IFTC

Internet Finance Technology Chain
IFTC

重构全球商业

V2.0

目录

一、项目背景

随着比特币的爆红，其底层的技术支撑——区块链逐渐走进人们视野。区块链技术因其在很多金融场景中能起到降低成本、提高效率的作用而被众多机构所关注，然而，区块链本身的技术瓶颈却阻碍了其在各行业领域大范围的应用落地。

至目前为止，整个行业应用落地的情况仍然是：通用的底层平台欠缺、且性能不完善、兼容性不足、交易速度缓慢等。导致绝大部分与区块链结合的商业场景仍然处于探索期。技术发展初期的缺陷，导致业务在匹配区块链时表现多为弱中心化，企业及应用也是依赖于现有资源，整个区块链行业也没有杀手级应用的出现。具体而言：

1、基础设施的搭建。类似在互联网初期，整个底层系统可能还没搭好，导致用户浏览一些简单的网页。

2、交易速度的缓慢。区块链应用程序(包括数字货币、智能合约等)，由于它们是一种去中心化的结构，网络是由一个个独立的节点组成。发生在节点中的各种操作，都会以交易事务的数据广播到网络中，通过矿工打包到新的区块。但是当节点很多，大量发生的交易就会来不及在正常的时间内被打包，因为它们都拥堵在网络中。比如，最典型的比特币，大约每隔10分钟生产一个区块，而每个区块有大小限制。即使在以太坊上面，由于大量智能合约的开发以及ICO，也会导致原有的网络拥堵。目前，比特币一次交易的确认时间是10分钟。如果拥堵程度越来越高，交易确认速度和区块大小等没有提升的情况下，交易确认时间还将拉长。在生活和工作中，金融交易等活动交易非常频繁。以支付宝为例，2017年双11则达到了256000笔。而VISA在标准的节假日，每秒处理4.5万笔交易，一个营业日则为数亿次交易。

因此，与之相比，现有的区块链交易效率远远无法满足商业化应用。简单说，交易确认时间太长、交易效率太低，区块链远远无法胜任高频的商业交易。

3、传统思维限制区块链商业化推进，由于市场对于区块链应用的落地太过急切，但现状又是底层去中心化的公有链对于各行业不能通用，智能合约太过简单不能支撑复杂的商业场景。

基于此IFTC（Internet Finance Technology Chain）提出了自己的解决方案：

IFTC团队依托于多年银行支付交易结算体系的开发经验与沉淀，独立研发了具有创新性与变革意义的全新区块链底层技术共识算法即双点逆向无环工作量证明（DRAW，Double Reverse Annulus Work）与双重区块冷藏技术（ Double Block Refrigerating Technology），优化了目前区块链算法效率迟缓与安全性能的问题，真正推动了区块链商业应用的落地，进而实现区块链在全社会的可持续发展。

DRAW共识算法技术实现原理：通过将单一成块运算速度1/N改变成为TX节点成块运算速度X/N以提高区块链的应用出块速度，把原来500tps运算速度提升至超过1万tps。

双重区块冷藏技术（DBRT，Double Block Refrigerating Technology）的设计原理：通过分散区块切割完成对区块的断点复制，降低区块复制的存储量，从而降低了复制区块的记账者能耗。

面对区块链未来的发展态势：接下来一段时期内，市场会出现大量行业解决方案提供商，竞争激烈的情况下，只有那些拥有强大技术能力、产业资源，还能将技术的价值融合到产业本身的公有链才能走到最后。未来，因为有IFTC这样高吞吐量的区块链平台，以及基于IFTC平台建立的加密数字子货币发行、支付交易结算系统及去中心化的数字货币交易所组成的可应用于垂直领域的基础链底层平台，才真正推动了区块链直接面向用户、实现了商业生态在区块链层面的应用与建设，从而重构全球商业。

二、设计原理

IFTC提供标准的项目底层操作系统，可以作为基础设施，为有需求的商业机构、组织、个人建立基于加密数字子货币发行、支付交易结算系统及去中心化的数字货币交易所开源的代码及实施方案，实现自己的商业模式架构。

IFTC的交易结算系统：利用DRAW算法完成三点记录消费者的每笔交易金额，账本完全复制后再进行确权结算，解决交易确认速度的问题。

IFTC去中心化交易所：IFTC构筑清算链中的锁定支付，保证两个节点之

间可以不需要中介化，直接进行交易的资产安全可控。

锁定支付：IFTC构筑清算链中的锁定支付，构筑了消费者自己的数字货币账户体系与商家的数字账户体系锁定。实现了消费者的预付、数字货币营销等金融生态的建设。

IFTC代币发行合约：很多具有特殊目的的高级金融协议，它们想拥有自己内部的货币来作为组织形式，IFTC建立一个去中心化的和自治的商业体交易组织形式，通过将公正公开的规则编入开源程序中，在无人干预和管理的情况下实现自主运行的组织机构。

IFTC基础链底层平台真正实现了基于加密数字子货币发行、支付交易结算系统及去中心化数字货币交易所的区块链化多领域的加速落地，助力于推动实体经济转型升级，降低实体经济成本、提升产业链协同效率、优化产业诚信发展环境、引导资金脱虚入实。同时也大幅度降低企业运营成本，提升了运营效率，最终实现企业效益和社会效益的双赢。同时，IFTC致力于用区块链思维构造新形态的商业、信用环境，为传统企业、互联网成熟产品的区块链化转型升级提供新模式。

三、技术结构

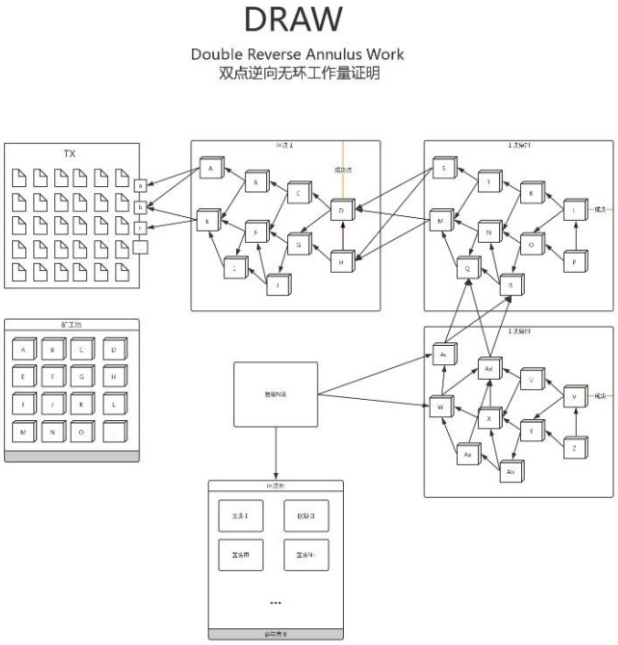
3.1共识机制

共识机制是分布式账本为了使得所存储信息的准确性与一致性设计的一套机制，机制的设计主要由业务与性能的需求决定，从PoW到PoS再到DPoS和各种拜占庭容错算法，共识机制不断创新，但始终满足不能满足商业应用的所需要的交易速度。基于此，IFTC提出了双点逆向无环工作量证明（DRAW，Double Reverse Annulus Work）与双重区块冷藏技术（ Double Block Refrigerating Technology）。大幅度提高了区块链交易的确认迅速以及交易吞吐量，使其满足现有的金融交易规模及绝大多数业务需求。

3.2 DRAW

DRAW算法设计思路：让每一笔交易都必须参与上两笔与接下来N笔交易的复制搭建，以反向交易顺序完成交易记账，并在X笔记帐单位后由最后一

个被搭复制者进行出块打包完成所有X笔交易的确权，形成最终交易组。交易发起后，向前面的TX发起搭建复制程序后直接广播全网，完成此笔交易记账，实现交易闭环，持续完成X笔后，由尾部最后一笔被搭建复制的TX完成整个交易的出块，以完成所有交易的确权。每一笔交易的记账者都需要完成前面所形成的所有区块的复制才能参与接下来每笔交易的记账。DRAW通过3点记账，出块确权的方式，进一步演优化了区块链底层应用的效率和安全性，是一种最全面的高校区块链应用底层解决方案。



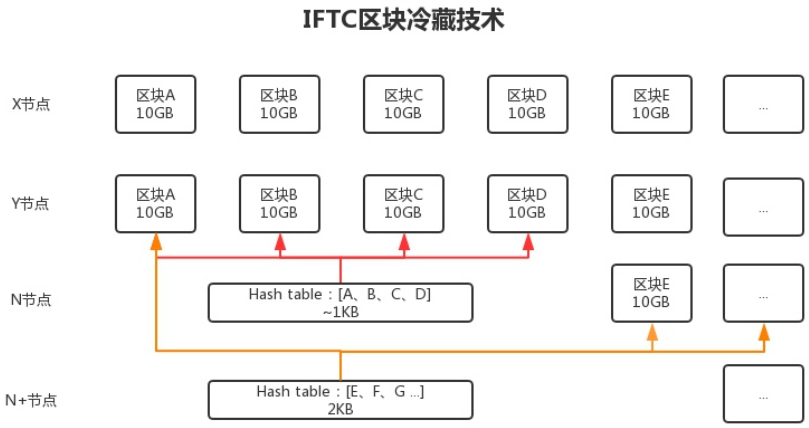
3.3 DBRT

DBRT设计思路：在当今的主流公共区块链上，所有公共节点都承担着存储交易、智能合约和各种状态的负担，这可能使其在为了获得更大的存储空间而进行巨大的花费，以维持其在区块链上的正常运转。为了解决这一问题，区块冷冻技术的可行方法已被提出。这一技术的关键是将整个存储区分开，让不同的节点存储不同的部分；因此，每个节点只负责托管自己的区块数据，而不是存储完整的区块链状态。冷冻的第一个也是最重要的挑战是创建N区块节点。需要开发一种机制来确定哪些节点可以按照安全的方式创建索引，这样就能避免那些控制大量特定节点的人所发起的攻击 。

打败攻击者的最佳方法是建立随机性。通过利用随机性，网络可以随机抽取节点形成索引。这样一种随机抽样的方式可以防止恶意节点过度填充单个索引。但是，我们如何建立随机性呢？最容易获得公共随机性的来源是区块，例如，交易的Merkle tree root。在区块中所提供的随机性是可被公开验证

的，并且可以通过随机提取器中提取统一的随机比特。

然而，简单地使用随机机制将节点分配给索引仍是不够的。我们还必须要确保网络的不同节点索引成员数据的一致性。这可以通过像工作量证明这样的共识协议来实现。



四、商业应用

IFTC（Internet Finance Technology Chain）是一个可应用于垂直领域的基础链底层平台。IFTC团队独立研发的DRAW共识算法与双重区块冷藏技术解决了商业金融应用中的记账速度及确权安全问题，让传统行业、 互联网成熟产品、实体商业实现了基于数字货币发行、支付交易结算系统及去中心化的数字货币交易所的区块链化应用，保证了DAPP的实际落地，为实体商业和互联网企业转型区块链提供了高性能、超高处理吞吐量的基础底层架构。让更多的区块链应用企业可基于IFTC快速实现通证经济的去中心化支付交易结算的应用和流通。真正推动了区块链直接面向用户、实现了传统企业、互联网成熟产品、实体商业在区块链层面的应用与建设。

五、团队介绍

1、核心团队

Edwin CLun 伦知竞

美国国际商业理学士，哈佛大学研修总裁管理课程；二十年亚洲及北美的策略性业务发展和营运经验；创办多家企业，包括IDS 控股、Mission 3-D 及Pharos Medical Device， 并领导家族企业及多间跨国企业。

Caleb 克莱布

UCL博士，资深Java全栈开发者，UCL区块链技术中心项目参与者，UCL金融计算研究中心项目高级架构师，阿兰图 灵大数据研究中心项目架构师。

曾在花旗银行、美国银行和美国运通等均担任过架构师及以上级别职位；

在 UCL 期间，负责对接与央行、投行、对冲基金、清算中心和科技企业的项目研究和开发。

Atticus 阿提格斯

毕业于伦敦商学院，拥有 MBA 和计算机科学硕士学位。来自 于巴克莱银行法国总部，拥有 8 年的零售银行商业战略和制 定经验，以及 6 年投资银行实时交易应用开发经验。

Xavier 泽维尔

1999 年于北德州大学取得软体计算机科学学位。

曾任职于 Nortel Network。任北京与台湾 SUSE Linux 的研发经理，以及 Symbio Mobile 的首席技术长。多年来他一直担任 SUSE 的 ceph 分散式档案系统顾问，以及 WeBank 与 5miles 的区块链顾问。

六、联系我们

网站：IFTC.IO

email：iftc@iftc.io

Facebook：@IFTCofficial/ Twitter：@iftc.io/ telegram：t.me/iftc_io/

Weibo：@IFTCIO