UOC:一个大型分布式应用程序的开源平台

UOC: a open source platform for large distributed applications

UOC
uocone@gmail.com
7, 2018

中本聪在 2009 年 1 月启动比特币区块链，向世人证明了完全通过点对点技术实现的电子现金系统是可行的、安全的。越来越多的人，尝试将区块链带来的新思维和新技术，应用到更多领域。

Satoshi Nakamoto started the Bitcoin project in January 2009,proving the world that a peer-to-peer electronic cash system is feasible and secure. As a result,more people are now using the underlying blockchain technology to solve problems in various industries.

UOC 在本文中，在以比特币为基础的区块链上，提出了在非金融领域的事务处理高效实现的可能，并且以网络游戏为首要应用方向。

This paper outlines how UOC, which inherits the underlying blockchain technology of bitcoin, and its revolutionary Specified Range Trusted Random Number Generator (SRTRNG) can help developers efficiently process transactions in nonfinancial spheres, such as online games.

为实现上述目标，我们分别在区块链技术领域、计算机技术领域、数学理论领域，提出了聚合约、自证存储链、博弈证明三项基础技术。

To achieve our goal,three basic techniques:Polymerized Smart Contract (PSC),Self-Certified Storage Chain (SCSC) and Proof-of-Game (PoG) are proposed.And they can be respectively used in teh field of blockchain technology, computer technology and mathematical theory.

1 关于转帐事务处理(Transactions)的本义

1. On the original meaning of the transactions

Transactions 是一个非常重要的定义，中本聪在比特币论文[1]中，将其作为前言概述之后，放在首位被定义的条目。歧义理解的话，在实际应用实现中，会造成南辕北辙巨大偏差。

It is important for us to define the word Transaction accurately. Satoshi Nakamoto knew that so he defined it meticulously in his Bitcoin paper[1]. If defined ambiguously, it will cause enormous difference in practice.

比特币关于 transactions 单词的描述，在许多文档中（特别是中文译文[2]），被解读为交易，UOC 以为这是不精准的解读，甚至是会带来歧义的解读。

The description of the word transactions in many bitcoin-related documents(especially the Chinese translation[2]) is interpreted as an exchange,which UOC believes is inaccurate or even ambiguous.

UOC 以为，用事务处理或者金融业务中常说的转账来解读更为合适。

例如：在标准的银行系统中，一个从 A 账户向 B 账户转账 X 元的请求是一笔转账事务，而不是交易。在习以为常的认知中，解释为交易的话，那么 B 应该向 A 提供 AB 双方约定的服务。

以下是比特币论文的英文原版，特意的标注，是为了更好的理解交易与转帐事务处理含义上的区别。

［*Transactions: We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.*］

由此可见，比特币的区块链，本义是在描述数字资产的归属权问题。

UOC believes that transaction processing or transfer in the financial context is more appropriate than exchange.

For example, in the banking system, a request of moving X dollar from account A to account B is a transfer instead of an exchange. An exchange, rather, means that A and B form an agreement and then one renders a service to another.

The following is the definition of transactions from the Bitcoin paper, which helps us to understand the difference between an exchange and a transfer.

［*Transactions: We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.*］

Apparently, the Bitcoin paper is mean to describe the ownership of digital assets.

2 关于脚本与公共资源

2. On Script and public resources

比特币区块链中，已经实现了脚本事务处理，但中本聪没有在其论文中进行过定义。

直到其等价功能的描述和比较，出现在以太坊区块链[3]中，智能合约[4]这个概念才在区块链世界广为人知。

Script transaction processing has been implemented in the blockchain of bitcoin,but Satoshi Nakamoto has not defined it in his paper.

It was not until the description and comparison of its equivalent functions appeared in Ethereum[3] that the concept of smart contracts[4] became widely known in the blockchain world.

比特币的脚本与以太坊的智能合约一样，都是为了解决更加复杂的转账需求，例如：如果怎样，则怎么样的，基于条件的，甚至是多方参与的转帐事务。

此设定，为事务处理提供了逻辑环境，带来了无限的想象空间。

Bitcoin scripts,like those of Ethereum smart contracts. Are designed to address more complex transfer requirements, such as executing something when a certain requirement is met, or even involving more than two parties in a transaction.

These settings provide transaction processing with unlimited possibilities.

比特币的脚本，与以太坊的智能合约，基础功能上是一致的。以太坊对比特币脚本的缺点描述，包括缺少图灵完备性、价值盲、缺少状态和区块链盲方面，UOC 是认同的。

但是，UOC 觉得因此对比特币脚本的改进，是不必要的。或者说，以太坊提出的智能合约改进方向，是有风险存在的。

Bitcoin scripts and Ethereum smart contracts are the same in terms of basic functions. We agree with Ethereum’s opinions on the disadvantages of Bitcoin scripts, including a lack of Turing-completeness, value-blindness, a lack of state, and blockchain-blindness.

However, UOC thinks that it is unnecessary to improve Bitcoin scripts. In other words, risks exist in Ethereum smart contracts.In other words,there are some risks in the improvement direction of Ethereum smart contracts.

比特币的事务处理，都是从外部创建的，包括脚本事务处理；以太坊的基于智能合约的事务处理，可以从内部创建。后一种方式，对应用的开发，带来较大危险。已经有很多基于以太坊的应用，在使用智能合约时，出现了重大漏洞。

All Bitcoin’s transactions are built from outside, including scripts transaction, however, Ethereum’s transactions can be built from inside. The latter approach brings substantial risks to application development, and now many Ethereum-based applications have already presented significant loopholes in the use of smart contracts.

UOC 以为，基于数字资产归属权的描述，只能是结果唯一的，不应该参与逻辑运行的过程。例如：博彩游戏胜负的结果，影响数字资产归属权，但博弈过程与数字资产归属权无关。

UOC 无意指责以太坊的智能合约的解决方案是错误的，只是以为可以有其他不同思路的实现。

UOC 以为，比特币的脚本事务处理方式是完美的，外部创建是安全的。只是其对数字资产归属权非你即我的描述过于单一，缺少对非排他性的使用公共资源进行描述。

即，公共资源，是可由所有人，非排他性使用的。

例如：土地资源、水资源、矿产资源、公共设施等等。还有，在网络游戏中的副本、怪物等，都属于公共资源，玩家可以刷副本、打怪物，从而获得装备或游戏金币等财富奖励。而游戏开发商，通过提供公共资源的服务，收取费用，继而循环，可提供更多的服务。

Scripting system is responsible for logic processing. UOC believes that logic processing should not involve digital assets ownership, which entails sole proprietorship.For example, the result of a lottery game has an effect on players’ digital assets ownership, but the process of the lottery has nothing to do with the digital assets ownership.

UOC is not saying that Ethereum’s idea of building smart contracts as a solution is wrong. What UOC is saying is that there can be a different approach to the problem.

UOC believes there are two kind of assets: exclusive and non-exclusive ones. Bitcoin deals with the former one perfectly but it fails to handle the non-exclusive ones.

UOC define the non-exclusive one as public resources that can be used by anyone.

For example, lands, water, minerals and public facilities are public resources. Instances and monsters in online games are public resources. Players can participate in the raid to obtain equipment, money or any other assets as reward.Game publishers offer public resources for a profit. The more the profit, the more they are incentivized to provide better service.

3 聚合约 PSC

3. Polymerized Smart Contract(PSC)

UOC 基于比特币区块链，提出了新的公共资源的概念，在无需改变比特币脚本事务处理的基础上，增加了一个外部的、插件式的解决方案，并将其定义为“聚合约”。

UOC 强调，基于数字资产归属权的描述，只能是结果唯一的，本身不应该参与逻辑运行的过程。

聚合约，旨在描述一个逻辑过程，并返回结果。

聚合约是安全的，由于执行过程不涉及资产归属权变化，所以，即便受到攻击或恶意诋毁，也不会对资产归属权造成影响。最差的实现情况是：B 没有对 A 提供服务，所以 A 的资产不会流向 B。

Based on Bitcoin, UOC brings in the concept of public resources. Without changing Bitcoin scripting system for transactions, UOC suggests an external plug-in solution which is referred to as Polymerized Smart Contract(PSC).

UOC emphasizesthat logic processing should not involve digital assets ownership, which entails sole proprietorship

PSC aims at describing a logic and returning a result.

PSC is secure. Because implementing PSC does not result in a change in the ownership of digital assets, there is no harm even when PSC is attacked or defamed. The possibly worst situation is that A does not transfer money to B, and B does not provide A with any service.

UOC 对这种情况的发生，是接受的。如同区块链的记账人，有可能会选择性的记录转账事务那样，某些事务处理请求被记账人忽略，甚至是恶意拒绝。

This situation is acceptable to UOC. Just as a bookkeeper may be selective about which transaction to be recorded, some transactions are neglected or even rejected maliciously.

UOC 的聚合约，运行在去中心化的节点上，采用自证存储的安全保护机制，所以攻击、诋毁和伪造是无意义的。

PSC adopts the Self-Certified Storage, which is in itself secure. Therefore, there is no point in attacking, defaming or forging PSC.

聚合约，是以插件模式，运行在区块链节点上的可执行语言，为脚本事务处理，提供了逻辑补充。它不对数字资产进行归属权描述，仅返回处理结果。

PSC enables executable language to run on blockchain nodes as plugin. It supplements transaction processing with custom scripting functions. It does not describe the ownership of digital assets but returns the result only.

区块链节点，可选择运行某个或某几个感兴趣的应用，为其提供聚合约的算力服务。是否提供算力服务，是节点的一个可选择的插件模式。

Blockchain nodes provide PSC with CPU power for one or more applications. CPU power is an optional plug-in model for nodes.

4 自证存储链 SCSC

4. Self-Certified Storage Chain(SCSC)

为了保证所有节点聚合约运行的结果一致性、抗攻击和诋毁，UOC 扩展了一种在较小领域中被广泛应用的技术。

这是一种在匿名网络中，很早就被熟练使用的、约定俗成的、基于时间轴的 P2P 加密信息传递方式，但尚无明确的名词定义。

为了方便理解，按照功能描述，UOC 将其定义为“自证存储”。

To ensure the consistency, anti-attack, and anti-defame of the PSC results of all nodes, UOC extends a technology that is widely used in smaller areas.

This technology, which has no clear definition yet, has long been used skilfully and conventionally in an anonymous network, and it is a P2P encryption information transfer mode based on time axis.

For better understanding, UOC defines it as Self-Certified Storage(SCS), according to its function.

这是一种精巧的信息传递方式，基于不对称加密方法，保证消息传递的各方，在传递消息过程中，不会产生歧义，同时保证数据不会被除了自己之外的人伪造。

例如：A 要发送一段消息给 B，首先 A 用自己的私钥对消息加密，这样可保证这一段消息无法被伪造。B 在接收到消息后，用 A 的公钥对加密消息进行解密即可获得明文。为了保证这个消息只能被 B 接受，这一段消息又会用 B 的公钥进行加密，保证了只有 B 才能解开。

SCS , a sophisticated information transfer mode, utilizes an asymmetric encryption method, can ensure that the parties involved in the message delivery do not have any ambiguity during the message delivery and that the data will not be falsified by anyone other than themselves.

For example, A is going to send a message to B. A encrypts the message with A’s private key, serving as a proof that A encrypted it and it is not forged. When B receives the message, B decrypts the message into its original form with A’s public key. To guarantee that only B has access to the original message, this message is also encrypted with B’s public key.

UOC 对“自证存储”加上了时间轴和消息 HASH 的链首与链尾，用以保证数据的唯一性和完整性。即便 A 伪造了不同的消息进行广播，那么 A 必须再发送下一条消息时候，对已经双

花的消息进行调整。但这种作弊是不允许的，因为 A 已经为自己的作弊行为留下了不可篡改的数字指纹证明。

UOC put a timestamp and hash at the beginning and the end of the chain of SCS so as to ensure the data uniqueness and completeness of the data. Even if A broadcasts forged messages, A will have to send another message to conceal the double spending problem caused by previous broadcasts. But what A will do is not allowed, for it has already left its digital fingerprint on the chain as a proof.

UOC 对这种基于加密安全的消息传递和存储机制，定义为“自证存储链 SCSC”。

This system of transferring and storing messages based on encryption is referred to as Self-Certified Storage Chain(SCSC) by UOC.

5 服务节点

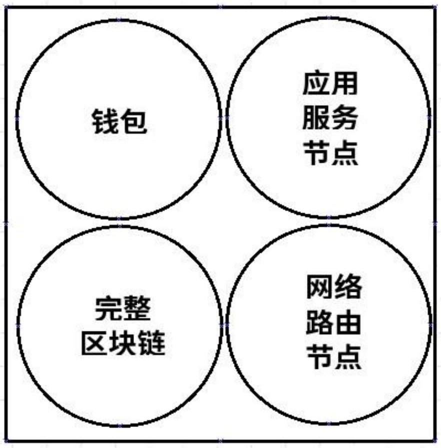
5. Service Nodes

UOC 在比特币区块链节点的基础上，增加了运行聚合约能力的服务节点，旨在节点为不同区块链脚本应用，提供插件方式的 CPU 算力支持。

UOC adds service nodes that run PSC based on Bitcoin nodes, with the intention of providing different applications with plugin CPU power support.

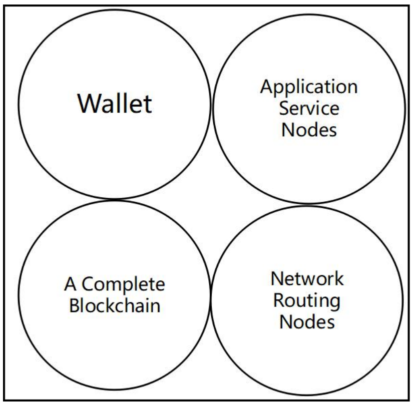
每个节点，可选择不同的应用提供 CPU 算力服务，服务节点选择运行聚合约，收集用户消息，执行验证后并打包，并递交最终的结果.

Every node is able to selectively support different applications with CPU power, and service nodes operate PSC, collect users’ messages, pack messages after verifying and deliver final results.



提供不同服务的节点组成了UOC的网络通讯网络

与比特币不同的是，原有的“矿工节点”因为采用了博弈共识机制，已经不存在了。新的位置被“应用服务节点”，它有选择的为不同的应用提供安全可靠的、去中心化的算力服务支持。



UOC network comprises of nodes offering different services.

Unlike Bitcoin, the original 'Mining Nodes' have gone because of proof-of-game. As a substitute, 'Application Service Nodes' selectively provide applications with reliable and decentralized CPU power service.

6 博弈证明 PoG

6. Proof-of-Game（PoG)

在选择记账人的共识机制上，UOC 没有采用比特币的一 CPU 一票的工作量证明机制，而是采用节点竞选机制，依照成绩排序来选择记账人，保证排名在前的链条将以最快的速度延长，并超越其它排名靠后的链条。

On determining representation in majority decision making, UOC does not adopt the one-CPU-one-vote proof-of-work as Bitcoin does. Rather, UOC adopts the Proof-of-Game. Bookkeepers are selected according to the gaming results. The chain with a higher rank will grow the fastest and outpace any competing chains behind it.

UOC，为此提出了一个全新的数学模型，将传统用于解决“不需要可信第三方即可以进行公平扑克游戏”数学问题的数学模型，推进到了高效且具备了普适性的地步，我们将其定义为“博弈证明”。

这是一个非常有趣的、同样也是基于数学模型的选举方法。

(1)所有的节点都有权利报名参与竞选。人人可参与的竞选，将杜绝钱权选择共识，带来的人为风险。

(2)无需要耗费计算机算力进行挖矿，因为博弈证明共识算法产生结果的速度非常快。于是可大幅度提高产出块的时间。

(3)节点报名需要缴纳报名费用，但竞选结束后，在扣除转账手续费后，将归还报名费。

(4)参与竞选的节点需要提前 24 小时报名，截至报名结束后 12 小时宣布结果。

UOC discovers a brand-new mathematic model, bringing the traditional mathematic model which is a solution to the mathematical problem of playing mental poker without a trusted third party with efficiency and universality. And we call it Proof-of-Game.

This is also a very interesting election system.

(1)All nodes have the right to sign up for an election. Everyone can join the election so as to prevent incentivization of money and power.

(2)No CPU power is required for mining. Because the consensual result is produced quickly, less time is required to generate a block.

(3)Nodes pay for election registration. This is a transaction. When the election ends, after the transaction fees are deducted, registration fees will be returned to nodes.

(4)Nodes can sign up for the election in 24 hours before the game starts. The result will be announced in 12 hours after election ends.

博弈证明的数学模型，即为解决“一副牌，ABC 三人想玩扑克游戏，因为相互不信任，也不相信第三方，在此前提下，在每一步都完全可信的环境中，完成洗牌和发牌。”的数学算法。

因为使用了博弈证明，所以 UOC 在保证人人参与竞争的情况下，还能做到 10 秒的高速出块机制。

The game-theory-based mathematic model is designed for solving the mental poker problem, i.e., there are three players in a poker game without trust in each other and a third party, and they can still play the game with fair shuffling and dealing in a trusted environment.

With the support of Proof-of-Game, UOC is able to involve everyone in the game and produce one block per 10 seconds, which is fast enough to maintain seamless gameplay.

7 结论

7. Conclusion

UOC，是在比特币区块链基础上的延伸实现。扩展了其对于数字资产的归属权描述，增加了“公共资源”的描述；使用了“博弈证明”，大幅度提高创建块的速度；采用“聚合约”为比特币脚本事务处理，提供了可无限想象的可编程插件模块；其中，“自证存储链”保证了聚合约的安全。

UOC 是完全去中心化的区块链平台，可实现无服务器的算力支持，为网络游戏的区块链化提供了可能和无限想象。

UOC continues the legacy of Bitcoin’s pioneers. UOC enriches the description of the digital assets ownership by adding the description of public resources; uses Proof-of-Game to greatly increase the speed of generating blocks; adopts PSC, a programmable plugin for Bitcoin scripting transactions; and protects PSC against risks by utilizing SCS chain.

UOC is a fully decentralized ecosystem that supports serverless CPU power, seeing unlimited possibilities in blockchain-based online games.

参考

References

[1] 中本聪《比特币：一种点对点的电子现金系统》

[1] Satoshi Nakamoto《Bitcoin: A Peer-to-Peer Electronic Cash System》
https://bitcoin.org/bitcoin.pdf

[2] QQagent（吴忌寒）《比特币白皮书：一种点对点的电子现金系统》中译版

[2] QQagent《Bitcoin: A Peer-to-Peer Electronic Cash System》Chinese Translation
http://www.8btc.com/wiki/bitcoin-a-peer-to-peer-electronic-cash-system

[3] 以太坊《下一代智能合约和去中心化应用平台》
[3] Ethereum《A Next-Generation Smart Contract and Decentralized Application Platform》
https://github.com/ethereum/wiki/wiki/White-Paper

[4] 尼克·萨博《智能合约》
[4] Nick Szabo《Smart Contracts》
http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html