P2P 协议 27
5 安网的技术方案 27
5.1 分叉技术方案 27
5.1.1 分叉原理 27
5.1.2 相关参数 27
5.1.3 配置文件 28
5.1.4 交易结构 28
5.1.5 区块难度和奖励 28
5.1.6 矿池 29
5.2 应用开发协议 30
5.2.1 应用注册 30

Archived copy · cryp2nova.com

5.2.2 应用命令设计 31
5.2.3 应用权限设定 32
5.2.4 应用数据写入 34
5.2.5 额外交易费 35
5.3 安付 35
5.3.1 即时支付 36
5.3.2 混币 36
5.3.3 增加转账备注 37
5.3.4 环签名发送 37
5.3.5 隐身收款 38
5.3.6 金额隐藏 39
5.4 安资 40
5.4.1 资产发行 40
5.4.2 追加发行 43
5.4.3 转账 43
5.4.4 销毁 44
5.4.5 发放糖果 44
5.4.6 领取糖果 45
5.5 安码 46
5.5.1 安全性 46
5.5.2 易用性 47
5.5.3 兼容性 48

Archived copy · cryp2nova.com

6 安网路线图 48

7 安网的技术创新点 49

7.1SafePOS 共识算法 49

7.2 安资协议 49

7.3SAPP 应用开发协议 50

7.4 安码智能合约系统 50

CRYP2NOVA

Archived copy · cryp2nova.com

安网是企事业单位实施“区块链+”战略的最佳应用开发和实践平台，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，其中的技术方案在不断更新和迭代中，请上安网官网(anwang.com)获取最新版。

1 前言

安网（SAFE）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 应用开发协议提供更安全的区块链应用开发解决方案，同时也提供安全性高、兼容 EOS 和 ETH 智能合约的独创性智能合约系统-安码。

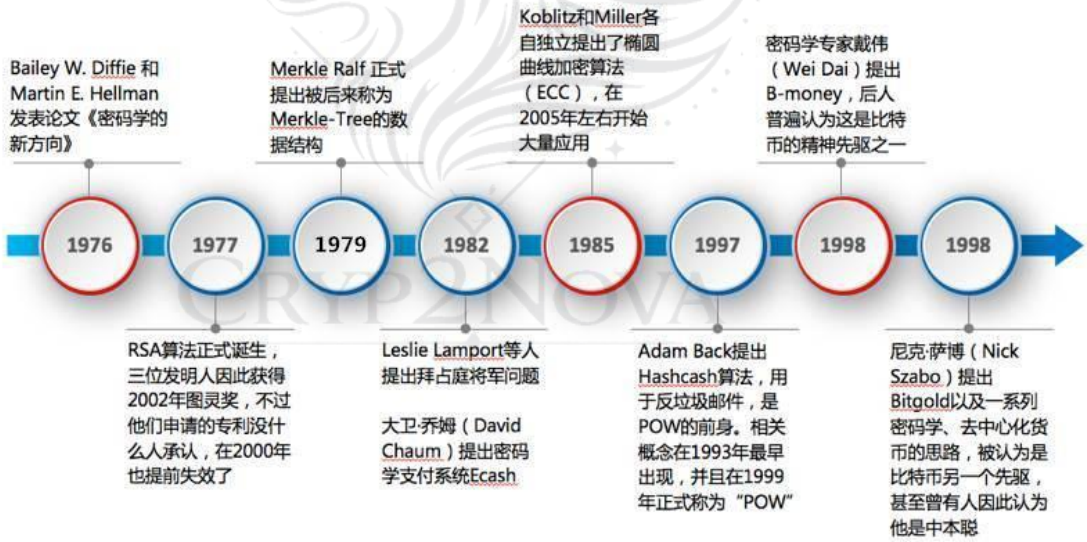
1.1 区块链发展史

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。

- 1976 年，BaileyW.Diffie、MartinE.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。
- 1979 年，RalfMerkle 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。
- 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。

Archived copy · cryp2nova.com

- 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。
- 1997 年 AdamBack 在一篇论文中提出了 HashCash 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。
- 图灵奖获得者 LeslieLamport 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。
- 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。



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：

Archived copy · cryp2nova.com

“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。

1.2 项目背景和意义

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

1.2.1 应用和资产安全性

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来发行代币和开发区块链应用，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。

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 的智能合约在自由社区很少有人使用，未爆出太多问题，但 Ethereum 和 EOS 的智能合约安全性问题已经非常突出。

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；

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。

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。

Archived copy · cryp2nova.com

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。

一方面，链上智能合约是一种开创性性的技术，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。

安网采用区块链协议“安资”协议来发行数字资产，与 Ethereum 用智能合约发行数字资产相比，有更高的安全性。智能合约是典型的程序，状态变化非常多，虚拟机的安全控制还不成熟，测试很难完全，出错的可能性更多。自从比特币出现以来，从比特币协议的漏洞中获得比特币的事件还未发生过，究其原因，是因为协议的状态变化非常有限，更容易测试和安全控制，安网使用协议来发行数字资产， 更为安全，而智能合约在安网上仅用于业务逻辑的实现。

1.2.2 发行资产的便捷性

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。

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。安网完全实现了这一点，使得非技术人员即可在手机 APP 上一键发行数字资产。

Archived copy · cryp2nova.com

1.2.3 隐私保护

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。

DNC（DarkNetSpace，项目名称暗网空间，后改名安网）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。

CrytpoNote 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，因而安网 3 把隐私保护的特性当成可选项。

1.3 安网历史

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。

2017 年 7 月，安网团队将安网 1 升级到安网 2（Anwang2），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。

- 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：
- 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。
- 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

Archived copy · cryp2nova.com

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。

- 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。
- 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。
- 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。

2018 年 1 月，SAFE 基金会决定分叉 DASH，合并安网 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。



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 25 日，项目进展如下：

- 安网已经有 1900 个主节点；
- 安网 SAFE 已经在 zb.com ,coinegg.com, dragonex.io , hb.top, kex.com, oex.com, chaoex.com，btctrade,im，coolcoin.com 上线交易；

Archived copy · cryp2nova.com

- 安网 SAFE 已上线矿池 vvpool.com，目前已经有稳定的算力；
- 安网 SAFE 已上线币看钱包 bitkan.com 和比特派 bitpie.com；

到 2019 年 1 月 3 日为止，项目进展如下：

- 2018 年 9 月支持安资协议和 SAPP 协议的安网主网 2.0 升级成功，PC 钱包， Android APP，IOS APP、区块浏览器上线；
- 2018 年 10 月 SAFE 提案管理系统已经上线；
- 2019 年 1 月 3 日安网已经有 3000 个主节点；

1.4 安网应用

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：

- 安资（资产管理与发行）：

  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。

- 安付（即时支持、安全支付）：

  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。

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。

Archived copy · cryp2nova.com

1.5SAFE 分配

SAFE 的分配比例如下所示：

（1）代币数量：近 2960 万枚，实际 SAFE 数量会更少，因为每区块 10%的奖励是在每月一个超级块中给出的，但是不是所有的超级块都被挖出（如 2018 年 1 月份-12 月份未产出超级块）；

（2）2.7%给原达世币持有者，约 80 万枚。

（3）37.2%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 3.67%，提案激励可能不会全部产出）；

（4）13.5%给团队，约 400 万枚；

（5）20.3%用于市场推广，约 600 万枚；

（6）26.4%用于兑换，约 780 万枚；

1.6 挖矿增益



Archived copy · cryp2nova.com

1.6.1 主节点和矿工收益

（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。

（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）；

1.6.2 活动增益

（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）；

（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：

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	

（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；

Archived copy · cryp2nova.com



1.6.3 增益活动执行情况

截止 2018 年 7 月 28 日，主节点和挖矿增益已经全部发放完毕。经统计，共发放增益 24 次，总计发出 142361.70199473 个 SAFE。

2 以往开发经验

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：

- 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；
- 2016 年 9 月发布联盟链（BLChain, Consortium Blockchain）；
- 2016 年 9 月发布商业银行抵押品区块链；

Archived copy · cryp2nova.com

- 2016 年 11 月发布数字积分区块链；
- 2017 年 3 月发布仓单质押融资区块链；
- 2017 年 7 月，暗网空间正式更名为安网，并发布安网 2 钱包；
- 2018 年 1 月 20 日分叉达世，安网 3 问世；
- 2018 年 9 月安网主网升级成功；安资、SAPP 开发协议上线；

由此可见，安网团队是一个在区块链行业耕耘 6 年多、开发过十几个区块链项目、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。

3 安网的商业价值

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。

3.1 应用开发

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。

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。

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。

Archived copy · cryp2nova.com

3.2 安付

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。

安付是安网的基础设施，安资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。

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。

3.3 安资

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。

安资的商业价值：

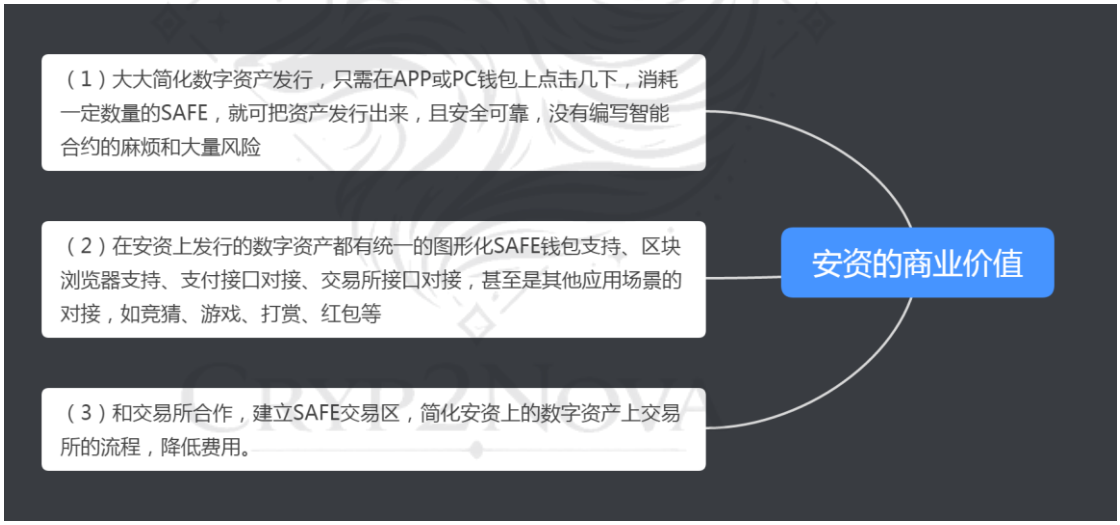
Archived copy · cryp2nova.com

（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；

（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；

（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。

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。

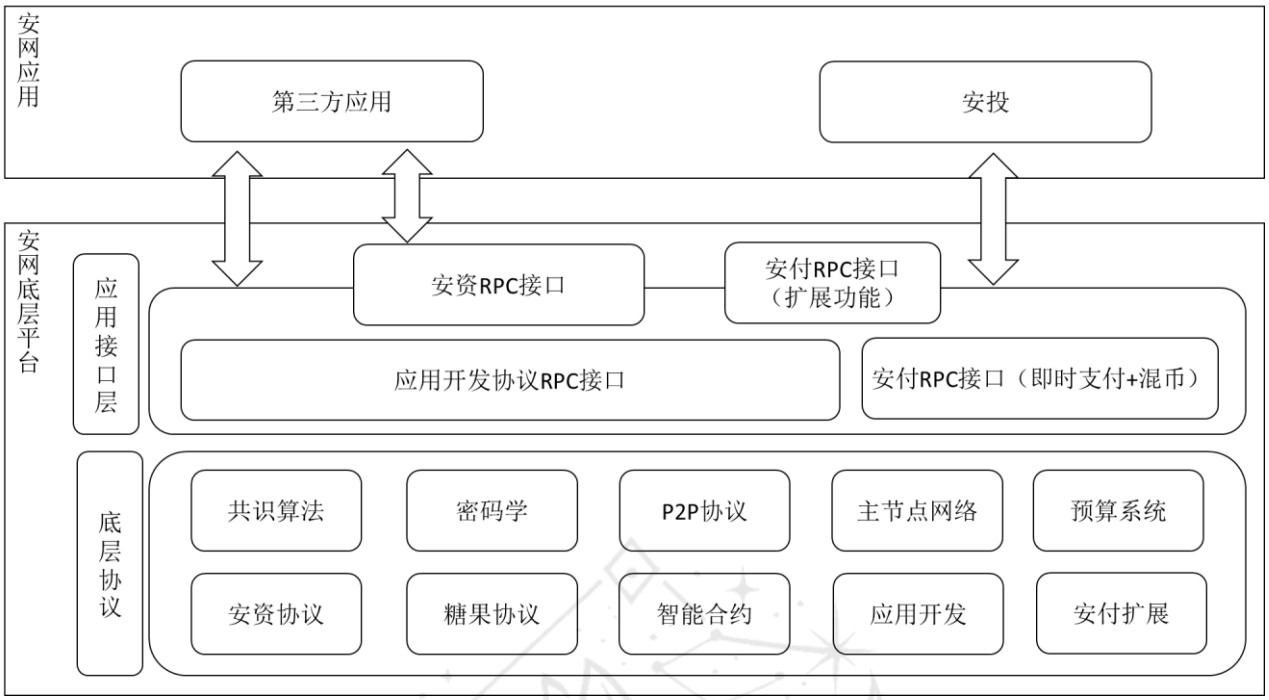


安资协议已经于北京时间 2018 年 9 月 26 日上午 10 点开始，正式启用。

4 安网的系统架构

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：

Archived copy · cryp2nova.com



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。

4.1 共识算法 SafePOS

1、安网 V2.1 以下版本的挖矿算法从 DASH 继承，未作修改。

（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）；

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

（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；

2、安网 2.5 版本将修改共识算法，从 POW 转换到 SafePOS，思路如下：

从全网主节点中随机选取记账者进行产块，好处在于:

Archived copy · cryp2nova.com

（1）大大缩短产块时间，极大提升交易性能。POW 产块时间 2.5 分钟，SafePOS 产块时间预计在 3-10 秒内，为后续的应用做准备；

（2）大大增强安全性，目前 SAFE 的算力很低，面临 DASH 算力的 51%攻击风险，转换成 SafePOS 之后不用担心 51%攻击。相比 DPOS，减少 DDOS 攻击风险；

（3）降低挖矿门槛，减少能耗。用户抵押 1000 个 SAFE 建立主节点就能挖矿，无需昂贵的 ASIC 矿机投入；

（4）记账更去中心化，在所有主节点中随机选取记账者，更加符合去中心化精神。

技术原理如下：

1）从所有主节点中选取 9 个记账者，每个主节点从全网主节点列表中选取在线时长大于 3 天主节点进入候选列表中；

3）对候选列表按照得分从高到低进行排序，得分计算规则： 用主节点抵押地址、当前链最新区块的时间生成一个 HASH 值，对 HASH 计算出一个整数；

4）从排好序的列表中随机选取 9 个记账者，该随机算法能保证每个节点选择出来 9 个记账者完全是一样的，具体原理请参考：http://xorshift.di.unimi.it/；

5）9 个记账者轮流生成区块，1，2，3，4，5，.....，9；

6）一轮区块产生完成后，重新随机选取 9 个记账者；

Archived copy · cryp2nova.com

4.2 密码学算法

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:

- 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；
- 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；
- 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；
- 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；
- 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；
- 同态技术：安付拟采用同态加密技术对金额进行加密隐藏；

4.3 主节点网络

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，2019 年 1 月 4 日已经有 3000 个主节点。

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：

（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

Archived copy · cryp2nova.com

VPS 提供商，该工具可在官网上下载；

（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，该脚本可在官网上下载；

（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；该功能已经在 V2.0 版本中实现；

（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；

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。

4.4 预算系统

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。



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

Archived copy · cryp2nova.com

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。

该功能所对应的提案系统已经在官网上线。

4.5 应用开发协议

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。

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。

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。

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。

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。

Archived copy · cryp2nova.com

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。

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。

该功能已经在 V2.0 版本中实现。

4.6 安资协议

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。

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。

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。

该功能已经在 V2.0 版本中实现。

Archived copy · cryp2nova.com

4.6 糖果协议

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。

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，每个代币最多发送 5 次糖果， 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 1-3 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。

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。

该功能已经在 V2.0 版本中实现。

4.7 安码/智能合约

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安码，即安网上的智能合约系统。

Archived copy · cryp2nova.com

安码的技术路线是移植 EOS 账户体系，兼容 EOS、ETH 和 FABRIC 的智能合约，形成独有的智能合约虚拟机 SVM，以及独有超强兼容性的安网智能合约平台，以便更易于从 EOS 和 ETH 中构建安网生态。

4.8 安付扩展



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：

4.8.1 增加转账备注

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。该功能已经在 V2.0 版本中实现。

Archived copy · cryp2nova.com

4.8.2 环签名发送

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。

安网 3 将继承该技术，实现环签名发送。

4.8.3 隐身收款

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。

环签名发送和隐身收款可以组成一个更隐私的交易。

4.8.3 金额隐藏

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。

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。

Archived copy · cryp2nova.com

4.9P2P 协议

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。

5 安网的技术方案

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。

5.1 分叉技术方案

5.1.1 分叉原理

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。

5.1.2 相关参数

	主网络	测试网
P2P 端口	5555	15555
RPC 端口	5554	15554

Archived copy · cryp2nova.com

ZMQ 端口	5553	15553
P2P 协议标识	62696ecc	52595ebb

5.1.3 配置文件

- 数据存放路径

  Linux：/root/.safe

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

- 配置文件名

  Linux:/root/.safe/safe.conf

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

5.1.4 交易结构

从区块高度 807085 开始，在交易结构的输出中，增加了两个字段：

（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；

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

5.1.5 区块难度和奖励

（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

Archived copy · cryp2nova.com

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；

（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；

5.1.6 矿池



矿池需要配合修改如下：

（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；

（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；

Archived copy · cryp2nova.com

5.2 应用开发协议

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。

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。

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。

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。

应用数据区中，应用头结构如下：

应用数据区	说明
safe	安网应用标识，小写
版本号	应用头版本号
应用 ID	根据注册应用信息生成的全网唯一应用 ID
应用命令	应用数据中的应用命令，由用户自定义

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。

5.2.1 应用注册

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；

Archived copy · cryp2nova.com

未注册的应用写入数据到应用数据区，将会被全网拒绝。

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。

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。

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。

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。

5.2.2 应用命令设计

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。

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

Archived copy · cryp2nova.com

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。

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：

发起人 / 应用命令	所有人	商家	开发商
注册商家	√		
商家审核结果			√
发布电影票信息		√	
付款下订单	√		
发送电影票 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。

5.2.3 应用权限设定

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。

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。

Archived copy · cryp2nova.com

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：

上述的在线电影票订单系统，假设它的应用 ID 为

cf4362534be51d429585ccf8cab7d2a07e190588c69bde9f56e4dfec09a0a666

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：

发起地址 / 命令号	所有地址	商家地址	开发商地址
注册商家 1	√		
商家审核结果 2			√
发布电影票信息 3		√	
付款下订单 4	√		
发送电影票 ID 5		√	

三条权限规则：

（1）公钥 0 + 1、4，即所有地址都可注册商家、付款下订单；

（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；

（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；

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，

Archived copy · cryp2nova.com

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。

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。

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。

5.2.4 应用数据写入

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。

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：

序号	应用数据项	说明
1	版本号	用于版本升级
2	与应用命令对应的自定义数据	自定义数据

如果有加密需求，则可上述两个数据项中间再加两项：

2	加密算法	无、AES 或 ECC
3	用接收方公钥加密的密钥	如果是 AES 加密的话

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。

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。

Archived copy · cryp2nova.com

5.2.5 额外交易费

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：

- 应用数据区只有 4 个字节（SAFE）数据，不收额外交易费；
- 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；
- 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；
- 额外交易费的体现和正常交易费一样，由矿工挖矿获得；

5.3 安付



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。

Archived copy · cryp2nova.com

5.3.1 即时支付

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：

（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；

（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；

（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；

（4）矿池把该锁定交易打包到区块并且广播到全网；

5.3.2 混币

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：

（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；

（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；

（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。

（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；

（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，

Archived copy · cryp2nova.com

你的资金已经被混淆了，不需要额外的等待；

5.3.3 增加转账备注

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。

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：

1	版本号	用于版本升级
2	加密算法	无、AES 或 ECC
3	用接收方公钥加密的密钥	如果是 AES 加密的话
4	转账备注	加密或非加密数据

5.3.4 环签名发送

环签名它主要由下列算法组成，假定有 n 个用户。

- 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；
- 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；
- 验证 Verify：输入 (m,R)，输出合法与否。

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。

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。

Archived copy · cryp2nova.com

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。

5.3.5 隐身收款

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：

（1）双密钥的隐身地址

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。

其使用场景如下：

- 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。
- 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。
- 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 $SHA256(dP)==SHA256(eQ)$。
  - 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 $T\neq T'$，不能计算出正确的目的地址。

Archived copy · cryp2nova.com

- ❖ 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。
- ❖ 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 $l = (f + s)$。

（2）单密钥的使用场景如下：

- ❑ 用户 A 公布隐身地址 $Q = dG$， d 为私钥，G 为椭圆曲线的基点。
- ❑ 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。
- ❑ 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 $SHA256(dP) == SHA256(eQ)$。
  - ❖ 如果用户 A 没有正确的私钥 d，计算出错误 s 和 T'，因而 $T \neq T'$，不能计算出正确的目的地址。
  - ❖ 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。

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。

5.3.6 金额隐藏

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：

承诺= SHA256（盲化因子||数据）

Archived copy · cryp2nova.com

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。

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）：

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。

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。

(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。

5.4 安资

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。

5.4.1 资产发行

可发行数字资产，发行代币必须消耗 500 个 SAFE，每月（17280 个区块）

Archived copy · cryp2nova.com

减少 5%，直到不少于 50 个 SAFE，目的是防止在安网上滥发代币。发行游戏装备类的数字资产可先首次发行一类资产，后续再追加发行其他类别资产，则追加发行不需要消耗 SAFE；

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；

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。

发行交易如下：

- 输出一：

输出金额：要消耗的 SAFE

输出脚本：正常转账交易脚本，接收地址为黑洞地址

vReserve 字段：safe

- 输出二：

输出金额：初次实际发行资产数量

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）；

vReserve 字段：应用头 + 应用数据（资产发行）

资产发行 应用数据	说　　明
版本号	2 字节
资产简称	最大 20 个字节，1 个汉字可能占 3 个字节
资产名称	最大 20 个字节，1 个汉字可能占 3 个字节
资产描述	最大 300 个字节，1 个汉字可能占 3 个字节

Archived copy · cryp2nova.com

资产单位	最大 10 个字节，1 个汉字可能占 3 个字节
资产总量	如果为 0，代表总量不受限，可一直追加发行
初次发行总量	第一次发行的数量
初次实际发行总量	
小数点位	最小 4 位，最大 10 位，例如：100000000，代表是 10 的负 8 次方；
是否可以销毁	有些资产可以销毁，有些不能，用户自行设置
是否分发糖果	是否给 SAFE 持有用户分发糖果
分发糖果比例	拿出总量的 0.1%-10%来发给 SAFE 的持有用户
糖果过期时间	以区块数计的时间，1-3 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。
备注	最大 500 个字节，1 个汉字可能占 3 个字节

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。

- 输出三：

输出金额：糖果数量

输出脚本：正常转账交易脚本，接收地址为糖果地址

vReserve 字段：应用头 +应用数据（转账）

转账应用数据	说　明
版本号	2 字节
数字资产 ID	为 0，即当前数字资产
数量	0.1%-10%数量
糖果过期时间	存放是月的个数，范围在 1-3 个月
备注	最大 500 个字节，1 个汉字可能占 3 个字节

Archived copy · cryp2nova.com

5.4.2 追加发行

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-糖果数量。

输出地址必须是发行时的输入地址之一，交易格式：

输出金额：追加资产数量

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）

vReserve 字段：应用头 +应用数据（转账）

转账应用数据	说　明
版本号	2 字节
数字资产 ID	要追加发行的资产 ID
追加数量	追加发行的数量
备注	最大 500 个字节，1 个汉字可能占 3 个字节

5.4.3 转账

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：

输出金额：资产数量

输出脚本：正常转账交易脚本

vReserve 字段：应用头 +应用数据（转账）

转账应用数据	说　明
版本号	2 字节

Archived copy · cryp2nova.com

数字资产 ID	要发送的资产 ID
数量	发送的数量
锁定时间	以区块计的锁定时间，0 表示不锁定
备注	最大 500 个字节，1 个汉字可能占 3 个字节

5.4.4 销毁

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。

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：

输出金额：销毁资产数量

输出脚本：正常转账交易脚本，输出地址是黑洞地址

vReserve 字段：应用头 + 应用数据（转账）

转账应用数据	说　明
版本号	2 字节
数字资产 ID	要发送的资产 ID
数量	发送的数量
备注	最大 500 个字节，1 个汉字可能占 3 个字节

5.4.5 发放糖果

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，但每种资产最多只能发放 5 次糖果。该接口必须由资产发行地址来调用，交易格式如下：

Archived copy · cryp2nova.com

输出金额：分发糖果数量

输出脚本：正常转账交易脚本，输出地址为糖果地址

vReserve 字段：应用头 + 应用数据（发放糖果）

转账应用数据	说　明
版本号	2 字节
数字资产 ID	要发糖果的资产 ID
分发资产比例	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。
糖果过期时间	以区块数计的时间，1-3 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。
备　注	最大 500 个字节，1 个汉字可能占 3 个字节

5.4.6 领取糖果

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：

输入：糖果对应交易 ID、输出项索引；一个 SAFE 输入，用于支付交易费；

输出：正常转账交易脚本，持有 SAFE 的地址；输出可能有多个，因为拥有 SAFE 的地址有多个；

金额：领取糖果数量；

领取规则：

（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；

（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；

Archived copy · cryp2nova.com

（3） 领取时间如果过期，则不让领取；

（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；

（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；

5.5 安码

安码将重点加强智能合约的安全性、易用性、兼容性。

5.5.1 安全性

（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。

（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。

（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。

（4） 智能合约的执行验证机制，SVM 向开发者提供友好的可编程性，同时对安网带来较大的性能开销，为最大程度避免对安网 UTXO 交易性能与稳定性的影响，将在全网投票选出 21 个硬件性能达标的超级节点，专职负责智能合约的执行验证，普通主节点专职负责 UTXO 交易的执行验证，对于智能合约则直接从某个超级节点获取合约的执行验证结果。

Archived copy · cryp2nova.com

5.5.2 易用性

（1） 智能合约的可读性名称，参考 FABRIC 及 EOS，在创建合约时指定类似互联网域名的便于人为阅读与记忆的名称，后续通过该名称使用合约，更加便于合约的推广。

（2） 智能合约的可升级机制，参考 FABRIC 及 EOS，分离存储合约代码及合约状态数据库，合约的 Owner 及其授权用户，可通过重新部署合约代码实现升级，避免如 EVM 必须通过重新部署合约与迁移合约状态数据库曲折地实现升级。合约使用者通过合约名称、合约版本号引用期望版本的合约，避免不知情地引用了未受信任的最新版本合约。除非合约使用者完全信任合约开发者，可指定虚拟的合约版本号，实现随时引用当前最新版本的合约。合约开发者不能为合约使用者指定引用某个版本的合约，但有权利根据智能合约升级演进的需要，停止某个版本合约的对外服务。

（3） 智能合约的状态数据库升级，参考 FABRIC 及 EOS，提供对应的智能合约 api，支持在智能合约运行期而非编译期可以动态地修改状态数据库结构，避免为修改状态数据库结构而需通过迁移实现升级，能够简化开发者的操作步骤，同时节省 SVM 的存储与性能开销。

（4） 智能合约的状态数据库存储，在 Sapp 的项目实践中，常见需要将 Sapp 存储于区块的应用数据，转存于关系数据库，以便进行结构化数据查询。SVM 将选型若干满足性能的关系数据库引擎作为合约状态数据库的存储后端，由合约开发者指定引擎类型，通过合约代码读写合约状态数据库，通过数据库引擎客户端只读合约状态数据库。合约状态数据库的访问权限控制、数据脱敏和隐私保护、脱敏过程保持数据特征及关联关系等，由合

Archived copy · cryp2nova.com

约开发者自行负责处理。

5.5.3 兼容性

（1） 智能合约的 api，目前安网通过协议实现了应用开发、安付、安资、安投四大功能版块，SVM 将通过智能合约的 api 向开发者开放关于各功能版块的可编程能力。

（2） 智能合约的燃料与奖励机制，参考以太坊 EVM，SVM 计算 GAS 用量，通过 GAS 价格换算为 SAFE 用量。SAFE 官方向特定地址发送特定的交易调控 GAS 价格。GAS 由合约调用者承担，且奖励给矿工。为鼓励开发者勇跃地贡献高质量的智能合约服务，SAFE 官方将与社区共同研讨：将部分 GAS 奖励给被当前合约调用的合约的开发者。

（3） 同时兼容多种智能合约源码，例如以太坊和 EOS，最大程度方便开发者导入和导出技术成果。安网更进一步地构思，在可以统一各类参照的区块链产品功能模型的前提下，求同存异，实现在安网体系内不同类型智能合约的相互调用。。

安码的具体技术方案还在继续完善中，将另出文档详细描述安码技术细节。

6 安网路线图

安网路线图如下所示，有任何调整，我们将在官网上通知。

Archived copy · cryp2nova.com



7 安网的技术创新点

安网有不少其他区块链不具备的技术创新点，表现如下：

7.1SafePOS 共识算法

安网 2.5 版本的独有的共识机制 SafePOS，从全网 3000 多个主节点中随机挑选 9 个在线时间长、稳定的主节点每隔 5-10 秒顺序产生一个区块，这一轮生产完了，再挑选 9 个主节点，依次进行。

SafePOS 比 POW 出块更快速，更不易受到 51%攻击；与采用 DPOS 的 BTS 的 101 个节点、EOS 的 21 个节点相比，出块节点更随机化、去中心化，因而更安全。

7.2 安资协议

安资协议以协议的方式进行数字资产发行，与智能合约发行资产相比，安全性更高，因为协议是有限状态机，可控性更强，而智能合约的行为更不可控。

Archived copy · cryp2nova.com

安资不但实现了资产发行、追加发行、转让资产、销毁资产等功能，而且还实现了区块链上的糖果协议，发行方可以在安网上分发糖果以及领取糖果。

7.3SAPP 应用开发协议

SAPP 应用开发协议是一系列 RPC 接口，包括了应用注册、应用权限设定、应用数据写入等几种，方便区块链应用开发者方便地写数据到安网区块链上。

SAPP 应用需要注册，并且 RPC 接口需要消耗 SAFE，以免像 ETH 和 BITCOIN 一样，谁都可以随意写入数据，垃圾数据泛滥。

7.4 安码智能合约系统

安码的最大的特点是安全性强、兼容性高、易用性高。安码将移植 EOS 账户体系，兼容 EOS、ETH 和 FABRIC 的智能合约，形成独有的智能合约虚拟机 SVM，以及独有超强兼容性的安网智能合约平台，以便更易于从 EOS 和 ETH 中构建安网生态。

到目前为止，还未出现该种兼容性的智能合约系统。

CRYP2NOVA

安网团队

2019 年 1 月 9 日

Archived copy · cryp2nova.com