everiToken

技术白皮书

版本 3.1

© 2019, everiToken 公链

瑞士，楚格

everiToken

更新于 2019 年 3 月 25 日

声明

- 本 everiToken 技术白皮书仅供参考。
- 本白皮书不代表任何明示或暗示的保证、证明、预期等。
- 本白皮书中编写的技术规范或技术实现方法可能会随着时间的推移而变化。
- 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。项目团队或其任何成员都不对将来使用此内容所产生的任何结果负责。
- 本白皮书中所述 Token 不具有任何实际价值，只在虚拟世界中使用，唯一目的是确认 Token 的用户权限。
- 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。
- 本技术白皮书中包含的所有内容可在非商业用途的前提下使用，但不得以任何方式修改或更改本技术白皮书。我们对使用本内容产生的任何影响不承担任何责任。

everiToken

目录

背景和愿景

通证（Token）经济到来

到 2019 年二月，区块链技术问世已逾十年。尽管其在此期间不断演变，一个核心问题仍然存在：区块链技术是否真的是一种革新从而为全球经济创造了价值？

让我们看看目前的数据，区块链管理的资产（称为“链上资产”）基本上是各种代币或数字货币，总市值大约 1500 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，人们一直想让这些代币成为一种支付货币，但到目前为止，它们主要作为数字货币使用，并没有发挥传统货币的作用。数字货币与其说是指它们发挥货币的功能，不如说只是一个符号。

一方面，发行货币是一种政治实现，货币权力必须属于国家。因此，加密货币很难取代法定货币。没有国家的授权和支持，所谓“数字货币”只是一种理想主义的追求。

另一方面，大多数全球主流资产（有形和无形）并不在区块链上（称为“链外”），区块链与链外资产之间的互动有限。

那么，通证只能是数字货币吗？当然不是！通证的基本含义是“符号，象征”，但它更应该被视为凭证而不是数字货币。这些凭证可以代表各种权利和利益，包括购物积分、优惠券、身份证、文凭、房地产、通行证、活动门票和各种权利和利益证明。回顾历史，权益证明是人类社会各文明的重要组成部分。账目、所有权、资格、证明等都是权益的代表。正如尤瓦尔·赫拉利在《人类简史》中所说，“正是这些‘虚构的事实’才是智者脱颖而出和建设人类文明的核心原因。”如果这些权益证明都是以数字、电子和密码学保护来验证其真实性和完整性的，那么人类文明将会有革命性的革新。我们称其为**通证经济**（Token Economy）。

在区块链上运行通证提供了坚实的信任基础和可追溯性，这是任何传统中心化基础设施所做不到的。因此，如果通证是通证经济的前端经济单元，那么区块

链就是通证经济的后端技术，二者是整体联系、相互依存的。

竞争分析

everiToken 是为通证经济而生的公链，目前有两个主要竞争对手：以太坊和 EOS。当我们分析市场中的优势、劣势、机会和威胁时，我们的竞争优势就会变得明显。

优势与劣势

everiToken 认为，通证经济的区块链技术应该有效管理权益证明，主要涉及以下三个方面：

1. **数字权益证明**：证书必须是一种可靠的数字权益形式，必须有内在和内在价值（有形或无形）的支持。
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，我们提出了一套满足通证经济基本需求的解决方案，以促进通证的流通和管理，为通证经济打下技术基础。具体来说，根据上述要求，我们实现了以下三个主要特点：

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**：拥有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

通过以太坊来满足通证经济的需求，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（FT，Fungible Token），ERC721 协议支持非同质化 Token（NFT，Non-Fungible 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。因为它们的复杂性，导致了安全和监管方面的担忧，同时也阻碍了大规模应用。
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是不可交换的，因此是孤立的。这不利于通证经济的生态发展，而且用户不能统一查询自己拥有的的各类不同通证资产。

EOS

EOS 在 2018 年六月份上线了主网。EOS 的主要目标是通过建立新的解决方案来解决以太坊遇到的问题。然而这带来了一些列全新的问题：

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。但是，基于智能合约的开发受限于开发者的熟练程度，很难确保所有类型的通证开发者都具有足够的安全意识。

   EOS 的智能合约基于 Web Assembly，这是一个相对较新的语言，仍处于测试阶段。此外，EOS 的智能合约代码图灵完备，权限过大，易受无意中出现的安全漏洞的影响。

   大多数人不能写安全的智能合约，为了发行和转移通证，用户必须依赖第三方应用，并且必须信赖第三方代码的质量。因此，资产的控制权并不在用户自己手上，而是由第三方来控制。
2. **非标准化**：与以太坊一样，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，缺乏一致性。然而，智能合

约的开发和测试需要时间，这使得在短时间内难以解决不同市场的需求。这将成为发展通证经济的阻碍。

everiToken 和其他公链相比的主要区别在于 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。然而，everiToken 能够满足通证经济中 99%的需求，并且 everiToken 是全世界所有人最安全、最具成本效益和用户友好的公有链。

机会和风险

凭借 everiToken 的优势，我们创建了 EvtLink 标准，用于通过各种数据渠道（包括 NFC，蓝牙和二维码）连接付款人和收款人。基于 EvtLink，everiPay 是一种基于 everiToken 公有链作为核心基础设施，everiPass 作为其通证所有权验证协议的面对面小额支付协议。

everiPay/everiPass 包括二维码生成标准和通信协议定义。通过我们的创新，我们获得了令人印象深刻的功能特性：

- **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**：区块链中的数据和内容无法被伪造或篡改，从而最大限度地保护用户的资产安全。
- **可扩展性**：everiPay/everiPass 支持 everiToken 支持的所有 Tokens，以及货币、积分，甚至是开门的钥匙。你几乎可以在任何地方使用它，只需要一部手机。
- **最方便**：即使你没有连接到互联网，你也可以完成交易。

基于以上五个特点，everiPay/everiPass 可以为面对面支付和通证所有权提供世界上最安全、最方便、最人性化的服务。

小结

一些威胁仍然存在。如前所述，以太坊和 EOS 可以成为通证经济中满足特定需求的大型公有链。然而，以太坊/EOS 最大的问题是智能合约的性质对用户造成的高进入壁垒。随着安全合约的发展，我们已经解决了这个问题，everiToken 现在准备为所有人支持全球通证经济。

基于以上分析，我们设计了一个完全适合大多数区块链应用的新概念，并提出了一条新的公链 everiToken 及其生态，以促进通证经济的发展。现实世界中

的资产、证书和凭证可以通过发行通证实现数字化，并且能以前所未有的安全性、速度和网络兼容性给每个人轻松使用。

技术创新

安全合约（Safe Contract）

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，智能合约往往无法提供足够的信任，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，安全合约可以增加可行性与 TPS。对于前者，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。对于后者，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。（主网 TPS 实测已达 10000tps：2018 年 12 月）

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，如果程序崩溃或重新启动，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，但提供了比 LevelDB 更好的性能和更丰富的功

能。它还允许对低延迟的情况（如闪存或者固态硬盘）进行优化。

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，代码是固定的，并删除了不必要的信息。与通用系统（EOS）相比，数据冗余度非常低，这也减少了区块的大小。

通证模型

概览

为通证经济而生，everiToken 有其独一无二的 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，FTs）和非同质通证（Non-Fungible Tokens，NFTs）。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。没有两块完全一致的石头。同样的，石头之间不能被简单地拼起来，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，正如非同质通证在我们系统中一样。

总的来说，非同质通证可以根据它们不同的价值属性分为不同的类型。我们可以把相似类型的非同质通证归纳成一个域（domain）。

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。

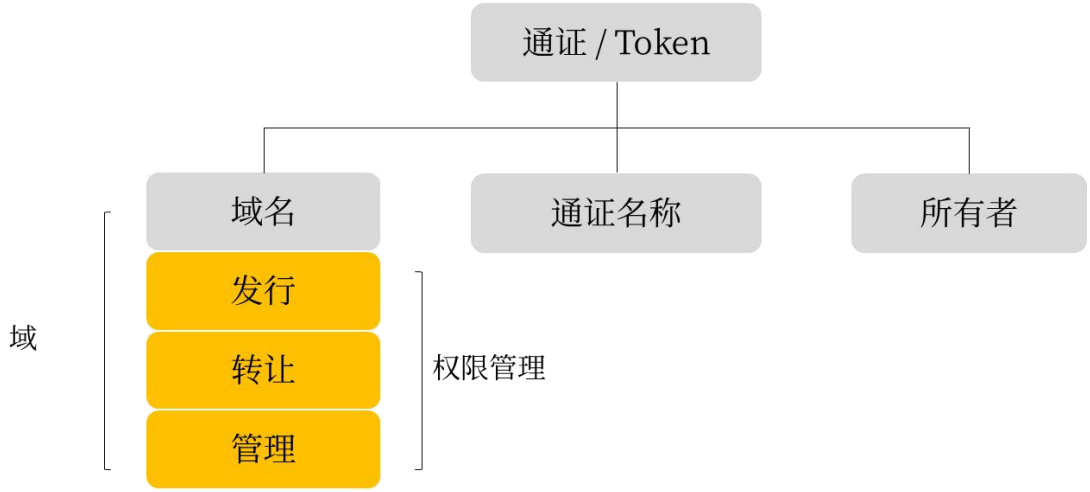


图 1. everiToken 通证基本结构

域的详细内容由域名来对应，每一个域展示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。

对非同质通证而言，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群组（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（Authorization Management）

everiToken 系统中关于权限管理有三种权限类型，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）

参与者分为三类，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所需阈值时，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。

通证的所有者有一个固定名为 owner 的特殊组名，它表示通证所有者的集合。它是动态且特别的，因为它总是指向当前通证的实际所有者，组的授权条件是组内的每个人都同意（即，组中的每个成员权重为 1，组的阈值为组中成员数）。

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：

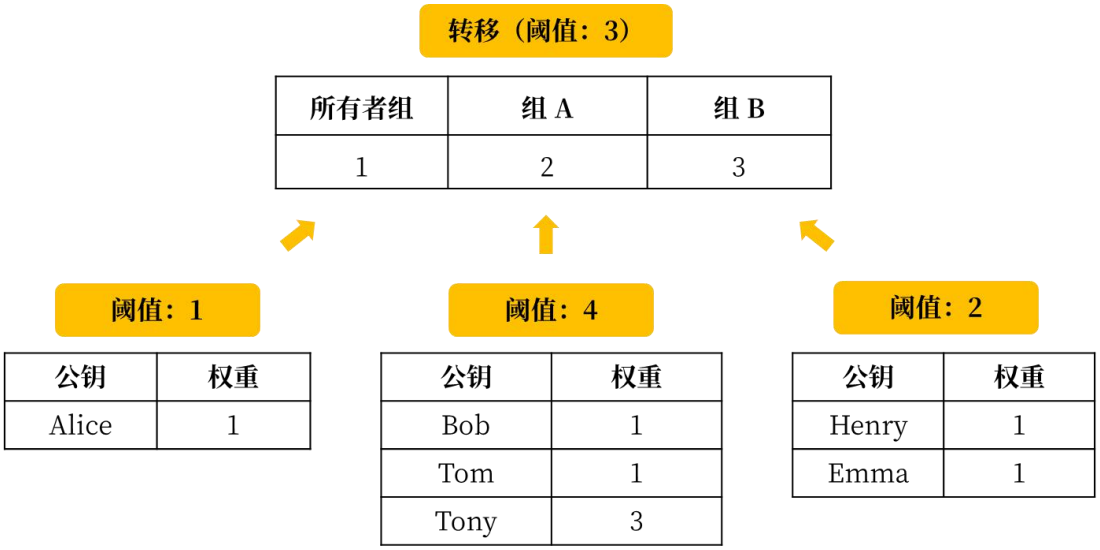


图 2 转移权限示例

图 2 描述了一个域的转移权限。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 必须要 Henry 和 Emma 共同授权才行。

任何用户都有权力发行通证，但是各个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（加起来权重达到 3 满足阈值），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 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

发行

任何人都可以在注册一个符号（例如“EVT”）之后发行同质化通证。用户可以设置流通总数，然后用户可以决定他们想要立即发行的数量。

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相关符号的同质化通证。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），它可以用于通证交易所中。

Token-Based 记账模型

概览

everiToken 使用 Token-Based 记账模型来处理系统中的所有通证。

简而言之，对于基于通证账本中的所有通证，我们创建独立的数据空间来存储通证所有者的完整记录。这样会很容易地进行切分并且多核运行，因为各个通证的数据空间互不相干。因此，系统可以轻松地以并行方式执行各种通证相关的操作而不会产生冲突。这使得系统具有非常优越的性能，并且我们可以通过分片或是增加更多 CPU 核心来不断提高系统的 TPS。

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上。

对一个基于 Token-Based 记账模型的区块链——比如 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）。

通证数据库是针对各种基于通证的操作，存储和管理所有非同质通证的数据空间。而区块数据库用于存储原始区块数据。

通证数据库和区块数据库都应该是一个多版本的数据库，以便在区块反转时快速回滚。everiToken 使用 Rocks DB 作为通证数据库的底层数据库系统。

通证数据库和区块数据库都是仅追加（Append-only）的数据库。因此，每当一条新纪录更新时，新版本会把增加的新值添加到数据库中。但是，包含旧版本的记录不会被删除。

通证数据库

通证数据库是一个带有索引的数据库，用于快速查找和更改区块链的最新状态，例如通证所有者或者一个账户的同质通证余额。

通证数据库可以看做一个**键值对**（Key-Value Pair）数据库。键表示通证的 ID，值表示通证当前的所有者。由于数据库是仅追加的，所以每个键都有许多值，但只有最新的值代表通证当前的所有者，其他值只用于历史引用或回滚。对于每个通证，都有一个独立的数据空间，包括其所有的所有者历史，就像一条单独的链。

这条链的初始值是其最初的所有者。举例来说，当执行一个操作时，新的所有者会被添加到数据库中，如果需要反转块并最终进行垃圾收集，则可以使用旧

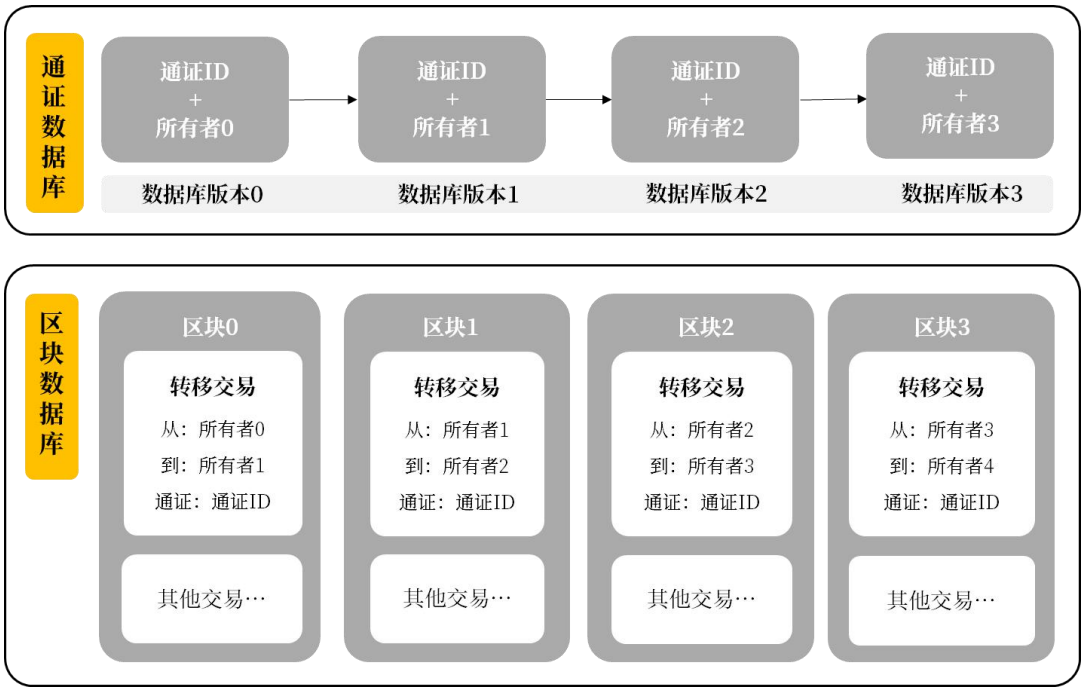
版本数据进行回滚。

因为每个通证都有独立的数据空间，所以分片变得非常容易。例如，如果一个节点由两台计算机组成，我们可以让每台计算机处理一半的通证。如果有 100 个通证需要处理，第一台计算机将处理 1-50 号通证，第二台计算机处理 51-100 号通证。因为更改一个通证的所有者并不会影响其他通证，所以两台计算机可以并行处理。

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，块上的签名和其他附加信息。

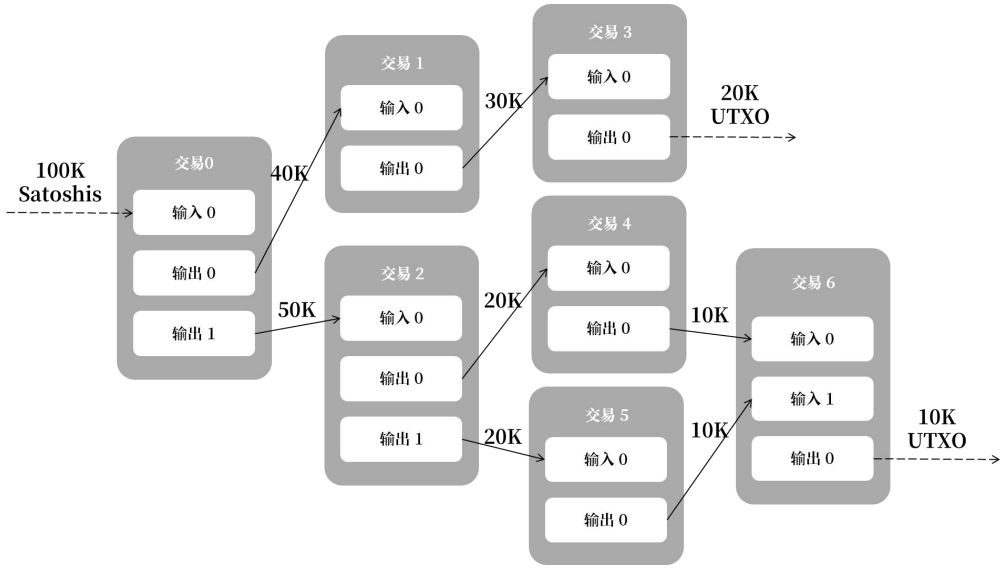
这张图片展示了两种数据库是如何一起为非同质通证工作的：



记账模型的比较

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。



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。（everiToken 支持所有的非同质通证和同质通证）

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、 账户模型（Account-Based）

账户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新数据库中的余额，而不需要创建新的 UTXO。因此 UTXO 模型并不适合非同质通证。

此外，账户模型并不适合分片，因为在向他人转账时，需要这样两个步骤：第一步修改原来持有者的账户，第二步是修改新持有者的账户。出于安全原因，你必须对这两个步骤进行原子操作，但在分片环境中，这很困难并且性能也很差。但是，在 Token-Based 模型中，只有一个步骤，即增加通证新的所有者。

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。

everiToken 核心代码库的安全性

截止 2019 年春季，everiToken 已经引入了四个组织来审查 everiToken 公链的所有核心代码，包括 Hacken-Proof、长亭等。进行了静态与动态分析。

由于 everiToken 使用的是安全合约，一旦我们的核心代码库被证明是安全的，那么基于 everiToken 的所有合约同样被证明是安全的。

签名器（everiSigner）的安全性

everiSigner 是一款离线签名工具（浏览器插件），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。

私钥遗失与找回

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。假设公司 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。

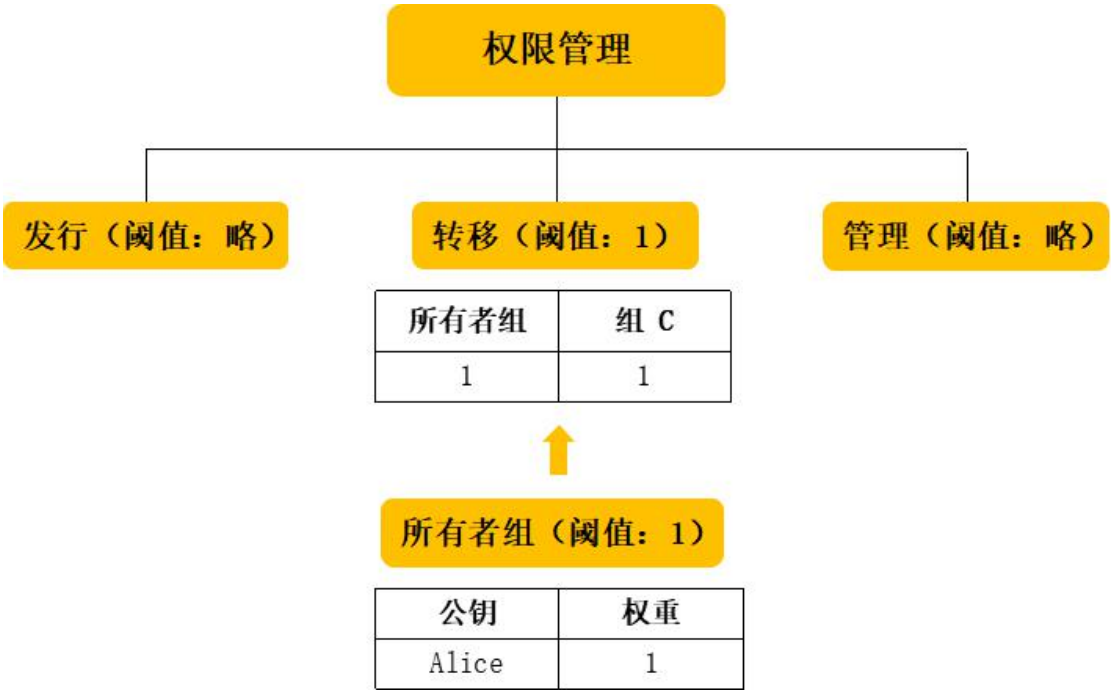


图 4 公司 C 提供通证找回服务

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。

共识算法

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 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。

everiToken 公链的出块节点是动态的。在最初我们设定为 15 个出块节点。之后这个数字将由*去中心化链上治理委员会*决定。为了方便起见，我们在本白皮书中假定使用 15 个出块节点。

在 everiToken 系统中，每 180 个块是一个轮次（每个块生成 12 个，有 15 个出块节点）。在每一轮开始时，15 个独特的出块节点会被 EVT 通证持有者投票选出。这些被选中的出块节点按照 11 个或更多出块节点同意的顺序进行出块。

如果一个出块节点错过了一个块，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。通过最小化不可靠出块节点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出块节点来签署所有的块，只要没有出块节点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 个出块节点签署了一个块，这个块就被验证通过并且不可逆转。任何拜占庭出块节点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。

分红设计（Bonus Design）

分红机制是在 2019 年 2 月发布的 everiToken3.0 中添加的新机制。这是一个强大、灵活、方便的机制，可以与现有的功能相结合。它的主要目的是根据一套规则将利润分配给利益相关者或股东。现在根据盈利方式的不同支持两种类型的分红：被动分红和主动分红。

被动分红是指，在一种同质通证的每笔交易中收取利润。因此，如果一个同质通证的管理者决定为其设定被动分红，那么在每一笔交易中，不仅将收取 EVT 作为燃料费，还将收取额外的分红费用。

在一次交易中，有几个选项可以控制实际费用。最主要的选项是交易比例（Transaction Rate）。一笔交易的实际费用就是这个交易比例乘上交易金额。我们还有最低和门槛等选项来控制最终费用的上限和下限。这样就避免了高价值交易出现无法控制的巨大成本。

同质通证的管理者可以决定如何收取手续费，例如由哪一方负责支付手续费，或者额外附加费用的方法。一种方法类似于信用卡，付款人支付金额为 n，但是收款人收到的金额少于 n，因为费用会从初始金额中减去。第二种方法更像传统的银行交易，如果想要将金额 n 转移到另一个账号，则需要在金额 n 的基础上支付额外的交易费用。

至于主动分红，它是手动发放的，类似于股票红利。由同质通证的管理者决定多少奖金用于分红。

无论是主动分红还是被动分红，它都有一套分配规则。当前有三种有效的规则：固定，百分比，和剩余百分比。固定规则是指为接收者提供担保的固定份额，百分比规则是指用百分比乘上奖金总额来计算。剩余百分比规则与前两个规则不同，将使用剩余金额乘上百分比。

对于每个规则，我们还需要分配它的接收者。接收者并不仅限于一个地址，也可以是一类同质通证的持有人，每个持有人可以根据其同质通证的额度与流通总量的比例来获得分红。此外，能参与分红的股东并不局限于用于盈利的同质通证，而是包括在 everiToken 上登记注册的所有同质通证都可以参与分红。因此，有可能只会发行一种奖金通证用于进行利润分配，这将从 everiToken 提供的透明度、公平性和流动性中受益。

在实施过程中，当接收者有多个地址时，需要对所有股东地址的余额进行快照。这将需要更多的存储空间，因为每个股东地址需要占据 34 个字节。我们已经高度优化了这种情形，在大多数情况下，每个地址只需要 4 个字节来存储了。假设现在有 100 万或更多的股东，成本将在 4 兆字节左右，而不是 34 兆字节。源于我们对通证数据库进行的优化，系统可以以非常低的成本读取和更新股东们的余额。

通证锁定功能

everiToken 系统支持锁定功能。它可以在一段时间内锁定非同质通证或者同质通证。这取决于锁定建立期设定的条件。无论锁定期间是否满足条件，在一段时间结束后，未锁定的资产将转移到指定的注册地址。目前，锁定条件只能通过公钥修改，这意味着在锁定期间，只有锁定条件批准的秘钥才能提供访问权限。

everiToken

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，对其弱点进行改进，以达到青出于蓝的目的。因此，我们采用了久经考验的石墨烯（DPOS+PBFT）共识算法作为我们的代码基础。在代码实现层面上，我们的共识算法从 DPOS 3.0（源于 EOS 代码库）产生，并在此基础上进行自己的改进。我们意识到 EOS 具有非常优秀的代码结构，因此我们在开发中保留了 EOS 的部分代码结构。但是除了这部分之外，整个公有链都是全新开发的。

在开发中，我们的重点主要包括安全合约（Safe Contract，用来代替智能合约）、全新的数据库模型（基于 RocksDB,用于获得更好的性能）以及通证支付协议（everiPay）。

这种实现方式有不少好处，例如：

1. 石墨烯算法受过长时间的验证。DPOS 以及其他核心机制已经在 BitShare、EOS 等项目完整测试过了。
2. 重用共识算法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核心功能的开发上。

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，因此授权操作也可以并行执行。

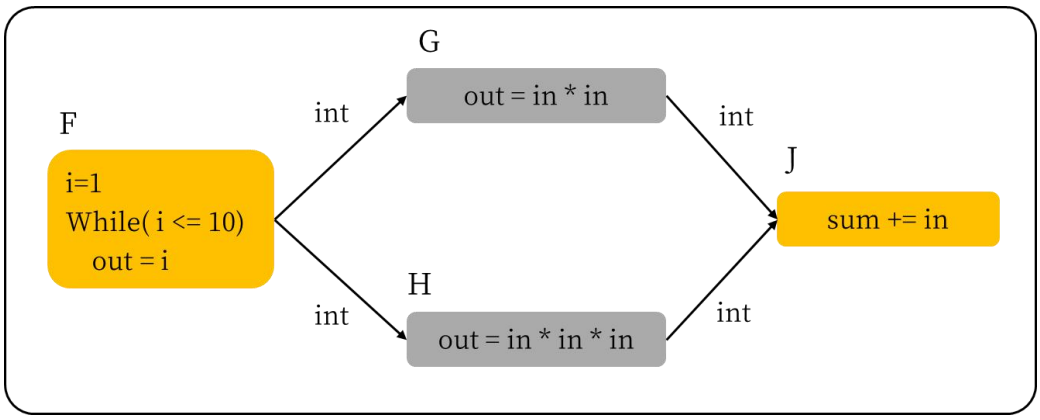
执行引擎

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，系统就是完全稳定的。

一笔交易的执行可以分为几个阶段，如恢复签名、授权验证、计算、写入数据库等。所有阶段都按顺序执行，但有些阶段在不同的交易中彼此独立。其中一个阶段叫做签名恢复（signature-recovering）。每笔交易的签名并没有任何逻

辑依赖性，交易的每个签名也是互相独立的。因此，签名恢复是可以完全并行执行的。另一个阶段是授权检查。乍一看，它似乎与签名恢复的功能相同，但请想象检查两个转移通证的交易，即使每个通证相互独立，如果两个交易需要转移同一个通证并且并行执行这些操作，系统将会报错。因为通证的所有者会在第一个交易中被更改，所以无法通过授权检查这一步骤。

因此，仍然有些阶段是没办法并行执行的，但是我们可以仔细设计这些情况。我们已经实现的在依赖关系图中显示如下：我们的系统使用图形并行性并行处理数据流，节点表示进行的计算，边表示计算之间的通信信道。



上面是一个如何计算从 1 到 10 的正方形和立方体序列之和的例子。在我们的实现中，每个节点代表交易的一个阶段，并且有一个调度器来接受交易并将它们拆分以构建整个图。

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。

everiPay/everiPass/EvtLink

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 everiPay/everiPass/EvtLink 的一些亮点：

- **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，也支持功能性的日常操作例如一把开门的钥匙。最棒的是你几乎可以在任何地方使用，只需简单操作你的手机。
- **闪电般快速**：everiToken 实现了非常高的 TPS，考虑到网络延迟与设备质量的差异，一笔交易可以在 1 到 3 秒内完成。
- **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，最用户友好的面对面支付服务。

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 的很多功能，例如付款码要求付款人必须连接到互联网来完成一次付款码交易，并且收付款人都必须手动输入交易金额，当交易完成时，他们也不会收到自动通知。

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简单地使用手机上 everiToken 支持的钱包来检查是否收到了付款人的钱，它适用于各种类型和规模的供应商，也包括个体之间的交易。

使用 everiPay 来代替付款码支付对任何人来说都是被推荐的，因为它更方便，更安全，用户体验更好。

EvtLink 如何工作？

EvtLink 是表示 everiPasy/everiPass 的二进制格式标准。everiToken 公链使用 everiPay 和 everiPass 操作来执行符合 EvtLink 标准的交易。

这是从技术角度看，通过 everiPay/everiPass 进行支付的过程：

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。这避免了重复支付的风险，因为链不允许两个 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，最后 get_trx_id_for_link_id 将返回交易 ID。

Base42 编码

Base42 是一种二进制到字符串转换的编码算法。它类似于十六进制编码，但是使用 42 作为基数，相应地使用独特的字母表。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很高效的。这种较小的二维码将可以有效提高扫描的成功率。

在 everiToken 公链中，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 通证作为系统的燃料。任何操作都会消耗一定数量的 EVT 作为燃料费，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资产类似。EVT 用于防止恶意攻击和奖励区块生产者提供的资源。

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（其中 14%属于 everiToken 联合创始人，1%属于其他核心贡献者）。

四亿 EVT（40%）将会提供给基于 everiToken 建立应用的社区成员，以及提供技术、资源、资金、推广等为 everiToken 生态做出卓越贡献的社区成员。

四亿五千万 EVT（45%）属于多轮投资中的投资者们。

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，用户需要再次尝试执行操作。

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 属于某个账户并且不能再次转移，这有利于空投给实际用户，因此公司和组织可以通过转换 EVT 来给一些特定账户，绑定 EVT 不能在地址之间转移。

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。为了安全，付款者需要对交易进行额外的签名。

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系统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

初始发行的 EVT 总量是 10 亿。everiToken 可能会每年增发一部分 EVT，实际的发行规则将会由 everiToken 链上治理委员会决定。在 2020 年 1 月前，我们不会增发任何 EVT。

区块生产节点

节点数：动态

我们的出块节点权限有限，因此它们很难去作恶。出块节点唯一能做的坏事就是拒绝服务（Dos）。为了平衡出块节点的受益并且确保去中心化，我们会使用一个大于等于 15 的动态节点数。在 2019 年我们会使用 15 个出块节点。之后，这个数字会由 everiToken 去中心化链上治理委员会决定。

生态

everiWallet

正如它名字所述，everiWallet 是支持 Web 端与移动端的 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 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/

去中心化链上治理委员会

everiToken 公链将有一个去中心化的链上治理委员会来决定重要的事情，例如出块节点的数量，EVT 的增发等等。委员会在筹备之中，预计将在 2020 年 1 月 1 日前上线。

公证公司

everiToken 不对通证的价值做任何干涉。通证的具体价值由托管公司背书。托管公司可以在通证发行过程中签署额外的签名，这样，如果用户信任在通证上签名的公司，那么他就可以信任这一通证。就像 SSL 一样。

结论

通证经济正朝着触及全球各个角落的方向发展。以太坊和 EOS 智能合约是一个良好的开端，但它们并不适合发展全世界所有人都能受益的通证经济。

everiToken 的目标是创建基于通证的区块链技术，是所有人所有地方都可以从中受益。我们已经构建了一个革命性的系统，使开发人员、企业和最终用户能够低成本并简单地在我们的系统中发行、转移和验证通证。我们的安全合约已经移除了图灵完备，这样大大减少了系统的抽象和复杂度。我们并没有不断地创建定制模型，而是创建了一个“一刀切”的模型，它将成为 99%以上的人们首选的解决方案。我们已经大大提升了建立高效繁荣的通证经济所需的速度、安全性、可操作性、稳定性，并且可以符合监管。同时我们为全世界所有人提供了一个去中心化的平台，以数字方式学习，创造，互动并且真正交换价值。

加入通证经济革命，欢迎访问我们的网站

https://everitoken.io

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（领英 ID Brady-everiToken）

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

全栈开发工程师、极富经验的系统架构师和连续创业者。拥有十多年的软件开发、创业、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，曾以 CTO、联合创始人等身份在两家公司任职。

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。