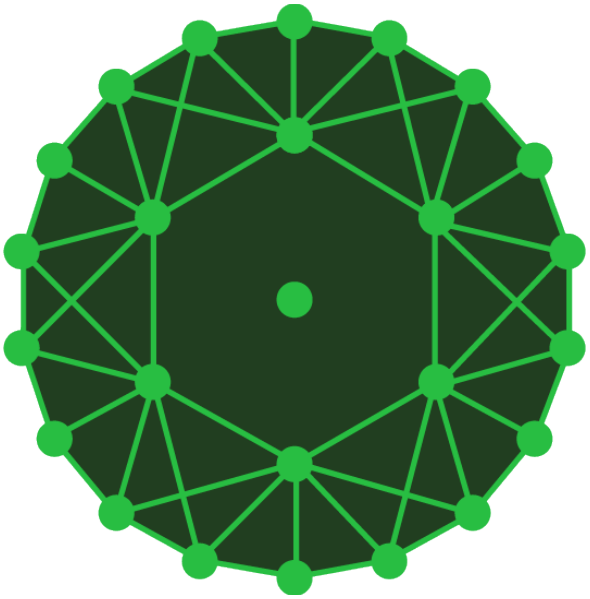


OWNERSHIP

Ownership Foundation

info@ownership.world

Ownership 白皮书中文版 V. 1.0

By Korda, Alexander and Snow

摘要.....3
免责声明.....3
鸣谢.....4
介绍.....5
1.1 区块链技术简介.....5
1.2 所有权.....6
Ownership系统.....8
2.1 系统概览.....8
2.2 账户体系.....9
共识算法.....10
3.1 为什么需要一个新的Blockchain?.....10
3.2 共识算法比较.....11
3.3 Lottery（彩票）共识算法.....12
经济模型.....15
4.1 系统经济模型.....15
4.2 OWN代币.....16
4.3 企业经济模型.....17
Ownership引擎.....19
5.1 概述.....19
5.2 零知识证明.....19
5.3 同态加密.....21
5.4 安全多方计算.....21
Ownership应用场景.....23
6.1 医疗数据.....23
6.2 金融数据.....24
6.3 其他.....25
我们的愿景.....25
参考文献.....26

摘要

*Ownership*是去中心化的安全数据计算和交换平台，旨在通过区块链技术在互联网OSI七层协议基础上构建全新的数据所有权协议，并借助零知识证明、同态加密和安全多方计算等密码学技术为各参与方提供安全高效的数据交换底层解决方案，从而打破零和博弈竞争带来的数据壁垒，构建数据共享和协作计算的新范式。

免责声明

本*Ownership*白皮书草案仅供参考。*Ownership Foundation*并不保证本白皮书得出的结论的准确性，白皮书按“现状”提供，不作任何明示或暗示的陈述和保证，包括但不限于：(i) 关于适销性、适用于特定目的、所有权或不侵权的保证；(ii) 本白皮书的内容没有错误或适合于任何目的；(iii) 此类内容不会侵犯第三方权利。所有保证均明确适用于前述免责声明。*Ownership Foundation*明确表示不承担因使用、参考或依赖本白皮书所含任何信息而导致的一切责任和损害赔偿，即使被告知有可能发生此类损害赔偿。对于使用、参考或依赖本白皮书或其本文包含的任何内容，*Ownership Foundation*均不会对任何个人或实体关于任何直接、间接、特殊或由此导致的损害赔偿负责。

Ownership Foundation

2017年5月1日

鸣谢

在此我们希望表达我们诚挚的谢意，没有帮助和支持，我们是不可能完成这个*Ownership*白皮书的撰写。首先，我们希望感谢比特币的发明人——中本聪先生，虽然没有人知道您的身份，但是您的卓越的工作将去中心化思想从理论变为了现实，*Ownership*项目也深受您的研究和实践的启发。其次，我们非常感谢图灵奖得主，*Whitfield Diffie*，您为人类密码学的发展作出了卓越的贡献，您提出的方向为我们指引了一条真正的去中心化实现之路。最后，没有朋友们的帮助，*Ownership*项目也不可能变为现实。感谢我们的朋友们——密码学和多方安全计算专家*Steven H.*博士以及互联网协议专家*Bryan Q.*先生给予的我们的建议和支持。

Korda、*Alexander*和*Snow*

2017年5月1日

献给热爱去中心化和数据分享的人们

第一章

介绍

1.1 区块链技术简介

2008年匿名人中本聪[1]发表了一篇名为“*Bitcoin: A Peer-to-Peer Electronic Cash System*”的论文[1]，之后比特币成为世界第一个去中心化的电子货币。比特币的去中心化是基于对于区块链，一个分布式账本的应用。

自从1969年10月份互联网诞生以来，人们从未停止对于电子货币的创造研究，美国国防部于1985年就展开对于发行电子货币的可能性的探究，但是直到2008年中本聪创造比特币，去中心化的电子货币一直是一个未完成的课题，究其原因是因为数据本身的特点。数据或者信息在互联网内是自由传播的，但是基于这一特性也产生出许多问题，例如，如果一张图片被分享给另外一个人，那收到图片的人可以立刻对这张图片进行复制然后分享给其他人，图片的发送者也可以再复制图片一次然后分享出去，这样就造成了数据所有权极难管理和维护。货币有两点基本属性，不可被复制以及不可被二次花出，任何电子货币也都需要满足这两点，所以传统的电子货币是通过一个中间机构来进行清算以此保证其不能被复制以及不能被花出两次。区块链技术的诞生让互联网里任意两个个体直接进行价值传递而不需要第三方（中间）机构介入。

拜占庭将军问题，是由莱斯利提出的点对点通信中的基本问题。 在分布式计算上，不同的计算机透过讯息交换，尝试达成共识；但有时候，系统上协调计算机或成员计算机可能因系统错误并交换错误的讯息，导致影响最终的系统一致性[2]。区块链技术是除了量子通信之外解决此问题的有效方案。现在区块链已经不再仅仅局限于“公共账本”，而是“公共电脑”。任何人不仅可以在上面存储非常可靠无法被恶意篡改的重要数据，还可以在上面运行程序，所有被运行程序的逻辑是所有用户达成共识后一致认可的，不会因为个人的意志而被改变。

[1] 中本聪：*Satoshi Nakamoto*，真实身份未知，比特币的发明人

1.2 所有权

所有权(*ownership*)[2]是什么？

1.2.1 所有权简介

从法律的角度讲，所有权是所有人依法对自己财产所享有的占有、使用、收益和处分的权利。中国的《商子》[3]中曾有一段关于所有权的经典描述，即“定分止争”的理论。秦孝公变法时，询问商鞅：如何治理国家？商鞅答曰：

> “一兔走，百人逐之，非以兔为可分以为百，由名之未定也。夫卖兔者满市，而盗不敢取，由名分已定也。故名分未定，尧、舜、禹、汤且皆如鹜焉而逐之；名分已定，贪盗不取。”

为什么山上的兔子被许多人追赶，而笼子里的兔子却无人抢夺，其原因就是定分止争的道理。此处的“分”，就是指所有权。所有权已定，则其他人就不能来抢夺，社会秩序由此建立起来。如果所有权未定，则大家都可以凭借其力来获取某物。如此之下，社会秩序就会混乱不堪。商鞅其实借助所有权的道理，阐明了治理天下的道理[3]。这个历史事件说明，早在春秋战国时期，人们就已经非常清楚地认识到所有权的基本价值和功能。

所有权是社会里的人们从事各种活动的基础，所有权的确定并不仅仅意味着财产归属的确定，而且意味着社会治理秩序的基本稳定。诺贝尔经济学奖得主罗纳德提出的科斯定理[4]指出，明确产权是通过市场交易实现资源最优配置的一个必要条件（即“产权明晰”）。综上，我们对于传统意义上的所有权有了一个了解。自1993年万维网诞生，互联网改变了人们生活的方方面面，那么互联网时代的所有权又应该如何定义呢？

---

[2] 小写的”*ownership*”用来表达所有权，大写的”*Ownership*”用来代表*Ownership*项目本身和平台

[3] 《商子》又作《商君书》、《商君》，春秋战国时期法家代表著作

[4] 科斯定理：*Coase Theorem*

1.2.2 数据所有权

2017年7月，美国最大的社交网络*Facebook*创始人扎克伯格宣布，*Facebook*的月活跃用户已突破20亿。这接近于世界人口的四分之一，比互联网使用人数的一半还要多[4]。随着社交网络、电子商务和移动互联网的发展，人类社会的数据量迅速激增，据统计，目前人类一年产生的数据量之庞大需要使用一个新的单位进行计算——“PB”[5]。在这样一个大数据时代，数据正和上文提到的“兔子”以及土地、劳动力、资本等成为一种非常重要的财产。数据所有权是什么？就是拥有对相关数据的支配、处置和获益等财产的权利。对于数据本身的增、删、改和查是数据所有权的一种表现。数据所有权的原则是谁的数据归谁所有，没有任何主题指向的数据是公共资源。

但是，数据因为其本质是在计算机网络里由0和1组成的数字，所以就和“兔子”产生一些明显的区别，也让数据所有权变的非常难以被明晰。首先，数据因为其数字的本质，就使得数据是非常容易被复制的，而且复制后得到的数据和原来的数据是一模一样没有任何区别的，而《商子》里的“兔子”是没有办法复制的。其次，当任何人得到了复制后的数据，数据的原主人就失去了对数据的支配，得到复制数据的人拥有了最初数据所有者一样的权利。因为上述的两个问题，当下让两个数据所有者之间进行数据的交换或者交易是非常困难的，一般要借助一个可信的第三方的帮助。但是现在的中心化的交易第三方又因为其逐利的本质而失去了其本应具有的中立和公正，产生出如数据沉淀、不注重数据所有者的隐私甚至造假等问题。

根据斯蒂文·列维在其所著的《密文》[6]一书中描述，密码学大师、图灵奖得主威特菲尔德·迪菲[7]早在20世纪60年代就提出了“去中心化的见证人”的概念，期望借此来构造合适的密码学工具以解决数据交换过程中的数据保护问题[5]。人类历史上第一个去中心化的电子货币——比特币为我们呈现了“去中心化”的魅力：

---

[5] PB：一个PB相当于2的50次方个字节。

[6] 《密文》：*"Crypto"*，由*Steven Levy*于2002年所著。

[7] 威特菲尔德·迪菲：*Whitfield Diffie*，世界著名密码技术与安全技术专家，“公钥加密”发明人。

> “比特币是根本不同的，原因在于比特币不是建立在什么人欠什么人东西的基础之上，比特币的系统是建立在所有权之上的，没有人可以审查、夺取或者冻结它”

安德里亚斯·安东诺普洛斯[8]在一次关于比特币的演讲中提到[6]。比特币系统是构建在区块链技术之上的，而作为比特币系统基石的区块链技术为我们在数据所有权保护的道路上指明了新的方向。

第二章

*Ownership*系统

2.1 系统概览

早在2002年11月5日，一本被大家认为是“深刻的预言”的小说《编码宝典》[9]由著名小说家尼尔·斯蒂芬森创作并发行。这本小说预测本世纪伊始将出现加密货币，并且加密货币将对我们的社会产生变革的影响。比特币的诞生似乎印证了作者的预测，在书中作者还大胆设想了一个位于东南亚的“数据避难所”——一个加密后的数据可以自由存储和交换的地方[7]。

*Ownership*的系统设计集合了“去中心化的见证人”和“数据避难所”两种思想。区块链技术的诞生，让威特菲尔德的“去中心化的见证人”理念得以变为现实，这体现在*Ownership*的系统中即是基于*Lottery*共识算法的*Ownership*区块链。“数据避难所”的实现是由*Ownership*引擎来完成。

---

[8] 安德里亚斯•安东诺普洛斯：*Andreas M. Antonopoulos*，安全专家、作家和比特币极客

[9] 《编码宝典》：“*Cryptonomicon*”，由*Neal Stephenson*在2002年11月5日创作发行

2.2 账户体系

*Ownership*的账户体系是整个系统的核心部分之一，是所有权系统内数据的掌控者，是逻辑上数据的承载者。不同于一般信息系统中的单密码单账户的体系结构，也不同于以太坊的纯双账户体系（内部账户和外部账户），*Ownership*的账户体系采用双账户多密码校验模式的账户体系，以支持系统边界内数据的授权访问控制。

2.2.1 账户体系的功能定位

概括来讲，*Ownership*账户体系的功能定位如下面的列表所示。账户体系的具体设计都将紧密围绕着其功能定位展开。

1) 所有权的主体

2) 数据的唯一控制者

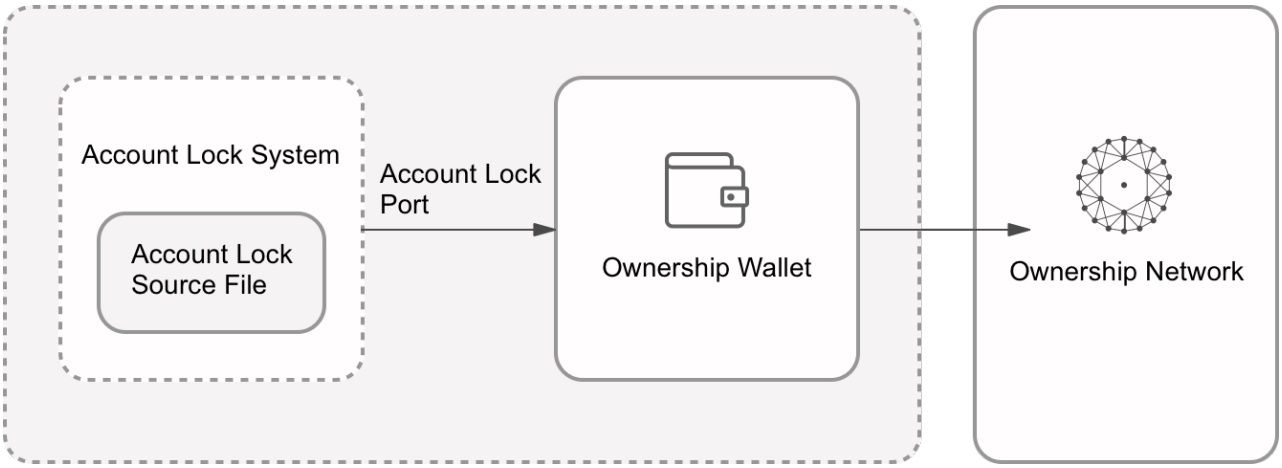
3) 智能合约授权控制者

4) 多方签名授权参与方

2.2.2 账户体系的组成部分

*Ownership*的账户体系采用双账户多密码校验模式的账户体系，主要包括账户锁系统、账户锁文件、账户锁接口、钱包客户端四大组成部分。首先，账户锁系统在*Ownership*安全认证协议的基础上，对需要授权的交易或数据进行加签或授权。账户锁文件是账户锁系统的驱动数据源，是由账户体系版本，账户验证类型，账户公钥，账户私钥，账户扩展数据，操作次序号等6个变量组组成的数据集合体，是账户体系的唯一标识，一般情况下，我们将不严格区分用户、用户锁文件、用户公私钥对、用户账户等概念。钱包客户端是*Ownership*公链体系的节点，在账户体系中承担发起数据加签、创建和验证交易等

功能，账户锁接口是账户锁账户与钱包客户端的通讯接口，是一套加签、加密操作的规范形式。



第三章

共识算法

3.1 为什么需要一个新的*Blockchain*?

继比特币成功之后，区块链的价值逐渐被社会大众发觉。人们在比特币的基础上进行了大量的创新，例如，彩色币、莱特币、以太币等等。随着对于区块链技术的不断深入挖掘，似乎区块链并不如想象中的那么完美。区块链技术在解决了多方信任问题的同时也产生了诸如趋向中心化、网络共识性能不高、区块链末尾分叉、大量消耗能源等一系列相关问题亟待解决。

例如比特币目前系统吞吐量大概为每10分钟一个区块，一笔交易的确认需要1个小时。其PoW共识机制是以大量的能源消耗进行无意义的计算为代价的。随着大型矿池的出现，原本以去中心化为目标的比特币等虚拟货币朝着中心化的方向发展。虽然在区块链探索的道路上，人们发明了侧链、闪电网络等技术去克服区块链技术的先天不足。但是算力中心化、性能问题等根本缺陷并没有得到改善。最活跃的以太坊社区也仅仅做到了15秒的出块时间，吞吐量也依然是每秒个位数。除此之外，在比特币系统中，区块链并不一定是全局

唯一的。实际上，比特币区块链的最后部分经常出现分叉。举个例子，对于用户甲来说，区块链的上的区块组合可能是$\beta_1, \beta_2 \ldots \beta_k, \beta_{k+1}$，对于乙用户来说，区块组合却可能是$\beta_1, \beta_2 \ldots \beta_k, \beta_{k+1}^w, \beta_{k+2}^w$。当并且仅当区块$k+1, k+2$已经加到链上之后，才能合理的认为前面的$k$个区块在所有用户中是一致的。由于上面的情况，有的时候比特币区块链上最后的区块交易是不能立即被信任为已经完成的，更谨慎合理的做法是等待和观察区块是否已经在链上有了足够的深度。

随着区块链技术产品化的不断探索，我们需要一个更加清洁、更加去中心化、更加可迅速达成共识、并解决了最终确定性问题的全新的区块链。

3.2 共识算法比较

名称	原理	场景	优点	缺点
PoW	解密码谜题获得区块记账权	*Bitcoin* *Litecoin* *Primecoin*	简单安全	耗费能源; 共识效率低不易扩展; 矿池中心化
PoS	消耗币龄等获得区块记账权	*Peercoin* *Blackcoin* *Nxt*	节省能源；共识效率高	nothing-at-stake等安全威胁，需要依赖保证金机制等
DPoS	将记账人角色专业化，先通过权益来选出记账人，然后记账人之间再轮流记账	*BitShares*	大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证	用户投票参与度低，受托人权力过高，可能被攻击或者内部腐败
PBFT	多数节点达成一致	*HyperLedger*	共识效率高，产生最终确认性	节点的通信成本过高。不适用于公有链。易被恶意攻击

3.3 *Lottery*（彩票）共识算法

3.3.1 概要

*Lottery*共包含三种角色：领导人、见证人、记录人。领导人节点负责建立新区块。见证人节点负责对领导人节点和新区块达成共识。记录人节点在验证了领导人节点签名合法且见证人节点对该区块达成拜占庭共识后，将该区块纳入到自己的链中[8]。该共识由三个部分组成：

（1）按照θ值的结果分布，随机选择候选领导人节点集合。

（2）见证人节点通过PBFT对领导人节点及其提议的区块达成共识。

（3）记录人节点校验当前领导人节点合法且见证人节点集合对该区块达成了共识，并将其纳入到自己的链中。

3.3.2 加密随机抽签

3.3.2.1 候选领导人节点集合选举

参数说明：

$r \geq 0$: 当前区块数

$s \geq 1$: 当前第r个区块的共识步骤

S: 使用节点i的私钥签名

$Hash()$: 哈希计算，计算结果随机分布

p: 期望的哈希计算结果范围

θ^r: 根据θ^{r-1}，r等与交易无关的信息签名并计算哈希值，选择候选领导人。

θ^0: 在创世块中指定

对于每个区块r、当前共识步骤s和前一个区块的θ值。第r个区块中的节点i使用自己的私钥对其签名并作哈希计算，如果小于参数p则节点i属于备选领导人节点集合。

θ^0在创世块中指定，θ值的计算与交易信息无关，仅根据当前共识的阶段和节点自身信息计算保证随机性。

$$Hash(S_i(r, s, \theta^{r-1})) \leq p \tag{1}$$

3.3.2.2 领导人选举

候选领导人集合中的节点会广播自己当前的θ值和提议的区块r。每一个候选领导人，会校验其它候选领导人广播的θ值并且选出θ最小的节点作为待共识的领导人并广播。当见证人节点集合中2/3以上的节点达成共识后，当前区块r具有最小θ值的节点i成为领导人，其提议的区块r经校验后达成共识并向全网广播。记录人节点验证领导人节点签名合法且见证人集合已经对该区块达成共识后，将该区块纳入到自己的链中。

$$\theta^r := Hash(S_i(\theta^{r-1}), r) \tag{2}$$

3.3.2 拜占庭共识

*Lottery*共识中的拜占庭算法选用拜占庭共识，*Miguel Castro*和*Barbara Liskov*在1999年提出的PBFT（*Practical Byzantine Fault Tolerance*）[9]将算法复杂度由指数级降低到多项式级。

参数说明：

pre': 预准备消息标识符

pre: 准备消息标识符

v: 广播消息的节点的地址

n: 待共识的区块的序号

d: 待共识的区块的摘要

m: 当前待共识的区块和θ值

i: 转发消息的节点的地址

PBFT分为三个阶段：

1) 预准备阶段：向备选领导人集合中广播预准备消息 $<<pre', v, n, d>, m>$；

2) 准备阶段：向备选领导人集合中广播准备消息 $<pre, v, n, d, i>$；

3) 确认阶段：当收到了$f+1$个见证人的预准备消息并且验证了$2f+1$个准备消息后，表示见证人集合对领导人及其提议的区块r达成了共识。

当见证人集合无法达成共识时，可生成一个空区块r，每个节点重新计算θ值。重新进行领导人和见证人选举，避免因领导人节点不在线导致无法达成共识。

$$\theta^r := Hash(\theta^{r-1}, r) \tag{3}$$

第四章

经济模型

4.1 系统经济模型

在*Ownership*系统里只有一种类型的经济角色即用户。所有的用户都是基于智能合约与*Ownership*区块链进行交互，不管他／她是使用*Ownership*引擎进行相关数据计算或者仅仅是进行*OWN*代币（*Ownership*系统里的代币）的转移。按照共识算法章节里的描述，*Ownership*区块链系统会选出一个领袖去创建区块同时会选出一些见证者去确认这件事情，所以所有的*Ownership*区块链用户都可以认为是比特币区块链里所谓的矿工。

在比特币的区块链经济模型里，用户激励是一个非常重要的部分，我们可以按照如下的数学模型来描述:

I^r: 任意一个区块r的总奖励（针对领导人、见证人和记录人）

$\bar{f}^r$: 区块r平均每个智能合约执行所需的费用

N^r: 区块r里所包含的智能合约数

I_s^r: 系统针对区块r的奖励

综上，我们可以得到:

$$I^r = \bar{f}^r \times N^r + I_s^r \tag{4}$$

通过观察等式(4)我们可以知道，如果*Ownership*系统保持稳定，则下面四点需要满足:

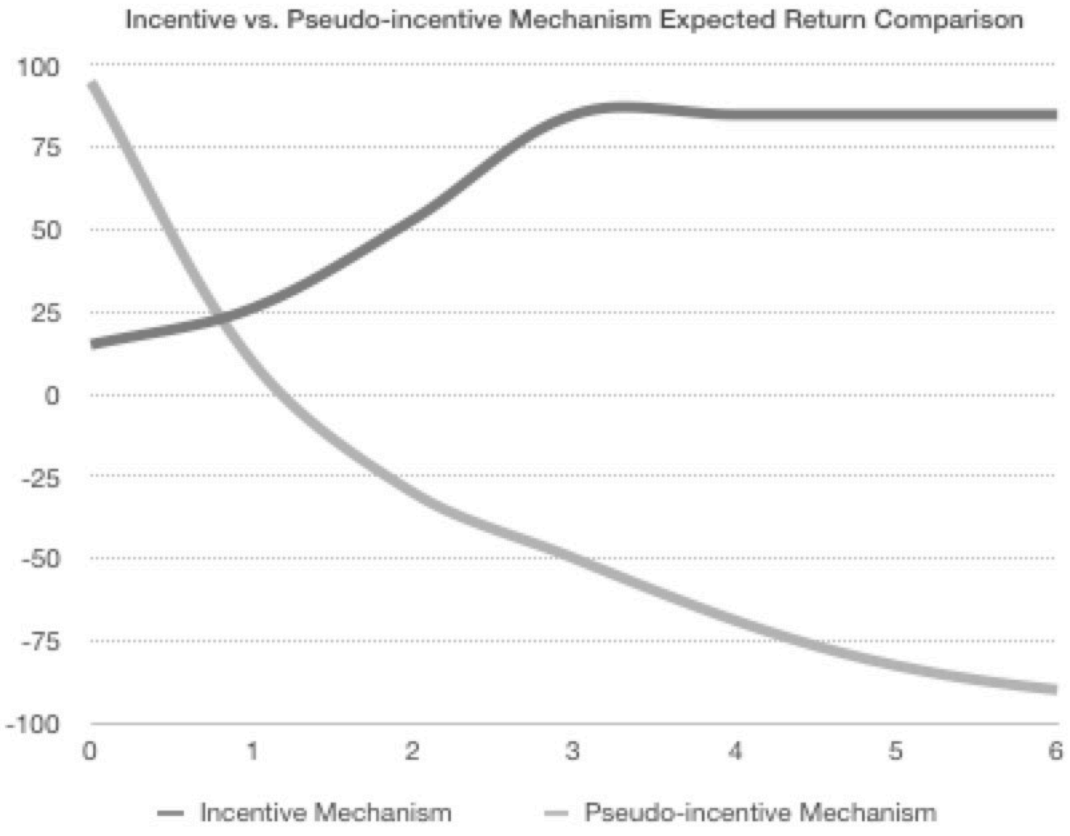
1) 总奖励I^r在特定时期需要保持在一个水平，从而鼓励用户去创建和见证新的区块;

2) 总奖励I^r不能超过某一水平，以防止用户去人为制造大量交易来变相挖矿;

3) 系统的费用$\bar{f}^r$需要保持在一个足够低的水平，从而不会影响一般用户去使用;

4) 总奖励I^r在初期需要足够高并且伴随着$\bar{f}^r$和N^r的增加而逐渐降低。

通过结合其他公有区块链的激励机制经济模型、P2P文件下载的免费模型和传统的彩票收益模型，我们提出伪激励机制。伪激励机制有别于免费或者主动给用户大量的回报来刺激用户接受的模式。针对每个用户个体，伪激励机制让所有参与者都有如同买彩票一样的获取相对高额回报的机会，但是即使通过大量购买彩票的方式来提高中奖概率，最后得到的总收益反而是下降的，伪激励机制可以帮助新的区块链系统从冷启动变为热启动，同时又可以在系统发展起来之后抑制大规模的挖矿行为。



4.2 *OWN*代币

为了防止恶意用户对*Ownership*的滥用以及维护系统的安全性和稳定性，所有希望使用*Ownership*系统的用户（转移*OWN*代币或者使用*Ownership*来进行数据运算）都需要支付一定的手续费。从*Ownership*的彩票共识算法我们可以知道，如果某些矿工希望采用类

似比特币的挖矿策略来赚取*OWN*代币，那么他／她们的预期收益伴随着投入的增加将趋近于负无穷，也就是说比特币的挖矿策略在*Ownership*系统里是无效的。对于手续费我们采用一个新的单位——燃料来表述。所有的使用*Ownership*系统的行为，都需要支付一定的燃料来完成。针对不同的使用行为，将动态对应不同的所需燃料。燃料通过*OWN*代币转化而来，燃料的价格通过*OWN*代币来体现。燃料的价格将随着系统里的用户数量和系统里可供使用的资源而变化。

4.3 企业经济模型

*Ownership*平台希望可以改变现存的企业和企业之间对于数据所有权以及数据外部合作交换的问题。在这个模型里，很多情形下两个企业或者多个企业之间由于高费用、高风险和政治因素等导致不能通过合作受益。我们抛却政治因素和由于技术缺陷导致的高风险不谈，针对高费用来进行分析。

首先以下是我们的一些基本的假设:

1) 所有企业的目的都是为了利益最大化;

2) 政治因素在某些情况下不会成为主导的否定合作的因素;

3) 合作是有成本的;

4) 合作成本可以达到一个很高的水平从而使企业不能从合作获益。

下面我们来定义一些变量:

P: 企业利润

R: 企业收益

C: 企业支出

^{N}: 没有*Ownership*的情况下

^{O}: 有*Ownership*的情况下

$_c$：各企业合作

$_n$：各企业不合作

在当前没有*Ownership*的情况下，各企业决定是否合作是由以下两个等式来决定的:

合作模式下的利润:

$$P_c^N = R_c^N - C_c^N \tag{5}$$

不合作模式下的利润:

$$P_n^N = R_n^N - C_n^N \tag{6}$$

综上，在没有*Ownership*的情况下，我们可以推出:

$$C_c^n - C_c^n > R_c^n - R_n^c \tag{7}$$

下面我们来看如果有*Ownership*，然后分析会对现存系统产生什么影响。首先我们可以确定一个假设，就是在不合作的情况下，*Ownership*既不会对企业产生新的收益也不会产生新的成本。只有R_c^O和C_c^O会受到*Ownership*的影响。因此我们可以得到，企业之间合作的基础是:

$$R_c^O - C_c^O > R_n^O - C_n^O \tag{8}$$

对于C_c^O，我们可以将其分为两个主要的组成，经济成本（费用）和非经济成本（政治因素和风险）。对于R_c^O，我们也可以分为两部分，直接的和间接的。通过*Ownership*，各企业之间可以直接通过合作获得如效率提高以及整体收益提升的成效。也因为合作，各企业间接的获得更多的相互信任和外部信任，从而开启新的合作经济商业模式，激发出更多的可能和利润增长点。

第五章

*Ownership*引擎

5.1 概述

*Ownership*引擎提供运行隐私保护去中心化应用的环境，核心目标是能够让参与者在完全掌控数据所有权的情况下实现多方协作计算，主要包含三个组件:

1) *OVM (Ownership Virtual Machine)*: 智能合约代码的执行引擎，支持同态加密等密码学原语;
2) *OOP (Ownership Oracle Protocol):* 智能合约与外部世界进行安全数据交换的标准协议;
3) *OAF (Ownership Application Framework):* 隐私保护去中心化应用开发框架和密码函数库等。

简而言之，*Ownership*引擎是在区块链技术基础上，高度抽象并整合零知识证明、同态加密、安全多方计算等密码学机制来支撑安全数据计算，实现隐私保护智能合约和去中心化数据计算应用的快速构建和部署。

5.2 零知识证明

零知识证明是由*S.Goldwasser*、*S.Micali*及*C.Rackoff*在20世纪80年代初提出的[10]，指的是证明者可以在不泄露任何有用信息的前提下，使验证者相信某个论断是正确的。

零知识证明系统是实现隐私保护安全协议的有效手段，首先我们给出交互式证明系统的定义:

交互式证明系统：称一对交互机器 $< P, V >$（其中P和V分别为证明者和验证者）是语言L的交互式证明系统，当它满足:

1）机器V是多项式时间的;

2）完全性（*Completeness*）: $\forall x \in L$，那么存在诚实的证明者P，使得V与P交互后，输出“$x \in L$”；

3）有效性（*Soundness*）:$\forall x \notin L$，那么对于任意的证明者P，V与P交互后，输出“$x \in L$”的概率很小。

零知识证明系统可以认为是符合零知识要求的交互证明系统，必须满足以下四个属性

1）验证者无法从协议中获得任何信息;

2）证明者无法欺骗验证者;

3）验证者无法欺骗证明者;

4）验证者无法同时伪装为其他零知识证明系统中的证明者。

零知识证明极其适合隐私保护业务场景，*Zerocash*就是其典型的应用案例。*Zerocash*是首个使用零知识证明机制的区块链系统，它在比特币的基础上提供完全的支付保密性，能够自动隐藏区块链上所有交易的发送者、接收方以及金额等，并允许选择性披露查看秘钥给他人来实现交易详情查询的访问授权。

*Ownership*引擎通过高度抽象零知识证明协议，在智能合约和去中心化应用底层提供零知识证明安全服务层，支撑*Ownership*数据计算对隐私保护的需求，如零知识身份认证、交易数据保密等。

5.3 同态加密

同态加密的问题最早是由*Ron Rivest*、*Leonard Adleman* 和 *Michael L. Dertouzos* 在1978 年提出[11]，而第一个全同态算法到2009年才被*Graig Gentry*证明[12]。同态加密是指具有同态性质的公钥加密体制，允许对密文进行处理后仍然得到加密的结果，即对密文直接进行计算，同对明文进行计算后再加密，得到的结果是等价的。假设E(m)表示m的加密密文，如果已知E(a)、E(b)，任何人都可以通过某种运算得到$a \oplus b$的密文$E(a \oplus b)$，将这个过程表示为$E(a) \otimes E(b)$（$\oplus$和$\otimes$分别表示明文空间和密文空间的二元运算符），由此可以将同态性质笼统表示为:

$$E(a \oplus b) = E(a) \otimes E(b) \tag{9}$$

同态加密包括加法同态、减法同态、乘法同态、除法同态等。同时满足加法同态和乘法同态，意味着能完成全部运算，称为代数同态即全同态。

同态加密对于区块链时代的意义非常重大。目前，从安全的角度讲，用户并不敢将敏感信息直接放到区块链上进行运算，如果有足够实用的同态加密技术，则大家就可以放心地使用区块链服务而不用担心信息的泄露。

尽管当前的同态加密尤其全同态加密技术需要消耗大量的计算时间，还远达不到大规模应用的水平，但对于数据规模较小且需求较迫切的业务场景，同态加密技术在智能合约层面的实现依然具有极强的现实意义。*Ownership*引擎在*OVM*底层原生支持同态加密运算符，实现加法同态算法*Paillier*、*Benaloh*以及乘法同态RSA、ElGamal等算法，便于快速构建隐私保护去中心化应用。

5.4 安全多方计算

传统方式下，为了能够完成某个计算任务，往往把所有参与者的输入都集中到某一个参与者处进行集中计算。这种传统方式虽然能够解决一些问题，但如果所有参与者中没有任何一方能得到足够的信任去知道所有的输入，那么对于每个参与者的输入，即他的私有信息如何得到保护，就成了一个首要问题。这样的情形在现实生活中有很多，比如:

1) Alice觉得自己可能患有某种遗传病。她知道Bob有一个包含各种疾病的DNA原型的数据库。Alice当然可以把自己的DNA序列样本送交给Bob，让Bob来诊断她是否患病。但是如果Alice关注自己的隐私，不想透露自己的DNA信息和诊断结果，那么上面的方法是无能为力的;

2) 经过一段时间的市场调研，A公司决定在某些地区扩展市场份额以获得更大的盈利。但是A公司担心竞争对手B公司也正打算在那些地区扩展市场。简而言之，A公司和B公司不想在相同的地区内竞争，所以他们想知道在他们的扩展计划里，是否有重叠的地区;而同时他们都不想泄露各自计划中地区的具体定位。因为这样的泄露会给双方带来巨大的损失，另一个公司C可能抢在A或B之前占领市场，或者房地产商在知道A或B对某块地感兴趣后会提高价位，所以他们需要一个途径来解决这个问题，同时保护自己的隐私。

以上两个例子的共同点是：两方或多方想在他们的私有输入的基础上进行合作计算，但是没有任何一方愿意泄露自己的输入给其他任何一方。问题是如何完成计算任务，同时保护了参与者的私有信息。该问题称为安全多方计算问题(*Secure Multi-party Computation Problem*)，简称为SMC问题。

安全多方计算由图灵奖得主A.C.Yao于上世纪80年代提出[13]，其主要目标是完成以下计算任务：在一个互相不信任的分布式网络中，两个或多个参与者能够在不泄露各自隐私数据的前提下合作计算某个约定函数并获得计算结果。安全多方计算在隐私保护的合作科学计算、隐私保护的数据库查询、隐私保护的数据挖掘、隐私保护的计算几何问题、隐私保护的数据分析等领域都有大量应用。

尽管*O. Goldreich*、*S. Micali*和*A. Wigderson*提出了密码学安全的可以计算任意函数的安全多方计算协议[14]，但是由于使用了大量的零知识证明，协议参与者之间需要传输大量数据，其适用性受到很大限制。因此，提高安全多方计算协议的关键是针对特定场景设计特定的协议，*Ownership*引擎对安全数据计算的场景进行归类，高度抽象了多种安全多

方计算协议并提供区块链计算模型下的底层解决方案，满足各个行业对隐私保护数据协作计算的需求。

第六章

*Ownership*应用场景

世界变得越来越紧密，商业合作对于一家企业的长期发展越来越重要。然而，目前商业合作存在众多问题，核心围绕信任和敏感信息问题。行业缺乏底层数据协议为数据存储、共享、及分析提供好的保障。核心矛盾在于如何同时实现信息的共享但又保持数据隐私，在不透漏敏感信息的情况下达成有效的商业合作。源数据共享存在的问题在于信息容易泄露和信息的确权和授权难以确认，因此企业合作成本较高，难以达成双赢的合作。有人提出基于区块链的数字交易平台，但这个本身存在的很多问题。数据交易后源数据依然容易被泄露出去，很难控制数据的流转，确权和授权难以确认。除此之外，在数据爆炸的时代，消费者和企业之间的数据关系也变的微妙起来。有些企业并不产生数据，但是通过作为数据的搬运工和储蓄员来把本由消费者产生的数据霸为己有并进行牟利。

6.1 医疗数据

从2008年到现在，随着医疗数据从纸质记录向电子记录迁移，各医疗机构和病人们都累积了大量的相关数据。越来越多的医疗数据需要被共享和分析。这种趋势主要来源于以下几个方面的发展:

1) 病人们需要一个更好的端到端的医疗服务体验

2) 医疗卫生领域的低数据需求的开发和研究已经越来越少

3) 病人们对于医疗数据的安全和隐私保护等问题越来越关注

针对上面的问题，基于*Ownership*系统可以开发出全新的解决方案。我们以制药厂为例，制药厂在开发新药的时候需要一些病人的数据作为临床测试参考，在现有的模式之下，数据的收集是一个非常繁琐并且费用高昂的过程，原因是病人担心个人隐私可能会被泄漏

对于数据的安全性有很大的顾虑。通过*Ownership*系统可以构建一个在隐私保护的前提下的去中心化的数据交换场所，病人们可以完全自主自由的分享／出售相关的数据给制药厂。数据的增、删、改、查等权限以及访问情况都能被病人们实时的掌握。当制药厂完成了对于数据的分析和使用后，病人们还可以通过智能合约获得相应的报酬。这对于病人们和制药厂是一个双赢的局面。

6.2 金融数据

在发展中国家，很多的人没有办法使用如借款之类的现代金融服务。传统的金融机构依据候选借款人之前的金融行为的表现如是否按期支付信用卡账单来决定是否发放借款。这样就形成了一个怪圈，那些在传统金融服务圈外的人几乎不可能获得信用卡或者一个可靠的信用分。但是，这些人中有很大一部分是符合条件的借款人。如果能够服务他们/她们，将会不仅有很大的经济效益也会有很大的社会效益。如果能够合理的使用个人数据将会为上文提到的困境找到一个可能的解决方案。例如， 如果一个刚毕业的对软件开发有兴趣的大学生经常按时交话费，他/她也选修了一些高阶 的课程，同时经常服务他/她的社区。虽然刚毕业，信用分也比较低，但是依然是一个不 错的借款候选人。

毫无疑问，如果能够使用大数据或者其他相关数据可以对很多的金融应用产生帮助。 事实上，已经有根据电信数据或者水电费来进行信用评级的报告[15]。但是，这些数据的服 务商把大量的这类数据据为己有，个人是很难访问和使用自己的相关记录。Ownership区块链和引擎是解决这个问题的方法，个人可以通过Ownership系统然后使用Ownership区块链授权自己的数据给金融机构使用。整个过程保证了只有被授权认可的机构才可以接触到这些个人数据，没有中间人或者其他机构可以。通过这种方式，Ownership系统确保了 在隐私保护和安全的前提下的个人数据的使用。

最后值得一提的是整个的过程是在一个点到点、端到端的全加密情况下，只有数据的所有者和被授权的用户才可以访问。通过剔除其他的参与者和中间人来进一步加强隐私保护和

安全性，这样也降低了整个过程的成本，金融机构不需要支付高昂的费用给第三方的数据平台或者数据服务商。

6.3 其他

*Ownership*不仅仅可以用于上述的场景，开发者可以针对*Ownership*区块链或者*Ownership*引擎开发各种去中心化的应用。根据使用场景，开发者还可以自由选择所开发的应用是否需要特别的隐私保护和数据安全处理。

第七章
我们的愿景

数据的共享可以带来很大的价值。通过科学的方法论，我们可以从数据中提炼出知识，并由此帮助制定行业策略。在机器学习蓬勃发展的今天，数据作为各种机器学习算法的“粮食”被各行各业所需求，但是“粮食”被锁在了“地主”们的地窖里，“地主”们因为各种各样诸如数据安全、隐私保护、数据所有权归属等等的担忧而让宝贵的“粮食”没能被合理的利用。借助于*Ownership*系统，我们希望可以真正的实现尼尔·斯蒂芬森的设想，一个全人类共有的“数据粮仓”。

第八章

参考文献

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

[2] Vukolić, Marko. "The Byzantine empire in the intercloud." *ACM SIGACT News* 41.3 (2010): 105-111.

[3] Duyvendak, Jan Julius Lodewijk. *The Book of Lord Shang*. Probsthain, 1928.

[4] Constine, Josh. “Facebook now has 2 billion monthly users… and responsibility.” *TechCrunch*, TechCrunch, 27 June 2017, techcrunch.com/2017/06/27/facebook-2-billion-users/. Accessed 17 July 2017.

[5] Levy, Steven. Crypto: secrecy and privacy in the new code war. London, Penguin, 2002.

[6] Antonopoulos, Andreas M. “Blockchain vs. Bullshit: Thoughts on the Future of Money .”

[7] Stephenson, Neal, and Jean Bonnefoy. *Cryptonomicon*. Paris: Payot & Rivages, 2000. Print.

[8] Micali, Silvio. "ALGORAND: the efficient and democratic ledger." *arXiv preprint arXiv: 1607.01341* (2016).

[9] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." *OSDI*. Vol. 99. 1999.

[10] R.Riv est, A. Shamir and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, Vol. 21, No 2, pp.120-126, 1978.

[11] Gentry C. Computing arbitrary functions of encrypted data[J]. Communications of the ACM, 2010, 53(3): 97-105.

[12] Goldwasser, Shafi, Silvio Micali, and Charles Rackoff. "The knowledge complexity of interactive proof systems." *SIAM Journal on computing* 18.1 (1989): 186-208.

[13] Yao, Andrew C. "Protocols for secure computations." Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on. IEEE, 1982.

[14] Goldreich, Oded, Silvio Micali, and Avi Wigderson. "How to play any mental game." *Proceedings of the nineteenth annual ACM symposium on Theory of computing*. ACM, 1987.

[15] Turner, Michael A. “Predicting Financial Account Delinquencies with Utility and Telecom Payment Data.” *PERC Results and Solutions*. 2015.