安网（SAFE）4 白皮书

v0.1

SAFE Foundation（Singapore）

2025 年 4 月 30 日

目　　录

安网（SAFE）4 白皮书

安网（SAFE），作为新加坡 SAFE 基金会于 2014 年 10 月推出的去中心化区块链，专注于安全支付与隐私计算领域，至今近 11 年，期间历经安网 1.0、2.0、3.0 三个重要阶段，成功迭代至安网 4.0 版本，在技术与应用层面均取得了诸多突破与进展。

安网 SAFE4.0（以下简称 SAFE4）携多年的实践经验和成果，以密码学理论和隐私安全为基础，以技术创新和应用创新为导向，着眼隐私保护，强化安全支付，优化资产隐私，引入跨链资产和稳定币，打造 SafeSwap 去中心化兑换，拓展更多商业化应用，旨在构建一个全球范围的安全支付和隐私保护生态圈。

1. 设计理念

1.1 去中心化

去中心化是区块链的精神所在，SAFE4 进一步优化去中心化设计，去中心化的特点体现在：无需任何人或机构的许可，即可参与 SAFE4 区块链；利用开源代码，轻松建立 SAFE4 区块链节点；无论是建立主节点获取收益，还是参与超级节点竞选获得挖矿奖励，人人皆有机会；此外，安网的运维参数及社区治理提案，均由超级节点发起并投票决定，等等。

1.2 隐私需合规

在个人信息被滥用的现今，我们始终相信个人的资产和数据不应该由大公司和大企业所把控，SAFE4 致力于开发隐私保护应用，以保护个人的数据资产和数字资产隐私。同时，SAFE4 也重视合规性，认识到隐私保护不应成为犯罪行为的掩护。因此，SAFE4 不支持绝对匿名，而是提供技术手段，允许在公共部门合法要求下，通过超级节点发起的投票程序，决定是否向公共部门披露非隐私化的区块链交易信息。

1.3 EVM 生态兼容

区块链的设计需有利于围绕区块链的生态建设，没有人使用的区块链是无效项目。建设好高速公路的同时，也要有更多的车辆愿意驶入此高速公路。因而必须吸引更多的开发者和使用者，才能使安网从众多优秀区块链平台中胜出。

SAFE4 采用 EVM 虚拟机，完全兼容 Web3 接口和 Web3 SDK，在此基础上加入 SAFE4 特有的区块链协议接口，方便引入更多的开发者和生态应用接入 SAFE4。

1.4 协议合约化

区块链协议的开发困难不小，一有错误将带来分叉和资产损失；经过近十年的探索和研究，我们决定把区块链协议合约化，业务流程尽可能由合约来实现，方便之后修改和更新，区块链底层改变越少越好。这些区块链协议包括主节点、超级节点、产块分红、投票分红、资产发行等；其中 SAFE4 资产发行完全由 SRC20（即 SAFE4 上的 ERC20）协议来实现，不再支持 SAFE3 协议层的资产发行；

1.5 其他约束

SAFE4 并非新项目，而是有着 11 年历史的老项目，资产延续是必须的，SAFE 的总量与分配状态不变，不增不减；另外安网 1、安网 2 和 SAFE3 的好思路和实践成果自然要延续下去，如主节点机制、提案机制、锁仓机制等；

2. 安网历史

2.1 安网 1—DNC

安网空间（简称安网）的代币 DNC 早在 2014 年 10 月份就已经上线，是中国最早的关注个人隐私保护的数字货币，最大的特色是支持环签名、隐身地址。

- 环签名

环签名是安网 1 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。

- 隐身地址

隐身地址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。其他验证者也可以验证币的数量没有变。

环签名发送和隐身收款可以组成一个更隐私的交易。

2.2 安网 2—DNC2

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聊天中；

2.3 安网 3—SAFE3

2018 年 1 月，SAFE 基金会合并投票链和安网 2 升级成安网 3，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，安网 3 正式上线。主要特色：主节点网络、SafeDPoS 共识、SAPP 应用开发、安资、安付、安投、安宝等等。

- 主节点网络：承担了安网的即时支付、隐私支付、对提案投票等功能，当前安网 3 存在的主节点数已达 8660+；
- SafeDPoS 共识：SAFE3 从全网众多主节点中随机挑选 9 个在线时间长、稳定的主节点每隔 30 秒产生一个区块，让每个主节点都有机会参与到安网 3 区块链的建设中，并能实现绿色共识，避免消耗过多的能源；
- SAPP 应用开发：支持用户在安网 3 上开发应用服务，并提供了区块链中间件服务；
- 安资：允许用户在安网 3 上开发各种代币和数字资产，包含发行、追加发行、转让、销毁、发放糖果、领糖果等功能；
- 安付：安网 3 除了普通转账功能外，还支持即时支付、混币（隐私支付）、转账添加备注、隐身收款、金额隐藏等功能；

以下的安投和安宝并非 SAFE3 的功能，而是生态产品。

- 安投：一款专门用于投票、选举和彩票领域的区块链应用，保证每个用户以真实或虚拟身份参与投票；
- 安宝：是安网团队出品的一站式数字资产安全管理硬件钱包，采用了国密级金融安全芯片确保种子密码和私钥的安全，私钥不触网，冷端离线构造出交易和签名，热端 APP 联网发送交易，冷热端通过二维码扫描的方式传输数据，具有极高的安全性；

SAFE3 从新加坡时间 2018 年 1 月 20 日上线，到 2025 年 4 月 25 日上午 11 点 6663611 高度后停止运行，共计运行了 7 年 3 个月。

2.4 安网 4—SAFE4

SAFE4 主网于新加坡时间 2025 年 4 月 26 日 11 点正式上线，SAFE4 是 SAFE3 的继承和延续：

- SAFE 总金额不变，产块时间不变，每块 SAFE 数量不变；
- 主节点功能不变，奖励金额不变，产块奖励数量不变；
- 每个地址内的 SAFE 锁仓状态不变，SAFE4 延续锁仓时间；
- 提案系统每个区块 10%的奖励不变，用于支持社区发展；

2.4.1 SAFE4 主网参数

- Web3 接口： https://safe4.anwang.com/rpc
- API 接口 ：https://safe4.anwang.com/api
- chainId=6666665
- WSAFE 合约地址： 0x0000000000000000000000000000000000001101
- 多签合约地址： 0x0000000000000000000000000000000000001102
- 区块浏览器： https://safe4.anwang.com

2.4.2 SAFE4 测试网参数

- Web3 接口： https://safe4test.anwang.com/rpc
- API 接口 ： https://safe4test.anwang.com/api
- chainId=6666666
- WSAFE 合约地址： 0x0000000000000000000000000000000000001101
- 多签合约地址： 0x0000000000000000000000000000000000001102
- 区块浏览器： https://safe4testnet.anwang.com

2.4.3 SAFE3 向 SAFE4 迁移

SAFE3 向 SAFE4 迁移，迁移规则如下：

- SAFE3 的 SAFE 可按 1:1 比例置换为 SAFE4 代币，此置换无时间限制，可随时进行。
- BSC/ETH/Matic 链上的 SAFE 代币无需置换，届时跨链至 SAFE4 即可。
- 快照时少于 0.03 SAFE 的锁仓记录、SAFE 金额少于 0.03 的地址将被忽略，这是一个折衷方案，为了保证尽可能少的数据量、忽略尽可能少的 SAFE。
- SAFE3 的主节点可迁移至 SAFE4，主节点地位不变；
- 产块奖励给到超级节点；锁仓和非锁仓 SAFE 皆可给超级节点投票；
- SAFE3 的主节点迁移至 SAFE4，未锁仓的主节点要加锁 3 个月，已锁仓的回锁 6 个月；

在 6663611 高度快照下，SAFE3 统计结果如下：

- 总金额： 2243.8028 万
- 总可用金额： 1041.0887 万 地址数： 4.2385 万
- 总锁仓金额： 1127.0611 万 地址数： 2.2961 万 锁仓记录数： 226.5852 万

上述金额将迁移至 SAFE4

总忽略可用金额： 113.93 地址数： 42.0424 万（这部分会补偿）

总忽略锁仓金额： 1.7016 万 地址数： 1.2827 万 （这部分会补偿）

忽略部分将不迁移，开发团队给予补偿。

2.4.4 SAFE4 跨链

SAFE4 继承了 SAFE3 与 BSC/ETH/Matic 网络的双向跨链功能，在 BSC/ETH/Matic 上的 SAFE 无需进行映射，只需等跨链功能开启就可转回 SAFE4 网络。

以下是 SAFE4 主网和测试网对应的 BSC/ETH/Matic 网络的 wSAFE 合约地址和资产池地址，其中 wSAFE 合约地址是 SAFE 在该区块链上的 SRC20 合约，而资产池地址则是在 SAFE4 主网或测试网上的地址，用于接收和发送对应区块链的 SAFE。

SAFE4 主网：

BSC 网络：

合约地址： 0x4d7fa587ec8e50bd0e9cd837cb4da796f47218a1

SAFE4 资产池地址： 0x471B9eB32a6750b0356E0C80294Ee035C4bdF60B

ETH 网络：

合约地址： 0xEE9c1Ea4DCF0AAf4Ff2D78B6fF83AA69797B65Eb

SAFE4 资产池地址： 0x30728eBa408684D167CF59828261Db8A2A59E8C7

Matic 网络：

合约地址： 0xb7Dd19490951339fE65E341Df6eC5f7f93FF2779

SAFE4 资产池地址： 0x960Bb626aba915c242301EC47948Ba475CDeC090

SAFE4 测试网：

BSC 网络：

合约地址： 0x3a5557AD6FA16699dD56fd0E418C70c83e42240a

SAFE4 资产池地址： 0x7756B490d4Ce394bB6FBA5559C10a8eDc7b102Fc

ETH 网络：

合约地址： 0x96f59C9D155d598d4f895F07dd6991cCB5FA7DC7

SAFE4 资产池地址： 0xaD016d35FE9148F2a8D8A8d37325ada3B7070386

Matic 网络：

合约地址： 0xe0D3ff9b473976855B2242a1A022aC66f980Ce50

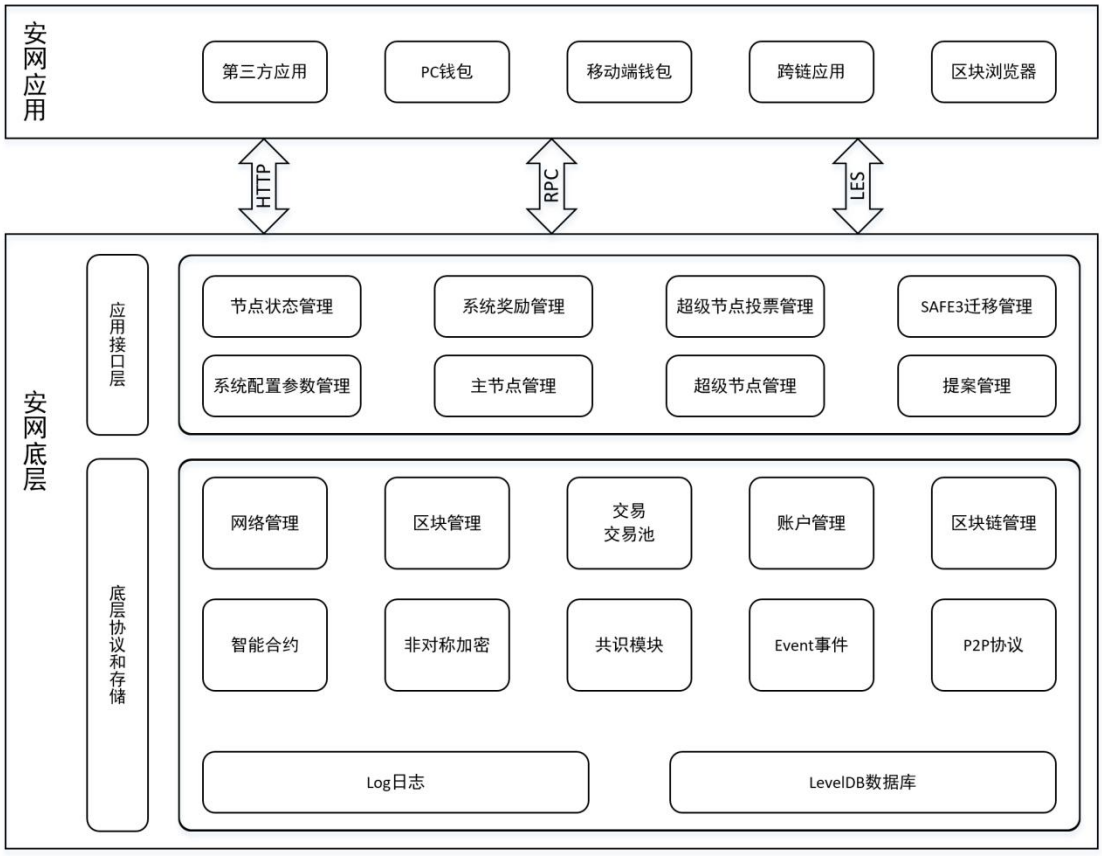
SAFE4 资产池地址： 0x8b151740b4a5B2bF7dA631AAD83Be627f97F5790

3 技术设计

功能和技术的创新和引入必须为设计理念服务，单纯的功能和技术堆砌是没有用的。比特币围绕着去中心化引入了一系列技术如工作量证明和 SHA256 挖矿、椭圆曲线签名算法、P2P 对等网络、默克尔树等，诞生了一个加密货币行业。

SAFE4 的功能和技术设计，也将围绕着上述设计理念来选择和创造所需功能和技术，并且将之有机结合。SAFE4 兼容 EVM，因而底层协议包括从 EVM 沿用过来的密码学、EVM 智能合约、Event 事件、P2P 协议、网络管理、区块管理、交易管理、交易池机制、账户管理、区块链管理等机制。

以下将阐述 SAFE4 的独有技术，包括网络架构、智能合约、奖励和共识、资产管理、主节点、提案机制、L2 协议、运维管理、超级节点、SafeSwap、资产跨链、隐私保护、原子兑换、SAFE3 迁移等。



3.1 网络架构

SAFE4 的网络逻辑架构分为三层，第一层是轻客户端（手机钱包或轻 PC 钱包），它们是最终客户端，向客户直接提供各种 SAFE4 功能；仅更新与客户相关的交易和区块；向主节点发送区块链交易；

第二层是主节点+非主节点+不完全节点（SAFE4 PC 客户端），它们保存完整的区块链和所有交易，从超级节点处获得新区块和交易，并且向超级节点和其他主节点传播。其中包括：

- 主节点，抵押 1000 个 SAFE，转发交易和区块，为上一层提供服务，获得主节点奖励；主节点可单人创建，也可众筹创建；
- 非主节点，是指未抵押 1000 个 SAFE 的节点，虽不参与收益，也为 SAFE 网络提供服务；
- 不完全节点,是指未能提供 SAFE 网络接入服务的 PC 客户端,会转发区块和交易；

第三层是超级节点，由 SAFE 用户投票产生，其功能是：执行共识机制、产生区块、保存完整区块链、挖矿收益分配、社区投票和治理、智能合约运行和验证等等；与主节点一样，超级节点可单人创建，也可众筹创建；因而每个超级节点都是一个推广社区，一个开发团队；

3.2 SafeCode

SAFE4 的智能合约系统，以及运行于 SAFE4 的合约，我们称之为 SafeCode。SAFE4 采用 EVM 作为合约虚拟机，以方便各种 ETH/BSC 应用的合约移植。所有已经在 ETH/BSC 上运行的合约，皆可无缝运行于 SAFE4；同时通过 EVM 的开发工具链开发 Solidity 新合约，编译成字节码后在 SAFE4 上进行部署和调用。这种兼容非常有利于在 SAFE4 快速建立应用生态。

类似于 ETH，合约的运行需要 SAFE 作为燃料 GAS，以 gaslimit 和 gasprice 的乘积作为最终 GAS 费用，作为燃料的 SAFE 最终为区块生产者所获得；运行合约时预先支付一定数量的 SAFE，如果 SAFE 有剩余，则返还剩余 SAFE 给合约调用人。

系统 SafeCode 是由安网技术团队开发的、用于维护 SAFE4 正常运行的系统级合约，包括账户管理合约、奖励合约、锁仓合约、提案合约、主节点合约、主节点状态合约、超级节点合约、超级节点状态合约、超级节点投票合约，SAFE3 转移合约、多签合约等。这是协议合约化设计理念的具体体现，更方便之后的业务修改和升级，无需涉及底层更改。每个合约的具体业务在之后将会在《SAFE4 系统合约开发指南》中公布。

系统 SafeCode 全部是可升级合约，方便后续升级和维护。并且，升级权限由 3/5 多签合约控制，至少 3 个程序员同意才能升级，以防形成单点故障，保证安全性。

SafeCode 完全兼容现有的 Web3 接口和 Web3 SDK，在此基础上加入 SAFE4 特有的系统合约接口，方便用户对上述系统合约进行各种操作，包括领取主节点奖励、超级节点挖矿奖励、投票奖励、创建主节点和超级节点等；

3.3 奖励和共识

SAFE4 继续采用 SafeDPoS 算法产块，从全网投票数 Top49 的超级节点中随机选取记账者进行产块，技术原理如下：

- 从所有超级节点中根据投票数排名据挑选出 Top49 超级节点群，必须要求每个正式超级节点是在线且正常运行的；
- 对正式超级节点列表按照得分从高到低进行排序，得分计算规则：用超级节点地址、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；
- 从排好序的列表中随机选取 7 个记账者，该随机算法能保证每个节点选择出来 7 个记账者完全是一样的 ，具体原理请参考：

  http://xorshift.di.unimi.it/；
- 7 个记账者在同一高度下同时生成新区块，其中一个区块难度是 2，其他 6 个区块难度是 1，这些记账者随后将区块广播到网络中；
- 当前高度下的区块产生完成后，重新回到步骤 1 生产下一个区块；

每个区块被产出后会有一定数量的区块收益，随后会按照以下机制分发给各收益地址。

- 45%的区块收益会被分发给超级节点对应的收益人集群；

超级节点收益人集群包括：超级节点的创建者、超级节点的联合创建者、超级节点的投票人，这些收益人是根据当前超级节点的分红比例获取对应的收益；

- 45%的区块收益会被分发给主节点对应的受益人集群；

主节点受益人集群包括：主节点的创建者、主节点的联合创建者。

- 10%的区块收益会被分发给提案奖金池

提案奖金池用于给每个确认通过后的提案发放费用。

3.4 资产管理

SAFE4 资产包括基准货币 SAFE、SRC20 附生资产、跨链资产、隐私资产。

基准货币：即 SAFE，它作为 SAFE4 中的基准货币，用于激励区块生产、奖励主节点、转账交易费、合约 GAS、SafeSwap 的基准交易货币之一等；

附生资产：即通过 SRC20 合约发行的资产，与基于 ETH ERC20 发行的资产无差别；附生资产仅能运行在智能合约中。其中提供 wSAFE 的系统合约，SAFE 可随时转化为 SRC20 的 SAFE，反之亦然；SAFE4 上的 SAFE SRC20 合约地址：

0x0000000000000000000000000000000000001101

跨链资产：跨链资产存在于合约 SRC20 中，是其他区块链资产如 USDT/BTC/ETH 通过跨链网关 SafeGate 转账到由 SAFE4 控制的资产池中，同时在系统 SafeCode 上形成的 1:1 资产映射，跨链资产可在 SAFE4 上隐私化、在 SafeSwap 中交易、销毁后从资产池中跨链转出。

隐私资产：上述各类资产都能隐私化。SAFE、附生资产、跨链资产可通过基于 Pedersen 承诺改进的 SafePrivacy 算法进行隐私化，或者通过 L2 协议如 zkRollups 来做隐私化。隐私资产的技术方案在合适时间再公开。

3.5 主节点

SAFE3 的主节点机制将在 SAFE4 中延续和扩展。用户抵押 1000 枚 SAFE，购买云服务器 VPS 安装 SAFE3 节点程序，即可建立主节点，获取对应的区块收益。

主节点是 SAFE3/SAFE4 网络中的区块和交易数据提供者之一，为众多连接而来的客户端提供数据存贮、转发等服务，在 SAFE4 中将强化主节点列表机制，把主节点列表和状态更新写在区块链智能合约上，防止出现一些细小分叉，同时主节点将承担更多角色如二层网络节点。

SAFE3 主节点的 SAFE 迁移至 SAFE4，即可兼容当前主节点状态，VPS 系统必须安装 SAFE4 节点程序。

按照创建类型可分为独立主节点和联合主节点，说明如下：

- 独立主节点：独立质押 1000 个 SAFE 且锁定 2 年的主节点，在分配区块收益时会独自获取 45%的区块收益；
- 联合主节点：由多个地址共同创建的主节点，其中创始人需要质押至少 200 个 SAFE 且锁仓 2 年，联合创建者需要质押至少 100 个 SAFE 且锁仓 2 年，在分配区块收益时会按照主节点分红比例分发创建者和联合创建者收益，创建者将独立获取属于创建者的分红，所有联合创建者按照质押金额/1000 的比例获取联合创建者收益；

主节点的状态更新：SAFE4 的主节点会定期向 SAFE4 网络发送心跳，这些心跳信息是用于判定节点运行状态的重要数据。各正式超级节点会归纳收集最近的心跳消息，对于未收到心跳信息的节点判定为异常节点，随后定期上传异常节点信息。

当超过 2/3 的正式超级节点认为异常节点属实时，对应的节点才会被确定为异常节点。异常节点无法参与获取区块收益。

3.6 提案机制

SAFE3 有提案系统机制，只需花费 5 个 SAFE 即可发起各种提案，提案获得 10%以上的主节点投票通过，即可在每月一个的超级块中给予 SAFE 资助。每年有 10%的 SAFE 是由提案产生的，如果没有提案就不产生超级块，则该月原本 10%的 SAFE 产出就会消失，SAFE 总量会随之减少。

SAFE4 将延续这一传统功能，所有用户都可以发起提案，使用智能合约来实现投票，完全去中心化，且在轻钱包实现投票功能，方便用户使用。具体提案规则如下：

- 提案的所有支出费用都来源于每个区块的 10%奖励;每个区块中的 10%奖励自动进入提案合约待分配；

- 提案发起时需要由发起人支付 1 个 SAFE，花费的 SAFE 将会被销毁；
- 每个提案需要在指定时间内确认完成，超过时间且未被通过的提案将会被抛弃；
- 提案发出后，由正式超级节点对提案进行投票，当 25 个正式超级节点赞同时该提案被通过，随后提案发起人将会按照该提案的支付规则获取对应的支出费用；

3.7 SAFE4 运维

区块链的长期运维中经常会遇到运维参数不合适的情况，如交易费、区块容量限制、共识参数、启停某些功能等等，一般区块链只能硬分叉改变如 BTC、ETH。

SAFE3 通过开发团队私钥来实现部分参数改变，SAFE4 拟把上述此类参数由用户通过智能合约投票来改变，一旦改变后在一定的时间内全网生效，一方面使 SAFE4 有更强扩展性，另一方面也使得运维进一步去中心化。

当前 SAFE4 已内置了一些关键参数用于 SAFE4 的正常运行的初始参数，具体如下：

参数名	初始值	说明
block_space	30	区块间隔时间，30 秒
gas_price	10000000	Gas Price，影响交易手续费
masternode_min_amount	1000	独立主节点创始人最少锁仓金额，1000safe
masternode_union_min_amount	200	联合主节点创始人最少锁仓金额，200safe
masternode_append_min_amount	100	主节点合伙人最少锁仓金额，100safe
masternode_min_lockday	720	主节点创始人最少锁仓天数，2 年
masternode_append_min_lockday	720	主节点合伙人最少锁仓天数，2 年

supernode_max_num	49	最大正式超级节点数，49 个
supernode_min_amont	5000	独立主节点创始人最少锁仓金额，5000safe
supernode_union_min_amount	1000	联合主节点创始人最少锁仓金额，1000safe
supernode_append_min_amount	500	超级节点合伙人最少锁仓金额，500safe
supernode_min_lockday	720	超级节点创始人最少锁仓天数，2 年
supernode_append_min_lockday	720	超级节点合伙人最少锁仓天数，2 年
record_masternode_freezeday	30	成为主节点合伙人的冻结期 30 天。即过了冻结期才能成为其他主节点的合伙人
record_supernode_freezeday	90	成为超级节点合伙人的冻结期 90 天。即过了冻结期才能成为其他超级节点的合伙人
record_snvote_lockday	7	成为超级节点投票人的冻结期 7 天。即过了冻结期才能转投其他超级节点。
miner_reward_percent	0	矿工获取交易手续费的比例，默认 0，范围[0,100]，多余的手续费将被燃烧。

上述的运行参数可以由正式超级节点投票进行更改，更改规则如下：

- 任何一个正式超级节点都可以对参数进行申请更新；
- 所有正式节点可以对该申请进行投票；
- 超过 33 个正式超级节点投赞同票后，该申请通过，将对参数进行更新；
- 超过 16 个正式超级节点弃权或者拒绝时，该申请将被移除；

3.8 L2 协议

SAFE4 拟引入 L2 协议技术，如闪电网络（Lighting Network）、ZK-rollups 或其他二层技术，主要思路都是把大量小额交易放到区块链之外，快速安全确认，仅在区块链上记录初始和最终状态，因而可以显著减少区块链记录的交易数量。

在安网 L2 协议上的交易，我们称之为闪电支付。安网的主节点和超级节点是现成的 L2 协议节点，SAFE4 把 L2 协议和区块链有机整合在一起。

SAFE4 融合 L2 协议有如下好处：

（1）快速支付：闪电支付实时完成，无需区块链确认，且更安全，可用于大规模线下支付，使得安网 SAFE 可作为零售行业的支付平台和货币；SAFE4 引入稳定币，则完全可作为一种稳定的、大规模的支付手段。

（2）性能提升：L2 协议带离了大部分交易，运行合约 EVM 的压力骤降，区块链容量减少，存贮区块链空间需求减少，使得 SAFE4 运行更快，无需提升主节点硬件配置，方便去中心化。

（3）隐私保护：闪电支付的众多中间交易状态并未记录在区块链上，仅记录初始状态和结束状态，因而有保护交易隐私的作用。

（4）无需费用：闪电支付的众多中间交易无需任何费用，仅记录在区块链上的交易需要费用，与合约 SRC20 的费用相比，近乎免交易费。

3.9 隐私与合规

SAFE4 从隐私逻辑上分为两层，第一层是透明层，第二层是隐私层。资产从透明层进入隐私层，我们称之为资产隐私化，反之称为资产透明化。基本思想如下所述：

（1）透明层是默认的、可追溯的 SAFE4 区块链体系，常规地址和合约地址在透明层，可以相互转账；初始状态下隐私层没有任何资产，SAFE 和所有类型的资产都在透明层。

（2）隐私层是基于多种隐私技术开发而成的一系列系统 SafePrivacy 合约。提供了隐私化功能，隐私地址在隐私层，可与常规地址和合约地址互转；

（3）资产隐私化是一个可选方案，SAFE4 并不要求所有交易如此，一切决定权归用户；如果需要透明，使用常规地址和合约地址；如果需要隐私化，则在 SafePrivacy 合约生成隐私地址，把资产转入隐私地址；

（4）SAFE4 保护个人隐私，但并不保护犯罪与洗钱，SAFE4 的隐私层具有超级私钥机制并且定时更换，超级私钥可解密某一段时间内的交易记录。一旦有各国的公共安全部门有反匿名的需求，由 49 个超级节点投票通过后把超级私钥提供给公共安全部门，之后更换超级私钥。

隐私层的技术设计还在进行中，开发团队将出具 SAFE4 隐私保护白皮书，敬请期待；

3.10 超级节点

超级节点是 SAFE4 网络的区块生成者，用户可以通过质押的方式创建超级节点，每个运行正常的超级节点都有可能创建区块获取对应的区块收益。

超级节点创建时需要分配创建者、联合创建者和投票人分红比例。更完善的分红比例将会吸引更多的投票数，投票数将直接影响该超级节点是否有机会创建区块。

按照创建类型可分为独立超级节点和联合超级节点，具体情况如下：

（1）独立超级节点：独立质押 5000 个 SAFE 且锁定 2 年的超级节点，在分配区块收益时会独自获取 45%的区块收益中的创建者分红和联合创建者分红；

（2）联合超级节点：由多个地址共同创建的超级节点，其中创始人需要质押至少 1000 个 SAFE 且锁仓 2 年，联合创建者需要质押至少 500 个 SAFE 且锁仓 2 年。在分配区块收益时会按照主节点分红比例分发创建者收益、联合创建者收益和投票收益，其中创建者将独立获取属

于创建者的分红，所有联合创建者按照质押金额/5000 的比例获取联合创建者收益，所有投票人按照投票人票数/总票数的比例拆分投票人收益；

任何非超级节点的地址都可以对超级节点进行投票，这些投票将直接影响到超级节点排名，投票数排名前 49 的超级节点才有可能产生区块，而对应的投票人才能获取对应分红。

根据资产的锁仓情况分配不同的票数，具体规则如下：

- 每个地址至少 1 个 SAFE 起投，如 1 个或 1.1 个 SAFE，少于 1 个 SAFE 的地址需要用户预先汇总至 1 个；
- 1 个 SAFE=1 票，1 个 SAFE 只能投一个超级节点，不能同时投两个；
- 锁定的一笔 SAFE 只能投一个超级节点，解锁后可随意拆分多笔投多个超级节点；
- 投票后锁仓 SAFE 不会移动，但自由 SAFE 将划转至账户管理合约且有 7 天的锁定期，7 天后投票地址才能赎回 SAFE 或转投其他超级节点，转投时无需赎回 SAFE；

SAFE 类别	权重（对应金额）
自由 SAFE（未锁仓或已过锁仓期的 SAFE）	1:1
一般锁仓 SAFE（除主节点锁仓 SAFE 之外的未过锁仓期的 SAFE）	1:1.5
主节点锁仓 SAFE	1:2

注意：

- 每个地址可能拥有以上三种类型的 SAFE，投票时需要区分三种不同类型的 SAFE；
- 每个地址可以进行多次投票和可以投给多个超级节点；

3.11 SafeSwap

SafeSwap 是运行于 SAFE4、ETH、BSC 上的去中心加密货币兑换安码应用，由 SafeSwap 的 SafeCode、网站 app.anwang.com、对外 API 接口等三个部分组成，是安网生态的重要成员。

SafeSwap 前期仅在 ETH/BSC 运行，SAFE4 上线后部署到 SAFE4，主要功能类似于 uniswap 和 sushiswap，基本功能如下：

- 币种兑换： 以 USDT、SAFE、wSAFE（Wrapped SAFE）为基础货币，初始包括 SAFE/USDT，wSAFE/USDT 两个交易对，用户自行兑换；
- 添加流动性：用户添加 wSAFE/USDT、SAFE/USDT 的流动性，获得交易费用分成；
- TOKEN 工厂：根据名称、简称、LOGO 部署 SRC20 合约生成新币种，同时 1:1 在 SafeSwap 中抵押 USDT 和新币种添加流动性；
- 流动性挖矿：带 wSAFE/SAFE 的交易对，根据 SAFE TVL 和交易量比例可挖其他代币；
- 后续根据情况增加功能，升级 SafeSwap 合约；

3.12 资产跨链

跨链资产（Across Chain Asset, ACA）是指 BTC/ETH/USDT 等其他区块链的资产转移到 SAFE4 主网上，在 SAFE 主网进行各种交易和应用后，还能转回至各自区块链；目前 SAFE4 采用中心化方式实现了资产跨链。

所需组件：

- SafeAcrossGate 资产跨链网关，处理双向跨链交易；

- SafeOriginPool 原生资产池，保存各种区块链的原生资产（Original Chain Asset, OCA）的资产池；
- SafeAcrossCode 系统跨链合约，生成、销毁各种跨链资产，要与资产池金额一致；

以 BTC 跨链为例，跨链的处理流程如下：

- 用户转移 BTC 到 SafeAcrossGate 指定的 BTC 地址，并且附带 SAFE 地址；
- SafeAcrossGate 监测到收到用户转来的 BTC，等待一定确认数；
- SafeAcrossGate 调用 SafeAcrossCode 生成对应金额的 wBTC 发送给用户 SAFE 地址；

跨出的处理流程如下：

- 用户通过 SafeAcrossCode 销毁 wBTC 且提供 BTC 地址；
- SafeAcrossGate 监测到用户的销毁 wBTC 金额，等待一定确认数；
- SafeAcrossGate 从 SafeOriginPool 发送 BTC 给用户 BTC 地址；

将来，SAFE4 有可能实现安全稳定的去中心化跨链。

3.13 原子兑换

原子兑换发生在 SAFE 和其他区块链的加密货币之间，如 BTC、BCH、ETH 和 ERC20 代币、BNB 和 BEP20 代币等，这就意味着 SAFE 钱包需要以 RPC 或 SPV 支持其他区块链的钱包。

假设有 A、B 两方，A 有 SAFE，需要 BTC；B 有 BTC，要交换 SAFE；他们可以把拥有的币种转到中心化交易所，然后直接兑换成 BTC 或 SAFE，或者卖成 USDT 再购买所需币种；如果他们想直接在钱包中以去中心化的方式完成彼此兑换，以 BTC 为例，遵照如下步骤进行：

3.13.1 前期准备

- A 确保 SAFE 钱包有充足金额的 SAFE；
- B 准备好充足金额的 BTC；
- B 把 BTC 转入 SAFE 钱包控制的 BTC 钱包或地址，以下三个方法都可以：
  - ✓ 以 SAFE 钱包连接 Bitcoin Core 钱包的 RPC 接口，确保 Bitcoin Core 钱包中有正确金额的 BTC；
  - ✓ 在 SAFE 钱包中按照 BIP39/BIP32 标准生成 BTC 地址，把 BTC 转入该地址；
  - ✓ 把有 BTC 的私钥导入到 SAFE 钱包，由 SAFE 钱包控制；

3.13.2 订单锁定

- A 在 SAFE 钱包的原子兑换功能中发布买单，花费 v 个 SAFE，以价格 p 购买 BTC（或 B 发布卖单，以价格 p 卖出 BTC，BTC 数量 w）， 该买（卖）单发布在 SAFE 网络上；
- B 在 SAFE 钱包的原子兑换功能中接受该买单（即发送一个买单锁定交易），表明同意该买单的价格和金额；在接受操作之前 SAFE 钱包会检查所控制的 BTC 钱包金额是否充足；
- 如果有两个用户同时接受该买单，以先包含该交易的区块为准，如果在同一个区块中则以交易顺序为先，被淘汰的买单锁定交易无效；
- 买单锁定交易所在区块 3 个确认后，A 的买单被 B 锁定，AB 双方开始兑换过程；

3.13.3 兑换过程（针对 BTC 系币种）

- A 选择一个随机数 X，计算 H=HASH160(X)，用于创建 SAFE 交易 1；
- A 创建 SAFE 交易 1，TX1@SAFE:"支付 v 个 SAFE 给<B 的公钥>如果 B 签名并且知道 X，或者 A 和 B 同时签名"；

- A 创建 SAFE 交易 2，TX2@SAFE:"从 TX1@SAFE 中支付 v 个 SAFE 给<A 的公钥>需要锁定 48 小时和 A 签名"；
- A 发送 TX2@SAFE 给 B，B 签名后返回 A；
- A 发布 TX1@SAFE 到 SAFE 网络，等待确认；
- B 检查 TX1@SAFE 并且获取 H=HASH160(X)，用于创建 BTC 交易 1；
- B 创建 BTC 交易 1，TX1@BTC:"支付 w 个 BTC 给<A 的公钥>,如果 A 签名并且知道 X，或者 A 和 B 同时签名"；
- B 创建 BTC 交易 2，TX2@BTC:"从 TX1@BTC 中支付 w 个 BTC 给<B 的公钥>,需要锁定 24 小时和 B 签名"；
- B 发送 TX2@BTC 给 A，A 签名后返回 B；
- B 发布 TX1@BTC 到 BTC 网络，等待确认；
- A 发布新交易花费 TX1@BTC 交易，从中获得 w 个 BTC，但泄露 X；
- B 利用 X，发布新交易花费 TX1@SAFE 交易，从中获得 v 个 SAFE；

3.13.4 意外处理

- A 和 B 随时可能作假和退出，在这两种情况要保证诚实一方的资产不会丢失；
- A 发布 TX1@SAFE 之前，双方随时可以停止交易，无需处理，不会损失任何资产；
- A 发布 TX1@SAFE 之后，B 作假或反悔退出，则 A 可发布 TX2@SAFE，48 小时后拿回自己的 SAFE 币；
- B 发布 TX1@BTC 后，A 未花费 TX1@BTC 也未揭露 X，则 B 方可发布 TX2@BTC 在 24 小时后拿回 BTC，A 可以发布 TX2@SAFE 在 48 小时后拿回 SAFE；

3.13.5 订单管理

- 订单包括购买（卖出）币种、购买（卖出）金额、价格、过期时间（默认 1 天）等；

- 拥有 SAFE 去购买其他币种的订单称为买单，反之拥有其他币种去购买 SAFE 的订单叫卖单，许多用户的买单和卖单共同形成一个订单本；
- 针对买单的接受交易，称为买单锁定；同样的，针对卖单的接受交易称为卖单锁定；
- 精准交易是针对众多订单中的一个订单进行锁定和兑换的行为，该交易行为不管价格高低，仅锁定特定订单兑换；
- 深度交易是发送卖（买）单，针对符合价格要求的多个买（卖）单进行交易的行为，该交易行为从最优价格开始兑换，直至交易到符合价格要求的最后一个订单；
- 兑换过程由拥有 SAFE 的用户 A 发起，拥有其他币种的为响应方 B；
- 订单被锁定后，就从订单本删除，转移到正在执行的订单池中，后续的订单锁定交易都不可受理；
- 订单状态：开放=>锁定=>SAFE 锁定=>其他币锁定=>A 获得其他币确认=>B 获得 SAFE 确认=>完成
  - SAFE 锁定详细状态： A 生成交易=>B 签名=>SAFE 锁定交易确认 =>B 校验 SAFE 交易
  - 其他币锁定详细状态：B 生成交易=>A 签名=>其他币锁定交易确认=>A 校验其他币交易
- 意外情况的订单状态，订单不可再回开放状态，用户需要重新:
  - 用户取消订单：开放=>A 或 B 取消；需要发送取消订单交易；
  - 订单过期：开放=>过期；无需发送交易；
  - 订单锁定后 30 分钟内 A 未发布 TX1@SAFE：开放=>锁定=>取消；具体状态看"SAFE 锁定"详细状态；

- A 发布 TX1@SAFE 之后，B 作假或反悔退出，B 未在 1 个小时内发布 TX1@BTC：开放=>锁定=>SAFE 锁定=>取消；具体状态看"其他币锁定"详细状态；
- B 发布 TX1@BTC 后，A 未花费 TX1@BTC 也未揭露 X：开放=>锁定=>SAFE 锁定=>其他币锁定=>取消；

- 订单要么不成交，要么全部成交，不存在部分成交的情况；
- 可同时发起多个订单锁定，只需资产足够，分别完成即可；
- 举例：如果有多个不同价格的买单存在，如 0.010，0.011
  - 精准交易：用户 B 仅锁定低价买单 0.010，则仅与 0.010 买单兑换，不与 0.011 的买单兑换；
  - 深度交易：用户 B 创建 0.010 的卖单，则发送该卖单的同时，锁定 0.010、0.011 两个买单进行兑换，如果 B 金额不足以应付两个买单，则仅成交 0.011；
  - 卖单情况也似；

3.14 SAFE3 迁移

SAFE3 上的资产 SAFE 和主节点等数据需要同步转移至 SAFE4 中，在迁移至 SAFE4 后用户可置换对应的 SAFE 和主节点，具体置换迁移分为两步：迁移和置换。

3.14.1 数据迁移

（1）当安网 3 暂停全网产块后，对安网 3 上的所有 SAFE 和主节点进行快照处理；

（2）统计快照中的可用 SAFE、锁定 SAFE 和主节点列表数据详情，包括具体地址、金额、锁定高度、剩余锁定高度等关键信息。其中对于已解锁的主节点来说，需要新增 3 个月的锁定；对于未解锁的主节点来说，需要增加 6 个月的锁定；

（3）在 SAFE4 初始化时，将第二步的关键信息都写入 StateDB 中；

3.14.2 SAFE 置换

置换时需要提供安网 3 地址私钥和 SAFE4 接收地址。

（1）置换可用 SAFE：置换成功后，安网 3 地址的金额将置换到 SAFE4 接收地址中；

（2）置换普通锁定 SAFE：置换成功后，安网 3 地址的金额将直接锁定到 SAFE4 接收地址中，解锁高度将是剩余解锁高度；

（3）置换主节点：置换成功后，安网 3 主节点的金额将直接锁定到 SAFE4 接收地址中，解锁高度将是剩余解锁高度，新的 SAFE4 主节点地址将是私钥对应的 SAFE4 地址，主节点创建者地址将是接收地址；

4 SAFE4 路线图

2025 年 4 月 SAFE4 上线，已经实现了大部分规划功能。如：智能合约、奖励和共识、资产管理、主节点、提案机制、运维管理、超级节点、SafeSwap、资产跨链、SAFE3 迁移等。

剩余的基础功能：L2 协议、隐私与合规、原子兑换，将继续论证开发的必要性和可行性，完善技术方案，在后续的开发中实现。SAFE4 应用功能：域名系统、密码恢复算力等。

上述研发内容和时间安排有可能会调整，开发团队会及时公告。