iWorld TECHNOLOGY WHITEPAPER

parallel virtual world based on decentralized storage,blockchain,VR/AR/HM.

hello@iworld.life

EDC，Aoyama Natsumi, Kim Hong Kook ,Fickr Sung,David Hong,

Helen Rong，Harword Shong,Baron Shong

Jan 2019

ABSTRACT:我们基于去中心化存储、边缘计算、区块链和 VR，采用渐进式四层解决方案，以原子世界为基础，结合独创的经济模型、治理模型和信用模型，打造一个未来虚拟世界的底层基础设施。众多开发者可以在ｉＷｏｒｌｄ基础设施之上构建一个无所不能的虚拟世界。

I. INTRODUCTION

A. CONSTRUCTION PROCESS OF iWorld

暂不对外公开。

B.MINING MECHANISM

暂不对外公开。

D.REDEFINE THE ASSET

暂不对外公开。

E.CELL

暂不对外公开。

F.系统的自我进化＆数据更新机制。

暂不对外公开。

G.数据所有权归属＆资产所有权转移

暂不对外公开。

II.FOUR LAYERS

iWorld基础架构采用分层解决方案，第一层是自然环境层，本层主要模拟地球的自然环境，包括土地、江河、湖泊、森林、沙漠等非人为参与的地面构造，以及海洋等水下构造，以及其他基础的地下构造。第二层为不动产层，本层主要模拟现实世界的不动产，包括建筑、道路、桥梁、隧道等。第三层为现实应用层，本层主要是开发者基于虚拟的真实场景建立的一些应用，例如虚拟旅游、全息导航、虚拟协作，这些需要依据真实的人物和场景建立。第四层为超现实应用层，本层主要是开发者依据虚拟的人物和场景建立一些应用，本层的应用是在虚拟的真实场景之上建立的打破物理定律，打破人类极限的超现实应用。

A.LAYER 1：CULTURE

ｉＷｏｒｌｄ会开启点亮世界计划，第一站就是点亮地球，地球的大部分区域依旧是由自然环境组成，那么点亮地球的第一步就是点亮这些自然环境，将这

些自然环境在ｉＷｏｒｌｄ中进行重建。本层是虚拟世界的基础，尽管挖矿机制和资产重新定义机制的存在可以激励用户获取数据并对数据进行渲染，但是基础自然环境优于在现实世界中的经济价值较低，因此在虚拟世界中对应的价值就会比较低，因此人们并没有特别强的动力去在虚拟世界中重建自然环境层，但是这些基础的自然环境也是虚拟世界中不可或缺的基础设施，所以需要ｉＷｏｒｌｄ基金会自身主导进行建设，当然，普通用户也可以对其进行。对于自然环境，我们会依据经纬度确定一个最小单位，我们称之为ｃｅｌｌ，对于每一个ｃｅｌｌ，在Ｄｃｈａｉｎ上都会有一个唯一的地址码与之对应，地址码采用的是采用ｈａｓｈ加非对称加密算法生成，并且永远不会重复。

我们的数据采集使用的是倾斜摄影，三个点连接成为一个面，而这个面就是我们资产归属的最小单位。当然这是现有数据采集技术的极限，我们也考虑到了大的技术迭代，例如未来的技术进步可以做到将数据的采集精度无限趋近于数学定义上的点的时候，那么我们的系统是需要具备自我进化的能力的。而系统这项能力的关键点在于我们在一开始设置的数据更新机制。

B.LAYER 2：REAL ASSET

对于不动产层的数据获取，主要会依托于我们的资产重新定义激励机制，不动产是人类改造自然最直接最明显的表现，也是现实世界中人们资产最主要的部分。同样在虚拟世界中，也会是非常总要的资产。虚拟世界中一份不动产的所有权由其所在的ｌａｙｅｒ　１的无数个ｃｅｌｌ的占有权组成。

关于每一份资产的唯一地址的生成方式，是由ｃｅｌｌ三角的垂心的经纬度

坐标拼接并取ｈａｓｈ运算得到的结果就是这份资产在虚拟世界的唯一地标，矿工采用自身的私钥对地标和地标之上的不动产数据，进行加密生成资产唯一标识Ａｓｓｅｔｉｄ，并向Ｄｃｈａｉｎ发起一笔资产登记交易，待交易得到确认，这份资产的所有权就归属发起交易的矿工，从实现了现实资产在虚拟世界中的重新定义。

实际上虚拟世界的不动产的产生是经过数据的采集、加工、渲染，最终成型的，所以对于一份虚拟世界的不动产，可能由多个协作者共有，并且相互之间的持有比例并不相同，此时就需要我们设计一套全新的所有权归属模式。数据采集矿工，将数据采集并加工之后，使用自己的私钥签名，并附加自己的所有权比例Ａ％，然后将签名后的数据，公开发布到社区，然后由数据渲染矿工依据数据的质量和剩余所有权比例（１－Ａ％＝Ｂ％）选择数据进行渲染，渲染完成之后，将成品数据加坐标进行签名，并发送到Ｄｃｈａｉｎ，最终这份资产的所有权Ａ％归数据采集矿工，Ｂ％归数据渲染矿工。

从表面上看，ｌａｙｅｒ　２的构建似乎是基于ｌａｙｅｒ１的，但是实际上并不是这样，ｌａｙｅｒ　１是伴随着ｌａｙｅｒ２的构建而同步完成的，本质上来讲，ｌａｙｅｒ　１是一个虚拟地球表面的虚拟概念。

C.LAYER 3：REALITY BASED APPLICATION

应用层之所以分两层是因为，我们认为虚拟世界的应用应该分两种，基于现实场景并且符合物理规律的应用和在现实场景之上构建的不符合物理规律的应用。从技术逻辑上讲后者是叠加在前者之上的，对应到ｉＷｏｒｌｄ里面，在每

一个场景都存在两种模式，ｒｅａｌ　ｓｃｅｎｅ和ｂｅｙｏｕｎｄ　ｒｅａｌ　ｓｃｅｎｅ，每一个用户在每一个场景都可以进行随意的切换。

当然，这是逻辑上的分层，与ｉＷｏｒｌｄ代码构建并不相关，但是在开发者基于本ｉＷｏｒｌｄ构建第三方应用时，这样的区分就显得十分重要。ＲＥＡＬＩＴＹ　ＢＡＳＥＤ APPLICATION只需要在现有的ｌａｙｅｒ２添加元素就可以实现应用的构建。

D.LAYER 4：BEYOUND REALITY　APPLICATION

BEYOUND REALITY　ＡＰＰＬＩＣＡＴＩＯＮ的构建需要在ｌａｙｅｒ２的基础上重新对场景进行渲染，最后再添加元素。明显LAYER 4是ｌａｙｅｒ２的升华版本加应用，至于是否还会有ｌａｙｅｒ　5，ｌａｙｅｒ　n的出现，我们并不确定，但是系统保留这样的扩展性。

E.CRYPTO LIFE CHANNEL

我们认为生命是一个特殊的存在，ｌａｙｅｒ　1到ｌａｙｅｒ４都只是不动产的虚拟化，而生命则是贯穿所有层的，无法归属到任何一个层面，因此在整套系统里，有一个贯穿所有层的加密生命通道，虚拟世界里的用户可以通过加密生命通道在系统的所有层级之间转移。

F．MOVABLE ASSET

此处的动产包括可移动的资产和动物，不动产可以无法结合经纬度坐标加海拔来确定，但是动产则只能依据自身的参数来进行唯一标识的确定，此处的动产

由分为ｌａｙｅｒ　３　动产和ｌａｙｅｒ　４动产，ｌａｙｅｒ　３　动产是将现实世界动产的参数进行输入从而获取虚拟世界动产的，但是ｌａｙｅｒ　４动产则是完全是开发者的依据自身的需要，进行动产参数的输入。在ｌａｙｅｒ３中是普通的猩猩，在ｌａｙｅｒ　４种则是人猿泰山。

此处的难点在于ｌａｙｅｒ　３的动产参数的确定，需要以现实世界的数据为依托，那么现实世界数据的依托，此处把动产分为移动资产和动物，动物是的唯一标识可以是基因，要在虚拟世界创建一个ｌａｙｅｒ　３动产，需要将现实世界的动物基因数据导入。对于可移动资产不做约束，因为理论上，可移动资产完全可以依据人类的意愿进行随意的改造，但是动物却不可以。

III. ARCHITUETURE

A.INTRODUCTION

ｉＷｏｒｌｄ基础架构是集合去中心化存储，去中心化计算，前置Ａｎｃｈｏｒ网络，零知识证明隐私保护，ｄｏｕｂｌｅ－ｋｅｙ共同构建的模块化架构。

B.DSTORG

Dstorg由DFS（decentralized file system）和dfscoin组成，DFS采用DHT（distributed hash table）的特性。区别于传统的http协议依据依据文件物理位置的网络唯一标识进行文件的寻址，而是依据文件的HASH值寻找文件的存放位置，DFS协议很好的解决了ip地址数量有上限的问题，同时解决了ip文件寻址无法将数据分块分散存储的问题。同时大数据量的存储，无论是中心化的数据库，

还是分布式存储，还是大数据都，无法满足iWorld大量历史数据和行为数据的存储。同时中心化存储的可扩展性和数据的安全性，数据的抗审查性都无法得到满足。dfscoin是存储系统里面的激励系统，是一个基于区块链技术构建的数据存储、数据检索、带宽共享的代币激励系统，用户通过提供自己的闲置存储和带宽进行挖矿。

DTSTORG既可以作为去中心化的文件系统，也可以作为去中心化的数据库。同时Dstorg也是一个独立的存储模块，既可以为iWorld提供基础的存储设施，也可以为其DAPP所用。

C.DCHAIN

Dchain是iWorld系统中的去中心化计算平台，也是iWorld底层基于P2P网络建立的价值传输网络，Dchain依旧会采用POW作为基本的共识算法。我们认同算力即权利的理念，同时认为也只有POW才是去中心化世界里应该唯一存在的算法，因为POW是一个去中心化架构的最小可用单元。Dchain会采用平行多链的架构，存在一条全局账户链和多条平行子链。

Dchain中的合约分为全局合约，分组合约，和私有合约，同时Dchain中的交易也分为合约创建交易，资产登记/更新交易，代币转移交易，代币转移交易又分为IWD代币转移和DTST代币转移，合约创建交易是实现复杂逻辑代码化的交易，资产登记交易是用户。

在Dchain矿工打包交易的时候，会接收到多种不同的交易类型，其中合约创建交易，资产登记/更新交易，IWD代币转移消耗的都会以IWD代币为燃料，DTST

会依据交易的币天进行增发，增发的,DTST会依据POES机制分配到每一个用户的DTST储备金池中，会依据一定的周期分配到用户的账户中，当用户发起DTST交易时，需要保证其DTST储备金池余额大于0，DTST交易时的手续费会从用户的DTST储备金池中扣除，同时DTST交易的手续费的A%会直接销毁，剩余的B%会以矿工费的形式发放给矿工。通常意义上理解，DTST的交易可以理解为不需要手续费，因为手续费是从增发的部分扣除的，当然用户也可以将自己的账户余额转入增发池进行抵扣交易手续费的抵扣。（具体的经济模型，请参考currency whitepaper） 。

D.DLAYER

Dlayer主要是将主要分layer1，layer2两层，将layer1和layer2的数据统一集成到Dlayer，并统一对外提供interface1和interface2，interface1主要是在资产确权、layer1数据更新、DAPP数据交互时使用，layer1的数据更新只有一种情况会出现，就是技术的进步使得数据采集的最小精度发生了变化。interface2主要是在资产确权、layer2数据更新、DAPP数据交互时使用，layer2的数据更新只有一种情况，就是现实世界的不动产发生了巨大的变化，有新的渲染数据上传，需要进行数据的更新和资产所有权的转移时。

E.DCORE

Dcore是用户接入系统的核心模块，用户通过DCLIENT通过网络与Dcore模块进行交互，DCORE模块主要完成VR模块与DCHAIN模块、Dstorage模块，Dlang模块的数据对接，捕捉Dclient模块的数据输入，同时将互动效果返回给

Dclient模块，Dclient是整个系通的数据交换中枢。

F.DCLIENT

Dclient模块主要负责通过网络与Dcore模块进行数据和逻辑的交互，DCLIENT需要适配各种硬件设备，包括普通的VR眼镜，跑步机，单车，穿戴设备等，其采集用户的输入信息，并将数据传输给Dcore，Dcore依据接收到用户的输入信息之后，会调相应的DAPP逻辑进行数据处理，并将相应结果指令返回给DClient，Dclient依据返回的指令，操作安装Client的硬件设备，模拟画面、声音、感觉、重力感应、气味等，从而给用户一种真实的体验感。

G.DLANG

Dlang是针对开发者的一门高级语言，会和JavaScript类似，用户通过Dlang创建Dapp。区别于传统的基于手机设备，电脑端的Dapp，此处以VR和可穿戴设备为Dapp的接入口。

H．ANCHOR

至今依旧有很多人认为比特币是匿名的，实际上比特并做不到在网络层的完全匿名，Zcash\Manero\Zencash 等币种都选择在原有的区块链网络基础上再设置一层匿名网络来确保交易和账户的匿名性，匿名网络的搭建则需要设置足够多的安全节点。

传统并且已经成型的匿名网络有 tor，i2P 等，都是经过时间验证可以做到一定的匿名性的，但是其自身也存在很多问题，Tor 和 i2p 本身已经被证明无法做

到 100%的匿名，微小的操作失误都会导致上网信息被监控。并且使用流程十分复杂。

因此我们发起了 anchor 项目，主打匿名性和易用性，在提高匿名性的同时简化普通用户的使用难度，庆幸的是 EDC 有来自美国海军试验的成员，他全程参与了 TOR 项目的研发，与此同时，我们详细研究了 I2P 和兰花网络的部分代码，我们确信我们的解决方案是匿名性最高，最容易使用的。不幸的是，这个项目还在开发中，目前并不能正常使用，尽管我们已经想好了如何去开发这样一个项目，但是这依旧需要一些时间。

I.DOUBLE_KEY SYSTEM

数字货币的监管困难一直是阻碍行业发展的巨大障碍，完全的自由主义者希望自己不被监管，不受任何约束，政府却希望对每一个公民都了如指掌，两者之间似乎有着不可调和的矛盾。但是我们认为应该给普通人自己选择的权利，接受监管也接受保护，或者完全的自由这也就意味着不受保护。基于这样一个理念，我们为系统设计了双重秘钥机制。

双重秘钥意味着每一个账户有两把秘钥，拥有全部功能的秘钥我们称之为 operation_key,此处的全部功能值得是不仅仅可以发起交易，并对交易进行签名，还可以随时查看账户的状态。另外一把秘钥，我们称之为 review_key，其只有查询账户状态的功能。

此处如果用户选择接受监管，则用户将自己的 review_key 交给政府的监管部门，这样监管部门就可以实时查看账户的状态和变动情况。但是执法只能通过线下找到账户的所有人，账户的变动状况只是作为证据而存在。如果用户想要拥有完全的自由，则用户需要保存好自己的两把私钥。

可能有人会说，作为一个区块链系统选择接受监管就是违背理想的妥协，也有人说监管是整个行业向前发展不可或缺的一部分。既然如此，我们就把选择的权力交给普通用户。

J.PRAVICY

隐私一直以来都是区块链从业人员十分头痛的一个问题，因为真的是没有很好的解决方案，在对比了广播协议和零知识证明之后，我们认为零知识证明是一个更好的解决方案，Zcash 首次在数字货币领域采用了零知识证明这样一门技术，Fickr 曾无数次告诉过我们 Zcash 价格突破 5BTC 的那个夜晚他是有多么的激动。隐私从来都不是小部分人的需求。

IV.DECENTRALIZED　S R T O R A G E　S Y A T E M

在去中心化系统到现在一直没有大规模商用的一个主要原因就是承载不了大量的业务数据，因为这些数据是无法放到区块链上的，而放到中心化存储，或者分布式存储中又有违去中心化产品的设计初衷。而基于 DHT 的去中心化存储网络则完美的解决了这些问题。既保证了存储的数据不会丢失无法篡改，也保证了数据的抗审查性，数据不再有任何的立场，只要数据被创造出来了，就会存储在那里，而数据的立场取决于看这份数据的人而不再是审查是这份数据的人。

V. DECENTRALIZED　C OMP U T I N G　S Y S T E M

任何一个系统都是由存储和计算组成，有了计算才有逻辑处理，我们的计算网络也有很大的创新，对于以太坊这样的世界计算机，每一份代码都会在系统中的所有机器上运行，虽然这样可以最大程度保证安全性（去中心化），但是并不能充分利用计算机的计算资源，尽管以太坊推出了分片和状态通道等解决方案，

但是我们认为这都不是最终的解决方案。去中心化的世界里需要一个既能保证安全性又能不浪费多余的就算资源的新的计算框架。在存储的世界里 DHT 完美的打破了安全性与效率不能共存的问题，但是在计算领域目前还没有出现一个成熟稳定的解决方案。团队仔细研究过 MapReduce，Storm，Spark 等分布式计算框架，从中得到了一些灵感，其实只要在上述这些分布式计算框架中加入合理的激励机制，同时考虑到计算网络中客户端的多样性带来的并发性故障就可以在保证安全性（去中心化）的前提下大大提高系统计算资源的利用效率。

VI. V R / A R / HM

VR/AR/HM 会是未来虚拟世界的入口，区块链、去中心化存储为虚拟世界提供了强大的基础支撑，但是对于普通用户来说，VR/AR/HM 则是使用层面最重要的技术支撑。

VII. DEEP THINKING IN PHILOSOPHY

有人说区块链所谓的去中心无非是想成为新的中心，对于这种观点 F i c k r 某种程度上是认同的，不过新的中心是以技术为支撑的公开透明，全民参与的中心，如今依旧会是金字塔结构，最顶层是以技术为核心的新中心，但是新的金字塔是从下而上建立的，下层的意愿决定了塔尖的形状和构成，而传统的金字塔是由上而下的，顶层的意愿决定了下层的形态。同时新的金字塔是完全由代码来创造的，由机器来执行的，代码永远是理性的，是真正的法治，因为代码即法律，而传统的金字塔是依靠每一个层级的人治来管理的，人治必然会存在腐败问题，因为人性使然，但是代码却永远不会腐败，只会按照既定的逻辑永久的运行下去。

VIII. DEEP THINKING IN ECONOMICS

我们从来都认为比特币不是数字货币，而是数字资产的一种。因为货币基本

功能是交易媒介和价值尺度，而资产的基本功能是保值增值。人们日常生活中不仅需要货币也需要资产，不幸的是，货币并不是资产。我们认为一个去中心化的系统必须要有货币和资产共同作为石油来推动系统持续向前，但是货币和资产内在的经济逻辑完全不同，以至于必须要分开发行。我想读者应该已经看到了很多将比特币与黄金进行比较的文章或者图表，明显比特币各个选项都已经或者即将高于黄金，但是金本位的货币制度的结束不仅仅是因为黄金不易分割，不易携带，流通成本过高，更主要的原因是因为黄金总量有限，尽管伦敦黄金交易市场的黄金交易量远远超过了地下黄金储藏量，尽管纸黄金可以随意制造，尽管我们并不精确的知道黄金总的储藏了是多少，但是在大众的认知里，黄金总量是有限的。任何一个总量有限的物品都只能是资产，而不能长久的作为货币，但也许可以在某一个极短时时间内作为货币。黄金到信用货币的历史演变，对应到数字货币领域，必然会是比特币等数字资产，将交易媒介的功能转移给新的稳定的供应量可调节的全球数字法币，而只保留自己数字资产的属性，以及危急时刻硬通货的功能。所以基于这样的经济学认知，我们设计了一个平行双代币的经济系统，稳定货币 BUT 和数字资产 IPST。BUT 是一个稳定币，然后这种稳定并不是，如同 DAI，这种锚定法币，也不是 USDT 这种以法币为背书，而是通过一个透明的增发与销毁机制严格控制货币的供应量来达到价值的稳定。IPST 和普通的数字货币并没有区别，既有使用价值也有价值，由于总量有限，并且永不增发和销毁，所以只能用来充当数字资产以及信任危机时刻的硬通货。

IVV. SOCIAL　SYSTEM

A.GOVERNANCE SYSTEM

基于分类合约的治理机制

B.CREDIT SYSTEM

基于币天的信用体系

VVI. ACKNOWLEDGMENTS

We thank E D C , Aoyama, Hong Kook & Fickr for his effort of writing this paper, we thank David,Helen & Baron for his effort of reviewing this paper.