**去中心化的泛娱乐化竞猜社交平台**



**猜猜猜区块链技术框架**

**Version 2.0**

|  |  |
| --- | --- |
| Author(s): | Bob Qin [Bobq@cai3.org](mailto:Bobq@cai3.org)  Libratus Wong [Libratusw@cai3.org](mailto:Libratusw@cai3.org)  Leon Liu [Leonl@cai3.org](mailto:Leonl@cai3.org)  Lynch Peng [LynchP@cai3.org](mailto:LynchP@cai3.org)  Beibei Zheng [Beibei@cai3.org](mailto:Beibei@cai3.org) |
| Version: | V2.0 |

AMENDMENT HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Editor** | **Changes** |
| V0.1 | Dec. 20, 2017 | B. Qin | Initial version  This document will be updated and re-versioned as requirements are ready |
| V0.8 | Dec. 26, 2017 | L. Liu | Core ideas to adapting the key players, in terms of process, main algorithm as well as technical frameworks |
| V1.0 | Dec. 31,2107 | B. Qin | V1.0 adapted from Yang’s draft |
| V1.6 | Jan. 29, 2018 | B. Qin, | Broad Entertainment idea |
| V1.8 | Feb. 18, 2018 | B. Qin | Public chain infrastructure, Enterprise blockchain framework |
| V2.0 | Mar. 01, 2018 | B. Qin | Cross Chain asset interexchange, Caicaicai chain space， |
|  |  |  |  |

**目录**

1 引言 4

1.1 背景 4

1.2 比特币的核心底层区块链技术 4

1.3 猜猜猜泛娱乐化竞猜社交平台 5

2 CCC系统 5

2.1 CCC是如何运作的 5

2.2 高效能比特币支付的核心概念 9

2.2.1 交易 9

2.2.2 CCC的可扩展性和高效能 14

2.2.3 CCC价值网络协议 – 分布的共识 16

2.2.4 CCC区块链空间 18

2.2.5 CCC均质和异质交叉链交换价值 19

3 CCC企业级区块链框架和用例 20

3.1 CCC企业级区块链框架 20

3.2 用例行为者概述 20

4 附录 22

4.1 参考 22

# 引言

## 背景

比特币是在2008年发表的题为“比特币：点对点电子现金系统”的论文中衍生出来的，比特币网络始于2009年1月3日创建的创世区块[1]，并从那时起推出了一个不可阻挡的价值网络。 今天，比特币是包含一系列概念的生态系统，该系列包括支付系统，加密货币，数字资产和底层区块链技术。 除了所有这些概念之外，还有一种信任机器机制，它能够跨越整个网络的节点之间建立对等或分布式的信任。

节点通过交换封装在加密数据的价值，通过持有，转移，交换资产来维护这个加密数据的生命周期，从而建立一个价值网络。节点都遵循比特币共识，这一个数据一致性协议，以保证数据完整性的原子性，一致性，隔离性和持久性。 目前，网络协议主要是基于TCP / IP的互联网，但实际上这并非必要 - 任何维护ACID数据达成共识的节点可以构建一个值得信赖的价值网络，私有，联盟或公共区块链。

比特币的本质[2]，也是协议，对等网络和分布式计算创新的代表。比特币货币实际上只是该发明的第一个应用。 比特币代表了数十年密码学和分布式系统研究的精华，包括以独特且强大的组合形式汇集的四项关键创新。

比特币包括：

* 分步式点对点网络（比特币协议）
* 公开的交易账本（区块链）
* 独立交易验证和货币发行的一套规则（共识规则）
* 有效的在全球区块链上达成分步共识的机制（工作量证明算法）

## 比特币的核心底层区块链技术

价值网络的基础技术是区块链技术，它是一套在其自己的领域内发展和进化了几十年的不同技术结合的框架，现在已经形成了一套构建信任的概念[3]：

* 密哈希函数
* 哈希指针数据结构
* 数字签名

加密技术使用散列函数和数字签名来加密区块中的信息或交易。而这些信息在分布式网络上承载数字货币或数字资产的价值。

## 猜猜猜泛娱乐化竞猜社交平台

猜猜猜泛娱乐化竞猜社交平台（CCC）旨在从技术角度改进比特币区块链基础设施的整体吞吐量和性能，主要用于支付和共同价值交换的用例构建一个全面的比特币生态系统。

猜猜猜泛娱乐化竞猜社交平台针对这一技术框架下正在建设中的特性。考虑以下限制：

1. 全球共识的点对点互联网的传输属性。
2. 集中的比特币/数字资产交易所和钱包可能会对转移，持有和交易比特币和其他数字货币产生意想不到的安全隐患。
3. 不同国家之间的加密货币政策差异。
4. 未成熟的区块链技术可能会导致不确定性。

猜猜猜泛娱乐化竞猜社交平台(CCC) 正在考虑以下比特币问题，并尝试提供最佳解决方案，以便在我们的日常生活中使用[5]：

1. 可扩展性
2. 通性
3. 隐私
4. 法规
5. 监管

# 猜猜猜区块链技术架构

比特币的亮点是，防止硬化资产，拒绝服务和双花，所有这些建立在一个信任系统，允许任何有意愿的双方直接将资产转移给对方，而不需要任何可信赖的第三方。比特币已经成功建立了信任和价值网络。然而，比特币现在（在写白皮书的那一天）每天处理近50万笔交易。 性能问题成为一个大问题。

## 猜猜猜区块链技术基本原理

政府中央银行使用实物货币来控制供应并增加防伪功能以防止欺诈并确保货币的安全性，与法定货币不同，比特币使用加密功能，哈希指针数据结构和数字签名来构建可信任价值网络[3]。

* 密码哈希函数 - 对于输入值验证，确保没有人可以使用给定的加密哈希值计算出您的密码
* 哈希指针数据结构 - 将哈希函数结果作为有组织数据的指针保存的特殊数据结构，确保数据的任何更改，哈希函数结果可以验证，验证机制保证数据一旦创建不会被修改，
* 数字签名 - 只有您可以签名并且任何人都可以验证，但没有人可以移动或更改。

A picture containing vector graphics

Description generated with high confidence

加密技术使用哈希函数和数字签名来加密区块中的信息或交易，该信息在分布式网络上承载数字货币或数字资产的价值。

**区块链如何工作 - 加密哈希函数**

**A close up of a logo

Description generated with high confidence**

**区块链工作原理-比特币SHA-256的哈希函数**

A screenshot of a cell phone

Description generated with high confidence

SHA-256哈希函数（简化）。 SHA-256使用Merkle-Damgard变换将固定长度的抗碰撞压缩函数转换为可接受任意长度输入的哈希函数。 输入是“填充的”，所以它的长度是512位的倍数。

**区块链工作原理 - 哈希指针和数据结构**

A screenshot of a cell phone

Description generated with very high confidence

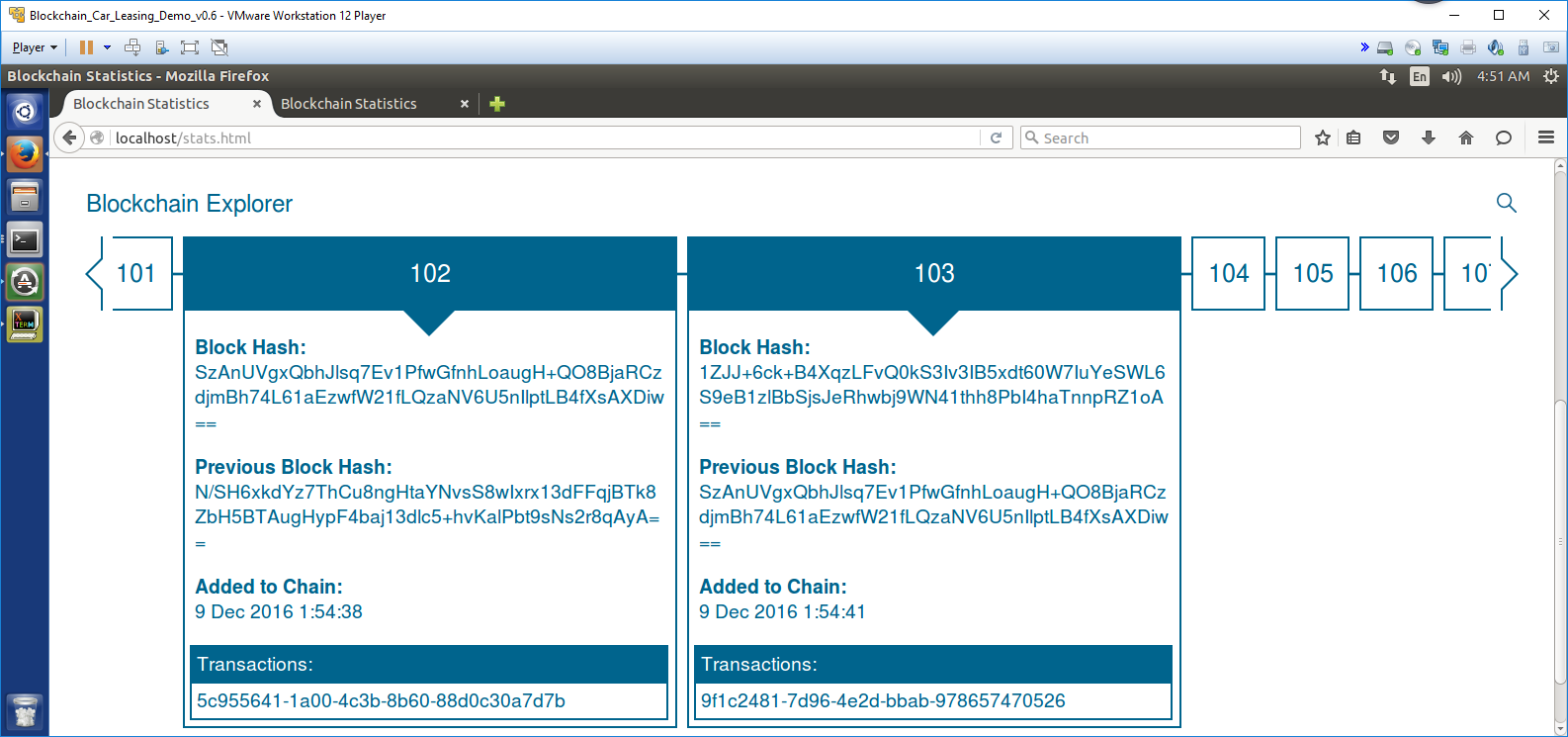
如果攻击者修改了数据块链中任何地方的数据，它将导致下一个数据块中的哈希指针不正确。 如果我们存储列表的头部，那么即使攻击者修改了所有指针以与修改后的数据一致，头指针也不正确，我们将检测到篡改。

A screenshot of a cell phone

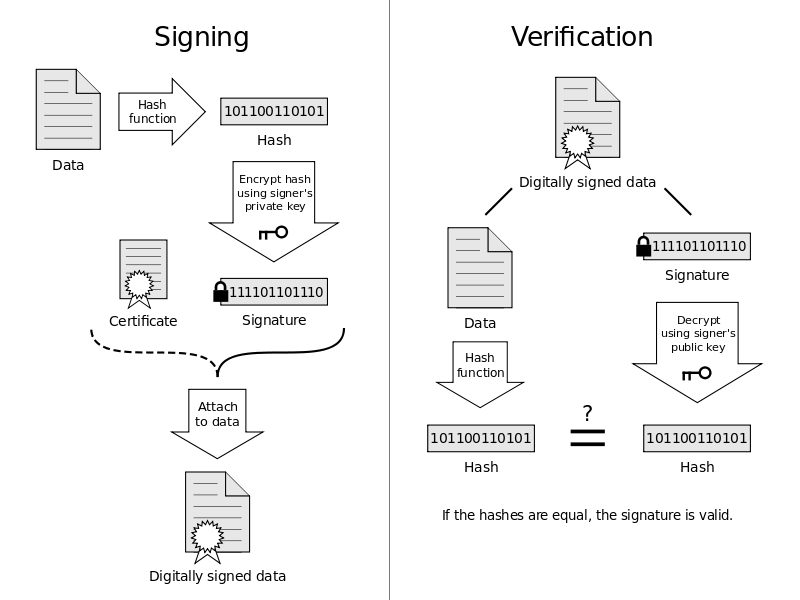
Description generated with high confidence

Merkle树中，数据块成对分组，每个块的哈希存储在父节点中。 父节点依次成对分组，并且它们的哈希在树上存储一级。 这一直延续到树根，直到到达根节点。

如区块链浏览器所示，一个真正的区块链数据块如下所示：



**区块链工作原理 - 数字签名**



**数字签名方案**[3]。 数字签名方案由以下三种算法组成：

* **(sk, pk) := generateKeys( *keysize* )**

generateKeys方法采用密钥大小并生成密钥对。 秘密密钥sk被私下保存并用于签署消息。 pk是你给每个人的公开验证密钥。 任何拥有此密钥的人都可以验证您的签名

* **sig := sign( *sk* , *message* )**

sign方法将消息和密钥sk作为输入，并在sk下输出消息的签名

* **isValid := verify( *pk* , *message* , *sig* )**

验证方法将消息，签名和公钥作为输入。 它返回一个布尔值isValid，如果sig是公钥pk下的有效签名，则返回true，否则返回false。

我们需要以下两个属性：

* *有效签名必须经过验证*

**verify** ( *pk* , *message* , **sign** ( *sk* , *message* )) == **true**

* 签名是不可伪造的

## 核心概念

我们在这里描述了猜猜猜泛娱乐化竞猜社交平台（CCC）的多个核心概念，关于CCC交易，持有交易数据的数据块，跨链交换机制以及解决比特币可扩展性问题的解决方案的真正功能意义。

### 交易

交易是比特币的基本组成部分; 原始比特币交易定义如下：Satoshi [1]：

1. 是一串数字签名
2. 所有者1签署从先前交易中获得的比特币，并使新交易拥有所有者1的签名
3. 所有者2通过在新交易中提供公钥来接受比特币
4. 矿工使用POW通过验证并提供签名来随机挖掘交易。

A screenshot of a cell phone

Description generated with very high confidence

实现的源代码中的实际事务更像以下模型：

1. 交易中有零个或多个输入，至少一个输出
2. 对于零输入是一个特殊情况，这意味着交易是一个新生成的交易，而比特币来自POW挖掘。
3. 输入或输出包含以前的所有者签名和当前所有者的公钥以进行验证
4. 事务具有事务哈希值作为地址 - 事务ID。
5. 每笔交易都是确定性的有限状态机

A screenshot of a cell phone

Description generated with high confidence

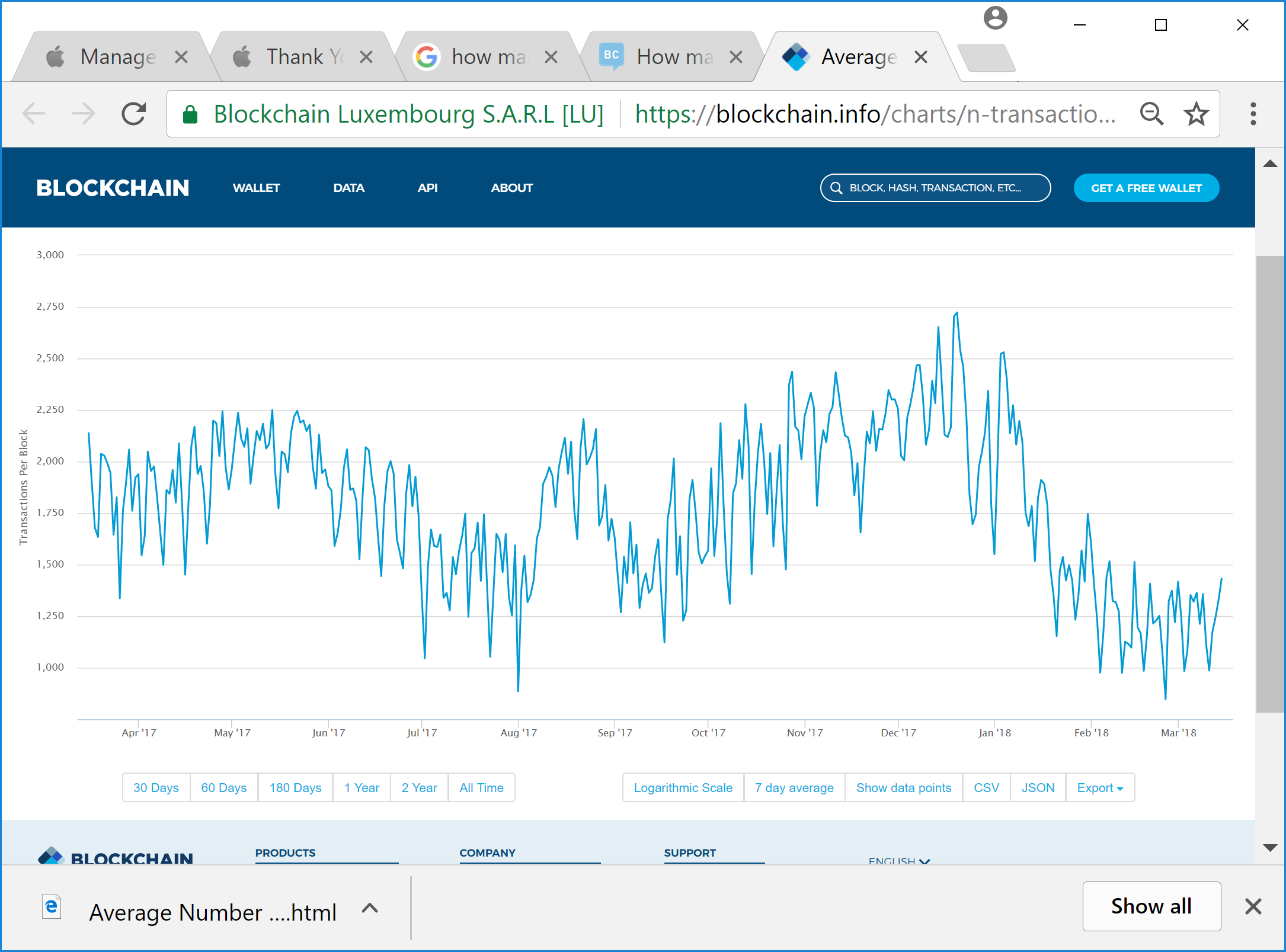
所有这些结合在一起，我们可能会得到以下关于比特币概念的账本，块，交易，交易输入和交易输出的模型：

1. 在merkle树中是信任数据的骨干，其中只有叶节点包含真实的交易数据以及认证（签名）数据。
2. 叶节点实际上是一个块，是账本的一个基础部分。账本系统起到记录所有比特币价值的作用。
3. 块是一组多个事务

A screenshot of a cell phone

Description generated with very high confidence

如上图所示，该块是分类账的一部分，一个块包含多个交易。 blockchain.info报告每块大约有2000个事务。[6]

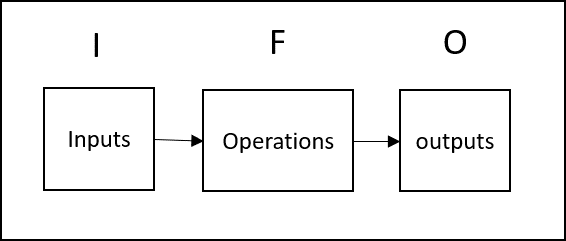


CCC交易视角可以更复杂地处理交易输入和交易输出。 输入具有以前的所有者签名以及交易功能的操作脚本，输出具有现有所有者的公钥和操作功能以及比特币单位的金额值。

A close up of a map

Description generated with high confidence

事务实际上是一个状态机函数：O = F（I），其中I是输入状态集合，O是一组所有输出状态，F是事务函数。



交易 （实际上与merkle树数据结构中的链接）排列在CCC区块链中。

1. 交易＃1 - 交易被挖掘，并且生成255个BBP硬币，分配给Alice的CCC地址
2. 交易＃2 - 来自Alice地址的一个输入，255个CCC作为输入，Alice是所有者。 Alice签署了将180个CCC传送给Bob的地址，并将75个CCC传送回Alice的地址
3. 交易＃3 - 从Tx＃2链接180个CCC作为输入，Bob签署并发送160个CCC给Carol并发送给他自己20个CCC
4. 交易＃4 - 从Tx＃2链接以及Alice'75 CCC作为输入，签名并转出两个输出：60个CCC到David的地址和15个CCC到Alice的地址
5. 交易＃5 - 从Tx＃3链接，Carol是拥有160个CCC作为输入的所有者。Carol然后签署并转让了100个CCC给David，60个CCC给Carol。

A screenshot of a cell phone

Description generated with very high confidence

### CCC的可扩展性和高效能

比特币网络建设有两个重要的阶段，在比特币历史刚刚开始的时候，最重要和迫切的问题就是建立信任度和建立价值网络。 一旦有更多的交易和更频繁的交易建立，比特币的性能就成为一个大问题。性能就是交易能够在区块链中处理的速度。

每块平均交易量为2000，控制开采比特币的时间间隔的参数设置为10分钟。 比特币性能有两个瓶颈，第一个是块的大小，第二个是生成块的时间。 就块的大小而言，实际上它取决于块中事务的组织方式以及可能引用其他数据结构的事务数据。

CCC的解决方案总结如下：

1. 将块大小增加到合理实用的数目
2. 更改事务/块的数据结构
3. 缩短交易处理时间
4. 缩短块生成时间

**块的大小**

比特币块大小最初由中本聪本人设定为1M。 在比特币早期应用，比特币的块大小并不是什么大问题，而大多数关注点都是尽可能地传播硬币和价值网络。 然而，随着近期比特币交易量的增加，由于增加块大小可能是提高每秒交易吞吐量的最简单方法，块大小成为热点问题。

**隔离见证**

A screenshot of a cell phone

Description generated with very high confidence

A screenshot of a cell phone

Description generated with very high confidence

### CCC价值网络协议 – 分布的共识

比特币一致性算法（简化），因为它能够以不易受女巫攻击的方式选择一个随机节点。 比特币共识协议被定义为以下5个部分：

1. 新交易广播给所有节点
2. 每个节点将新事务收集到一个块中
3. 在每一轮中，随机节点都可以广播它的块
4. 其他节点只有在其中的所有事务都有效时才接受该块（未花费的，有效签名）
5. 节点通过在其创建的下一个块中包含它的哈希表示它们接受该块

A picture containing device

Description generated with high confidence

一旦定义了核心价值网络协议，节点就可以自动建立社区并形成一个分散的社会。 只要两个节点可以互相认同，那么DApp就是一个不可取代的应用。

A close up of a logo

Description generated with high confidence

**CCC Automata - 通用智能合约引擎**

**CCC链上数据是确定性有限自动机M =（Q，Σ，δ，q0，F）**

1. 新交易广播给所有节点
2. 确定性有限自动机M是一个由5元组（Q，Σ，δ，q0，F）组成
3. 一组有限的状态（Q）
4. （Σ）代表的有限输入符号集合，
5. 转换函数（δ：Q×Σ→Q）
6. 初始状态或开始状态（q0∈Q）
7. 一组接受状态（F⊆Q）

A necklace on a black background

Description generated with high confidence

CCC State Machine transition function

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Inpu/State | S0 | S1 | S2 | S3 | S4 | S5 | S6 |
| Payment Request | S1 | S1 |  |  |  | S1 |  |
| Payment Rejected |  | S0 |  |  |  |  |  |
| Payment Accepted |  | S5 |  |  |  |  | I |
| Transfer Request |  |  | S2 |  |  | S2 |  |
| Transfer Rejected |  |  | S5 |  |  |  |  |
| Transfer Accepted |  |  | S5 |  |  |  |  |
| Credit Request |  |  |  | S3 |  | S3 |  |
| Credit Rejected |  |  |  | S5 |  |  |  |
| Credit Accepted |  |  |  | S5 |  |  |  |
| Withdraw Request |  |  |  |  | S4 | S4 |  |
| Withdraw Rejected |  |  |  |  | S5 |  |  |
| Withdraw Accepted |  |  |  |  | S5 |  | Final |

### CCC区块链空间

CCC是一种在区块链上进行可扩展计算的方法，其创建的经济激励机制可以自主地执行，并在创建者没有进行主动状态转换管理的情况下持续运行链条。节点本身可以通过激励来操作链。这种结构允许外部参与方能够持有资金和进行合约运算，CCC在现有区块链上运行，因此不需要为每个状态更新在底层链上创建交易（包括添加用户的账本条目），以及用于合并状态更新达到最小数据上链。

主链是全局所有计算的执行者，但只有在存在欺诈证据的情况下才进行计算和处罚。 许多CCC子区块链可以与自己的业务逻辑和智能合约条款共存。 在CCC中，子链将由运行的在主链的智能合约组成，仅处理最小化的提交，这些提交代表非拜占庭情况下非常大量的计算和账本的条目。

A close up of a logo

Description generated with very high confidence

CCC的子链设计由五个关键组成部分组成：

* 以经济高效的方式提供持续计算的激励层
* 以树形式安排子链的结构，最大限度地降低交易结算成本效率
* MapReduce的计算用于构建这些嵌套链中状态转换的欺诈证据的框架，以便与树结构兼容，同时将状态转换改造为高度可扩展的设计
* 一种依赖于重现比特币根区块链的共识激励结果的共识机制
* 以及一个位图 – UTXO交易结构，用于确保根区块链准确转换状态，同时最大限度地降低批量退出成本。

在数据不可用情况下或其他拜占庭行为下，允许退出是CCC运作中的关键设计点之一。

实际上，我们能够创建状态转换，这些状态转换只是定期提交给父链（然后流向根区块链）。这实现了难以置信的计算规模和账户状态数据，因为我们只能将原始数据提交给拜占庭条件下的父（或根）链。因为可以从父链获取来保障子链执行状态，从而实现部分拜占庭条件下恢复的成本最小化。

这个子区块链运行在根区块链（CCC）之上，并且从根区块链的角度来看，它只能看到定期提交事物，在合同中绑定的通证用于执行区块链的共识规则和业务逻辑。

这在最大化块可用性和最小化确认通证使用方面具有显着的优势。

### CCC同质和异质交叉链交换价值

中心链和侧链

这里我们描述一个分布和可扩展性的新模型。 CCC提供支持的众多区块链的网络。虽然现有的提案旨在创建一个全球交易订购的“单一区块链”，但CCC允许许多区块链在保持互操作性的同时同时运行。

在此基础上，CCC枢纽中心链管理许多称为侧链的独立区块链。侧链发布最近块的信息状态的到枢纽中心链上。同样，每个侧链都与中心链的状态保持一致。然后通过发布Merkle证明作为信息发送和接收的证据，然后将信息包从一个侧链传送到另一个侧链。这种机制被称为区块链间通信，简称IBC。任何侧链本身都可以是中心链以形成非循环图形。



中心链

CCC中心链是一个区块链，托管一个多资产分布式账本，其中的通证可以由个人用户或侧链持有。这些通证可以在一个特殊IBC数据包中从一个侧链移动到另一个侧链。中心链负责保持区域中每个令牌总量的全局不变性。IBC数据包交易必须由发起人，中心链和接收方区块链承担。

由于CCC中心链充当整个系统的中央账簿，因此中心链的安全性至关重要。虽然每个侧链都可以是不同区块链，中心链必须由全球分布的一组验证程序进行保护，这些验证程序可以承受最严重的攻击情况。

侧链

CCC侧链是一个独立的区块链，与中心链交换IBC消息。从中心链的角度来看，侧链是一个多资产动态成员的多重签名账户，可以使用IBC数据包发送和接收通证。就像一个加密货币账户一样，一个侧链不能传送比它的余额更多的通证，但可以从其他人那里接收通证。侧链可以被指定为一种或多种通证类型的“来源”，赋予其发行该通证供给权力。

BBP中心链的通证可能被连接到中心链的侧链的验证者抵押。虽然对这些侧链的双花攻击会触发CCC的分叉问责导致通证的削减，但投票能力>⅔的拜占庭侧链可以设置提交使其无效。CCC主链不验证或执行在其他侧链上进行的交易，因此用户有责任将通证发送到他们信任的侧链。未来，CCC中心链的治理体系可能会通过中心改善提案来解决侧链故障现象。例如，来自某些（或所有）侧链的通证传输可能会受到限制，以便在检测到攻击时允许紧急断开侧链（通证传输暂时停止）。

区块链间通信（IBC）

现在我们来看看中心链和侧链如何相互通信。例如，如果有三个区块链，“Side1”，“Side2”和“Main”，并且我们希望“Side1”生成通过“Main”发往“Side2”的数据包。要将数据包从一个区块链移动到另一个区块链，将在接收链上发布证明。该证明指出发送链发布了针对所指定目的地的数据包。对于接收链来检查此证明，它必须能够同步上发起链的块头。这需要两个交互链通过存在证明数据包（事务）的双向流来相互通信。

IBC协议可以使用两种类型的事务来定义：IBCBlockCommitTx事务，它允许区块链向任何观察者证明其最近的块哈希，以及一个IBCPacketTx事务，它允许区块链向任何观察者通过对最近的块哈希进行Merkle验证，证明数据包确实是由发起人发布的。

通过将IBC机制分成两个独立的事务，我们允许基于收费市场机制的接收链独立确定哪些数据包被提交（即确认），同时允许在发送链上完全自由地发布出站数据包。

A screenshot of a cell phone

Description generated with very high confidence

## 猜猜猜去中心化泛娱乐竞猜社交平台三层代币体系

# CCC企业级区块链框架和用例

中心链和

## CCC企业级区块链框架

A screenshot of a cell phone

Description generated with high confidence

## 用例行为者概述

**多功能的行为者**

参与多个功能区域使用案例的行为者

**行为者描述：**

* 访客 - 想要浏览网站的未注册用户
* 用户-想要执行受限功能的用户注册用户
* 买方 - 继承用户属性并且具备进行购买活动属性的行为者
* 卖家 - 继承用户属性并且具备继承出售活动属性的行为者
* 代理 - 继承用户属性并且具备代理活动属性的行为者
* 买方代理人 - 继承代理属性代表买方的行为者
* 卖家代理 - 继承代理属性代表卖家的行为者
* 管理员 - 可以访问管理控制面板做管理工作

分布式交易所

就像比特币通过分布式，大量复制的账本变得更安全一样，我们可以使交易所通过在区块链上运行，变得更不容易受到外部和内部黑客的攻击。这样的交易所我们称之为分布式交换所。

加密货币社区当今称之为分布交易的基础是所谓的“原子跨链”（AXC）交易。通过AXC交易，两个不同链上的两个用户可以在两个账本上一起提交两个转账交易，或者所以交易根本不发生（即原子性）。例如，即使比特币和以太坊没有互相连接，两个用户也可以使用AXC交易将比特币交易以太坊（或两个不同账本中的任意两个代币）。在AXC交易上运行交易的好处是用户不需要相互信任或交易匹配服务。缺点是双方都需要在线才能交易发生。

另一种分布交易是一种大规模复制的分布式交易所，它运行在自己的区块链上。这种交易所的用户可以提交限价订单并关闭电脑，交易可以在用户不在线的情况下执行。区块链代表交易者撮合并完成交易。

集中交易所可以创建限价订单的深度订单，从而吸引更多交易者。流动性在交易所世界中会带动更多的流动性，因此在交易所业务中具有强大的网络效应（或至少是赢家获胜的效应）。今天，加密货币交易所的当前领先者是Poloniex，其销售额为2400万美元，其次是Bitfinex，24小时销售额为500万美元。鉴于如此强大的网络效应，基于AXC的分布交易所不可能在成交量上赢得集中交易所。对于分布式交易所与集中交易所竞争，它需要支持限价订单的深度订单。只有区块链上的分布式交易所可以提供这种交易。

CCC提供了更快的事务提交的优点。通过在不牺牲一致性的前提下确定快速终端的优先级，CCC的区域可以快速完成交易 - 用于交换订单交易以及来往于其他区域的IBC通证传输。

鉴于当今加密货币交换的状态，CCC的一个很好的应用是分布式交易所（又名CCCDEX）。交易吞吐能力以及交付延迟可以与集中式交易所的交易吞吐量相媲美。交易者可以提交可以执行的限价订单，而无需双方在线。通过CCC枢纽和IBC，交易员可以快速地将资金充值或提现进出交易所 。

# 附录

## 参考

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/ bitcoin.pdf, 2009.

[2] Mastering Bitcoin Programming the Open Blockchain, Andreas M. Antonopoulos

[3] Bitcoin and Cryptocurrency Technologies, Arvind Narayanan, Joseph Bonneau, Edward Felten,   Andrew Miller, Steven Goldfeder

[4] <https://en.wikipedia.org/wiki/Bitcoin_scalability_problem>

[5] <https://www.forbes.com/sites/outofasia/2017/12/22/five-issues-preventing-blockchain-from-going-mainstream-the-insanely-popular-crypto-game-etheremon-is-one-of-them/#507adf7a6fad> retrieved at Jan. 3rd, 2018

[6] The average number of transactions per block - <https://blockchain.info/charts/n-transactions-per-block>

[7] Ethereum white paper. https://github.com/ethereum/wiki/wiki/White-Paper.