Value Negotiable System——VNS

——基于区块链的价值互联系统

--Value Interconnection System Based on Blockchain

AMT Community

2018 年 8 月 15 日

August 15, 2018

目录

Content

一、 VNS 理念

I. VNS Idea

（一） VNS 背景介绍

(I) VNS Background

VNS 是 AMT 社区在经历多年的理念沉淀后，充分融合了 AMT 价值理念的第一个生态平台项目。VNS 的理念内涵与 AMT 社区价值思考息息相关，可以说是 AMT 社区经年累月的思想结晶。

VNS is the first eco-platform project that fully integrates AMT value idea after years of accumulation of experiences of AMT Community. The idea connotations of VNS are closely related to the value reflections of AMT Community, which can be called the crystallization of thought of AMT Community over the years.

AMT 社区相信区块链技术必将改变人类生活方式，未来社会的联通将会在现有的信息互联的基础上进化成价值互联，在区块链构建的信任体系中，各式各样的人或物将自我价值通过区块链网络进行传递，形成丰富的价值互联网络生态，这最终将极大地提升社会生产效率。

AMT Community believes that the blockchain technology will certainly change human lifestyle, the communication of future society will evolve into value interconnection on the basis of the current information interconnection, and in the trust system constructed by blockchain, all kinds of people or things will deliver their value via the blockchain network, to form a rich ecology of value internet, to eventually increase the social production efficiency greatly.

因为“创造价值、传递价值、实现价值互联”的共识，让一群来自不同行业、不同地区的 AMT 社区成员走到了一起，为了实现共同目标而贡献自我价值。也正是这样的一群人，为了实现共同的理想，在这样的背景下共同创造出了价值互联平台——VNS，VNS 平台将承载 AMT 社区理念，汇聚全球价值创造者，为每个生态参与者提供全面的支持与服务，助力生态价值的流动，实现生态参与者互惠共赢、共同成长。

The consensus of “create value, deliver value, and realize value interconnection” has brought AMT Community members from different industries and regions together, to contribute self-worth so as to achieve common goals. Under such background, it is those people who have jointly created the value interconnection platform—VNS, in order to realize their common ideal. VNS platform which carries the idea of AMT Community, will gather global value creators, and furnish every ecology participant with full support and services, to drive the flow of ecological value and achieve the mutual benefits and joint growth of ecology participants.

（二） VNS 责任与使命

(II) Responsibilities and Missions of VNS

AMT 社区使命：创造价值，传递价值，实现价值互联。

Missions of AMT Community: to create value, deliver value, and realize value interconnection

创造价值：利用 AMT 生态资源，帮助生态参与者梳理自身能力、开发自身潜能，最终协助生态伙伴创造价值。

Creating value: Helping ecology participants analyze their abilities and develop their potential by using AMT ecological resources, to eventually assist them in creating value.

传递价值：利用 VNS 网络，搭建价值传递的桥梁，帮助生态参与者进行价值交换，促进生态参与者价值提升。

Delivering value: Building the bridge for value delivery by using VNS network, to help ecology participants exchange value and promote them to enhance value.

实现价值互联：利用 AMT 生态共识与 VNS 区块链技术，打造安全可靠的价值流转网络，让人与人、人与物、物与物实现真正意义上的价值互联，生态参与者付出即有所得，“**All for one, one for all**”。

Realizing value interconnection: Building a secure and reliable value transfer network by using AMT ecological consensus and VNS blockchain technology, to achieve the real value

interconnection among humans, between humans and things, and among things, and have ecology participants reap what they sow. “**All for one, one for all**”.

二、 VNS 技术特点

II. Technical Characteristics of VNS

（一） 基础技术

(I) Basic Technologies

1、 支持智能合约

1. Supporting Smart Contracts

区块链技术的智能合约是一组情景一一应对型的程序化规则和逻辑，是部署在区块链上的去中心化、可信息共享的程序代码。签署合约的各参与方就合约内容达成一致，以智能合约的形式部署在区块链上，即可不依赖任何中心化机构自动化地代表各签署方执行合约。智能合约具有自治、去中心化等特点，一旦启动就会自动运行，不需要任何合约签署方的干预。

The smart contract of blockchain technology is a set of programmed rules and logic that respond to scenarios, and is decentralized, shareable program code deployed on the blockchain. After the contracting participants reach an agreement for the contract content, it will be deployed on the blockchain in the form of smart contract, namely, the contract will be performed automatically on behalf of the contracting parties without depending on any centralized institution. Smart contracts are characterized by autonomy and decentration, etc., and will automatically run once being started, without any intervention of any contracting party.

VNS 智能合约的运行过程如下:智能合约封装预定义的若干状态、转换规则、触发条件以及对应操作等，经过各方签署后，以程序代码的形式附着在区块链数据上，经过区块链网络的传播和验证后被记入各个节点的分布式账本中，区块链可以实时监控整个智能合约的状态，在确认满足特定的触发条件后激活并执行合约。

The running process of VNS smart contract is as follows: the predefined several states, transformation rules, trigger conditions, and corresponding operations, etc. are encapsulated in the smart contract, which will be attached to the blockchain data in the form of program code after being signed by the parties, and then recorded in the distributed ledger of each node upon spread and verification of blockchain network; the blockchain can monitor the state of the entire smart contract in real time, activating and performing the contract after the confirmation that certain trigger conditions are met.

支持智能合约，对 VNS 来说有重要的意义，智能合约不仅赋予了 VNS 底层数据可编程性，为 VNS 价值互联、安全度、信任度奠定了基础；还封装了区块链网络中各节点的复杂行为，为建立基于 VNS 的上层应用提供方便的接口，共享给 VNS 生态参与者，帮助不同的生态参与者根据自身情况开发满足自身需求的 DAPP 应用，从而让 VNS 区块生态网络可以更好的为其服务。拥有了智能合约的 VNS 的前景极为广阔。

Supporting smart contracts is of great importance to VNS because not only can smart contracts give VNS underlying data the programmability and establish the foundation for VNS value interconnection, security, and credibility, but also encapsulate complex behaviors of each node in the blockchain network, providing convenient interfaces for establishing upper-layer applications that are based on VNS, and share them to VNS ecology participants, helping different ecology participants develop DAPPs that meet their own demand according to their situation, thus to receive better services from VNS block ecological network. VNS that possesses smart contracts will enjoy quite broad prospects.

2、 VNS 安全保障

2. Security Assurance of VNS

VNS 的信息安全及密码学技术，是整个 VNS 网络安全保障的基石。在 VNS 中，也大量使用现代信息安全和密码学的技术成果，主要包括：哈希算法、非对称加密、数字签名、数字证书、同态加密、零知识证明等。本章从安全的完整性、机密性等维度，简要介绍 VNS 安全及密码学技术的应用。

The information security and cryptographic technologies of VNS are the cornerstone to the security assurance of the entire VNS network. Technological achievements of modern information security and cryptography are also widely used in VNS, mainly including hash algorithms, asymmetric cryptography, digital signatures, digital certificates, homomorphic encryption, and zero knowledge proof, etc. The application of VNS security and cryptographic technologies is briefly introduced in this section from the perspective of the security integrity and confidentiality, etc.

（1） 完整性（防篡改）

(1) Integrity (tamper-proofing)

此部分为区块链最基础的部分，区块链采用密码学哈希算法技术，保证区块链账本的完整性不被破坏。哈希（散列）算法能将二进制数据映射为一串较短的字符串，并具有输入敏感特性，一旦输入的二进制数据，发生微小的篡改，经过哈希运算得到的字符串，将发生非常大的变化。此外，优秀哈希算法还具有冲突避免特性，输入不同的二进制数据，得到的哈希结果字符串是不同的。

This part is the most basic part of blockchain. Hash algorithms are used to protect the integrity of ledgers on the blockchain. A hash algorithm can be used to map binary data to a shorter string, and is input sensitive: any micro tampering to the input binary data will lead to a great change to the string obtained through hash operation. In addition, a good hash algorithm is collision resistant, that is, it is impossible to produce the same hash value (in the form of string) for different input binary data.

区块链利用哈希算法的输入敏感和冲突避免特性，在每个区块内，生成包含上一个区块的哈希值，并在区块内生成验证过的交易的 Merkle 根哈希值。一旦整个区块链某些区块被篡改，都无法得到与篡改前相同的哈希值，从而保证区块链被篡改时，能够被迅速识别，最终保证区块链的完整性（防篡改）。

With the input sensitive and collision resistant characteristics of hash algorithms, each block generates and contains the hash value of the previous block, with Merkle root also generated there for those validated transactions. Once certain blocks of the entire blockchain are tampered, this could not lead to the same hash values with those before the tampering. This can help us quickly detect the presence of tampering, to eventually guarantee the blockchain integrity (tamper-proofing).

（2） 机密性

(2) Confidentiality

加解密技术从技术构成上，分为两大类：一类是对称加密，一类是非对称加密。对称加密的加解密密钥相同；而非对称加密的加解密密钥不同，一个被称为公钥，一个被称为私钥。公钥加密的数据，只有对应的私钥可以解开，反之亦然。

Encryption and decryption technologies can be divided into two broad categories: symmetric cryptography and asymmetric cryptography. Symmetric cryptography uses the same key for encryption and decryption, while asymmetric cryptography uses different keys: a public key and a private key. Data encrypted using the public key can only be decrypted using the corresponding private key, and vice versa.

VNS 使用的为椭圆曲线非对称加密，这种加密方式将使 VNS 的加密过程变得更加安全、更加快捷，同时私钥更加轻便。此外，VNS 中还将应用现代密码学最新的研究成果，包括同态加密、零知识证明等，在 VNS 区块链分布式账本公开的情况下，最大限度地提供隐私保护能力。这方面的技术，AMT 社区将继续发展完善，确保 VNS 区块链网络的安全性。

VNS uses the elliptic-curve asymmetric cryptography which will make the encryption process of VNS more secure and quicker, and the private key easier to use. Furthermore, VNS will also use the latest research results of modern cryptography, including homomorphic encryption, and zero-knowledge proof, etc., to maximize the privacy protection when VNS blockchain’s distributed ledger is open to the public. AMT Community will be developed and improved in such technologies, so as to ensure the security of VNS blockchain network.

VNS 的区块链安全是一个系统工程，系统配置及用户权限、组件安全性、用户界面、网络入侵检测和防攻击能力等，都会影响最终区块链系统的安全性和可靠性。VNS 区块链系统在实际构建过程，

是在满足用户要求的前提下，在安全性、系统构建成本以及易用性等维度，取得一个合理的平衡融合的完美结果。

The blockchain security of VNS is a system engineering, including system configuration, user access, component security, user interface, network intrusion detection, and attack defense capability, etc. which will affect the security and reliability of the final blockchain system. The blockchain system of VNS is perfectly built on a reasonable balance of security, system building cost, and ease of use, etc., while meeting user requirements in the actual construction process.

3、 POW 共识机制

3. PoW Consensus Mechanism

基于 VNS 去中心化的思想，同时为了通过提高 51%攻击成本来极大地保证安全性，再结合 AMT 社区理念，付出即有回报，多劳多得，VNS 主链选择了 POW 方式进行生态基础激励。

In order to greatly guarantee the security by increasing the 51% attack cost, PoW mechanism is selected for parent blockchain of VNS, for ecology fundamental incentive, based on the decentralization idea of VNS, and in combination with the idea of AMT Community, i.e.: you reap what you sow and more pay for more work.

（二） VNS 技术进阶

(II) Advanced Technologies of VNS

1、 安全进阶保护

1. Advanced Security Protection

（1） 同态加密用户交易隐私保护

(1) Using Homomorphic Encryption to Secure User Transaction Privacy

区块链可以防篡改、去中心化，其在非信任的网络中运行，但是用户的账本对参与组织是透明的，任何组织都可以访问到相同的数据，如果将用户的隐私的数据放到链上将会放大用户隐私泄露的风险。当前在比特币等其他公有链系统中，所有的交易信息都是公开的（包括交易金额）。但是，在金融业的交易中，金融交易信息是敏感数据，非业务相关方不应该查看，但同时要满足监管机构的监管要求，而大部分的区块链并没有满足隐私性要求。

The blockchain is tamper-proof, decentralized, and can operate on an untrusted network. However, user ledgers are transparent to participant organizations, that is, the same user data can be accessed by any organization. Placing users' private data on the chain may increase the risk of data leakage. Currently, all other public chain systems, including Bitcoin, display all the transaction information (including transaction amount). But in the financial sector, financial transaction information is highly sensitive data and should never be opened to non-related parties, and regulatory requirements should be met, while, most blockchains do not satisfy privacy requirements.

VNS 区块链交易解决方案中：（1）将提供同态加密库，对用户的交易数据用其算法进行加密保护，交易的时候都是密文运算，最终账本中内容为加密后保存，即使节点被攻破，获取到账本记录也无法解密；（2）将提供范围证明校验，利用智能合约设置对密文进行背书，无需解密就能校验交易的正确性，从而识别出恶意交易风险，保证了智能合约的正确执行。VNS 将开发出保密交易系统，通过改良的算法，比起使用传统的加法同态加密与基于环签名的范围零知识证明，性能将大幅提升。

VNS blockchain transaction solution will (1) provide a homomorphic encryption library to encrypt users' transaction data using its algorithms: as the transactions are processed and stored in the final ledger in an encrypted form, the ledger information will remain intact even if the nodes are hacked; (2) offer range proof verification: the smart contract settings can endorse the ciphertext and verify the transaction without decryption, to identify risks of malicious transactions and guarantee the proper performance of smart contracts. A confidential transaction system will be developed for VNS, using an improved algorithm, which will provide greater performance than the traditional additive homomorphic encryption and ring-signature-based zero knowledge range proof.

（2） 零知识证明

(2) Zero Knowledge Proof

零知识证明能够在不向验证者提供任何有用的信息情况下，使验证者来相信该结论是正确的，证明过程中不向验证者泄露被证明的消息。VNS 区块链方案将会提供零知识证明能力，对用户的隐私数据进行保护，减少用户隐私泄露风险。

Zero knowledge proof is a method in which the verifier can be convinced that the conclusion is correct without conveying any useful information or information about the conclusion. VNS blockchain solution will provide zero knowledge proof to protect users' private data and reduce risks of user data leakage.

（3） 智能合约安全

(3) Smart Contract Security

当智能合约运行错误或者编程错误时，就会导致“DAO”的事件，从而让用户遭受巨大损失，VNS 区块链方案可提供智能合约检测工具，防止恶意的企图通过智能合约漏洞入侵用户数据的行为，同时将提供安全容器，持续监控容器的运行状态，若发现漏洞即进行有效的隔离，严格对容器的访问权限进行控制，从而保证合约安全运行。

In case of run-time error of a smart contract or programming error, a DAO attack will occur, causing huge losses to users. VNS blockchain provides a smart contract detection tool that aims to prevent the smart contract vulnerabilities from being exploited by hackers, therefore stopping them from accessing user data. In the meantime, VNS blockchain provides a security container, the operation of which is closely monitored. If a vulnerability is detected, the container will be effectively isolated and the access of the container will be strictly controlled, to ensure the secure operation of the contract.

（4） 账本安全

(4) Ledger Security

每个节点的本地账本可能会被篡改，如果出现大部分节点的本地账本都被修改，就可能造成 51%的攻击。VNS 区块链将提供基于社区共识建设与 POW 共识建设，保持去中心化思想，节点分布式布局，极大地提高 51%攻击成本，保护账本安全稳定。

The local ledger of each node is likely to be tempered with. If most of the nodes' local ledgers are tampered with, a 51% attack may occur. VNS blockchain will provide the community-consensus-based construction and PoW consensus construction, keep the decentralization idea, and distributed layout of nodes, to greatly increase the 51% attack cost and protect the ledger security and stability.

2、 离链通道

2. Off-chain Channel

单位时间内交易处理能力仍是区块链大规模应用的主要瓶颈之一。受限于区块链的分布式架构特性，节点间不均等的计算能力，不同的网络状况等因素，全网共识往往无法快速达成，从而导致交易速度难以提升。现阶段比特币网络每秒仅能处理约 7 笔交易，支持智能合约的以太坊交易处理速度约为每秒 15 笔。相比之下，中心化服务器支持的 VISA 系统峰值吞吐率可达 56,000 笔，支付宝在 2017 年双十一期间则达每秒 256,000 笔峰值吞吐率。交易拥堵，交易费攀升已极大限制区块链的规模性应用。

Transaction processing capacity in unit time is still one of the main barriers to the large-scale application of blockchain. Limited by the factors like the distributed architecture of blockchain, varying computing capabilities of nodes, and differing network conditions, the consensus on the entire network cannot be achieved quickly, resulting in the difficulty to increase the transaction speed. Currently, the Bitcoin network can process only about 7 transactions per second, and the figure for Ethereum that supports smart contracts is about 15 per second. In contrast, the VISA system, with its central server, supports maximum 56,000 transactions per second. Alipay's transactions peaked at 256,000 transactions per second during the 11.11 Global Shopping Festival in 2017. Congested

transactions and rising transaction costs have greatly restricted the large-scale application of blockchain.

区块链社区对交易扩容方案的争论与尝试由来已久，现有的主要方案包括区块扩容，共识算法改良，安全硬件(TEE)辅助，隔离见证，闪电网络，交易/状态分片，多层子链等。但无论哪种方案都难以同时兼顾去中心化,可扩展性，安全性三个关键需求。值得注意的是区块链具有应用强相关性，在特定应用场景仍可找到各要素间的平衡点以满足总体业务需求。在大规模 DAPP 应用中，往往小额支付占据了大部分交易请求，而小额交易并无必要在主链及时获得确认，例如共享经济中广泛存在的小额支付场景。如果将海量小额交易在链下通道处理，交易过程中不与主链交互，而在交易通道关闭或交易方退出时才请求主链记录交易最终状态，这将极大缓解主链的处理压力，这也是离链微支付通道的设计思想。典型应用包括比特币框架下的闪电网络(LightningNetwork)和以太坊智能合约框架下的雷电网络(RaidenNetwork)。离链通道涉及到“链上锁定-链下执行”等一系列操作，其中交易双方的状态变化(资金分配比例)与交易执行过程由链上合约监督执行。

The blockchain community has long discussed and tried the solutions to expand transaction capacity. The existing main solutions include block expansion, consensus algorithm improvement, security hardware (TEE) aiding, isolation witness, lightning network, transaction/status fragmentation, and multi-layer subchain, etc. However, none of them takes into account the all three key demands: decentralization, scalability, and security. It is worth noting that the blockchain is application-based, and a balance among those factors can still be achieved under certain application scenario, to meet the overall business requirements. In large-scale DAPP applications, micro-transactions account for the majority of transaction requests, but do not need to be verified promptly by the parent blockchain. For example, micro payments are very common in the sharing economy. If most micro transactions can be processed in the off-chain channel, without interacting with the parent blockchain during the transaction, but only request the parent blockchain to record the final transaction status after the transaction channel is closed or when the transaction parties exit the channel, the processing pressure on the parent blockchain will be effectively alleviated. And this is the design idea of the off-chain micro-payment channel, and the typical applications include the Lightning Network for Bitcoin and the Raiden Network for Ethereum smart contracts. The off-chain channel involves a series of operations from chain locking to off-chain execution, and the status changes of the transaction parties (fund allocation ratio), as well as the transaction itself, are monitored by the contract on the chain.

AMT 社区将会开发并拥有适用于 VNS 生态场景的的离链通道交易系统，通过交易方高效安全的握手协议，实现用户间单通道高 TPS 的交易性能。随着离链交易通道数的增加，可进一步提升系统在单位时间内交易处理能力。

AMT Community will develop and possess the off-chain channel transaction system applicable to VNS ecology scenarios, to achieve the single-channel high-TPS transaction performance of users through the efficient and secure handshake agreement of transaction parties. The system transaction processing capacity in unit time can be further improved with the increase of the number of off-chain transaction channels.

当然，基于前期的实际市场需求与时间限制，AMT 也不会排除在获取社区共识的情况下，采用目前已有的成熟技术，如雷电网络等技术均可以根据需求快速配置到主网。

And certainly, based on the actual market demand at the early stage and time restrictions, AMT may also use the existing mature technologies, such as Raiden Network, to rapidly deploy them to the mainnet according to demand, under the circumstance of obtaining community consensus.

3、 VNS Name Service

3、 VNS Name Service

（1）VNS Name Service 的架构设计

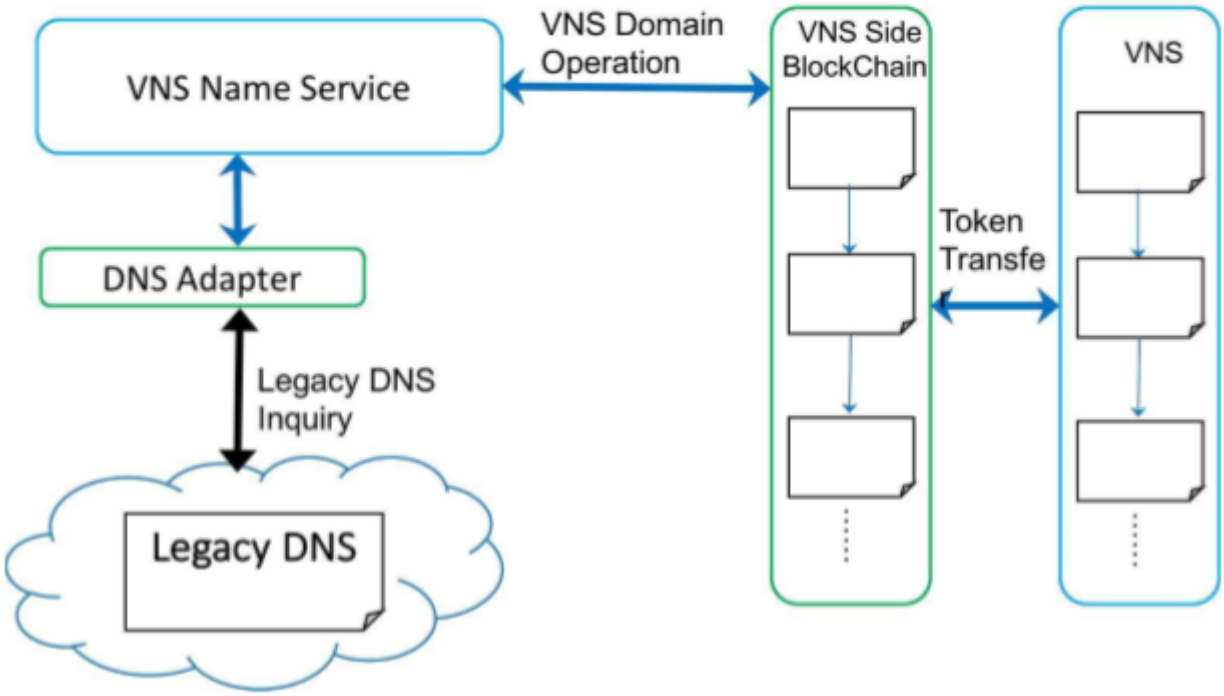
(1) VNS Name Service Architecture Desig

VNS Name Service 采用主链侧链的设计架构，单独作为 VNSCoin 主链的一条侧链存在。作为一条侧链，VNS Name Service 不产生新的代币，而是与 VNSCoin 主链代币系统实现双向兑换绑定。VNS 主链的代币系统，通过锁定 VNS 代币的方式，在 VNS Name Service 侧链相应的产生对应数量的 VNS 代币，反之通过销毁 VNS Name Service 侧链的 VNS 代币来解锁 VNSCoin 主链锁定的代币。从而实现主链和侧链的双向代币兑换和绑定。

VNS Name Service adopts the design framework of the main chain-side chain and exists alone as a side chain of the VNSCoin main chain. As a side chain, VNS Name Service does not generate new tokens, but implements a two-way exchange binding with the VNSCoin main chain token system. VNS main chain token system generates a corresponding number of VNS tokens on VNS Name Service side chain by locking VNS tokens, and unlocks the tokens locked by VNSCoin main chain by destroying tokens on VNS Name Service side chain, and thus achieves two-way token exchange and binding of main chain and side chain.

作为一条侧链，VNS Name Service 可以独立的发起 transaction，考虑到发展成为通用 key-value 数据存储的可拓展性， VNS Name Service 可提供两种独立类型的 transaction。 第一种 transaction 与 Namecoin 类似，我们可以直接将 value 数据直接写。

As a side chain, VNS Name Service can initiate a transaction independently. Considering the scalability evolving into common key-value data storage, VNS Name Service can provide two separate types of transaction. The first transaction is similar to Namecoin, and we can write the value data directly into the transaction. The second transaction only writes the hash value of the value data, and the content data is supported by DHT, BitTorrent or other decentralized storage services.



在 transaction 中。第二种 transaction，只写入 value 数据的 hash value, 其内容 数据通过 DHT,BitTorrent 或者其他去中心化存储服务作为支持。

为兼容和支持现有互联网体系架构下的各种服务，例如在使用 VNS Name Service 服务的同时，同样可以正常使用现有域名解析服务，访问.com, .cn 等等顶级域名，VNS Name Service 在区块链侧链的基础上，建立一种与现有 DNS 服务兼容的标准化的域名解析服务层。从而避免用户在解析非.vns 域名时，域名解析服务更换的问题。同时此标准服务层会对区块数据进行索引缓存，以提高域名查询速度。对个人用户来说，不需要索引和缓存完整的区块条目。兼容层可以选择性的从区块中查询用户经常访问的地址，将其缓存以提高查询速度。

In order to be compatible and support various services under existing Internet architecture, the existing domain name resolution service can also be used normally to access top level domain names such as .com and .cn when using the VNS Name Service, and VNS Name Service can

build a standardized domain name resolution service layer compatible with existing DNS services based on the blockchain side chain, thus avoiding the problem of domain name resolution service replacement when users resolving non-.vns domain names. At the same time, this standard service layer will index the block data cache to speed up domain name lookup. For individual users, there is no need to index and cache complete block entries. The compatibility layer can selectively look up frequently accessed addresses from the blocks and cache them to speed up the lookup.
我们将拥有完整区块数据，并愿意对外提供域名解析服务的节点称为主节点。主节点需要对 区块数据做完整的索引。类似于比特币 SPV 机制，其他用户如果不想本地存储区块数据 可以只下载区块的 header，或者直接使用主节点提供的域名解析服务。为了鼓励主节点 的建设，使用主节点的服务的用户将向主节点服务支付 VNS 作为费用。为了保证主节点的 可信性，主节点需要锁定固定数额的 VNS 作为提供稳定可信服务的抵押。
We call the node that has the complete block data and is willing to provide domain name resolution services as major node. The major node needs to make a complete index of the block data. Similar to the SPV mechanism of bitcoin, other users can download the header of a block only or directly use the domain name resolution service provided by the major node if they do not want to store the local block data. In order to encourage the construction of major node, a user using the major node's service will pay VNS as a fee to the major node service. In order to ensure the authenticity of the major node, the major node needs to lock a fixed amount of VNS as a mortgage for providing stable and trusted services.

（2）VNS Name Service 安全性分析

(2) Security Analysis of VNS Name Servic

VNS Name Service 作为一种去中心化的服务，从根本上杜绝了隐私泄露，内容审查， DDOS 攻击，中间人攻击等等各种风险的可能性。每一个独立运行 VNS Name Service 的用户的节点，都可以从电脑本地查询解析 DNS。本地解析 DNS 请求，同时也节省了网络 封包在网络上传输的过程所花费的时间。
As a decentralized service, VNS Name Service virtually eliminates the possibility of various risks such as privacy leaks, content censorship, DDOS attacks and man-in-the-middle attacks. The node of each user that runs VNS Name Service independently can resolve DNS from a local computer. Resolving DNS requests locally also saves the time it takes for network packets to transfer over the network.
与 Namecoin 类似，VNS Name Service 的主要风险来自于 51%攻击。为得到足够算力保 证，VNS Name Service 侧链可以与 VNSCoin 联合挖矿。
Similar to Namecoin, the main risk for VNS Name Service comes from 51% attacks. VNS Name Service side chain can mine in conjunction with VNSCoin for sufficient computational power.

（3）VNS Name Service 拟支持标准

(3) Standards to be supported by VNS Name Service

VNS Name Service 支持.vns 为后缀的顶级域名解析服务，支持 new_name(新建域名)，update_value(更新 value 值)和 transfer(域名转让)三种基本操作。兼容层符合现有 DNS 系统查询服务标准。
VNS Name Service supports top-level domain name resolution service with suffix .vns and supports three basic operations: new_name (new domain name), update_value (update value) and transfer (domain name transfer). Compatibility layer meets standards of existing DNS system lookup service.
VNS Name Service 的条目主要包含 Name 字段和 Value 字段。Name 字段拟支持 RFC1035 标准：域名命名要符合 RFC 1035 域名标准:必须以字母开头，以字母或者数字结尾，中间字符可以包括字母，数字和连字符，长度不能超过 63 个字符, ASCII only, 不支持 unicode。校验正则表达式: ^[a-z]([a-z0-9-]{0,62}[a-z0-9])?$
The entries of VNS Name Service mainly include the Name field and Value field. The Name field is intended to support the RFC1035 standard. The domain name must conform to the RFC 1035

domain name standard. It must start with a letter, end with an alphanumeric character, and the middle characters can include alphanumeric characters and hyphens. The length mustn't exceed 63 characters. It is ASCII only and doesn't support unicode. The regular expression for validation: ^[a-z]([a-z0-9-]{0,62}[a-z0-9])?$

Value 字段以 json 格式字符串形式，支持 namecoin 支持的命名空间，包括:
The Value field, in the form of json string, supports namecoin-supported namespaces, including:

Namespace	Application
d/<domain>	Domain names for .bit TLD
id/<identity>	Public online identity system (e.g. addresses for BTC, NMC, email, ...)
p/<personal>	Personal namespace for PGP, SSL, identities, etc.
m/<message>	Messaging system for Namecoin users
a/<alias>	Alias system to map a name to another address
tor/<domain>	Domain names for .tor TLD for onion websites

三、 VNS 应用展望

III. Outlook of VNS Application

（一） Token 经济

(I) Token Economy

1、 共享积分方案

1. Shared Point Solution

商户积分的 Token 化，将会完美解决现有积分沉睡，消费者黏性不足的难题。积分一旦流通，将会脱离原本体质束缚，将以高渗透的方式在市场中流转，自动去寻找潜在用户，对于商户而言，将会拥有更多不同的促销手段，去让积分变得好玩、去让消费者变成自己的推销员。

Changing merchants' points into tokens will provide a perfect solution to the current difficulties of inactive use of points and insufficient consumer stickiness. Once circulated, points will break free from the original system, flow in the market in a highly permeable way, and automatically look for potential users; and merchants will have more different promotion means, and more interesting ways for consumers to spend the points, to turn them into own salespeople.

今后将不再是从前单方面的推广、单方面的"单动"，未来将会变成商户与客户、客户与客户、商户与商户之间的真正互动，这种互动将会为积分赋能，积分不仅仅是积分，更是商户价值的体现，积分的流动将成为商户价值的流动，每经过一个"节点"，会将价值传递至此，并辐射节点所触达区域。

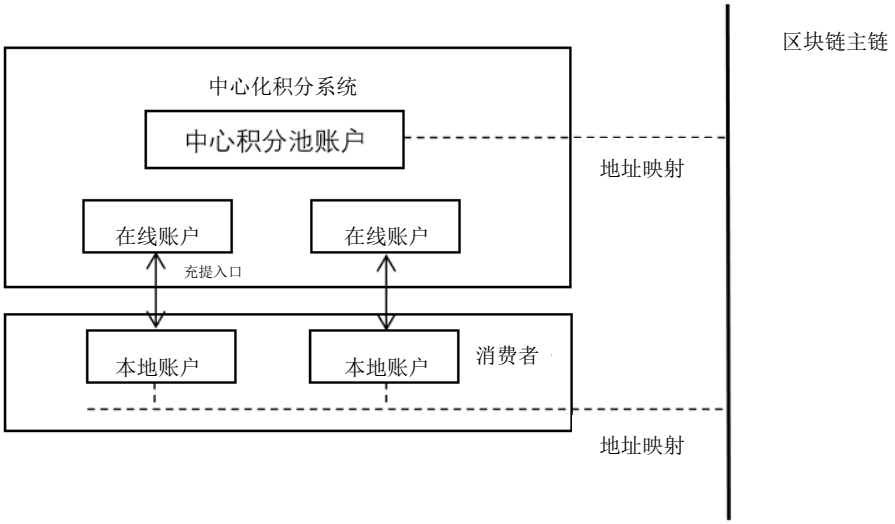
The one-sided promotion and "single action" will no longer be applied in future; instead, the real interaction between merchants and customers, among customers, and among merchants, will be realized, which will enable the points. Points will be more than points and they will reflect value of merchants; and the flow of points will become the flow of value of merchants: value will be delivered to every "node" it passes by, covering area that the node can reach.

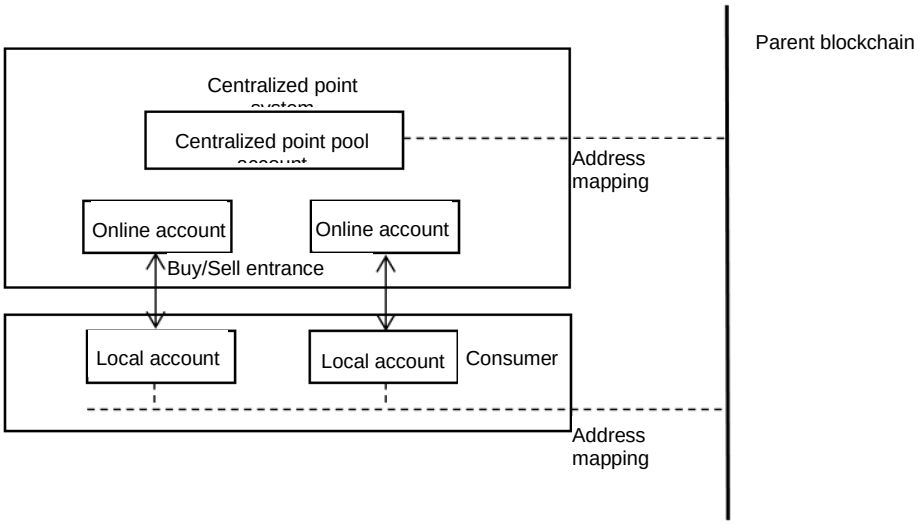
而积分联盟的产生，也将共享价值，通过共享让市场消费者的消费能力最大化，方便商户之时，也方便了消费者，更快地满足双方需求，这样的市场才是真正的良性市场。

Point alliance will also realize the value sharing, to maximize the spending power of market consumers through sharing; it can bring convenience to both merchants and consumers, to faster satisfy demands of both sides, and lead to a real benign market.

积分提取模型图：

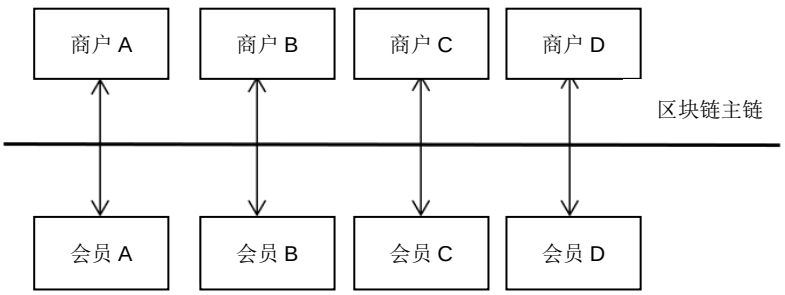
Point Extraction Model Diagram:

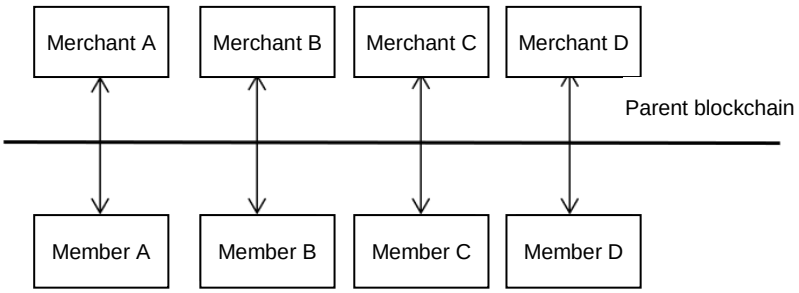




商户积分联盟模型图：

Merchant Point Alliance Model Diagram:





2、 数字票据

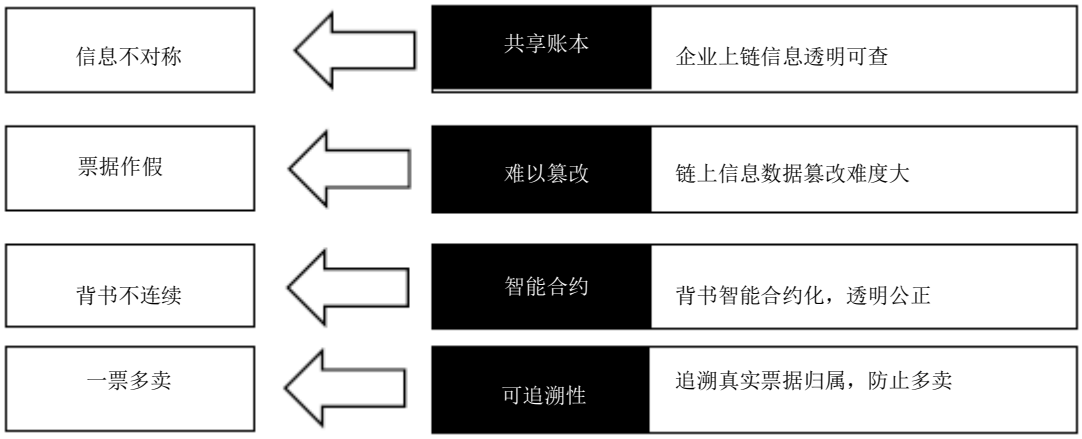
2. Digital Draft

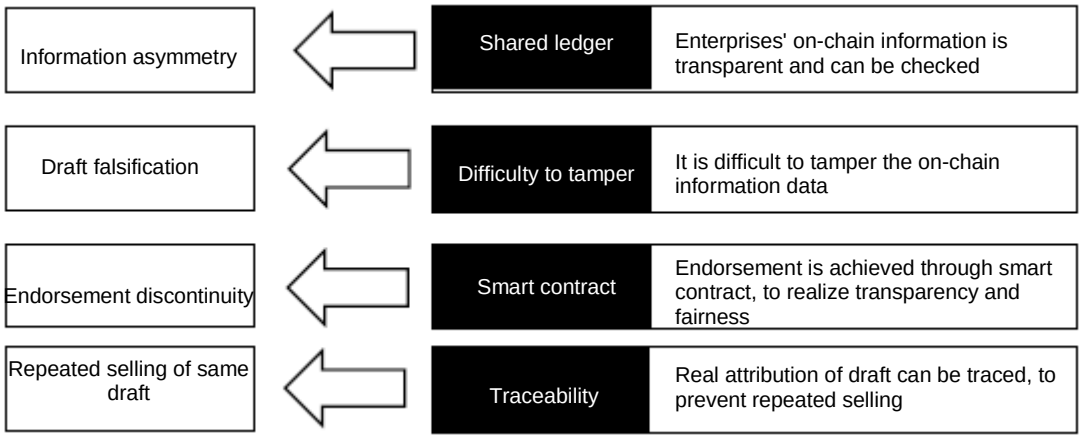
传统票据业务存在着四个问题。第一，信息不对称。由于信息不透明的存在，会导致信息不对称，无法了解票据签发方真实的背景情况，导致票据失去信用；第二，票据作假。票据造假难度低，造假者非常容易进行复制或者修改；第三，背书不连续。票据背书的不连续，容易出现纰漏，导致持票人丧失票据权利。虽然票据背书的不连续并不绝对地使持票人失去票据权利，但是依然具有出现这种问题的可能性。第四，一票多卖。传统中心化机构为了利益，可能会出现用票据清单以短期代持或者短期回购的方式从银行套取资金用于周转或者投资。

There are four deficiencies in traditional note business. The first is information asymmetry. The information opacity results in information asymmetry and no knowledge of the real background of the draft issuers, leading to loss of credit of draft; the second is draft falsification. Counterfeiters can copy or modify draft easily as the draft falsification difficulty is low; the third is endorsement discontinuity. The discontinuity of draft endorsement easily leads to glitches, resulting in the possibility of the holders' loss of rights to the draft. Although the endorsement discontinuity of the bill does not absolutely deprive the holder's rights to the instrument, it still has the possibility of such a problem; the fourth is repeated selling of same draft. For their benefits, the traditional centralized institutions may illegally obtain funds for turnover or investment in the manner of short-term holding on behalf of short-term repurchase using the draft list.

基于以上四个问题，利用区块链的特点可以大大降低问题风险，具体对应关系如下：

The characteristics of blockchain can be used to largely reduce risks of the above four deficiencies, with the specific correspondence as follows:





3、 权益凭证

3. Equity Vouchers

权益凭证指的是拥有某项权益的证明，这种证明可以是分红权、使用权、投票权等权益，传统的权益凭证的执行依靠约定、合同或者其他第三方机构来进行监督实现，而传统的实现方式由于存在违约、造假的可能性而存在不确定性的风险，大量资源被消耗在信任的产生上。区块链的应用可以很好的改善这一件情况，在人们拥有共识的前提下，利用智能合约的约束，可以去中心化地公平、公正、公开地执行这些高信任度的权益分配。人们在既定规则下，只需要去完全信任对方，去完成自己的责任与义务即可获取自己相应的权益，而不用担心权益因为他人的失信而受到损失。这样就会提升整体的工作效率，减少信任成本，帮助现有的生产力的提升，确保权益的准确分配。

Equity vouchers refer to the proof of possession of certain equity which can be dividend right, use right and voting right, etc. The traditional execution of equity vouchers is done in reliance of agreements, contracts or under the supervision of other third-party institutions, and has the uncertainty risks due to possibility of breach of contract and falsification, with a large number of resources consumed in order to generate trust. However, the application of blockchain can well improve this situation. Given the consensus, highly trusted equity allocation can be executed in a decentralized, and just, fair and open manner, under the smart contracts. Under the established rules, people only need to completely trust the other parties and complete their own responsibilities and obligations to obtain their corresponding equity, without worrying about losses due to dishonesty of others. This way will increase the overall work efficiency, reduce cost of trust, help increase existing productivity, and ensure the proper equity allocation.

4、 股票、物权的登记、交换与转移

4. Registration, Exchange and Transfer of Stocks and Property Rights

目前股权、物权的登记、交换与转移大多数是中心化处理的行为，虽然经过多年的完善与发展，股权、物权的登记相关问题已经得到了相当程度的改善，但是依旧存在一些问题，对于非上市公司体系来说，通常情况下，需要通过人工处理纸质股权凭证、期权发放和可换票据。如果出现频繁的股权变更，股东名册的维护将变得繁琐，历史交易的维护和跟踪也变得困难。而对于绝大多数物品来说所有权并不明确。

Currently, the registration, exchange and transfer of equities and property rights are mostly centralized processing behaviors. Registration of equities and property rights have been improved considerably after years of improvement and development, however, there are still some deficiencies. Generally, for non-listed companies' system, manual handling of paper share certificates, option issuance, and convertible draft is needed. If the equity alternation is frequent, the maintenance of register of shareholders will become tedious, and the maintenance and tracking of historical transactions will become difficult. Furthermore, for most items, the ownership thereof is ambiguous.

对于股权来说，区块链技术将会对这一切进行数字化管理，使其变得更加高效和安全。区块链众筹股权登记，将充分利用区块链账本的安全透明、不可篡改、易于跟踪等特点，记录公司股权及其变更历史。对于物权来说，通过区块链可以将物品购买情况、归属情况充分上链，上链后将给与物权

所有人发放相关凭证。在需要查明物权归属时，经过物权所有人的授权后，被授权人可以通过链上确认物品归属，从而解决大多数物权归属信息问题。

Digital management will be adopted for the registration of equities with the blockchain technology, to make the process more efficient and secure. The crowdfunding equity registration through blockchain technology will fully utilize the security, transparency, tamper-resistance and traceability of blockchain ledger, to record the equities and the alternation history of the company. For property rights, the item purchase situation and ownership situation can be fully placed on the chain through blockchain technology, and then the property right owners will be issued the relevant vouchers. When there is a need to check the property right ownership, the person authorized by the property right owner can confirm the item ownership on the blockchain, thus to solve the issue of ownership of most property rights.

同理，解决了登记问题，交换与转移问题即也可得到同样的解决，区块链可以解决信任风险和信任成本，增强人之间的互信，交换与转移均在链上进行，加入智能合约的保护，交换与转移均可以在智能合约的机制下去中心化运转，从而增加运转效率，提升运转准确度。

The exchange and transfer of equities and properties rights can be solved similarly with the registration solution. By using blockchain, trust risks and cost of trust will be solved, and the mutual trust of people enhanced. Exchange and transfer can be carried out on blockchain and protected by smart contracts; they can operate in a decentralized manner under the mechanism of smart contract, thus to increase efficiency and increase accuracy.

（二） 共享经济

(II) Sharing Economy

共享经济带来得颠覆性意义已经是不言而喻的，这里的共享经济指的是真共享经济，利用闲置资源拿出去进行共享，资源持有者获得了经济利益，资源使用者也获得了便利与优惠，这是一种双赢的局面。而绝非现在市面上的创造资源再去租赁，例如现在的共享充电宝、共享单车，本质上是一种租赁行为，并未提升社会的资源利用效率，甚至可能已经造成了资源的浪费。

It is already self-evident that sharing economy is subversively significant. The sharing economy mentioned here is the real sharing economy in which idle resources are shared so that the resource holders obtain economic benefits and resource users obtain convenience and preference. This is a win-win situation, but not the creating existing resources in the market. For example, the power bank sharing and bicycle sharing at present are essentially a rental behavior, which does not increase the utilization efficiency of social resources, but may have caused resource waste instead.

在现有共享经济市场中，最方便、最高效、最快捷的应用场景是应用到基于物联网的共享经济，因为传统的基于物联网的共享经济拥有诸多问题。例如中心化控制成本高、隐私保护难度随着市场规模的扩大而增加、硬件资源接入共享网络后容易遭受攻击等。

In the existing sharing economy market, the most convenient, most efficient, and fastest application scenario is the application to the IoT-based sharing economy. The traditional IoT-based sharing economy has many deficiencies, for example, the centralized control cost is high, the privacy protection difficulty increases as the market size expands, and hardware resources are likely to be attacked after being connected to the shared network.

而区块链可以完美的解决中心化控制的 IOT 共享经济体系中遇到的问题，利用分布式计算与智能合约降低系统计算压力与中心化控制成本；利用身份认证体系与零知识证明，保护用户隐私，用户使用无需透露自身敏感信息即可获得信任；利用分布式账本存储控制信息，保证设备运转的正确性，防止被奴役等等，这些均可以通过区块链技术去改善现有的物联网共享经济体系。

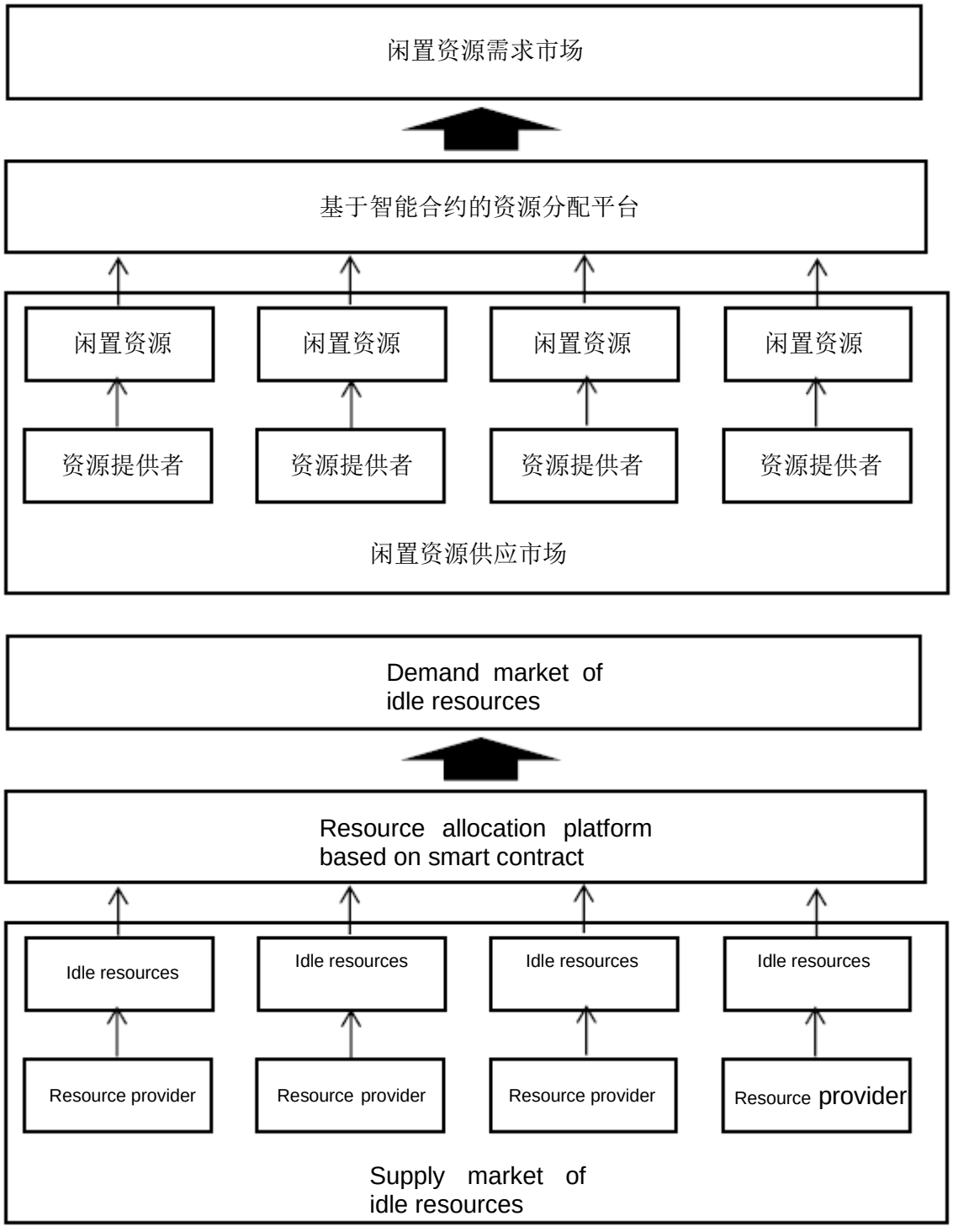
However, with blockchain, the IoT-based sharing economy system under centralized control can be improved, to reduce the system computing pressure and centralized control cost by using distributed computing and smart contracts; protect user privacy using identity verification system and zero-knowledge proof, so that users can gain trust without revealing their sensitive information; store the control information using distributed ledger, to guarantee correctness of equipment running and prevent enslavement, etc., showing that blockchain technology can be used to improve the existing IoT-based sharing economy system.

最后可以通过芯片或者硬件手段，去和实物共享体系相结合，利用成熟的物联网技术去升级现有的实物共享体系，实现实物基于区块链与物联网的共享经济。这将是未来 VNS 的共享经济应用的相关展望，VNS 也将在共享经济上持续探索，与生态合作伙伴共同研究区块链在此领域的应用。

Eventually, blockchain technology can be combined with the real object sharing system by means of chips or hardware, and mature IoT technology can be used to upgrade existing real object sharing system, to realize the sharing economy of real objects based on blockchain and IoT. This will be future of the sharing economy application of VNS. Moreover, VNS will continue to explore the sharing economy, and study the application of blockchain in this field together with ecology partners.

1、 基于 IOT 的闲置资源的基础共享方案

1. Basic Sharing Scheme of IoT-based Idle Resources



如上图所示，资源提供者将自身的闲置资源提供出来，通过 IOT 技术链接到基于区块链智能合约开发的资源分配平台，通过平台来面对资源需求市场。而资源需求市场的资源需求者，可以向资源分配平台提出资源使用需求，由资源分配平台调用闲置资源为资源需求者提供需求服务。与此同时，资源需求者需要通过区块链支付资源使用费用到智能合约，由智能合约根据资源提供贡献情况进行收益分配。

As shown in the above figure, resource providers provide their idle resources which are linked to the resource allocation platform developed based on the blockchain smart contract and face the resource demand market via such platform. And the resource demanders of the resource demand market can raise the resource use demands to the resource allocation platform and have the latter allocate idle resources at their demand service; in the meantime, the resource demanders need to pay the resource use expenses to the smart contract via the blockchain, and the smart contract will distribute the revenue according to the resource supply and contribution situation.

基于智能合约的资源共享平台，可以很好地减少中心化服务器处理带来的计算压力，同时可以更加公开公平地分配收益，资源提供者也将更加信任去中心化的平台的处理结果，这种信任也将促进更多的资源提供者大胆的将他们的闲置资源提供出来而不用担心遭到中心化平台的“剥削”或者私人信息泄露。这将极大的提升社会闲置资源利用效率，促进共享经济体系的形成。

The resource sharing platform based on smart contract can well reduce the calculating pressure from the central server processing, and can also distribute the revenue in a more open and fairer manner; and resource providers will trust more the processing results of the decentralized platform. With such trust, more resource providers will be promoted to provide their idle resources, without worrying about the “exploitation” or private information disclosure of the centralized platforms, which will greatly increase the utilization efficiency of social idle resources, and promote the formation of the sharing economy system.

这种平台模型均可以应用在 IOT 相关领域，闲置计算资源、闲置存储空间、闲置带宽甚至闲置电力资源等，通过将资源接入IOT，用网络传输的方式流动起来，再利用智能合约进行利益收取与分配，保证了系统的高效性、公正性、透明性。

Such platform model can be applied in relevant fields of IoT. Resources such as idle computing resources, idle storage space, idle bandwidth, and even idle electricity can be connected to IoT and can flow by means of network transmission, and then benefit collection and allocation can be conducted using smart contracts, to guarantee the high efficiency, fairness and transparency of the system.

2、 基于 IOT 的闲置资源进阶解决方案

2. Advanced Idle Resource Solutions Based on IOT

在现有体系下，可以接入 IOT 的软硬件闲置资源均可以利用上述方案进行共享经济的打造。但是现在依旧拥有许多实物的闲置资源，这些实物闲置资源并未接入网络，所以在进行共享经济的打造的时候可能会些许障碍，但是可以借用目前伪共享经济的“OFO”的方式，利用现有的硬件芯片技术给予实物链接物联网的能力。这是一种 IOT 共享经济的进阶，通过购买平台的智能芯片，与实物进行绑定，然后将实物共享给需求方，利用智能芯片确定实物的交付与接收，同时利用事先在智能合约中部署的共享回报算法计算回报收益，让需求方事先在智能合约平台中预存押金用于使用后的回报支付，需求方在使用完毕并交还供应方后，智能合约将计算对应回报并支付给共享方，这样双方就获得了各自需求的好处。

Under the current system, all software and hardware idle resources that have access to IOT can be used to build the sharing economy according to the previous scheme. As many physical idle resources are not available in the network at present, it would be difficult to realize sharing economy. By using the existing “OFO” mode of fake sharing economy, however, we can put physical objects on the IOT by applying the hardware chip technology. This is a kind of advanced IOT sharing economy. After purchasing a smart chip on the platform, we can bind the chip and the physical object together and share them to the demander. The smart chip is used to confirm the delivery and receipt of physical objects and sharing return algorithm stipulated in the smart contract is used to calculate the return. The demander is required to pay in advance the deposit on the smart contract platform

for subsequent return payment. After occupancy, the demander gives back the physical object to the supplier and the smart contract will compute relevant returns and transfer the payment to the sharing party. In this way, each side takes what it needs.

如此一来，传统的实物闲置资源也将借 IOT 的能力被利用起来，通过区块链的去中心化平台，让社会绝大多数可以想到的闲置资源可信任地再利用、再流转，从而产生价值，让参与者均可以从中获益。由于一切建立在去中心化之上，所以将不再有一个中心化平台去束缚资源的共享，每个人均是一个共享节点，可以利用区块链智能协议自主地去共享、去获取闲置的资源，这样的资源共享是一个几何效率的提升，VNS 相信，在这样的高效的共享经济的体系下，社会的生产力、环境保护效果、生产成本均会得到高效的提升。

In such a circumstance, traditional physical idle resources can be utilized by using IOT. On the blockchain decentralized platform, most imaginable idle resources in the society can be reutilized and recirculated on trust to yield value, which benefits every participant. Due to decentralization, there is no centralized platform to restrain resource sharing and everyone becomes a shared node. Idle resources can be acquired and shared freely via the blockchain smart protocol to improve resource sharing efficiency in a geometrical way. According to VNS, social productivity, environmental protection effect, and production cost saving will be promoted to a great extent under such highly efficient system of sharing economy.

3、 基于 VNS 的去中心化网站系统

3、 Decentralized Website System base on VNS

基于 VNS 主链和 VNS Name Service，我们提出去中心化互联网的概念。现有互联网架构 下的网站系统，最典型的架构是基于公有云服务。基于公有云的服务有着非常明显的缺陷。公有云服务商并不能提供绝对安全的服务，例如公有云服务数据中心的数据异地备份困难是数据中心常见的问题，中国曾出现某巨头公司因为数据中心网络问题造成上亿中国用户不能正常使用服务的情况。托管在云上意味着敏感的数据和代码也都全部托管给第三方机构，用户必须承担由此带来的安全性风险。除此之外，用户也不得不依赖云服务商提供的防范网络攻击的服务，如防火墙等等。

We propose the concept of decentralized Internet based on the VNS main chain and VNS Name Service. The most typical architecture of a website system under the existing Internet architecture is based on public cloud service, which has very obvious flaws. Public cloud service providers can't provide absolutely secure services. Forexample, remote data backup in public cloud service data centers is a common problem in data centers. In China, a giant company ever encountered a problem that hundreds of millions of Chinese users couldn't use its services because of network problems of its data center. Hosting on the cloud means that sensitive data and codes are also all hosted to third parties, and users must assume the resulting security risks. In addition, users also have to rely on services provided by cloud service providers such as firewalls to prevent cyberattacks.

随着硬件的发展，目前个人 PC 的硬件水平已经完全可以满足建设小型站点的硬件需要。与现有托管在云上的系统相比，去中心化网站系统有如下优点。第一，完全免费，网站全部内容都在用户电脑上，所以免去了支付给云服务商带宽，存储，计算能力 以及其他服务的费用。第二，安全性保障。去中心化网站系统建立在 VNS 主链和 VNS Name Service 的基础上，利用 VNS 主链提供对网站，数据等内容的百分之百的所有权认定和内容掌控，并且可以实现完全匿名化的访问和服务，去中心化的结构保证了网站系统不受单点故障的影响。第三，VNS 代币系统提供的代币可以在去中心化网站上流通。站点访问的 URL 是通过 VNS 主链提供的公钥生成，所以访问者可以方便的将代币发送给网站持有者，以鼓励网站持有者进行内容上的更新和创作。另外配合 VNS Name Service，公钥地址还可以映射成易于记忆的字符串，使 VNS 在去中心化网站系统中更易于流通。第四，更快速的域名解析服务和更快速的访问速度。DNS 解析服务使用 VNS Name Service，可以在本地完成域名解析，免去了 DNS 请求封包在网络上传输的时间。网站的所有内容都要先下载到本地浏览 器解析，在此我们将使用 BitTorrent 协议，以提高网站内容下载速度。第五，去中心化 站点系统将全面兼容现有互联网服务，用户可以正常连接到现有所有网站系统。具体技术路径如下：

With the development of hardware, the current PC hardware has fully met the hardware needs of building a small site. Compared with the existing systems hosted on the cloud, the

decentralized website system has the following advantages. First, it's completely free. With all the content on user computers, it eliminates the expenses in bandwidth, storage, computational power and other services paid to cloud providers. Secondly, the security is guaranteed. Decentralized website system is based on VNS main chain and VNS Name Service. It uses VNS main chain to provide 100% ownership and content control over websites, data and other content, and can achieve completely anonymous access and services. The decentralized structure ensures that the site system isn't affected by single point failure. Thirdly, the tokens provided by the VNS token system can be circulated on a decentralized website. The URLs visited by the site are generated through the public key provided by the VNS main chain, so visitors can conveniently send the tokens to the website holder to encourage the website holder to update and create the contents. In addition, with the VNS Name Service, public key addresses can also be mapped into easy-to-remember strings to make VNS easier to circulate in a decentralized website system. Fourthly, faster DNS service and faster access speed are available. DNS resolution service uses VNS Name Service to complete the domain name resolution locally, eliminating the need for the DNS request packet transmitting on the network. All content of the website must be downloaded to the local browser to resolve, and we will use the BitTorrent protocol to increase the downloading speed. Fifthly, the decentralized website system will be fully compatible with existing Internet services, and users can access to all existing website systems properly.he specific technical paths are as follows:

（1）本地站点托管

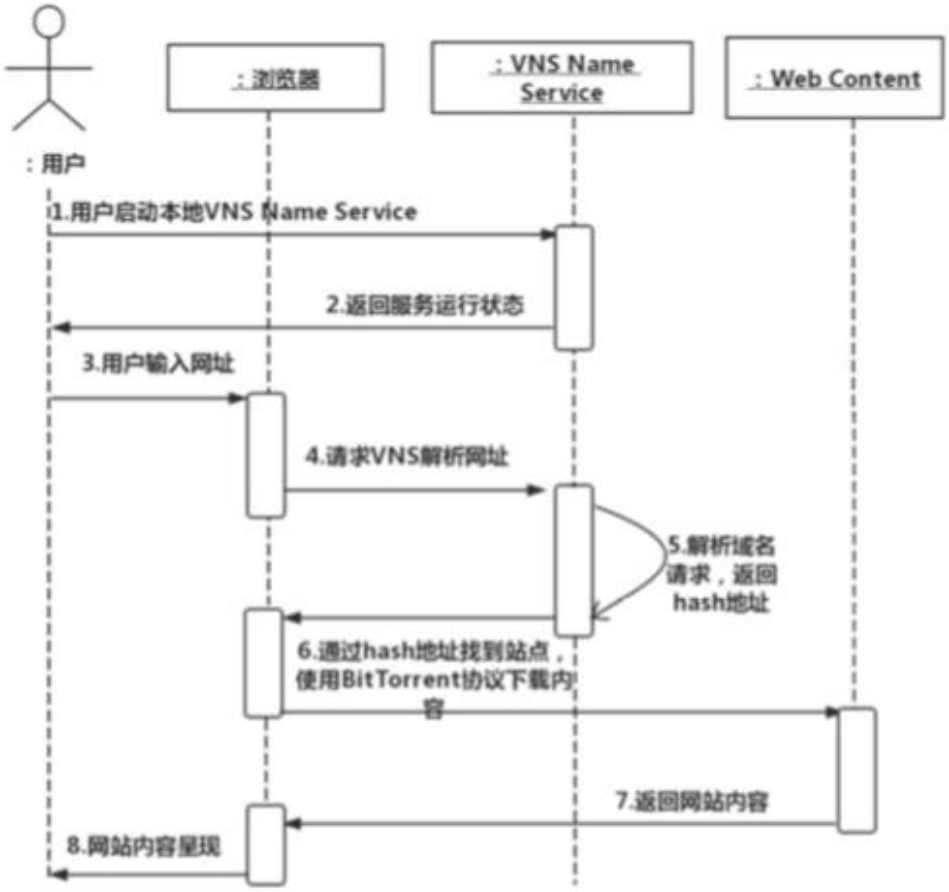
（1）Local Site Hosting

将站点托管在本地个人 PC 上并不是新概念，在现有体系下使用，托管在云端的服务完全可 以架设在本地电脑上。然而一个现实的问题是，普通用户很少拥有公网 ip 地址，也就无法 正常的通过 DNS 解析等等。虽然在现有体系下，在本地架设站点十分容易，但是想要对外 正常提供服务，对普通用户来讲过程十分复杂，并不具有可操作性。

Hosting your site on local PC is not a new concept. Under the current system, the services hosted on the cloud can be built entirely on local PC. However, a real problem is that ordinary users rarely have a public IP address and thus normal DNS resolution is impossible. Although it is very easy to set up a local site under the current system, it is very complicated and not feasible for common users to provide normal services.

VNS 去中心化网站系统，将使用 VNS 地址作为网站索引寻址的地址而不是 IP 地址，例如使用 分布式哈希表（DHT）来建立网站地址索引，这就解决了普通用户缺少 IP 地址的问题。由于要实现基于 hash 的网站地址索引，现有的 web 服务器，如 apache, nginx 等会存在兼容性 的问题，所以 VNS 去中心化网站系统，将提供一套完整的 web 服务器功能，提供一个嵌入式 的小型数据库以便于使用者进行站点开发。网站访问方面，用户可以通过使用现有主流浏 览器访问网站内容。简要工作流如下图:

VNS decentralized website system will use the VNS address rather than IP address as the address for site index addressing. For example, using a distributed hash table (DHT) to establish the site address index solves the problem of IP address shortage for common users. To achieve hash-based website address indexing, existing web servers such as apache and nginx will have compatibility issues. Therefore, VNS decentralized website system will provide a complete set of web server functions and provide an embedded small database for site development of users. For site visits, users can access the site content by using their existing popular browsers. The brief workflow is as follows:



（2）安全性及隐私

（2）Security and Privacy

VNS 主链使用了非对称加密的私钥公钥体系。基于 VNS 主链的去中心化网站系统也基于同 样的加密体系。对于网站建设者来说，私钥唯一保存在建设者手里，网站建设者可以对拥 有的网站的内容签名，以确定其所有权。VNS 主链，可以保证网站建设者通过建设站点得 到的 VNS 代币的安全性。对于网站访问者，VNS 去中心化网站系统将运行在独立沙盒 （sandbox）中，访问者如果遇到病毒站点等等，将其内容从本地删除即可。同时，对于 访问者来说，由于身份暴露在整个系统中的是自己的 VNS 地址，他人无法追踪追踪 VNS 地址持有者的真实身份，所以整个访问过程是匿名的。我们也会考虑提供对 TOR 的支持，以 提高匿名和保护隐私的需求。

VNS main chain uses a private key - public key system that is asymmetrically encrypted. The decentralized website system based on the VNS main chain is also based on the same encryption system. For website builders, the private key is uniquely stored by the builder, and the builder can sign the content of the owned website to determine its ownership. VNS main chain ensures the security of VNS tokens obtained through the construction of website. For site visitors, VNS decentralized website system will run in a separate sandbox. If a visitor encounters a virus site, its content can be deleted locally. At the same time, the visitor is not allowed to track the true identity of the VNS address holder because his or her identity is exposed to the entire system as a VNS address, so the entire visit is anonymous. We also consider providing support for TOR to increase anonymity and privacy needs

（三） 智能合约（合同）

(III) Smart Agreement (Contract)

1、 智能合约（合同）运作执行的保障

1. Guarantee of Smart Agreement (Contract) Fulfillment

签署合同的双方就合同内容达成一致后，通过将合同写成智能合约并附着在一个区块链交易上的方式来创造一个智能合约。智能合约将传统合同中的自然语言转换成程序编码，传统合同中的条款即转换成编码中预定义的规则，整个合约呈现“if－then”的状态，即如果达到特定时间或发生特定事件，则执行相应情境下的行动。

After two parties have reached an agreement on the contract contents, a smart contract will be created and attached to the blockchain as a transaction. The smart contract transfers the natural language in the traditional contract into program codes and converts terms in the traditional contract into predefined rules in the code. The whole contract is interpreted in the “if-then” format. In other words, actions will be taken accordingly, at a specified time point or a specific event occurs.

基于“去中心化”这样的一个最显著的特点，智能合约合同将被在不属于任何一方的区块链网络上自动执行，这样的执行是强制性的，无法更改与操控的，区块链网络将会实时监控合约允许状态，当达到合约执行条件后将会自动触发执行动作。

Based on the most significant feature-“Decentralization”, the smart contract will be fulfilled automatically in the blockchain network not owned by any party. The fulfillment is compulsory, immutable and uncontrollable. The blockchain will monitor the contract status in real time and automatically initiate actions when the contract fulfillment conditions are satisfied.

智能合约在被部署在区块链上的同时，也被盖上了“时间戳”。“时间戳”使得智能合约具有了不可篡改和不可伪造的特点，这也是区块链的一般性特点。区块链采用单向哈希算法，同时每个新产生的区块严格按照时间线顺序推行，由于时间的不可逆性，任何试图入侵区块链内部篡改信息的行为都很容易被追溯。在传统的中心化网络中，只需对中心节点进行攻击即可破坏整个网络(例如银行)，但在一个去中心化的区块链中，仅攻击单个节点无法控制或破坏整个网络。

When the smart contract is attached to the blockchain, it is stamped with a “Timestamp”. “Timestamp” endows the smart contract with immutability and unforgeability, which are also general features of the blockchain. One-way hash algorithm is applied to the blockchain and each newly emerged block proceeds in chronological order strictly. Due to time irreversibility, any act that tries to invade the blockchain and falsify data can be traced easily. In a traditional centralized network, an attack on the central node will destroy the whole network (for example, the bank). In a decentralized blockchain, however, the whole network cannot be controlled or destroyed by an attack on a single node.

这样的公正性保障、合同安全性保障、自动执行保障机制下，智能合约可以很好的替代现有的第三方机构去高效地监督合同的执行，这样就为合同参与者带来了高度的信任基础。

Under such mechanism that guarantees equity, contract security, and automatic implementation, the smart contract can be a good substitute for any existing third-party organization to effectively supervise performance of contract, which will build a highly reliable foundation for contract participants.

2、 减少合同参与者信用成本，提升工作效率

2. Reducing Credit Cost for Contract Participants and Promoting Work Efficiency

智能合约的去中心化使得交易不再需要中介机构或权威的介入，能够降低交易成本，提高交易效率，同时提高交易的安全性。降低成本，意味着交易中给第三人的费用支出得以减少，这不仅适用于金融领域，例如银行收取手续费的减少，也同时意味着法律相关费用的降低。合同设定合同双方的权利义务关系，在大多数情况下，合同以双方的义务履行为终止，仅当一方违约或对合同条款发生争议时，合同另一方才会诉诸法院。合同当事人在诉诸司法救济希望得到公平的风险分配的同时，也常常承受了大量时间、金钱、精力的投入，特别是在英美法系国家，有时一个民事诉讼案件的诉讼费用甚至高于合同的实际价值。法院的介入是一种事后法律救济手段，那么智能合约则可作为一种保证合同履行的事前措施，能够大大提高合同履行的效率。当一个智能合约被放在区块链上时，它一定程度上已经脱离了合同双方的控制，成为一个公正无私的第三方，一旦预先设定的条件被满足，就会执行合同，一定程度上实现了强制履行的效果，且其内置的违约责任的执行，也很大

程度上不再需要司法机关的介入。

Thanks to decentralization of the smart contract, an intermediary organization or authority is no longer required in transactions, which reduces the trade cost and improve efficiency and security of transactions. Cost reduction indicates a lower third-party expense. For example, it can be applied to cut the service charge collected by the bank in the realm of finance and also decrease expenses related to laws. The contract stipulates rights and obligations of both parties and in most cases the contract termination is subject to obligation performance of two parties. Only when one party breaks the contract or a dispute occurs over contract terms will the other party file a lawsuit. When a party concerned is appealing for fair risk allocation, it often sacrifices plenty of time, money, and energy. Especially in countries where Common Law is executed, the litigation cost for a civil lawsuit sometimes is even higher than the real value of a contract. Taking legal actions is a legal remedy after the event while the smart contract can be regarded as a beforehand measure which guarantees and accelerates fulfillment of the contract. When a smart contract is attached to the blockchain, it is free from the control of two contract parties to some extent and becomes an impartial third party. Once the pre-established condition is satisfied, the contract will be carried out automatically and thus the compulsory performance is realized to a certain degree. Due to pre-established liability enforcement for breach of contract, judicial intervention is no longer needed for most cases.

智能合约在本质上是一套计算机编码。相对于传统合同中自然语言具有的含糊不清的特性，计算机语言的准确性将会大大减少合同双方对于合同条款理解上的歧义，在这样的区块链智能合约的市场环境下，市场参与者间的信任将被极大的提升，人们只需要将精力集中到生产力的提升，去进行合同履约即可，在合同履约完成后，智能合约将公正地完成利益的分配，从而极大地提升经济市场的工作效率。

The smart contracts are essentially a set of computer codes. Compared to ambiguous natural language expressed in the traditional contract, the accurate computer language will greatly eliminate ambiguities of contract terms interpreted respectively by contract parties. In the market where the blockchain smart contract is applied, trust between market participants will be vastly increased and people only need to concentrate on productivity promotion to fulfill the contract. When contract performance is completed, the smart contract will distribute profits in a fair manner and thereby maximizes work efficiency of the economic market.

（四） 账本共享

(IV) Ledger Sharing

1、 应用于供应链金融

1. Application in Supply Chain Finance

VNS 关心区块链在金融行业的应用场景，区块链加速了信息的安全分发，呈现，传输和处理。从区块链技术中受益最多的往往是那些参与者之间信任度较低、交易记录安全性和完整性要求较高的行业，而金融业正是其中之一。相关咨询报告显示区块链或分布式账本技术每年可为金融行业节省成本 50-70 亿美元，这种成本的降低主要来自于区块链对现有业务的改进，如跨境支付价值链的改善、对账流程的优化、用户身份认证/反洗钱流程的效率提升和供应链金融以及普惠金融中的信息共享等。

VNS focuses on application scenarios of the blockchain in the financial industry and the blockchain accelerates safe distribution, presentation, transmission, and processing of data. Those industries featuring distrust between participants and higher requirements on security and integrity of transaction records benefit the most from the blockchain technology. The financial industry, for example, is one of them. According to relevant consulting reports, the blockchain or distributed ledger technology reduces cost for the financial industry by USD 5 to 7 billion each year. Such cost reduction benefits from improvements of existing services via the blockchain, including the improved cross-border payment value chain, optimization of account checking procedures, efficiency promotion of user identity authentication/anti-money laundering procedures, information sharing involved in supply chain finance and inclusive finance.

“区块链+供应链金融”是区块链在金融领域的最佳应用场景之一，具有广阔的市场空间。供应链金融

具有系统性、结构性的业务理念，决定了信息流是供应链金融风险把控的关键。如何获取真实、全面、有效的数据，既是供应链金融风控的基础，又是风控的难点，通过区块链的分布式账本等技术可以在供应链参与中的众多企业、众多金融机构间搭起一张可信的信息网络，从企业经营信息的源端获取信息，然后通过区块链达到端到端的信息数据透明、不可篡改，所有参与方都通过一个去中心化的记账系统分享商流、物流、资金流信息。银行根据真实的企业贸易背景、实时产生的运营数据开展授信决策，缩短资料数据收集、校验、评估的作业时间，降低风险成本，提升决策的精确性和效率。而企业通过供应链金融可以获得更低的贷款成本，更快速迅捷的金融服务，帮助业务的顺利开展和拓广。

“Blockchain + Supply Chain Finance”, characterized by broad market space, is one of the best application scenarios for the blockchain in the financial field. The supply chain finance is in accordance with systematical and structural business ideas, which determines the key role of information flow in risk control of the supply chain finance. The method of acquiring real, comprehensive, valid data is the foundation and a difficult point for risk control of the supply chain finance. Technologies such as distributed ledger on the blockchain help build an information network for enterprises and financial organizations participating on the supply chain and acquire information from the source end of business operation. Thanks to peer-to-peer, transparent, tamper-resistant information data transmitted on the blockchain, all participants share information of business flow, logistics, and capital flow in a common decentralized billing system. According to the real trade background of enterprises and real-time operation data, the bank can make credit decisions, shorten working hours for data collection, verification, and evaluation, lower the risk cost, enhance accuracy and efficiency of decision-making. The supply chain finance, on the other hand, also help enterprises to cut down the loan cost, acquire quicker and more convenient financial services, and facilitate development and expansion of business.

具体而言，区块链技术可以为供应链金融在以下方面提供强有力的支持：

To be more specific, the blockchain technology strongly supports the supply chain finance in the following aspects:

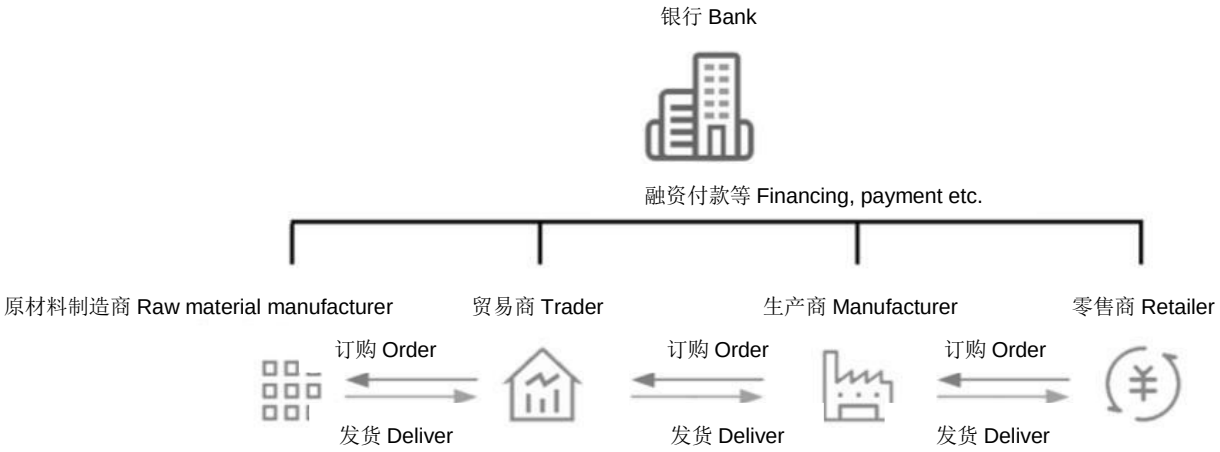
通过区块链的不可篡改性，记录供应链金融中上下游企业和周边企业的资金流、物流、商流过程，降低供应链金融过程中，可信数据采集、传递的难度；为金融机构获取第一手的供应链信息提供便利。如果企业广泛部署物联网终端，结合企业信息化系统的进销存信息，可以真实的勾勒出企业的运营情况与资产情况；企业透过企业网银、银企直联等渠道与上下游企业产生资金往来，提供真实的财务资金信息；这些信息将帮助金融机构在进行贸易融资、仓单贷款、应收账款贷款过程中极大简化信用评估流程与成本，以此降低企业融资的成本，提供融资的效率；

As data on the blockchain cannot be tampered with, the capital flow, logistics, business flow processes of upstream and downstream firms engaging in supply chain finance as well as peripheral enterprises are truly recorded. It becomes easier to collect and transmit credible data when doing business related to supply chain finance; financial organizations have convenient access to the first-hand supply chain information. Suppose that an enterprise has deployed IoT terminals extensively, together with its purchase, sales, and inventory information recorded in the enterprise information system, we can sketch the outline of the enterprise’s real operation status and assets status; an enterprise’s real financial information is rendered by its capital transactions with upstream and downstream firms via channels like corporate E-bank, host-to-host etc.; such information helps financial organizations to simplify credit assessment process and greatly reduce cost in case of trade financing, warehouse warrant, loan of receivables, and finally decrease corporate financing cost and increase financing efficiency;

通过“智能合约”等技术手段，为企业间“合同信任”关系之外，添加新的保障措施，简化企业间互担保、风险分摊、回购、履约等经营行为的流程，降低违约纠纷处理的时间成本和资金成本。以合同融资为例，合同的买方与卖方建立起中长期的供应关系，采购方的销售数据衍生出对原材料的采购需求的评估数据，市场的真实供需关系是融资回收的第一保障；若采购方企业提供风险缓释措施，在风险条件触发后，采购方是否按指令进行回购、退款等风险补偿履约措施，直接影响融资贷款是否产生不良资产。现行的操作中，上述履约约束主要来源于“合同信任”，但履约过程中可能存在法律争议，后期将增加法律纠纷的处理时间及成本。引入区块链“智能合约”，将上述合同约定事项上链，

使其变为自动触发与操作，从技术的角度弥补履约中的意外过程和主观违约可能，保障融资安全。

Depending on technical means such as “Smart Contract”, new safeguard measures can be added besides “Contract Trust” between enterprises and simplify processes of operations like mutual guarantee between enterprises, risk spreading, counter purchase, contract fulfillment to cut down the cost of time and capital when coping with a contract breaching dispute. Taking contract financing as an example, the buyer and the seller establish a long-term supply-demand relationship and the evaluation data related to procurement demand for raw materials can be inferred according to sales data of the buyer. The real supply-demand relationship of the market is the first important factor to guarantee financing recovery; provided that the buyer enterprise offers risk mitigation measures and risk conditions have been triggered, the buyer’s implementation or non-implementing of risk compensation measures like counter purchase and refund according to instructions will directly result in non-performing asset derived from financing credit. In practice, the above contract fulfillment is mainly controlled by “Contract Trust” and once a legal dispute occurs during contract fulfillment, time and cost will be increased to deal with the legal dispute. The “Smart Contract” will be introduced to place the contract terms on chain and automatically execute corresponding operations. Therefore, it offsets accidents and the possibility of subjective breach of contract during contract fulfillment in a technical way and thus ensure financing security.



订单记录、发货记录、物流信息、贷款信息均上链记录，供供应链所有参与者参考。

The order history, delivery record, logistics information, and loan information are recorded on the blockchain and provided to all participants on the supply chain for reference.

2、 应用于保理业务

2. Application in Factoring Business

在传统保理行业风险的考虑下，传统的保理业务仅仅愿意针对核心企业有应收账款义务的上游供应商或者对其直接下游经销方提供预付款融资或者存货融资服务，因为保理商对于核心企业的控货能力或者调节销售能力是信赖的。反之，除了一级供应商或者经销商外，一般是不愿意直接授信的。

Due to the risks in traditional factoring business, the traditional factoring business only targets the advance payment financing service or the inventory financing service provided to direct downstream distributors or upstream suppliers who have obligations of accounts receivable to core enterprises because factors trust the cargo control or sales adjustment competence of core enterprises. On the contrary, direct credit is only available for tier one suppliers or distributors.

另外,在实际操作上,保理商非常关注应收帐款债权“转让通知”的法律效力,所以都会要求一级供应商或核心企业签回“债权转让同意书”,如果一级供应商或核心企业无法签回,也会造成保理商不愿授信。在这样的现实条件下，催生了保理商在区块链技术支持下,开发一个供应链金融“智能保理”业务应用系

统的渴求。

In practice, factors are very concerned about legal force of “Notice of Transfer” of creditor's rights in terms of receivables. They will ask tier one suppliers or core enterprises to sign back “Declaration of Consent to Transfer of Creditor’s Rights”. If tier one suppliers or core enterprises fail to sign back, factors may not offer credit. In such a circumstance, with the support of the blockchain technology, factors are eager to develop an application system for “Smart Factoring” business in the field of supply chain finance.

这个系统将提供给所有供应链上的成员企业使用,利用这个系统核心企业可以将自己的债权和授信以区块链 Token 化，这样在体系中，债权和授信权将流动起来，保理商可以根据区块链上承载的债权和授信权拥有人信息对拥有人进行金融服务，这样一来改变了现有体系的供应链边缘参与者融资尴尬的问题。拥有了区块链这样的一个流转工具，依托其不可篡改的绝对性，可以让授信范围以核心企业为核心有了一个很好的衍生延展，可以快速激活供应链体系，达到资金迅速流转，高效生产的效果。

This system is available for all member enterprises on the supply chain. In this system, a core enterprise can transfer its creditor’s rights and credit into tokens while creditor’s rights and the credit granting right become circulative. Factors can offer financial services to the owner according to creditor’s rights and credit information related to the owner, which solves the problem that marginal participants on the supply chain have no access to financing in the existing system. As an tamper-resistant circulation tool, the blockchain extends a larger credit scope for core enterprises, activates the supply chain system quickly, and facilitates faster capital circulation and highly-efficient production.

与此同时保理业务的实际履约情况也将真实地记录在区块链网络之上，在未来的保理业务过程中，参与者也将根据对方的履约情况决定是否要和对方进行保理业务，于是由于履约情况的记录每个参与者的行为将会受到约束，否则将会在区块链网络上留下永久的污点，从而确保了保理业务的持续良性进行。

In the meantime, the actual performance of every enterprise on factoring business will be recorded truly on the blockchain network. When taking part in factoring business in the future, participants can determine whether or not to cooperate with another party according to its contract performance. Due to performance recording, each participant's behavior will be constrained by the record of performance, otherwise, his/her misdeeds will be permanently recorded on the blockchain, which ensures sustainable and virtuous factoring business.

3、 应用于 P2P 业务

3. Application in P2P Business

基于以上的智能合约合同基础，只需要根据需求，制作几个标准化借贷模板智能合约，然后在此智能合约平台上搭建 P2P 借贷平台，在这个平台上，人们只需要相互信任去完成借贷提供与需求发布，再由智能合约进行撮合即可。撮合完成后进行转款操作，接着在借贷期限结束之后，将执行事先约定好的利息与本金的转移。这个过程完全是智能合约操作，难以篡改，由此形成一个不会跑路、全透明的 P2P 平台。

With the help of the smart contract, it only needs to create several smart contracts based on the standardized debit and credit template and then build a P2P lending platform on the smart contract platform. On this platform, demands of debit and credit are published on the basis of mutual trust and the smart contract service is responsible for matching the two parties together. After that, money is transferred to the borrower. When the credit period expires, the interest and principal will be transferred as agreed. The tamper-resistant smart contract helps form a fully transparent P2P platform where breach of contract never occurs.

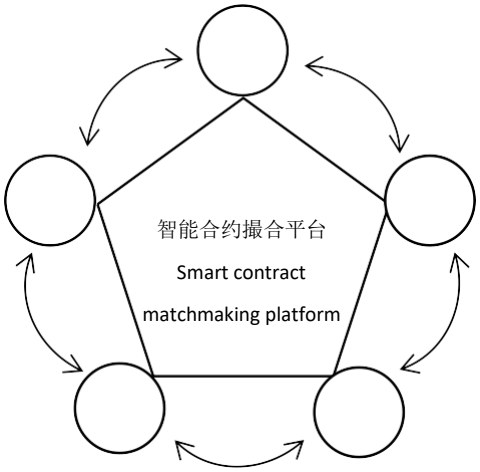
因为借贷活动是在区块链网络上完成，因此可以利用零知识证明技术，在一定限度内保护借贷参与人的隐私，同时也保证了信息的准确可靠，展现的是加密后的身份信息，而且这些身份信息也是值得信赖的。

As borrowing and lending are completed on the blockchain network, the zero knowledge proof can

be used to protect privacy of borrowers and lenders to a certain degree, ensure accuracy and reliability of information, and show encrypted and reliable identity information.

与此同时，人们在 P2P 业务上的信用信息将会记录并共享至共同账本之中，参与借贷活动的参与者会从区块链中获取到对方的完整的信用信息和履约情况。此信息将会是完全真实记录的，没有经过任何的修改，根据这些信用信息，也将帮助借贷者决定是否和对方进行借贷行为。

At the same time, people's credit information revealed in P2P business will be recorded and shared in a common ledger. One party engaging in debit and credit can acquire complete credit information and contract performance status of the other party, which are completely true without being tampered with. These credit information will help the lender or the borrower to decide whether to cooperate with the other party.



（五） 鉴证证明

(V) Verification and Certification

解决信息不对称，信息透明化，加强公众监督

Dealing with information asymmetry, enhancing transparency of information, and reinforcing public supervision.

1、 公益捐款

1. Public Welfare Donations

区块链上存储的数据，高可靠且不可篡改，天然适合用在社会公益场景。公益流程中的相关信息，如捐赠项目、募集明细、资金流向、受助人反馈等，均可以存放于区块链上。在满足项目参与者隐私保护及其它相关法律法规要求的前提下，有条件地进行公开公示，方便公众和社会监督，助力社会公益的健康发展。

As data stored on the blockchain is highly reliable and tamper-resistant, it is applicable to the public welfare scenario. All information related to the public welfare process can be stored on the blockchain, including donation projects, fund-raising details, fund flow, feedbacks from recipients etc. On the premise that program participants' privacy is well protected and relevant laws and regulations are complied with, conditional disclosure will facilitate social supervision and healthy development of public welfare.

应用区块链技术支撑公益项目的阳光、透明和可追溯，爱心物资经由高效的物流体系直接配送到公益项目地，并由公益机构执行人员发放至受助人手中。捐赠人可通过客户端或者区块链浏览器实时查询所捐赠物资的物流状态，直观地看到物资发放到受助人手中的全过程。

The blockchain technology guarantees positive, transparent, traceable public welfare programs. Caring goods and materials are directly delivered to the public welfare site via an efficient logistics system and then issued to grantees by the personnel from public interest organizations. The donator can inquire the real-time logistics status via the client or the blockchain browser to see intuitively the whole course until goods and materials have been issued to the recipients.

从选购爱心物资开始的全部流程信息、参与主体信息均使用区块链技术来记录，从而防止篡改，确保公益透明性、可追溯，极大增加公益平台的权威性和可信度。

Including the procurement of caring goods and materials, all information related to the whole process and participants are recorded with the blockchain technology, so as to prevent tampering, and ensure the transparency and traceability of public welfare, have greatly increased the authority and credibility of the public welfare platform.

2、 追本溯源

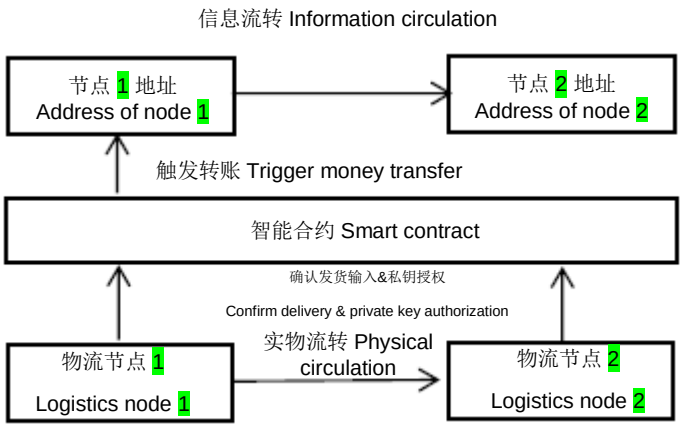
2. Traceability

利用区块链的可追溯性、不可篡改性以及时间戳功能，用下列方案可以很好的进行货物的追溯记录，将货物的物流运转过程准确的、公正地记录上链，保证消费者在查询的时候获取完整准确的物流信息，从而对货物进行追本溯源，从而打破这个现状：供应链由供应商、制造商、分销商、零售商、消费者等多类参与主体构成，商品生产和供应过程中产生的各类信息分散于各个环节，信息的不透明导致假冒伪劣商品这样的问题很难彻底消除。

In view of the traceability, tamper-resistance, timestamp of the blockchain, the following scheme can be used to record the logistics process of cargos on the block chain accurately and fairly and guarantee the complete and accurate logistics information inquired by consumers. As all cargos can be traced to sources, it breaks the status quo: on the supply chain, there are a variety of participants such as the supplier, the manufacturer, the distributor, the retailer, the consumer and thus all kinds of information related to commodity production and supply is scattered in various links. As a result, information opacity makes it difficult to eliminate fake and shoddy goods.

方案即：使每个物流节点均登记上链，并获得对应的物流节点地址；物流节点 1 向物流节点 2 发送货物时，首先扫码发货并私钥确认授权，待物流节点 2 接受到货物后扫码确认，每次确认均将传输到智能合约中；智能合约得到了双重确认的输入指令之后，对节点 1 地址进行向节点 2 地址转账货物对应编码信息的操作，这便是一个货物流转向区块链映射的过程。像这样的多个节点环环相扣链接，最终消费者在获得货物后，只需要扫码向区块链网络确认，即可获得完整的货物流转信息，从而对货物的真伪进行判断。

The scheme is to make the blockchain record every logistics node and display its logistics address; when logistics node 1 delivers goods to logistics node 2, it is required to scan the code for delivery and confirm private key authorization. After receiving goods, logistics node 2 scans the code for confirmation. Every confirmation will be recorded in the smart contract; after receiving the double confirmation as input, the smart contract orders node 1 to transfer the corresponding coded message of goods to node 2 according to the address. This is the course where circulation of goods is mapped on the blockchain. Thanks to interlocking links at multiple nodes, the ultimate consumer can get the complete goods circulation information by scanning the code for confirmation on the blockchain network after receiving goods, and thereby determine whether they are genuine or not.



3、 个人与企业的身份认证

3. Identity Authentication for Individuals and Enterprises

身份及接入管理服务是区块链技术应用的一个重要领域，不仅如此，由于区块链技术可以带来高可靠性、可追溯和可协作等特质，使得其在身份及接入管理服务的应用领域具备成为基础技术的潜力。

Identity and access management services are important applications of the blockchain technology. The blockchain technology, featuring high reliability, traceability, and interoperability, has the potential to become a basic technology applied in the field of identity and access management.

伴随着数字化进程的加速，身份及接入管理服务的应用领域将越来越广泛，包括互联网、物联网、社会和经济生活等。在这些应用领域中，身份及接入管理服务的典型作用是保障具备合法身份的用户或设备可以安全、高效的接入和享受服务。身份及接入管理服务在各个应用领域中所处的位置至关重要，但目前该服务也一直面临着隐私泄露、身份欺诈以及碎片化等问题，给用户、设备和系统均带来极大的挑战。

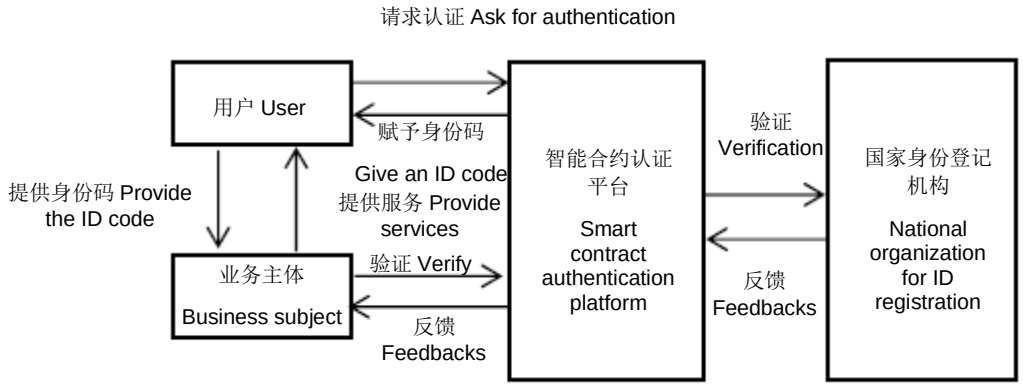
With the development of digitization, identity and access management services will be applied to more fields, including the internet, internet of things, social and economic life， etc. In these application fields, the typical effect of Identity and access management services is to ensure the user or equipment that has legal identity has access to and enjoys the service in a safe and efficient way. Identity and access management services are crucial in all application fields, but it also exposes weaknesses like privacy disclosure, identity fraud, fragmentation, which creates formidable challenges to the user, equipment, and system.

区块链技术的引入和发展，为进一步解决上述问题提供了新的思路。将区块链技术应用到身份及接入管理服务中，将有可能形成一种协作的、透明的身份管理方案，有助于企业、组织更好的完成身份管理和接入认证。

The introduction and development of the blockchain technology offer a new way of thinking for further solving the previous problem. When the blockchain technology is applied to identity and access management services, it is possible to form a collaborative and transparent identity management scheme for enterprises and organizations to better perform identity management and access authentication.

VNS 区块链技术在身份及接入管理服务的应用，未来将依托新的硬件、软件和区块链平台等的配套支持，为企业、组织提供专业、安全、高效的身份和管理服务，身份认证的应用示例如下所示：

Based on the VNS blockchain technology, identity and access management services, supported by ancillary facilities such as new hardware, software, the blockchain platform, will offer professional, safe, highly efficient identity and management services to enterprises and organizations. The following diagram shows the application of identity authentication:



基于以上模型，即可以在验证个人/企业信息的同时，保护相应的隐私。这一点在个人角度尤其的重要，现在个人在社会中进行任何活动的时候，都会不断的被要求验证身份信息，而这些身份信息也随着不断地被验证不断地被泄露，最终我们如同裸奔在大街上的人，毫无隐私。这些在影响了我们生活便利的同时，也极大地影响了我们的财产与人身安全。

On the basis of the previous model, privacy can be protected at the time of verification of personal/enterprise information. It is especially significant for individuals. When people participate in social activities, the personal identity information is verified and disclosed constantly. Eventually, our information will be disclosed, as we end up streaking down the street with no privacy. These bad effects do harm to our life convenience and also threaten our property and personal security.

未来 AMT 社区也将致力于让每个人拥有自己的“最后的遮羞布”，保护人们最后的隐私，利用区块链技术让人们未来无需透露自己是谁即可证明自己的身份。并且利用智能合约的便利性，可极大的便捷人们的自证过程，加速数字化社会的发展。

The future AMT Community will endeavor to offer everyone “The Last Fig Leaf” to protect people’s last privacy. With the blockchain technology, people are able to prove his/her identity without revealing who he/she is. The convenient smart contract will greatly simplify the process of identity proof for people and accelerate the development of the digital society.

4、 所有权保护（知识产权、物权）

4. Protection of Ownership (Intellectual Property, Property Right)

（1） 著作权

(1) Copyright

著作权制度不同于专利和商标制度，著作权权利自作品创作完成之日起自动产生，无需经过国家行政机关的审查登记。创作作品的公民、法人或其他组织是作者，对其作品享有著作权，如无相反证明，推定在作品上署名的公民、法人或其他组织为作者。但作者是否在作品上署名，署真名、笔名还是假名，完全由作者自主选择。在作者署假名或匿名的情况下，作品在传播过程中极易导致作者身份不明，使作品成为“孤儿作品”。孤儿作品的存在对著作权权利的行使和作品的后续使用不利，计划使用作品的第三方难以找到著作权人，向其索要使用作品的授权许可，因此第三方要么会放弃使用作品，要么在后续使用中面临着著作权确权后的侵权风险。我国虽然建立了著作权登记制度，可以用于证明著作权权属，但该制度属于自愿登记，登记费用可高达上千元，不利于中小企业和个人进行著作权登记；而且登记申请中需要填写著作权人的真实信息，阻碍了匿名作者进行权利登记。基于区块链技术能在每一份信息上加盖时间戳，保证信息的完整、有效和不可篡改，并根据对信息的更新和产生的新信息形成按时间顺序连接的区块链，区块链技术有利于对作品每阶段的创作进行记录，并确认作品的创作者，同时又能保证希望匿名或署假名的作者对其个人隐私的保护。区块链中加盖的时间戳能够证明某人在特定时间访问了特定文件，时间戳被保存在区块链中，全网中的任何参与者都能看到时间戳，作品的创作者通常是第一个访问该文件的人，其作者身份因此能够得以证明。区块链上作者和作品信息与某一特定公钥和网络地址对应，当他人要向作者获取授权使用作品时，会通过网络地址和公钥获取作品，避免了在作品交易时透露创作者在现实中的真实身份。作者基于区块链的一次著作权登记成本最低只有几分到几毛，登记几乎在瞬间便可完成，极大降低了著作权登记的成本和周期时间。

The copyright system is different from the patent and trademark system. The copyright is automatically generated from the date of completion of the creation, without any need to be examined and registered by the state administrative organs. Citizens, legal persons or other organizations that create works are authors who have copyright in their works. If there is no contrary evidence, citizens, legal persons or other organizations who sign on the work are presumed to be the authors. However, it is completely the authors’ right to choose whether sign on the work in the real name, pen name or the pseudonym or not. In the case of the author uses the pseudonym or anonymity, the author can easily become unknown in the process of spread, making the work an "orphan work." The existence of orphan works is unfavorable for the exercise of copyright rights and the subsequent use of works. It is difficult for a third party who plans to use the work to find a copyright owner and ask for the using permission. Therefore, the third party will either abandon the use of the work or face the risk of infringement after the copyright is confirmed in subsequent use. Although China has established a copyright registration system, which can be used to prove the copyright ownership, but the registration is voluntary, and the registration fee can be as high as several thousand Yuan, which is not conducive to the registration of copyrights by small and medium-sized enterprises and individuals; and the registration application needs the real identity information of the

copyright owners, preventing anonymous authors from registration. Based on the block chain technology, each message can be appended a timestamp to ensure that the information is complete, valid and tamper-resistant, and the block chain connected in time series is formed according to the information update and new information generation. Block chain technology facilitates the recording of each stage of the work and confirms the creator of the work, while at the same time ensuring the protection of the personal privacy of authors who wish to be anonymous or under the pseudonym. The timestamp added in the block chain can prove that someone has accessed a particular file at a particular time. The timestamp is stored in the block chain, which can be seen by any participant in the network. The creator of the work usually is the first person to access the file, and its authorship can therefore be proved. The author and the work information on the block chain corresponds to a specific public key and network address. When someone else wants to obtain the authorized use of the work from the author, the work will only be obtained through the network address and the public key, avoiding revealing the true identity of the creator during the transaction. The cost of a copyright registration based on the block chain is only a few cents or pennies, and the registration can be completed almost instantaneously, greatly reducing the cost and cycle time of the copyright registration.

（2） 商标

(2) Trademark

与应用于著作权登记类似，区块链技术同样可以用于证明商标的在先使用。根据我国《商标法》，商标需要经过商标局核准注册，才能使商标所有人享有注册商标专用权。但我国采用商标自愿注册制度，没有经过核准注册的商标也能在商业中使用，这就涉及使用在相同或类似商品上、设计相同或近似的在先使用商标和在后注册商标权利间的协调问题。2013 年修订后的《商标法》明确指出在先使用的有一定影响的商标所有人不会侵犯在后商标注册人的权利，在先使用人可以在原使用范围内继续使用商标。判定在先使用和原使用范围需明确考量在先商标开始使用的时间、商品或服务范围、地域范围、销售对象、销售途径、广告宣传时间和程度等因素，人工统计一定程度上会有遗漏，尤其针对某些有一定影响的商标，统计数据多、耗时长、成本高。区块链技术的时间记录性能较好解决证明商标在先使用的问题。如果每笔交易都将商品上的商标信息记录在区块链中，则根据区块链和智能合约中的信息就足以统计出商标第一次在商业活动中使用的时间，以及这些使用是否使商标具有了显著性和影响力。此外，区块链技术对在先使用的证明也能帮助缺乏固有显著性的商标获得注册，因为没有固有显著性的商标在使用中如果获得了显著性，能使该商标在申请注册过程中不会因为缺乏显著性而被商标局驳回。

Similar to the application to copyright registration, block chain technology can also be used to prove the prior use of a trademark. According to the Trademark Law of China, the trademarks need to be approved and registered by the Trademark Office, so that the trademark owners could enjoy the exclusive right of the registered trademarks. However, China adopts the voluntary registration system for trademarks, and trademarks that have not been approved for registration can also be used in commerce, which involves the coordination problem between the rights of prior-using and post-registration of trademarks with the same or similar designs used on the same or similar goods. *The Trademark Law*, amended in 2013, clearly states that the prior trademark owner who has some influence will not infringe the rights of the subsequent trademark registrant, and the prior user may continue to use the trademark within the original scope of use. Judging the scope of prior use and the original use needs to explicitly consider the time when the prior trademark is used, the scope of goods or services, the geographical scope, the sales target, the sales approach, the time and degree of advertising, etc. There are some omissions of the artificial statistics to some extent, especially for certain trademarks with some influence, whose statistical data is large, making the work to be time-consuming and costly. The time recording performance of the block chain technology is better to solve the problem of proving the prior use of trademark. If the trademark information on the commodity in each transaction is recorded in the block chain, then the information in the block chain and the smart contract is sufficient to count the first use time of the trademark in commercial activities, and to prove whether these uses make the trademarks distinctive and influential. In addition, the block chain technology used to prove the prior use can also be used to help a trademark without inherent distinctiveness get registration, because if a trademark without inherent distinctiveness obtains this feature in use, it will not be rejected by the Trademark Office for lack of distinctiveness

in the process of registration application.

（3） 物权

(3) Property Right

利用 IOT 技术将物与区块链绑定，在区块链上设置一个虚拟的权限凭证，证明物品的归属与使用权，当该物品的归属权在使用者绑定的区块链地址之中时，智能合约才将给予该使用者操作权限。例如汽车设置指纹开启，指纹与使用者、使用者地址进行绑定，当使用者地址中拥有该汽车的物权时，智能合约授予该使用者使用的权利，此时使用者方可使用指纹对汽车进行解锁操作，当物权归属不在使用请求人地址中时，将无法用指纹进行解锁。这样也很好的解决了物权的交易，利用智能合约可以快速的进行物权的交易，而交易后将立刻进行物权判定，获取物权的一方将可以执行该物品的使用权利。这样节省了大量的物权登记变更的时间成本与金钱成本，快速地进行了物权的变更登记且过程清晰可查，大大加快了物权登记变更效率。

Making use of IOT technology to bind the thing to the block chain, and a virtual permission certificate is set on the block chain to prove the ownership and use rights of the item. Only when the ownership of the item is in the block chain address bound by the user, the smart contract will give the user access to the operation. For example, if a car is set to use with a fingerprint, the fingerprint will be bound to the user and the user’s address. When the user's address has the real right of the car, the smart contract will grant the user the use right, and the user can use the fingerprint to unlock the car at this time. When the ownership of real right is not in the requester's address, the car cannot be unlocked by the fingerprint. This approach also solves the transaction of real rights very well. The transaction of real rights can be quickly carried out by the smart contract, and the real right will be determined immediately after the transaction. The party acquiring the real right can execute the use right of the property, which saves a lot of time and money costs of the change of real right registration, quickly changing the registration of real rights with a clear and easy-to-check process and greatly speeding up the efficiency of changing real right registration.

附件

Attachment