everiToken 技术白皮书 2.5

声明

本白皮书的目的仅为信息说明。

本白皮书不代表任何明示或暗示的保证、证明、预期等。

本白皮书上写的技术指标或技术实现方式可能会随时间推移而改变。

技术团队随时可能解散或重组，或出现核心技术人员流失而导致项目无法完全实现。

本白皮书只是原样提供。项目团队及其任何成员都不为能否实现白皮书的任何内容负任何责任。

Token 不具有任何实际价值，只代表你通过数字加密手段持有这个 Token，唯一用途是确认你对拥有该 token 的权限。

使用本白皮书所述技术运行的区块链或其衍生品上出现的任何事件，都是由程序自动化生成，团队无法对其后果负责。使用后果由使用者自己负责。

任何人都可以在不修改白皮书的前提下非商业性地使用白皮书的所有内容，但是团队不对任何后果负责。

目录

背景和愿景

通证（Token）经济到来

2018 年四月，区块链技术问世十年。除此之外，一个核心问题始终存在：区块链技术是否真的在世界经济中创造了价值?

我们来看一组数据: 目前, 全球区块链上管理的资产基本上都是各种同质化代币，总市值大约 3000 亿美金。这些链上资产普遍具有高波动性和强投机性的特点，难以造福世界经济。实际上，从中本聪开始，人们都曾想让这些同质化代币成为支付货币，但是这些数字资产并没有发挥货币的作用。强调数字货币名不副实。事实上，发行货币是一项非常重要的权力，是政治的体现，货币权力必须属于国家。因此，想让通证取代货币很难，没有国家或政权的支持，所谓数字货币只是自欺欺人。

另一方面，目前全球主流资产（有形或无形）并不在链上，区块链和这些链下资产尚无过多交集。

但是 Token 只是一种代币吗？并不绝对。Token 是一种符号，令牌，翻译成通证会比数字货币更为准确。通证可以代表一切权益证明，包括身份证明、文凭、访问密钥、活动门票、卡片优惠券等等。回首历史，人类社会的全部文明可以说都是建立在权益证明之上的，所有的账目、所有权、资格、证明都是权益证明。就像尤瓦尔赫拉里在《人类简史》里说的，“正是这些虚构出来的现实才使智人脱颖而出，从而建立起人类文明。”如果这些权益证明全部数字化、电子化，并且用密码学来保护和验证其真实性、完整性、隐私性，人类文明将会彻底变革。我们称之为“通证（Token）经济”。

在区块链上运行通证提供了坚实的信任基础，这是任何传统中心化基础设施所做不到的。因此，通证是通证经济的前端经济形态，区块链式通证经济时代的后端技术，二者合作无间。

竞争分析

作为为通证经济而生的公链，我们认为 everiToken 有两大主要竞争对手，以太坊和 EOS。我们会从优势劣势，机会与风险两个方面来分析。

优势与劣势

综合人类历史的进程和区块链技术的发展，我们认为下一代区块链技术需要并且应该做到高效的资产权益管理。主要包括以下三个方面：

1. **数字权益证明**：通证必须是以数字形式存在的权益凭证，必须具有内在的真实价值（不论有形还是无形）。
2. **安全、加密地授权管理**：通证必须是可验证的，防篡改的，隐私保护的，并且可监管。通过密码学加密保护，并且经过对应授权才可使用。
3. **可流通性**：通证可以方便地交易或兑换。

根据以上需求，我们提出了一系列解决方案来满足通证经济的广泛基础需求，为了促进通证的流通和管理，建立通证经济的技术基础。

具体而言，我们针对上述需求实现了以下三大特性：

1. **快速方便的 Token 发行**：用户不需要编写代码，通过使用接口的应用（app 或网页）就可以轻松发行自己的 Token。

2. **高效的 Token 流转**：实现 Token 的秒级流转，并且可以承载数以亿计的 Token（这里应该指的非同质 Token）同时成交。
3. **灵活的权限管理**：一套简单优雅的模型来实现权限管理。可以支持共同持有，私钥找回，多重签名，合规性，政府监管等复杂需求。并且无需额外的编程。

我们来看看以太坊和 EOS 是怎么做的：

以太坊：ERC20 和 ERC721 协议

通过以太坊达到通证经济需要开发基于 ERC20 和 ERC721 协议的智能合约。其中 ERC20 协议支持同质化 Token，ERC721 协议支持非同质化 Token。然而，这种方式存在严重的问题。

1. TPS：目前，以太坊每秒只能支持十几笔交易，无法满足 Token 流转的实际需求。
2. 开销：实现智能合约的每一步都需要消耗 gas 费。对于拥有复杂商业逻辑的功能来说（例如多人共同持有，监管，合规性等等），开销会非常高并且不可控制。
3. 普及：以太坊实现通证经济基于智能合约，非开发人员无法实现，必须使用第三方应用。
4. 非标准化：由于不同的智能合约可能采取完全不同的开发思路，这些虚拟通证的元数据互相无法交互。这不利于通证经济的生态发展，另外，用户无法使用统一的方式来查询其所拥有的的各种不同通证资产。

EOS

EOS 在 2018 年六月份上线了主网。EOS 针对以太坊存在的问题进行了一些改进，通过 EOS 来发展通证经济可以解决部分以太坊的问题。然而还是有一些问题存在：

1. 安全问题：通证交易可能对应极其珍贵甚至不可再生的现实实体，不容许出现半点安全问题。然而，基于智能合约的开发受限于开发者的水平，很难保证不同种类通证的开发者都具有足够的安全意识。

   EOS 的智能合约基于 Web Assembly，这是一个新生目标汇编语言，仍处于测试阶段。此外，EOS 的智能合约代码是图灵完备并且拥有过大的执行权限，容易形成安全漏洞。

   绝大多数人不会编写智能合约，为了发行和转移通证，必须依赖第三方应用，用户必须信赖第三方代码编写的质量。因此，资产的控制权并不在用户手上，依赖于第三方的保证。
2. 非标准化：类似于以太坊，不同智能合约的元数据难以互相交互或合作。
3. 监管、信任与合规：由于非标准化代码阅读所需的专业型，政府很难实现监管。另外，非开发者无法判断是否可以信任相关的代码，这使得区块链难以被普通人和政府接受。
4. 执行效率：为了满足多样化的需求，EOS 的智能合约功能复杂，系统模块众多，资源调度和分配相对困难。这些大大增加了系统的复杂性，降低了运行的速度。由于不同数据和功能间可能出现的冲突，想用多线程执行来提高速度并不容易，也需要付出大量调度时间。
5. 普及难度：全球经济的商业需求往往复杂多变，每一个智能合约都需要时间

来开发和测试，难以在较短时间跨度内满足市场的多样性。这将成为发展通证经济的阻碍。

everiToken 和其他公链相比一个最大的不同在于 everiToken 使用安全合约来替代智能合约。这意味着 everiToken 并不是图灵完备的，存在一些复杂的应用场景 everiToken 系统不能满足。但是我们认为 everiToken 能够满足通证经济中 95%的需求，并且 everiToken 会是最安全、最友好的公链并且对大部分用户来说几乎免费。

机会和风险

除了这些优势以外，everiToken 创造了生成 everiPass/everiPay 二维码的协议 EvtLink。everiPass/everiPay 是针对面对面小额支付的协议，基于 everiToken 公链。

everiPass/everiPay 包括二维码的生成标准与通讯协议的定义，具有以下五个特点：

即时清算：一笔交易本身就是一次结算。

去中心化：点对点支付，没有中间平台，没有人可以篡改链上数据，每个人都可以参与到定价中来。

最安全：记录上链的数据和内容无法被伪造，最大限度保障用户的资产安全。

可扩展性：everiPass/everiPay 支持 everiToken 链上的所有 Token，不光是货币，也包括其他代币和积分，或者是开启一扇门的钥匙。并且你几乎可以在任何时候任何地方使用，只需要带上手机。

最方便：即使你没有连接到互联网，你也可以完成交易。

基于以上五个特性，everiPass/everiPay 可以提供最安全，最方便，用户体验最好的面对面支付服务。

一些风险仍然存在。如我们之前所说，以太坊和 EOS 也能在通证经济中成为非常棒的公链。如果以太坊能够切实提高它的 TPS 通过例如分片技术，它会成为非常强大的竞争对手。尽管智能合约现在存在非常多的问题，但随着时间推移，智能合约的缺陷可能会被慢慢解决，这将会极大提高以太坊和 EOS 的竞争力。毕竟它们现在具有更多的关注和更多的用户，这也是为什么 everiToken 真正专注于实际落地应用与生态。

小结

基于以上考虑，我们为通证经济量身打造了最适合区块链应用落地的平台和生态系统，一条全新的公链 everiToken。真实世界的资产、证书和各种凭证都可以通过发行通证来数字化，并且以前所未有的安全性和速度在网络上流通。

技术创新

安全合约（SafeContracts）

智能合约在理论上讲是一种有效的进行分布式商品交易和服务交易的数字手段。但是实际上，智能合约存在广泛的安全漏洞可能产生不恰当的代码执行或者逻辑错误从而导致出现账户锁定，访问泄露，服务终止等等问题。因此，智能合约往往不能起到提供信任的效果，反而可能被视为比传统合同更加不可靠。

everiToken 引入了安全合约的新思想，用户不需要直接编码，而是通过使用安全

合约接口来方便快速地进行通证的发行和转移。通过原生集成功能的核心需求，所有的安全合约接口都经过充分的审查和验证，安全合约确保链上所有的交易都是安全无漏洞的。尽管安全合约并非图灵完备，它仍旧可以通过接口实现通证经济绝大多数必要的功能，并且为通证的发行者提供了完成离线服务的可能。

此外，安全合约可以增加系统利用率来提高速度。使用接口使得突发事件更容易进入现有工作流中而不用从头编译中断代码。另外，接口使得不同种类的数据转换变得清晰，系统知道什么操作处理什么数据，可以更方便地把不冲突的操作进行并行处理以提高系统速度。内测版本已经达到 5000tps。

数据库

EOS 为了支持回滚操作使用了基于多索引的内存数据库，所有操作的结果都存在内存数据库中。为了在合约代码异常时支持分叉和需要恢复时的回滚，每个操作中都需要记录回滚相关的额外数据。此外，把所有的数据都存在内存中处理，可以预见到的是，随着时间的推移、用户量和交易的增加，对内存的需求将会显著增加。这对节点的存储容量提出了很高的要求。并且，如果程序崩溃或从新启动，内存中的数据将会丢失，为了恢复数据我们需要重复之前区块中的所有操作，从而导致漫长而不合理的冷启动时间。

在保留 EOS 内存数据库的同时，我们开发了一个基于 RocksDB 的通证数据库，它有几个好处：

1. RocksDB 是一个非常成熟的工业级键值对数据库，已经在 Facebook 等核心集群中得到了充分的验证和使用。
2. RocksDB 是基于 LevelDB 的，提供了比 LevelDB 更好的性能和更丰富的功能。

它还对低延迟的情况（如闪存或者固态硬盘）重点进行了优化。

3. 在必要的情况下，RocksDB 也可以当做内存数据库使用。

4. 基于 RocksDB 的体系结构天然支持版本回退等特性，并且几乎不会影响性能。

我们的通证数据库使用 RocksDB 作为底层存储引擎。我们针对通证相关操作进行了最大程度的优化以提高性能。借助 RocksDB 我们可以以较低成本实现回滚操作。此外，通证数据库还支持数据固化，定量备份，增量备份等可选功能，也解决了冷启动的问题。

由于 everiToken 所有的操作都是高度抽象的，操作类型都是已知的，并且删除了不必要的信息。与通用系统（EOS）相比，冗余度非常低，这也减少了区块的大小。

Token-Based

概览

为通证经济而生，一个最大的不同是 everiToken 的 Token-Based 通证管理方法。通证有别于央行发行的数字货币（digital currency）或者加密货币（BTC 或者 ETH）。我们定义通证（Token）是你对一项资产、某一段时间或某一个地点内具有排他性共享经济、或是一段特定人提供的时间服务的证明。通证分为两种类型，同质化通证（Fungible Tokens）和非同质通证（Non-Fungible Tokens）。它们的应用场景和数据结构存在一定的差异，根据我们的分析，非同质通证在通证经济中可能扮演更广泛的角色，因此我们首先介绍非同质通证。

非同质通证

（请注意，本节所有通证均指非同质通证）

在理解非同质通证前，让我们考虑沙滩上的一大堆石头。在现实生活中，每一个石头具有不同的重量、外观和类型。没有两块一模一样的石头，就像没有两片一样的树叶。另外，你不能简单的把两块石头拼起来，因此我们说每一块石头都是独一无二（individual）并且不可结合（not to be combined）的。

一个区块链实例就是以太猫（CryptoKitties），以太猫曾经十分火热，每一只猫拥有独一无二的编号和属性。

一个非同质通证就像是现实世界里一块独一无二的石头，或者一只以太猫。它们在现实世界里天然的不同，在 everiToken 系统中也是。

总的来说，非同质通证可以根据他们不同的价值属性分为不同的类型。我们可以把同一类型的非同质通证归纳成一个域。

专注于通证使得 everiToken 得以具有高标准化的特点。所有由用户自定义发行的通证满足同样的结构。具体来说，每一个通证都有一个域名（Domain name）用于对应一个特定的域（Domain）。这个域就是通证所属的类别。同时，通证发行者需要设定一个在这个域中独一无二的通证名字，通常来说通证名字往往具有丰富的内涵。例如产品的条形码可以用作命名规则，它包含了产品的原产地和制造商等信息。每一个通证在系统中的唯一性由其名字和域名共同决定。另外，每一个通证至少具有一个所有者（Owner）。

正如上面所说，通证的 ID 由通证名字和域名共同决定。一个通证的基本结构如图 1 所示。除了通证 ID，结构中还有所有者和其他必要的数据。

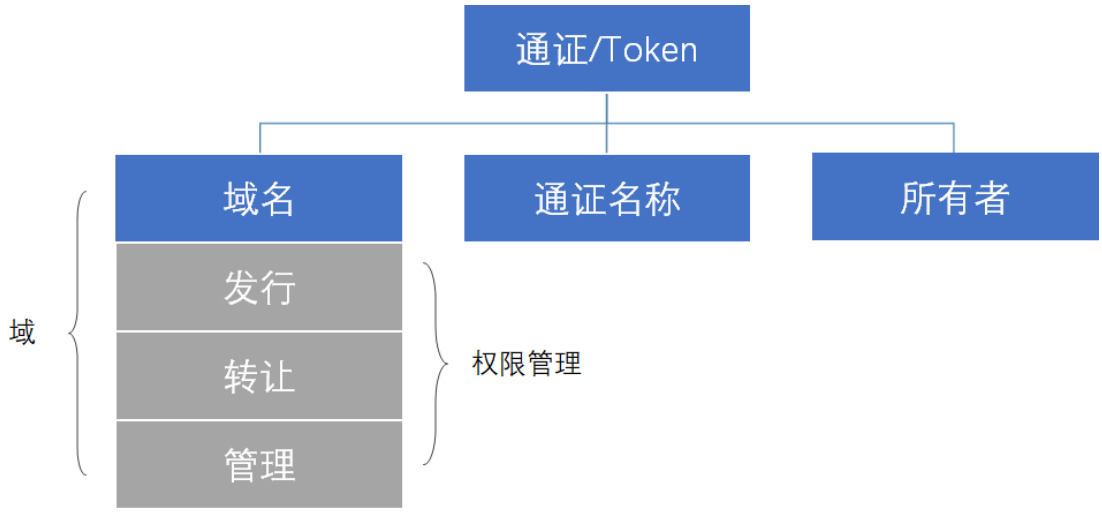


图 1.everiToken 通证基本结构

域的详细内容由域名来对应，每一个域描述了它对应的权限管理的信息。

每个人都有权力发行自己的通证。通证本身不具有价值，价值由发行者的真实信用背书。一旦一个新的通证被发行出来，它就可以通过转移操作转给他人。

在 everiToken 系统中，通证转移的本质上就是变更通证的**所有者**。每个通证上都记有该通证的所有者（可以有一个或多个的所有者）。需要变更所有者时，参与该通证流通的成员可通过签署数字签名确认该次操作，由 everiToken 节点确认满足权限要求并同步到其他节点后，该 Token 的所有权即发生变化。

权限管理

everiToken 系统中权限管理包括三种权限类型，即发行，转移和管理。

发行（Issue）是指在该域中发行通证的权限。

转移（Transfer）是指转移该域中通证的权限。

管理（Manage）是指修改该域权限管理的权限。

每一个权限都由一个树形结构来管理，我们称为权限树（Authorization Tree）。

从根节点开始，每一个授权都包括阈值，以及与之相对应的一个或多个参与者

（Actor）。

参与者（Actors）

参与者分为三种，账户（Account），组（Group）和所有者组（Owner Group）。账户是独立的个体用户，组是集群账户，所有者组是一个特殊的组。

一个组可以是俱乐部，公司，政府部门或者基金会，甚至可以只是一个人。组包含组的公钥，以及每个成员的公钥和权重。当批准操作的组中所有授权成员的权重总计达到阈值时，该操作就被批准。

同时，持有组公钥的成员可以授权对组成员及其权重进行修改。我们称这种机制为**组内自制**（Group Autonomy）。

当一个组第一次创建时，系统自动生成一个组 ID 分配给它。发行者在域中设计权限管理时，可以通过直接引用现有的组 ID 作为其权限管理的某一个组。由于组内自制，每一个组都可以方便的重复使用。

一个通证的所有者是一个特殊的组，它的名字固定为所有者组，包含所有该通证的所有者。这个组的特点是不同通证的所有者组不同，并且每一个成员的权重都是 1，而组的阈值时组内成员的总数。

管理

权限管理由通证发行者设定，每一个权限至少由一个组来管理。当一个通证发行时，发行者必须指定每一个权限下相关组的权重和阈值。在一个域下执行任何操作之前，系统会验证该操作是否得到了足够的权重，只有当得到授权的权重达到阈值，操作才会被执行。这种灵活的权限管理与分组设计适用于现实生活中的许多复杂情况。图 2 就是一个例子：

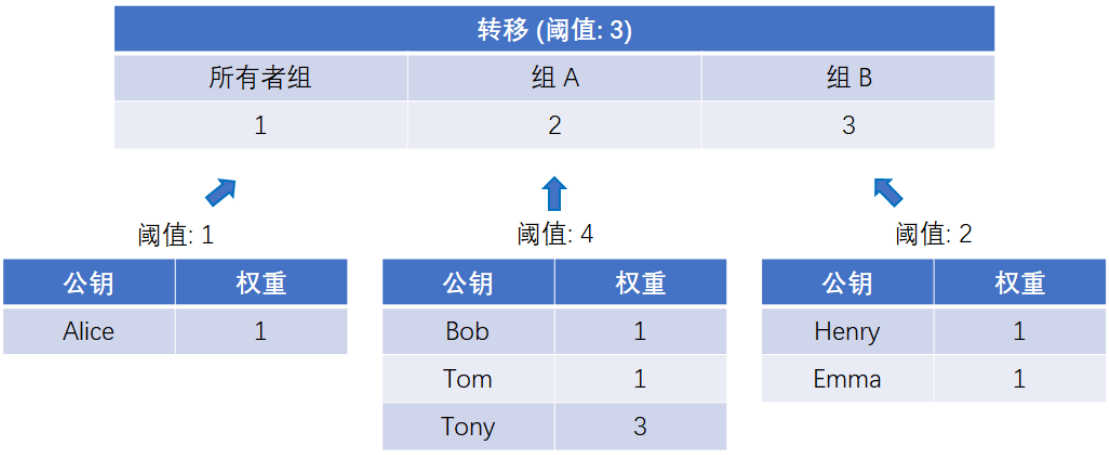


图 2 一个转移权限示例

图 2 描述了一个域中的转移权限。整体的阈值是 3, 与转移权相关的共有三个组，分别是所有者组，组 A 和组 B。基于它们三个组各自的权重（分别是 1,2,3），所有者组和组 A 需要共同授权才能授权一次转移, 而组 B 可以单独完成转移授权。在每个组内，所有者组里面只有 Alice 一个人，组 A 可以由 Bob 和 Tony 两个人授权或者 Tom 和 Tony 两个人授权。而组 B 需要 Henry 和 Emma 共同授权才行。任何用户都有权力发行通证，但是不同域中通证的应用场景各不相同。房产的转移一定要得到政府授权并且处于严格的监管之中；会员卡和优惠券需要公司商标来背书；一场音乐会的门票看完之后就失去了价值，但是一个停车位的所有权可能随时间在变化。

当发行通证时，通证发行者可以通过设置域中的权限来实现对通证的权限管理。下面这个场景展示了权限管理可以带来的便利。

图 3 展示了 everiToken 的权限管理机制如何解决现实生活中的复杂问题。

一个公司新建了一栋写字楼，并且希望就其产权和收益权发行 1000 个通证。公司成立了 SPV 来负责维护和管理这些通证。在现实中，这些通证的发行和转移都需要得到地方房产局的认可和授权。它们必须符合地方的法律法规，然后通证的具体信息（总数，发行方，权限管理结构等等）将会被公布在 SPV 的官网上。

在此之上，中央房产部拥有最高权限来限制和管理地方房产局以及房产所有者。

图 3 权限管理结构图

通证发行者和最初的通证所有者都是 SPV，组 S 代表 SPV，组 L 代表房产局，组 C 代表中央房产部。

在大多数情况下，转移一个通证需要所有者和地方房产局授权即可，这样一来，房产通证的转移即受到了地方房产局的监管。在一些特殊情况下，例如一个通证的所有者意外去世或者遗失了自己的私钥，中央房产部可以在法律认可的情况下把通证转移给拥有合法继承权的人。

如果有一部分通证的 ID 遗失了（这也是有可能发生的），或者 SPV 和通证持有者们都同意就该写字楼增发一部分通证，他们可以通过满足发行权来增发一些通证以满足实际需求。更进一步，这套权限管理机制还可以解决一些极端情况，比如说中央房产部需要紧急冻结这批通证，它可以用自己的管理权通过更改域内的转移权阈值来达到这一效果。

同质化通证（points）

发行

任何人都可以在注册一个符号之后发行同质化通证。用户可以选择是否设置总数，然后用户需要设置他们这次想要发行的数量。

转移

任何拥有他们私钥的用户都可以转移他们的同质化通证给其他人。

其他

每个账户都会记录它持有的不同符号的同质化通证。我们准备了独立的键值对空间来存储不同符号同质化通证的基本信息。用户可以授权其他私钥的持有者转移他们具体数量的特定符号的同质化通证。这一功能叫做通证许可（Token Allowance），主要用于通证交易所中。

Token-Based 记账模型

概览

everiToken 使用 Token-Based 记账模型来管理非同质通证。

简单来说，对于一个 Token-Based 账本，我们在通证发行之初建立一个包含通证 ID 和所有者的记录，然后可以在每次转移给其他人时更新它的所有者。这对于非同质通证来说是一种很高效的方式。这使得更新和查询通证信息变得非常快，因为我们有一个专门为此设计的通证数据库。

Token-Based 记账模型由 everiToken 的几个核心成员发明，并且已经完美地运用在 everiToken 系统中的非同质通证。everiToken 可以被认为是一个状态机，当且仅当对每个不可逆区块执行操作时才改变其状态。对一个使用 Token-Based 记账模型的区块链，像 everiToken，我们可以把数据库分为两个部分，一个是通证数据库（Token DB），一个是区块数据库（Block DB）。这两个数据库都应该是一个版本化的数据库，可以在区块反转时快速回滚。everiToken 使用 RocksDB 作为通证数据库。

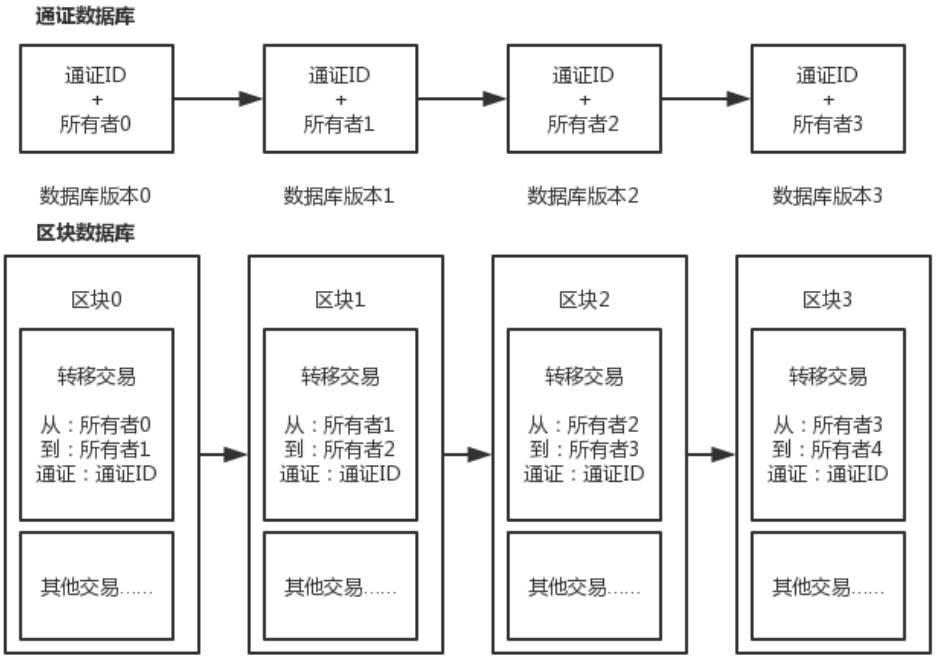
通证数据库

通证数据库是一个索引数据库，用于快速查找区块链的最新状态，例如通证所有者或者一个账户的同质通证余额。当一个交易执行时，在数据库中更改所有者。通证数据库是一个只扩展的数据库，只允许添加新的数据，并且更新到新的版本，旧的数据并不会直接删除。老版本的数据可以用于回滚如果这个块发生了反转，最终反转的块会被垃圾回收。

区块数据库

区块数据库负责存储链上所有的原始不可逆块，每个块存储所有的细节信息，包括执行的操作名称和参数，块上的签名和一些附加信息。

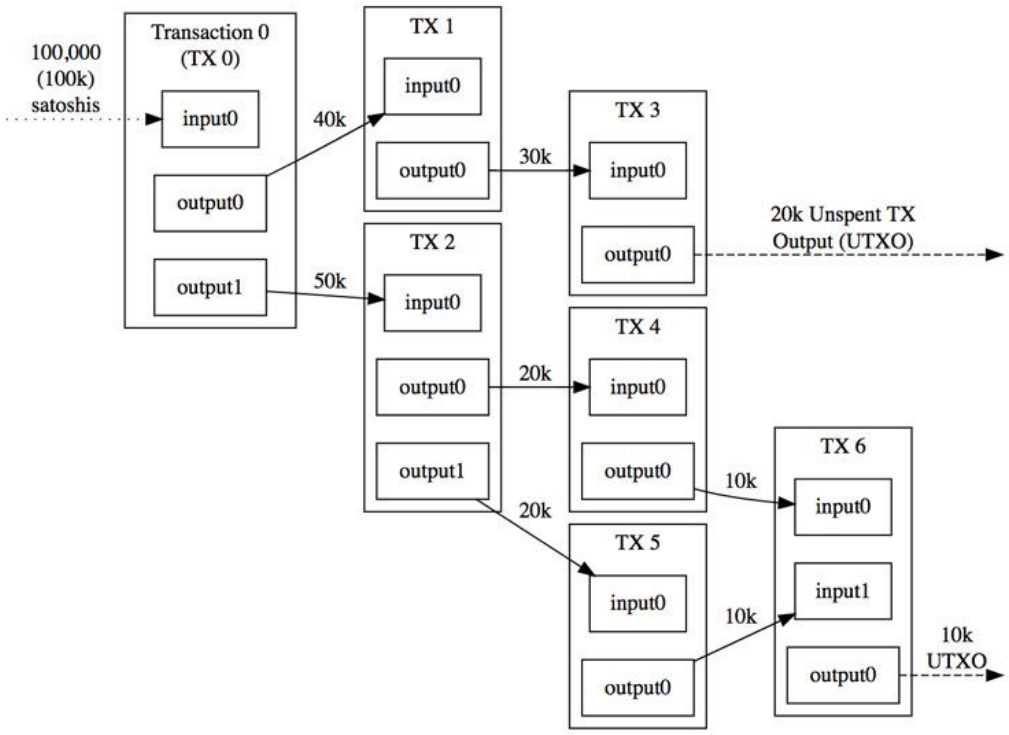
这张图片展示了两种数据库是如何一起为非同质通证工作的：



与其他记账模型比较

一、 UTXO

在 UTXO 模型中，用户通过对前一个交易的哈希值与接收者的地址进行数字签名并添加到下一个交易的末尾来进行转移操作。这种机制本质上是对输入和输出的连续超越，代币的所有者并不直接拥有代币，而是拥有输出中的一部分然后通过签名作为新所有者的输入，之后新的所有者控制新的输出。



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

这张图直接摘自 bitcoin.org

如你所见，UTXO 可以有效地避免双花但是显然每个输入只能被使用一次。它还有其他一些缺点：

比特币并不是一种非同质通证，而是同质化通证。对它来说没有必要让每个 UTXO 独一无二。

UTXO 是一次性的，当存储大量 UTXO 交易是对计算资源和硬盘空间的浪费。

二、 余额模型（Balance-Based）

余额模型就像银行的做法。你可以在银行创建一个账户，然后在账户里存钱。银行更改你账户里的余额。它与 UTXO 做法完全不同。它比 UTXO 更高效因为它只用更改数据库里的一个数字。显然余额模型并不适合非同质通证。

安全性

着眼于通证相关的功能，everiToken 简化了很多不必要的抽象，不仅大大提高了效率，而且具有显著的安全性能。虽然 everiToken 中的通证种类很丰富，理论上可以是无穷多，但统一的通证结构使得系统或者任何第三方机构可以按照相容的原则来对他们进行审计。可以认为，系统只用识别一种形式的智能合约从而避免了复杂的审计和相应的安全问题。

签名器（everiSigner）

everiSigner 是一款离线签名工具，整个签名过程都是在插件中完成的所以用户的私钥不会暴露出来。网站通过创建一条新的信道来保障安全，网站将需要签名的内容传入该信道，然后 everiSigner 返回给已经签过名的数据。

私钥遗失

基于权限管理机制，第三方可以提供很多服务，比如通证找回。公司 C 专门提供密码保护服务，Alice 担心自己遗失了私钥可能会失去自己的通证，她可以通过设置转移权限为所有者组权重 1，组 C 权重 1，并且设置转移阈值为 1 的方式.在这种情况下，即使 Alice 遗失了自己的私钥无法自己完成通证转移的授权，她仍

然可以通过向公司 C 证明自己 Alice 的身份（通过身份证或指纹等）来让公司 C 提供授权，这样 Alice 可以通过把通证转移到一个新的账户上避免失去自己的通证。

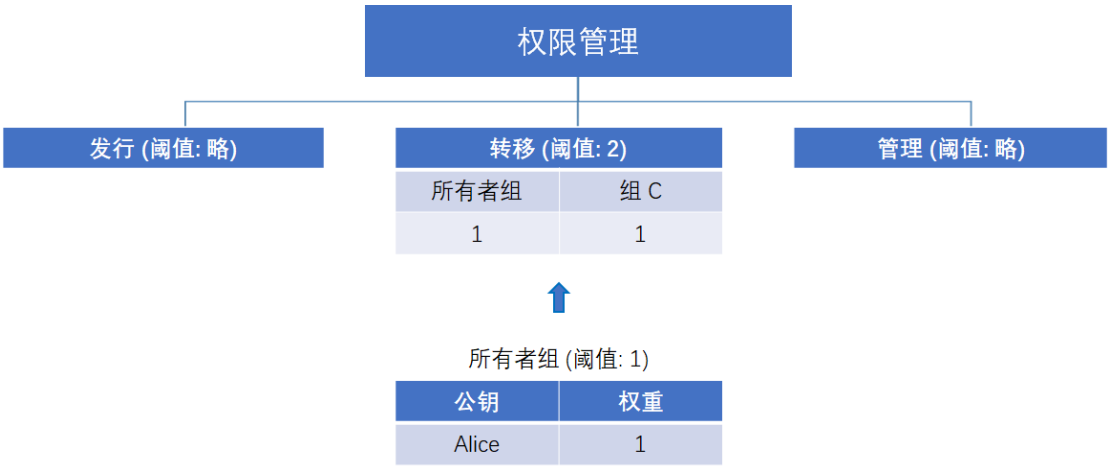


图 4 公司 C 提供通证找回服务

当然，公司 C 可能会作恶从而偷走 Alice 的通证，但是所有的操作都会被记录在链上，无法篡改无法抵赖。一旦被发现，公司 C 将会彻底失去信誉。

共识

everiToken 使用 BFT-DPOS 作为其共识算法。DPOS 已经被证明能够满足区块链应用的要求。在这一算法下，所有持有 EVT 通证的人可以通过连续的投票系统来选择生产区块的节点。任何人都可以参与区块生产，只要他能够说服通证持有者投票给他。

everiToken 每 0.5s 生成一个区块，并且同一时间只有一个生产者被授权产生区块。如果该区块没有按时产生，则跳过这一时间段的块。当一个或多个区块被跳过时，区块链上可能存在 0.5 秒或更多秒的空隙。

在 everiToken 系统中，每 180 个块是一个轮次（每个块生成 12 个，有 15 个生

产者)。在每一轮开始时，15 个独特的区块生产者会被 EVT 通证持有者投票选出。这些被选中的生产者按照 11 个或更多生产者同意的顺序进行出块。

如果一个生产者错过了一个块，并且在过去的 24 小时内没有生产任何块，它会被移出生产者直到它向区块链表达再次出块的意愿。通过最小化不可靠生产者漏块的数量来保证网络运行的流畅性。

拜占庭容错算法允许所有的生产者来签署所有的块，只要没有生产者用同一个时间戳或块高度来签署两个不同的块。一旦有超过 11 个生产者签署了一个块，这个块就被验证通过并且不可逆转。任何拜占庭生产者签署了两个相同时间戳的块或者相同高度的块都将成为他们作恶的密码学证据。在这个模型下，一个不可逆共识可以在 1 秒内达成。

其他技术细节

基础链

我们并不想重新造轮子。因此我们吸收了现有公有链中优秀的部分，以达到青出于蓝的目的。我们采用了 EOS 的基础框架作为代码基础，因为我们认为 EOS 是目前设计最好，最先进的区块链平台之一，并且 EOS 具有非常优秀的代码结构。在此基础上，我们自主开发了所有针对通证流转的功能，并进行优化。同时，针对基于通证的特点，我们对 EOS 的数据结构进行了优化以获得更好的性能。

采用 EOS 的基础框架有许多好处：

1. EOS 具有完整的受过良好测试的基础框架。DPOS 以及其他核心机制已经在 BitShare 等项目完整测试过了。
2. 重用基础框架的部分可以大大减少不必要的工作量，使得我们有更多的精力

放在优化通证相关的操作上。

3. 在这个过程中，对 EOS 基础架构的改进也会上传到 EOS 的 Github 上，符合开源社区的精神。

在 EOS 中有两种形式的区块链操作（actions）。一种是原生代码，即用 c++编写的代码，可以直接编译成二进制文件。另一种是用 Web Assembly 执行，需要由先由 JIT 编译。我们移除了后一种模式，全部采用原生代码实现。

授权操作

everiToken 的授权操作主要包括多重签名、权重计算、阈值设置等。由于每个通证是相互独立的，通证的转移可以并行的执行（这里指非同质通证，不同符号的同质通证也是可以并行执行的）。此外，由于每个组的许可彼此独立，也可以在不同的组之间并行执行发行和管理的操作。

每一个操作都是由数据包加签名列表的结构组成。在授权验证时，我们只需要验证每一个签名，由于签名之间没有任何关系，因此也可以并行执行。

执行引擎

在 everiToken 系统中，每一个通证操作都是完全独立的，所以并行执行并不需要额外的分区负担。另外，由于通证操作的种类有限，并且所有代码都是原生在链上的，只要这些操作经过了反复的测试，系统就可以确保完全稳定。

每一个区块的生产过程可以分为三个阶段：准备阶段，转移阶段和结束阶段。在创建新的域或者发行通证时，系统会在准备阶段进行处理，以确保操作的正确性。然后我们对通证的变更和分发操作进行并行处理，以获取更好的性能。最后我们

在结束阶段关注异常处理，以保障系统的稳定性。

挂起交易

一个挂起交易是指它会在一些延迟之后完成。通常非挂起交易会一次完成，并且在提交交易时所有条件都必须满足，比如说所有的签名者必须一起签名。但是在实际情况中，很多交易是分阶段完成的。例如一个交易的参与者可能不能同时完成签名，挂起交易允许签名者一步一步地完成签名，知道最终交易成功进行。

EvtLink/everiPass/everiPay

everiPay/everiPass

everiPay/everiPass 是针对面对面小额支付而诞生的使用 everiToken 公链的支付方式。

EvtLink 包含二维码生成标准和通讯协议的定义。

以下是 EvtLink/everiPass/everiPay 的亮点：

- 即时结算：一笔交易就是一次结算。
- 去中心化：点对点的支付，没有中心化平台，没人可以篡改链上数据，每个人都可以参与到定价中来。
- 最安全：链上数据和内容无法伪造，最大限度保护用户的财产安全。
- 最方便：即使没有连接到物联网，你也能够完成交易。付款方并不需要手动输入交易的金额。首付款双方都会在交易成功后立即收到通知。
- 可扩展性：everiPay/everPass 支持所有 everiToken 上的通证，不仅是货币，还包括代币和积分等，也可以是一把开门的钥匙。并且你几乎可以在任何地

方使用，只需要带上手机。

- 快速：everiToken 具有很高的 TPS，我们认为在考虑到网络延迟的情况下一笔交易可以在 1 到 3 秒内完成确认。
- 标准化：与钱包方面的技术不同，EvtLink 是直接针对整个生态系统的跨链跨钱包跨应用标准，你可以使用任何应用来创建和解析它。

基于以上七个特点，everiPay/everiPass 可以提供最安全，最方便，最友好的面对面支付体验。

对于 everiPay/everiPass 来说，收款方必须要使用支持解析 EvtLink 并且上传交易到 everiToken 的应用。我们提供易于使用的 API 和样例代码会使这个过程变得非常简单。这类似于添加支付宝支付或者微信支付到你的商店中，甚至更加简单。

付款码

付款码无法支持 everiPay 的一些功能，例如付款码要求付款人必须连接到互联网，并且收付款人都必须手动输入金额，当交易完成时，他们也不会自动收到通知。

然而，收款人不需要使用支持这种支付方式的应用程序。实际上，收款人需要做的只是用手机上的钱包来检查是否收到了付款人的钱，它适用于一些小型商店或者个人。

使用 everiPay 来代替付款码支付对任何人来说都是被推荐的。

EvtLink 技术细节

EvtLink 是用于执行 everiPass/everiPay 的二维码格式。everiToken 公链使用

everiPass 操作和 everiPay 操作来执行 EvtLink 交易，我们使用名为 evt_link 的结构体来表示 EvtLink.

这是通过 everiPay/everiPass 执行支付操作的技术步骤：

1. 付款人选择一种要使用的通证，钱包会生成一系列动态二维码，包括唯一的 128 位 LinkID，付款人签名，和付款人选择的通证符号。注意，LinkID 在二维码变换的过程中不会改变，除非相关的交易被执行了。否则的话，会有重复支付的风险。链不允许两个 EvtLink 操作拥有相同的 LinkID。
2. 然后，付款人钱包通过调用名为 get_trx_id_for_link_id 的 API 来查询与该 LinkID 相关的交易 ID，直到返回一个有效的交易 ID。之后钱包会在下一次展示二维码时更改 LinkID 的值，之后钱包应该通过查询交易 ID 来显示交易结果。付款人的钱包不需要直接发送交易。
3. 同时，收款人使用手机、扫描仪或者智能网关扫描二维码。在 EvtLink 被扫描和解析后，它应该被打包在一个交易中然后上传上链。之后，所有链节点将会同步结果，因此 get_trx_id_for_link_id 将返回交易 ID，而不是 404。

Base42 编码

Base42 是一种二进制到字符串转换的编码。它类似于十六进制编码，但是使用 42 作为基数，相应地使用不同的字母表。字母表中的字符与二维码中的字符相同，因此将 Base42 编码的字符串编码为二维码是有效的。因此，二维码的大小可以做到更小。

在 everiToken，Base42 被用于编码 EvtLink 的内容。

经济模型

燃料 EVT

为了避免 DDos 攻击等恶意行为，也为了给 DPOS 共识机制提供权益证明，同时可以奖励区块生产者提供的资源。我们将会发行 EVT 作为系统的燃料。任何操作都会消耗一定数量的 EVT 作为服务费，同时作为奖励给区块生产者。EVT 的收取费用会自动浮动，收费的目的是防止恶意攻击，不会影响到用户的正常使用。

EVT 的发行与转移方式与主流区块链加密货币类似。EVT 仅仅用于防止恶意攻击和奖励区块生产者提供的资源，不具有其他价值。everiToken 的十亿枚 EVT 将分为三个部分：

一亿五千万 EVT（15%）将会留给核心团队。

四亿 EVT（40%）将会提供给社区贡献者。

四亿五千万 EVT（45%）将作为公私募的部分。

everiToken 上所有的服务都会按照下列公式收费：

$$ServiceFuelCost = FuelUsed \times R$$

在这个公式中，FuelUsed 是指调用某个具体的操作所需要的价格，单位是 EVT。R 代表调整系数。区块生产节点可以在任何时候独立地决定调整系数例如链上资源紧张或者遭到攻击。如果 EVT 的价格太高，15 个区块生产节点也会降低 R。R 的实际取值是 15 个区块生产节点投票的中位数。

当用户希望执行操作时可以先假定 R 的值是 1.如果 R 的值没有改变，操作将会完成，如果 R 的值发生了变化，操作会提示失败，从节点处得到新的 R 值后，用户可以再次尝试执行操作。

举例来说，如果创建一个账户的费用是 2EVT，通常一个用户创建账户就会花费 2EVT，如果 R 被提高到了 1.1，创建账户的费用就会变成 2.2EVT。

我们采用中位数的方式来确定 R 的值，如果三个生产者提议 R 为 1.15，五个生产者提议 R 为 1.2，两个提议为 1.1，两个提议为 1.3。1,1.4 和 1.45 各有一个提议。那么最终 R 的值会确定为 1.2。

绑定 EVT（Pinned EVT）

一个绑定 EVT 就是一个无法转移的 EVT。它只能用来支付手续费。用户可以把 EVT 转成绑定 EVT，转换系数固定为 1。绑定 EVT 不是货币，它可以安全地空投给需要使用它的用户。

一般来说，普通用户并不需要把 EVT 转换成绑定 EVT，因为他们可以直接支付 EVT 作为燃料费。一旦你把 EVT 转换成绑定 EVT，系统就会自动把绑定 EVT 绑定到接收者的账户上。

绑定 EVT 不能再次转移，因此公司和组织可以通过转换 EVT 给一些特定账户，一旦转换完成，这些绑定 EVT 就不能再次转移了。

一个付款者（Payer）是支付一次交易手续费的账户。everiToken 允许用户指定一个付款者来帮助他支付交易费用，这个功能在创建账户时很有用。

每一个域都有一个特殊的绑定 EVT 余额。在转移或销毁一个域的通证时会优先使用该域的绑定 EVT 余额。用户能够把自己的 EVT 转成一个域的绑定 EVT 余额。

EVT 的增发

我们按照下列公式每年增发一部分 EVT

$$R = \begin{cases} 0.05 - 0.005 \times Y \ (0 \leq Y \leq 5) \\ 0.02 \ (6 \leq Y) \end{cases}$$

Y 表示当前时间距离主网上线的时间。Y 是从 0 开始计算的。

每年增发的 EVT 总量等于 R * 当前 EVT 总数。

其他信息

区块生产节点

节点数：15

与 EOS 不同，因为节点太多意味着开销越大。我们希望把更多的 EVT 留给社区，

而不是节点。

15 个节点已经足够去中心化了。

公证公司

everiToken 只知道通证的名字，通证的价值是由公证公司背书的。这些公证公司

可以通过加上自己的签名在通证的发行过程里，这样每个人都可以相信这些通证，

如果这些通证有值得信赖的公司签名。就像是 SSL 数字证书。

生态

工具

everiSigner 签名器

everiSigner 是一个开源的插件，它允许用户在浏览器中运行 everiToken 的应用。

everiSigner 包括一个安全的标识库以及用户界面来管理不同站点上的身份并验

证区块链交易。它存储用户的私钥，并且是与 EVT、ETH 和 EOS 的相关插件兼容。

everiWallet

就像它的名字，everiWallet 是基于 everiSigner 的 everiToken 钱包。请访问这里以获取更多信息。https://www.everiwallet.com/

EVTJS

EVTJS 是基于 JavaScript 的 everiToken 接口库，同时支持 NodeJS 和浏览器。它也支持 everiSigner，所以你可以轻松地使用这个库来开发 everiToken 上的网络应用。更多信息请访问 https://www.github.com/everitoken/evtjs

evtScan

evtScan 是 everiToken 的区块链浏览器。任何人都可以查询 everiToken 测试网（将来可以查询主网）每一个区块的具体信息。包括交易、账户、组和域等等。对开发者来说，evtScan 是一个高效的工具用于确认信息是否上链了。对于用户来说，它提供了一种验证交易是否执行的方法。更多信息请访问 https://evtscan.io/

应用场景

在通证经济网络中，区块链上记录通证发行，交易确认，记账对账和清算等。通证经济网络中，包括通证发行方、通证交易方、交易所、流通渠道、公证平台等各个上下游机构，可以按照自身角色借助 everiToken 公链开展业务。

链上只记录通证相关的核心内容，因其不可篡改的特性，作恶成本巨大从而解决信任问题；原生支持模块化功能，满足大部分通证经济需求，因而更快更好用。短期内，everiToken 选择以下三个应用场景作为切入点，易于合作与落地。

优惠券（Coupons）

everiToken 正与北美购房网（www.beimeigoufang.com）合作以支持他们的优惠券体系。

具体方式如下：北美购房网会开发一个平台（web 端），其子用户可以在平台上发行各种包含北美购房网签名的优惠券（使用 everisigner），平台同时提供交易优惠券的功能。通过我们提供的接口，优惠券 Token 的发行、转移和管理（包括核销）是在链上的，但子用户和最终用户都可以直接在 web 端进行操作。各种优惠券 token 的发行记录都可以在 everiscan 上查到，因此超发多发可能性很低。由于优惠券的实用价值，例如最初发行时标价为 100 美元一张，但是如果购买对应的房子可以抵消 1000 美元，又由于 Token 化之后方便快速的流通，不论是北美购房网还是其子用户，或者最终需要购买房子的用户，都可以从中受益。

游戏协议（Gaming Protocol）

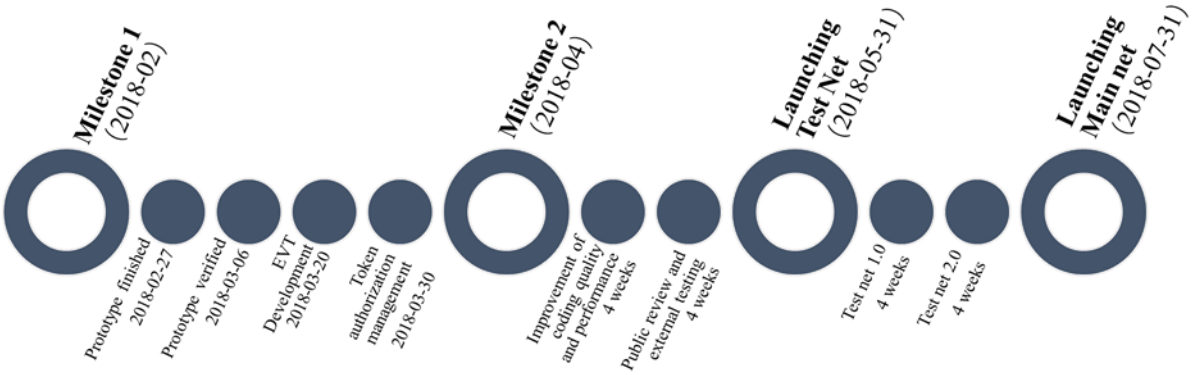
everiToken 正在与 FastX 合作。

FastX 针对以太网上拥堵速度慢的问题，为基于以太坊的游戏提供这样一种协议，用户可以将游戏数据通过一个智能合约把数据状态锁定到智能合约上，同时在 FastX 将在子链上生成相同的游戏数据，数据的变化在子链上进行，定期与主链

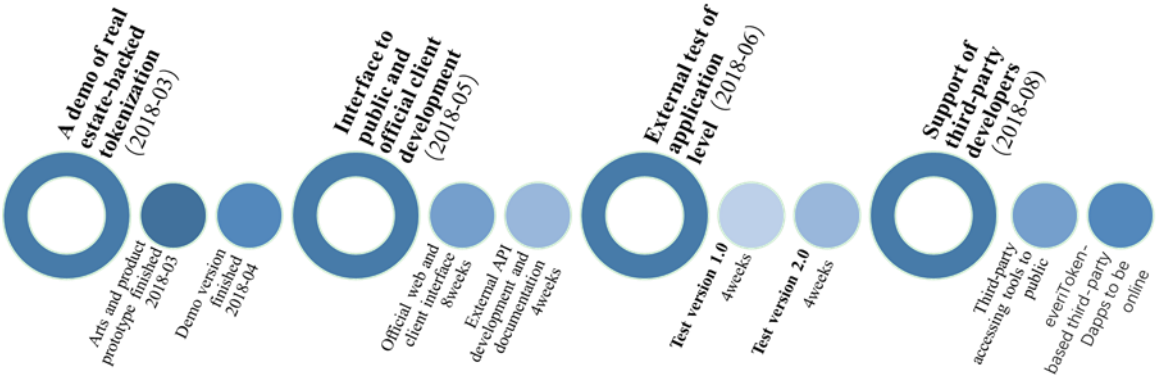
交互完成状态变更（借助 merkel 树可以快速审查）。everiToken 因其安全方便的 Token 转移与管理等特点可以作为这些游戏协议的子链，即游戏数据的变化等在 everiToken 链上进行。其实对于大部分游戏而言，所有游戏内容上链是没有意义的，链上只需记录最为重要的通证部分，大部分逻辑完全可以由链下去完成。

时间表

公链开发时间表



应用落地时间表



结论

通证经济时代即将来临，然而以太坊或 EOS 的智能合约并非适合 Token 经济时

代的可行路线。

everiToken 通过基于以通证为中心的核心思路，基于区块链技术构建了一个便于通证发行、流转、验证的特化系统。该系统牺牲部分图灵完备性，但也因此降低了系统内抽象层次，提高了速度、安全性、互通性、稳定性、可监管性，可获得更为高效的执行能力，让世界每个人都可以理解、创造、交互，真正万物价值互通。

同时，作为数字世界和现实世界的媒介，everiToken 立志于将区块链技术服务更广泛的现实需求，用于解决现实世界的痛点问题，让任何人都可以享受到技术带来的便利，进而提高整个社会运转的效率，降低信任的成本，让区块链技术回归本源。

团队成员

蔡恒进 教授 首席科学家

武汉大学教授、博士生导师。发表学术论文 80 余篇，主要著作《机器崛起前传——自我意识与人类智慧的开端》获得 2017 年吴文俊人工智能科学技术奖。2005 年应武汉大学邀请回国，任国际软件学院教授、博士生导师，主要从事服务科学、人工智能、金融信息工程等领域的研究和教学工作。2011 年入选武汉市第一批「黄鹤英才计划」，2012 年武汉大学「杰出教学贡献校长奖」获得者。

Brady 罗骁 CEO

罗骁是坚定的全球区块链技术通证经济信仰者。北京航空航天大学通信工程学士，美国 Brandeis University 金融研究生，英国牛津大学 Said 商学院区块链战略课

程。连续创业者，曾当选第三批上海千人计划（创业组）。工作经历包含美国纽约 Oppenheimer Funds 另类资产投资部（CDO 为主的资产证券化产品） 以及日本最大的金融集团三菱 UFJ 证券（东京总部及上海）。

陈柏臻 COO

英国阿斯顿大学工商管理学士，电商服务、服装供应链 B2B 服务、社交短视频、政府电商项目连续创业者。拥有丰富的社会资本与政府项目运作经验，执行、沟通、公关能力强。任互联网大会永久举办地-桐乡市的电子商务公共服务中心、青年互联网创业服务中心主任，曾获全国农村青年致富带头人、最美浙江人-2017 青春领袖等称号。

程希冀 CPO

武汉大学软件工程学士，全栈开发工程师、系统架构师、连续创业者。小学即开始编程，具有十多年开发经验、丰富的创业经历、团队管理和产品设计经验。曾获全国信息学奥林匹克联赛一等奖。职业经历包括腾讯科技（深圳）和两个创业公司 CTO、联合创始人等。

王昊 CTO

武汉大学软件工程硕士，系统开发工程师，曾在天风证券上海自营分公司任职，后作为技术合伙人参与创办私募，负责量化交易系统开发工作，拥有十多年的系统开发经验。