CROS

商业流程

自动化的

区块链开放平台

CROS 技术白皮书

2018年1月

摘要

自从比特币诞生以来，区块链技术已经证明了这种新的数据存储概念将极有可能革新我们的商业运作方式。通过可靠、透明和不可篡改的分布式账本，区块链可以使网络和交易更高效。

CROS是一个基于区块链基础架构的开放式商业平台，适用于所有希望利用区块链技术来改善和自动处理商业流程的企业。虽然许多专有区块链技术已经在各行各业中逐步展开，但区块链在商业流程上的运用一直比较缓慢。 这是因为从零开始搭建区块链技术有较高的技术门槛，同时也没有一个跨链协议来沟通分属于不同机构甚至不同行业的专属链。

CROS的目标是提供一个开放的区块链操作系统，使得企业应用开发人员不再需要过多关注区块链底层技术。CROS能够实现：

- 不用编程就可以部署私有链，降低应用门槛。
- 将企业数据安全地存储在区块链中。
- 在区块链上进行商业交易。
- 同企业已有的ERP系统和IT应用系统集成
- 基于合同模板库创建和部署智能商业合同。
- 用BPMN脚本创建和部署跨机构的工作流。
- 生成和发行自定义的区块链Token，在跨机构的工作流里可以用Token支付。

目录 CONTENT

区块链技术的商业应用

01

区块链是比特币及其他加密货币所采用的底层技术。它是一个分布式的数据库技术体系，每条记录都有时间戳，并且不能被篡改。在个体不被完全信任的网络世界里，区块链技术创新性地建立了一种可以完全被信任的交易机制。这背后的技术保障是通过点对点网络、共识机制、密码学和市场机制来实现的。

区块链确保了数据完整性和透明度，使网络即使在拜占庭故障下也能正常运行。区块链的所有数据在每一个链节点上都有拷贝，通过POW(工作量)证明或POS(份额)证明来达成共识。

区块链技术比加密货币有更广泛的应用前景：本质上它是基于点对点技术的数据库，可以查询到所有的历史数据和状态。有些区块链版本提供了执行用户定义的脚本的能力，即所谓的智能合约。例如，以太坊区块链支持智能合约的图灵完备性编程。他的代码的运行结果是确定性的，因为在运行时只使用来自区块链中的信息。

类似于任何其他交易，将智能合约代码部署到区块链后就不可更改。一旦部署，智能合约会在区块链网络上直接执行代码，例如在满足特定条件的情况下转移资金。这样，没有互信的双方可以通过真实执行的代码建立信任。智能合约可以用来实现一般的商业协作，特别是跨机构的商业流程。基于区块链的分布式账本技术，在开放环境中的协作已经成功地在多个领域有了案例，包括钻石交易一直到证券结算。

区块链促使人们重新思考怎样管理商业流程这种特别的企业资产。这个技术的核心特质使得企业协作的范围可以远超资产管理，可以包括供应链管理，跟踪食物以增加安全性，或在保证隐私的前提下共享个人健康记录等。

区块链技术的商业应用

目前在商务上采用区块链有两个主要瓶颈：一是没有正式标准，二是市场上还没有哪个区块链技术能够支持各种商业应用。

目前，比特币和以太坊存在以下一些不足：

- 速度和吞吐量。比特币每秒只能处理7笔交易。
- 自定义业务数据的数据存储不够。比特币是200GB，以太坊600GB，这比大多数企业的数据库规模小得多。
- 与企业现有的ERP系统和IT应用系统没有整合。

许多企业和行业开发了自己的专属私有链。
其中最知名的有Ripple、R3和Hyperledger。但目前市场仍然还没有建立完善的行业标准。这种局面很像上世纪90年代互联网之前的私有计算机网络。这些私有链都是孤立的，无法进行跨机构的协作。

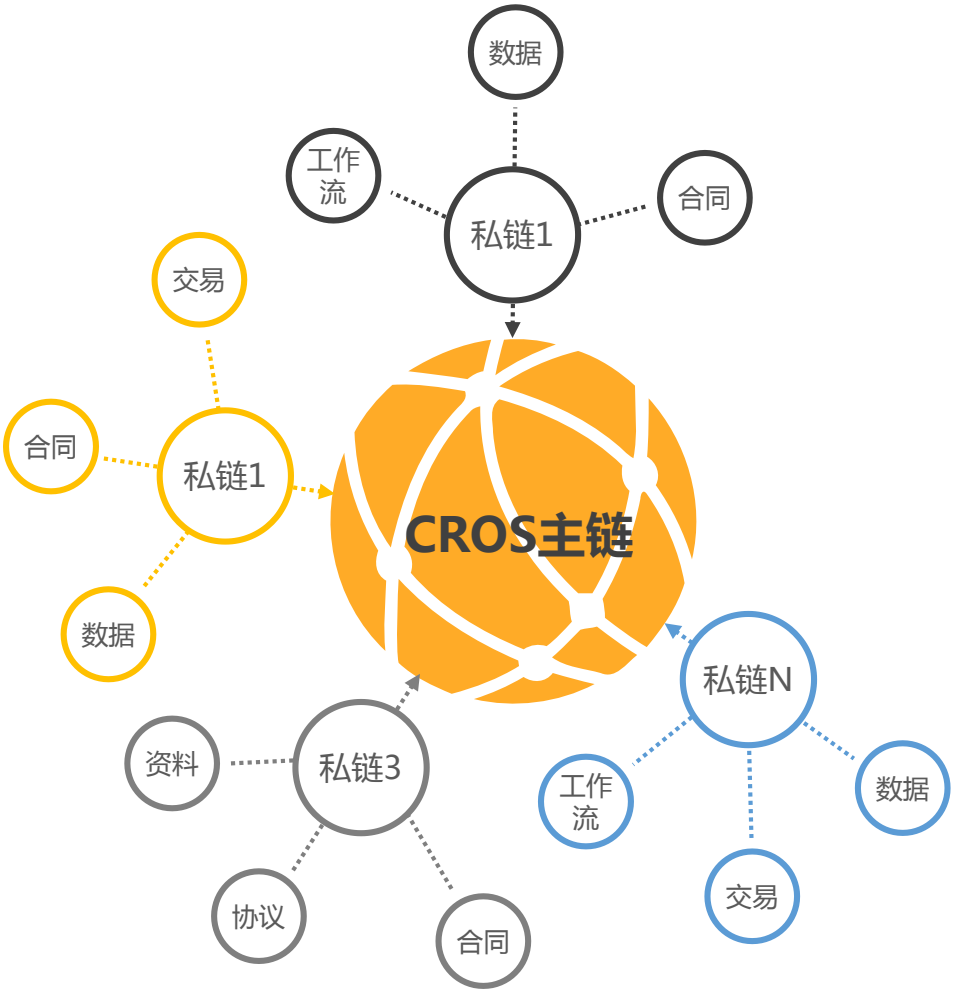
企业开发区块链技术的另一大障碍是把各种零散组件整合在一起的技术复杂性。还没有成熟的基础架构或框架，几乎每家企业都必须从头开始做，工作量巨大。

CROS 是什么？

02

CROS是一个适用于所有商业行为的开放式区块链平台。

它提供了一套行业标准工具来创建和管理企业的私有链，以及一个使得参与者可以通过工作流自动处理来进行协作的开放协议。

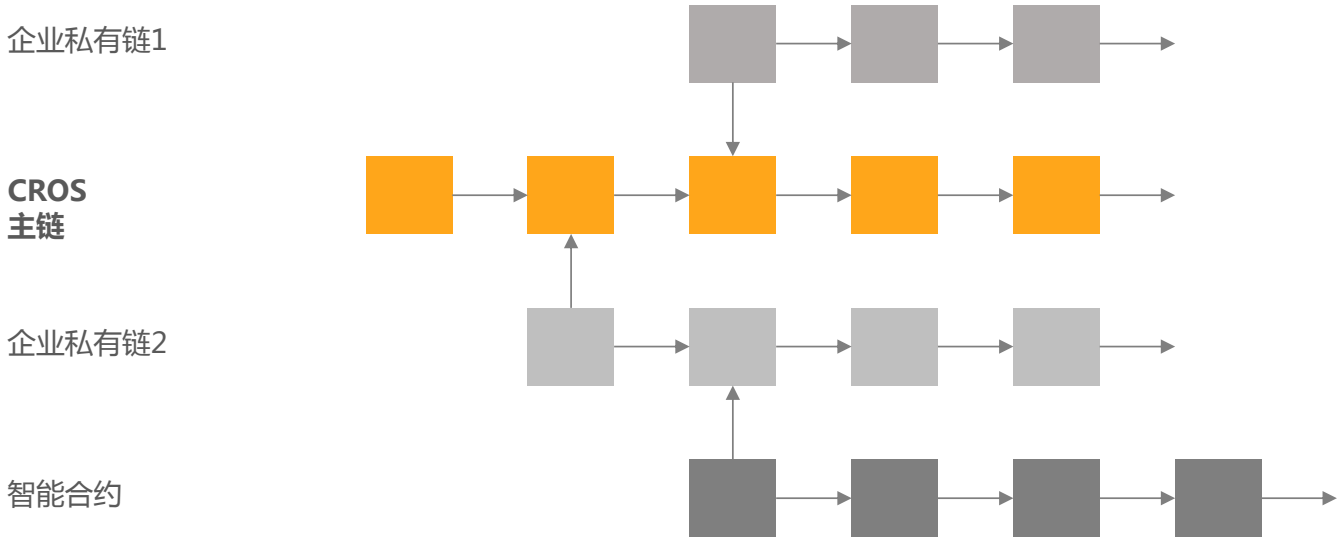


2.1 CROS主链

与比特币或以太坊区块链类似，CROS主链的唯一的开放账本存储了所有用户账户和Token交易记录。这个公共账本是被网络的所有参与者所共享的，并保持尽可能小的规模以避免网络同步延迟。CROS主链还包括了企业的私有链的元信息，私有链以侧链形式实现以保证数据存储的完整。

2.2 企业私有链

每个参与CROS网络的企业会有一个或多个私有链。企业通过私有链存储他们自己的数据，并与其它企业的私有链隔离。私有侧链将被锚定在CROS主链上，与主链有同样的可信度。



当一个企业部署智能合约或者商业流程工作流时，第三层的侧链将会被自动衍生，用来存储合约实例和交易。

2.3 商业交易

企业可以在侧链里快速创建和发行他们自己的定制Token。定制Token可以有两种用途:

- 可以在企业侧链内部，或者跨机构工作流内部为Token分配货币价值。比如，某船运企业可以发行他们的定制Token，对提供给其他企业或者个人的船运服务可以接受Token支付。
- 企业可以将其物理或数字资产的价值转换为Token，并利用区块链系统来交易这些资产。比如，一个托管企业可以发行他们的多个定制Token，每个Token与他们的托管业务中的一个不动产相绑定。CROS使用”彩色币”方法来确保每个Token有唯一标识，并可以在区块链上交易和追溯。

2.4 商业合同

商业合同可以被数字化并存储在区块链中。CROS将提供商业合同模板库，企业可以通过简单地更改其使用条款和参数（例如合同方名称，日期，金额等）来定制。例如，一个雇佣合同可以通过数字方式在新员工和企业之间签订，双方签名后会永久保存在区块链上，带有时间戳，任何一方在之后都不可能篡改它。

这个模板库将降低构建和部署商业应用的成本并增加网络本身的价值。企业也可以创建他们自己的合同模版，发布到库中供其它企业使用并赚取一定的使用费。

2.5 商业流程

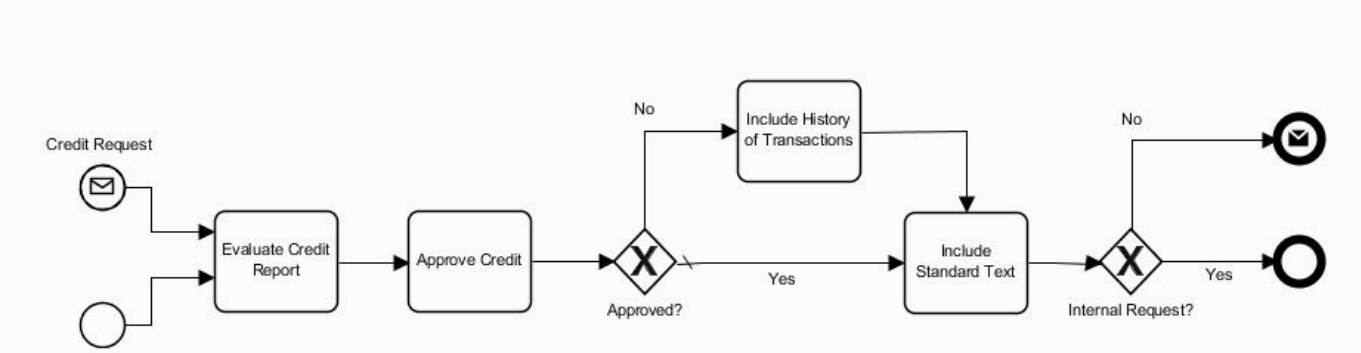
商业流程将使用BPMN（Business Process Management Notation）语言编写并部署到CROS网络上。CROS有一个内置的工作流引擎来执行和自动处理业务流程。

BPMN (Business Process Management Notation)

BPMN用图形化的表述方式来描述商业流程的步骤。它完整描述了商务的端到端流程，被专门设计得适合协同在一组相关的活动中的不同参与者之间的过程和消息的顺序。

BPMN的目标是通过为商业用户提供比较直观的文本和图形表示的标准，但同时能够表示复杂的流程语义，使得技术用户和商业用户双方都可以用它来管理业务流程。BPMN规范还提供了符号图形和底层执行语言，特别是BPEL语言，之间的映射。

以下是一个信用审核和批准流程的示例。



BPMN脚本以XML格式存储。例如：

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions ...>
    <process id="sid-0" ...>
    ...
    <task id="sid-1" name="Veryfy BANF">
        <incoming>sid-A</incoming>
        <outgoing>sid-B</outgoing>
    </task>
    ...
  </process>
  <bpmndi:BPMNDiagram id="sid-1234-56789">
    ...
    <bpmndi:BPMNShape bpmnElement="sid-0" ...>
        <omgdc:Bounds height="452.0" width="824.0" x="15.0" y="30.0"/>
    </bpmndi:BPMNShape>
    ...
  </bpmndi:BPMNDiagram>
</definitions>
```

CROS支持BPMN 2.0标准版本，以及BPMN脚本部署到CROS平台后的CROS扩展。

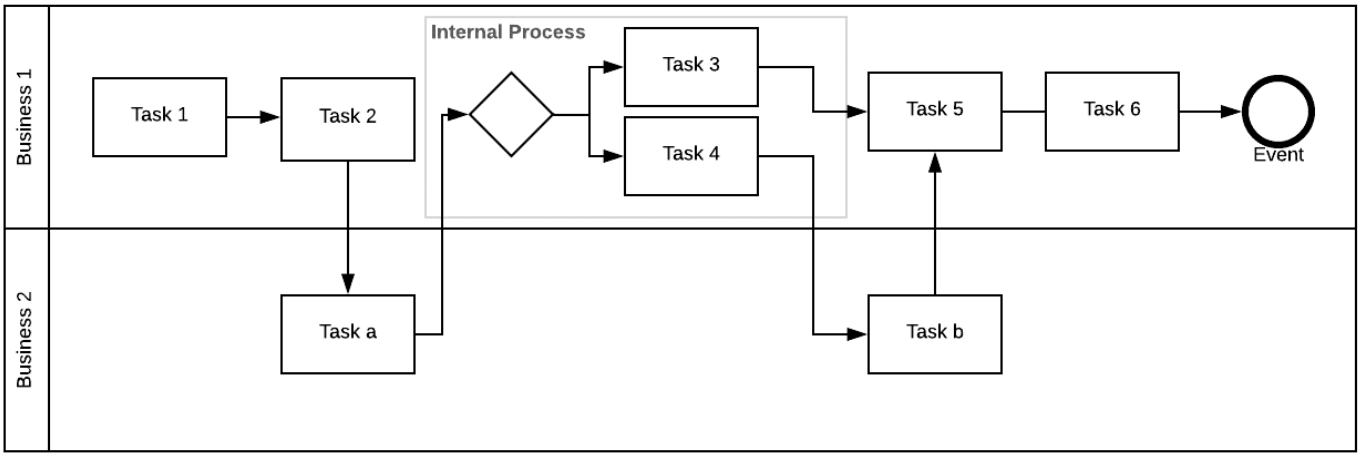
2.6 跨机构工作流

商业流程的工作流可以跨企业。跨机构的工作流会被部署到CROS主帐本上，执行时会跨越各机构的企业私有链。

跨机构的工作流可以为流程参与者提供各种好处，例如更高的透明度，更高的集成度，更快的通讯和更高的吞吐量。

由于实际的流程逻辑直接存储在CROS区块链上并进行加密，所以各方可以放心他们与其他参与方达成的协议不可能被损坏或受到计算机病毒和恶意软件的影响。CROS的基础设计保证了所有交易的端到端安全性，而不需要依赖于任何其他方包括CROS系统运行的服务器和硬件的可信性。CROS区块链支持BPMN子流程，企业可以选择在跨机构工作流情形下对其他参与者隐藏内部业务流程。一个子进程是BPMN脚本可以包含的两种类型的活动之一。每个子进程代表业务流程中的一系列活动。

下面的例子里，企业1将跨机构工作流的一部分设置为内部子流程，所以企业2可以参与到工作流里但是看不见企业1的内部流程和执行过程。



我们的目标

CROS旨在为企业和个人提供如下服务：

给任何有意愿利用区块链技术优势的企业一个低成本，易于使用的平台;

给企业一个在可信赖和有透明度的环境中合作和执行商业交易的一个开放的标准和平台;

能够帮助企业改善和自动处理现有商业流程的跨机构工作流引擎;

能够使企业生成和发行用于支付目的的定制Token的区块链Token工厂。

我们的最终目的是通过桥接分散的商业系统，只用现有技术手段的很小一部分成本帮助所有实体参与进全球交易网络中去，促进资金、货品和服务的流通，我们的使命就是成为这样的生态系统和工业标准的驱动者。

CROS 技术体系

04

4.1 技术架构

数据层

CROS使用了最强大的加密和散列算法，包括ECDSA Secp256k1和双SHA256。

同时内置支持了符合中国加密数据保护条例的SM2 / SM3算法。

CROS的账本存储在分布式的NoSQL数据库中，以便更快速地保存和检索数据。

技术架构

网络层

CROS主链使用POBV(商业价值证明)共识协议。作为POS(份额证明)共识机制的一个变种，POBV更重视参与者带给CROS的商业价值。商业价值包括以下:

- CROSToken的份额比例；
- 交易数量和CROS燃料消耗数量；
- 所贡献的合约模版数量和被采用比率；
- 商业流程数量；
- 跨机构流程数量；
- 其它所有能给CROS整体网络带来正向商业价值的活动。

服务层

- CROS智能商业合约引擎；
- CROS商业工作流引擎。

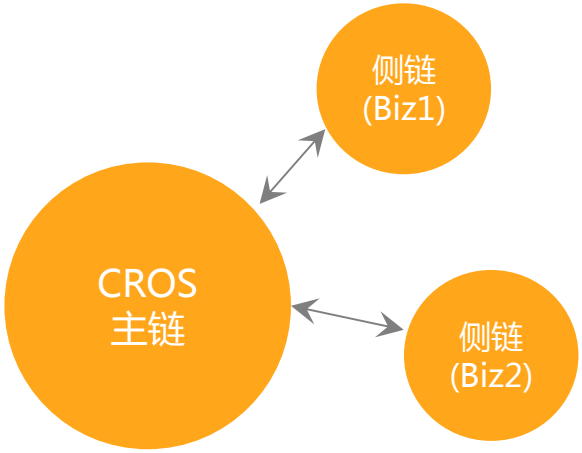
接口层

在这一层，CROS为企业提供了一系列与私有链交互的工具：

- 使用网页界面查看，监视和查询区块链状态和存储的数据；
- 一个SDK和API库，可将现有企业ERP或IT应用程序集成到区块链；
- 一个创作，定制和部署智能商业合同的网页工具；
- 一个使用BPMN图表和脚本，创作和部署内部业务流程或跨机构工作流的网页工具。

4.2 侧链技术

为了避免类似于比特币和以太坊的性能和吞吐量局限，CROS用一个CROS主链和N个侧链开发其框架，每个侧链对应于一个企业账户。创建新企业帐户时会创建侧链。

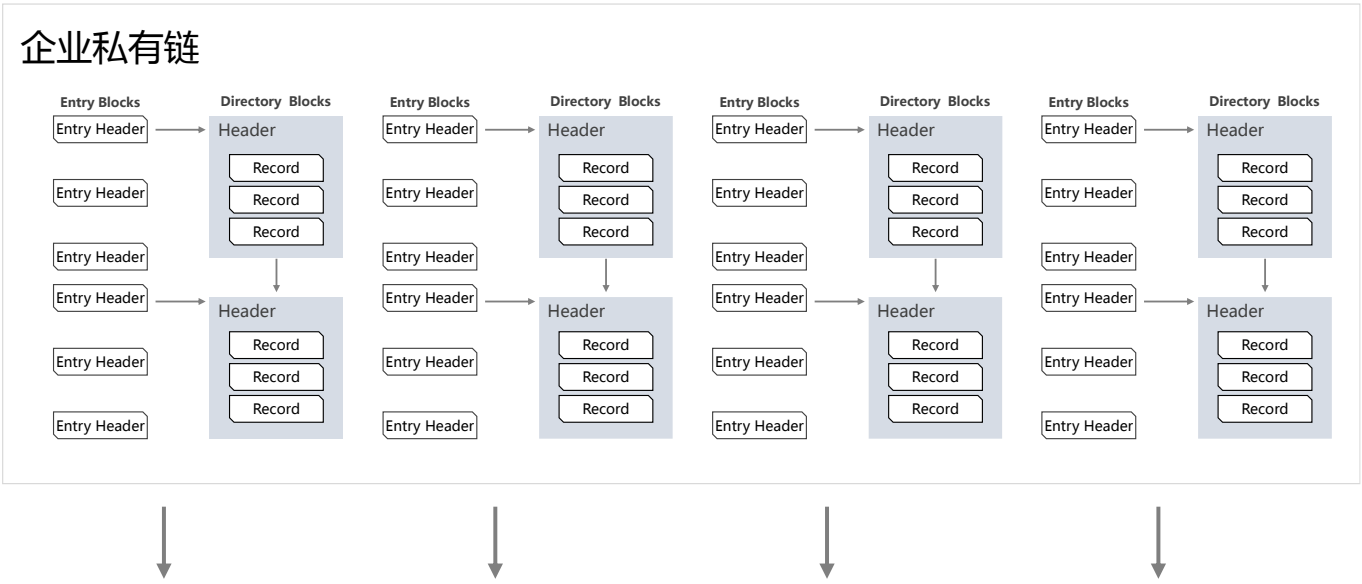


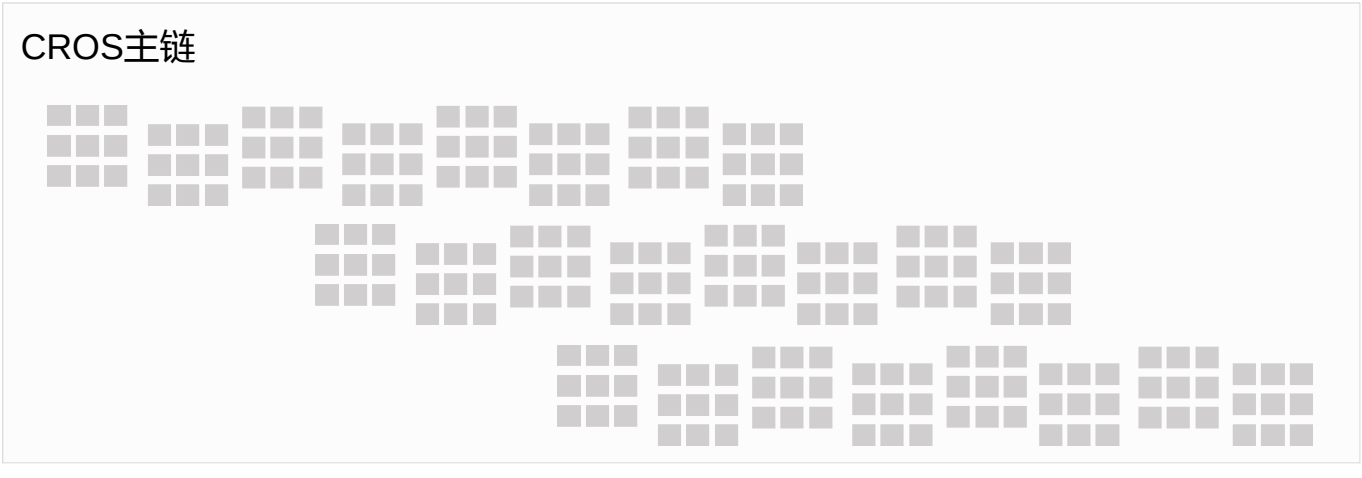
与比特币公共账本相似，CROS主链只包含企业账户信息、Token交易记录、智能合约脚本、工作流脚本和最小的元数据（例如，加密签名，散列值和侧链锚定散列等）。CROS与比特币的主要区别就是使用企业侧链来存储企业数据和智能合约实例。

CROS主链每15秒产生一个新块。大多数侧链的交易少得多，因此每10分钟左右才生成一个新块，但是这个可以根据企业需求动态地进行调整。当一个新的侧链块生成时，Merkle树算法将被应用来生成Merkle树根哈希值。这个侧链的哈希值将被发布并永久地包含在主链中。从那一刻起，对侧链数据的任何篡改都将触发块哈希值和主链上的值之间的数据差异。

侧链技术

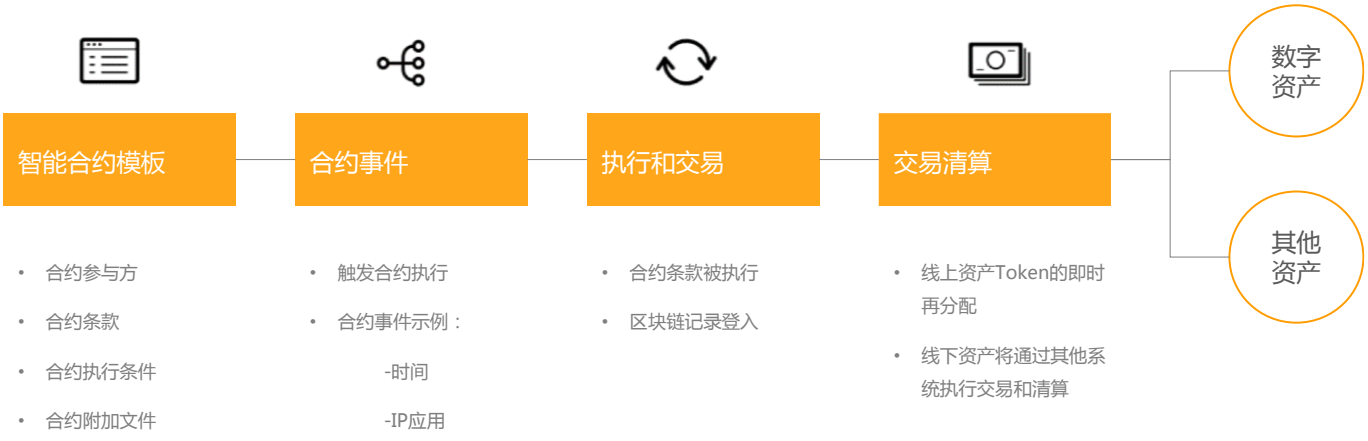

视频
图像
文本
隐私信息
Hashed
信息
新闻
合约
公开信息
Not Hashed


企业私有链
Entry Blocks
Directory Blocks
Entry Header
Header
Record


CROS主链

4.3 智能合约模板

CROS有一个特殊的侧链作为商业合同模板库。商业用户能够浏览和选择一个模板，或使用网页界面创建他们的自定义模板。



4.4 ERP系统集成

市场上大多数区块链解决方案的主要局限之一是缺乏与企业现有的ERP系统和IT应用程序的系统集成。这使得区块链Dapps孤立和不可扩展。CROS通过灵活的企业适配器框架支持ERP系统集成。

4.5 安全性

企业数据在CROS网络中受到多层安全功能的保护：

- 加密。所有数据在保存在CROS链上之前都被加密。
- 企业侧链与其他企业隔离。只有企业允许的数据对象才会传过CROS主链的跨机构工作流。
- 企业帐户在CROS链上默认是匿名的，除非用户特意公开它。
- 对于需要更高安全性的企业，CROS利用zk-SNARKs算法（一种零知识证明算法）隐藏所有交易和身份。
- 跨机构工作流里的子流程在缺省状况下对其他企业是不透明的。工作流参与者只共享了尽可能少的数据和流程。

4.6 平台性能

CROS网络每秒能够处理数万笔交易，这要归功于它独特的基础框架设计：
1条主链+ N条侧链广播交易并允许并行处理交易。POBV共识算法不需要很多计算资源。大部分的CROS网络中的区块链交易可以在3秒内得到确认。

CROS 实施路径

05

基于开发时间节奏考量和给所有利益相关方以及用户一个更好的知情，CROS网络计划了3个里程碑阶段:

阶段1：开发平台

阶段1里CROS团队将在开放平台上开发基础的CROS网络和基础功能。CROS主链将锚定比特币公共账本以保证可信度和公平度。

用户将可以创建私有链来存储企业数据，编写和发布智能合约。初版也将会包含一些合约模版库以供使用。

阶段2：公共账本

阶段2里所有参与节点将可以在CROS基础公共账本上基于POBV共识算法挖矿CROSToken。在这个阶段有完整的智能合约模版库，完整的跨机构工作流所需函数。

阶段3：Token经济

企业将能够在CROS上发布自己的定制Token。并在智能商业合同和跨机构工作流中使用自定义Token。企业和个人都可以在CROS网络中快速成立自己的去中心化自治机构从事商业行为。

CROS - 跨机构工作流

06

6.1 概览

两个或两个以上独立的经济实体之间的工作流一直存在信任问题，尤其当需要为产品和/或提供的服务及时支付的时候。比如90+天后结款时因为所谓货品损坏只收到了部分款项，或者没有收到任何付款还必须付出运输费拿回退货，或者在最后时刻订单被取消，或者缺乏信用的企业的使用各种花招以榨取供应商或者客户一些利益。

CROS平台重新定义了商业体之间进行商业交易的标准。
购买产品或服务至少需要关注以下这些问题：

- 报价的有效性
- 交付产品的详细规格
- 交易对手确实存在，并且不是伪冒
- 库存可用性和交货时间
- 对订单的接受意愿
- 产品安全认证CE，CSA，UL，TUV，ETL
- 专业人员，律师，工程师等都具有资格证
- 服务相关的资源和人员问题
- 运费和交货担保
- 产品缺陷和退货条款
- 付款条件
- 转移资金和付款确认
- 报关
- 不履行时的损害和处罚

需知上面的列表并不全面，列出的每个项目可能会有很多与特定行业如何运作有关的差别和微调。

比如制药企业可能需要面对假药有关的问题，可能有潜在的巨大法律责任，而这是废金属经销商根本不需要考虑的。废金属经销商可能有与接收金属有关的问题，比如收到的金属有多氯联苯（PCBs）污染，而在某些地区有针对该污染的严格管制，虽然所有的企业都是一样的买卖东西，但各自的业务细节都不一样。

CROS框架能够解决所有这些现有的信任相关问题，大大提高效率并降低成本。能够有效完成这些目标的关键是CROS主链，它将把在各种业务安排中各方之间进行交换的交易和信息记录下来。

作为一个公开发行并经过验证的信息数据库，CROS区块链将允许交易中的所有各方完全相信与协议有关的所有条款和条件都是明确的并且已被大家接受。

这样可以免除所有与信任有关的风险、节省时间、人力和金钱，使参与CROS网络的企业具备更多的竞争优势。进而形成正向激励反馈，竞争力提高的企业会增加销售额，迫使其他企业也采用CROS技术。

CROS - 跨机构工作流

以下我们列出CROS可以促进跨机构工作流的部分方式：

身份验证

区块链上会存储每个企业对其名称，地址，分支机构，法属，股权结构以及他们认为重要的其他相关事实的一个全面法律描述。每个企业可以自定制一个标准数据模板， 可以按照需要包括非标准信息。

企业可以规定哪些数据字段公开，哪些数据是私有的和加密的。私有数据只能当另一方请求并且其所有者授权允许后才能被分享。可以定义特定数据的发布模板，这样，根据正在执行事务的类型，只释放特定数据字段。因此，企业可以存储他们自己的任何信息，因为这些信息是完全自己掌控的。

关键敏感信息将通过侧链机制进行存储， 然后锚定在主链上，数据随时可以删除。这种区块链数据存储的不可改动和可以改动的设计组合提供了最大的灵活性，为早期采用者提供了安全感，因为在CROS数据库中存储了他们的信息之后无需任何控制也不会泄露敏感信息。但是, 正在执行之中的合约所用到的数据不能被改动, 也不能从侧链删除它, 已经发布给第三方的历史数据会被永久保存在侧链里。

信用获取和财务审计

企业可以以任何级别的细节在CROS账本上安全地存储他们希望披露的相关信用数据，简单如信用额度，权限，复杂如从公认的会计师事务所获得的审计报告。当查询信用信息时，查询方还可以选择查询结果的类型， 包括是/否类型，或实际信用额度（须小于或等于其真实的信用授权），一直到完整的审计报告类型。至于具体给出什么信用信息将完全取决于提供信息的企业。 CROS智能合约有内置的自动选项指定什么类型的信用信息在什么条件下可以被给出。 因此，企业可以很方便地给出他们的财务细节，将其存储在CROS链中，然后不再费心。

存储在CROS链中的数据也可以附有过期日期，到时企业会被提醒去更新和验证已有数据。CROS语言完备支持所有类型的过期时间自动处理，从简单的提醒，完全删除，到第三方审核签字后的重新提交。

动态信息处理

CROS智能合约还能够安全地连接到企业的内部ERP系统。这将有助于集中CROS框架内的所有跨机构数据流。在这种情况下，CROS区块链被查询时只验证企业请求数据的真实性，然后充当转发数据时的安全通信通道。这将显著减少需要存储在CROS链中的数据量，但同时享有CROS提供的所有安全性。

ERP连接器将使CROS框架能够直接从企业获得执行智能合约所需的信息。各个企业完全控制暴露给CROS的信息，绝不会泄露任何私密敏感信息。

CROS - 跨机构工作流

支付处理

CROS的底层有一个完全集成的支付处理引擎，能够在几秒钟内对邻近或远隔重洋的对象转移资金，交易费用几乎为零。唯一的实际成本是银行收取的支收费用。不可避免银行会有一些时间延迟，但通过在全球所有主要国家建立的办公网络，CROS将充作货资金交易的临时托管。客户可以在CROS中存入资金作为保证金，这样当交易双方都是CROS注册用户时， 双方不再需要经过现有的银行系统就可以转移资金。CROS也能够提供外汇服务，未来甚至可以在ICO世界或现有的股票，债券，期货和衍生品交易市场提供投资服务。

CROS智能合约的技术有能力在合约执行过程中自动处理所有支付。包括清晰地和智能地处理某方不履行合同条款的机制。

6.2 技术实施

CROS有自己的智能合约开发语言CVML（CROS Virtual Machine Language），它超越了现有区块链技术，如以太坊的Solidity，的功能和限制。
CVML语言的设计背后有的两个重要原则：

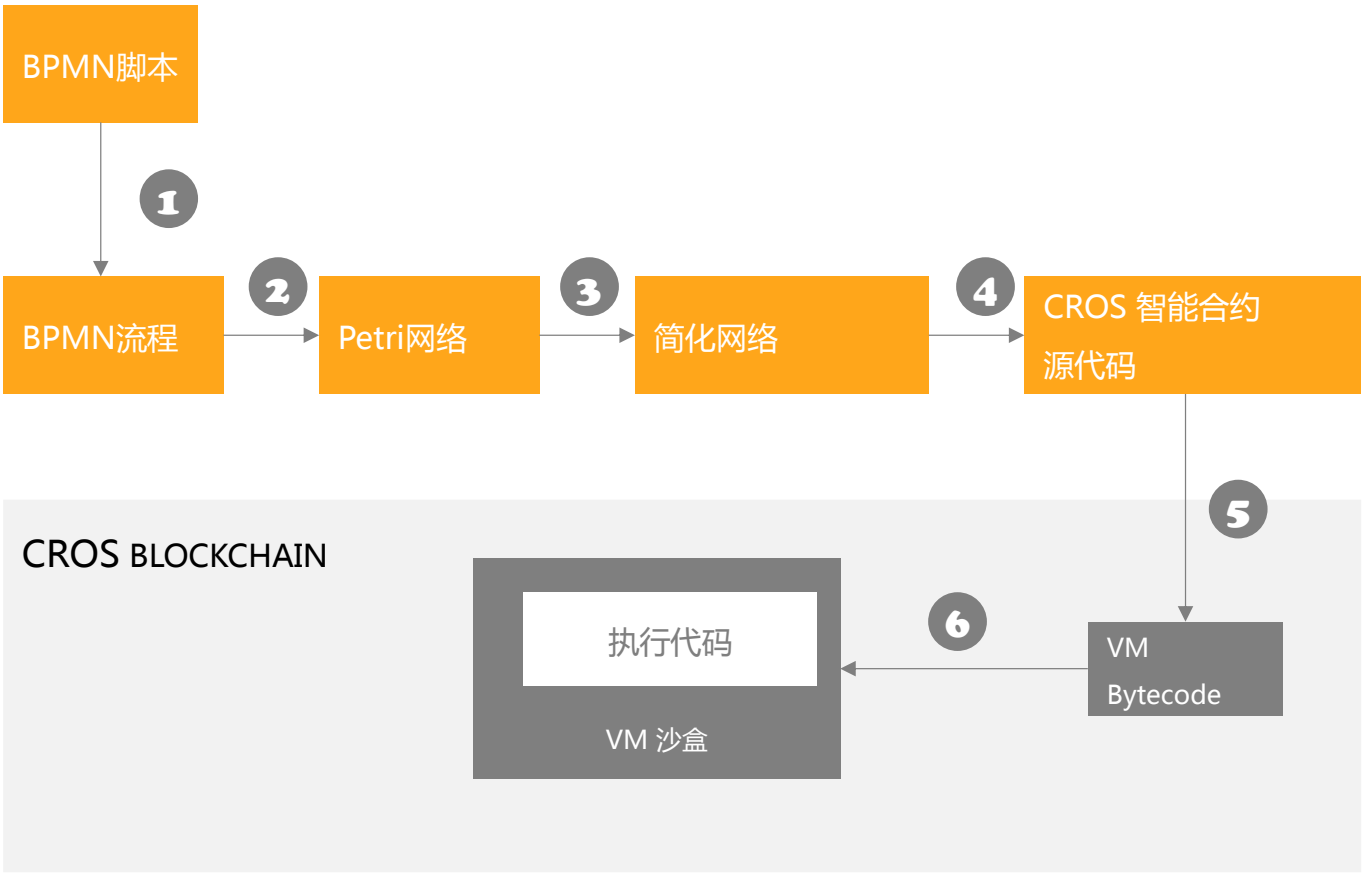
- 对开发人员上手容易，使用简单，类似JavaScript的语法。
- 具有足够的灵活性来处理任何可能的合同。如果任何人可以描述它，CVML就可以运行它。

大多数情况下，用户将不需要看到甚至意识到CVML源代码，因为CROS框架有一个BPMN代码生成器引擎模块，它将把BPMN的定义文件自动编译为CROS虚拟机语言。

其实对于大多数使用场景，用户甚至不需要创建BPMN图，因为CROS模板将能够处理大多数标准的业务交易。因为可以直接使用BPMN文件，同时有许多用户已经熟悉的行业标准工具，在开发和定制方面非常灵活。

CROS - 跨机构工作流

下图描述了通用流程，从BPMN图表用户文件一直到在CROS链内的CROS虚拟机上运行编译好的CVML代码。BPMN图通常被存储为BPMN标准定义格式的XML文件，XML文件可以被认为是程序脚本。



图中第2点时CVML编译器开始介入，它创建符号表，执行语义分析，并生成有向图的内含定义。内含定义将被转换成Petri网类型结构，这将支持CROS利用现有的强大工具来执行对内含定义的正规优化和验证步骤。

Petri网是描述分布式系统的数学模型语言。它用有向, 有值, 双向的图来表示, 节点代表位置(条件, 用圆圈表示)和状态转变(可能发生的事件, 用柱形表示) 。有向弧（用箭头表示）用来描述某个位置是某个状态转变的前置条件和/或后置条件。Petri网有正规语义, 使得数学可证的操作可以在上面执行以进行验证和优化，它还有图形化符号描述逐步过程，包括选择、迭代和并发执行。

CROS使用Atlas转换语言（ATL）并基于一组转换规则来实现这两种不同语言之间的转换。接下来，简并操作会被执行, 以消除冗余或虚假的状态变化和条件，这将优化bytecode, 最大程度地减少了CROS链的资源加载。

这些简并转换使得工作流的拓扑结构总是只有一个入口和出口点, 保证了所产生的智能合约bytecode的语义正确性，即智能合约不会陷入死循环，死锁之类的多节点处理环境中可能存在的问题。

在编译处理图中的第3步，CVML智能合约的源代码文件将根据Petri网的定义自动生成。开发人员可以轻松地修改这个过渡文件以处理复杂的逻辑规则，而BPMN图本来是无法定义这些复杂逻辑的。极端情况下，开发人员可以禁用可选的Petri网的简并和优化功能，这样生成的CVML源代码更接近于原始的BPMN图，使修改代码更容易。这个功能很少会用到，但至少给开发人员提供了一个处理任何可能情况的灵活性，所以开发人员从来不会被迫为简单的问题创建复杂的解决方法（以太坊有这个技术缺陷）。

现在我们来看看编译过程的后端步骤，这时CVML编译器接管并生成CVM兼容bytecode。 CVML编译器是基于LLVM，以及一个定制化的前端词法分析器和语法分析器。

在最后一步（6），LLVM将再次被CROS虚拟机的实时编译器（CVMJIT）所使用，它将生成目标操作系统的可执行机器代码，包括WIN32 / 64 X86、Linux x86、Linux ARM，以及目前所存在的任一操作系统。

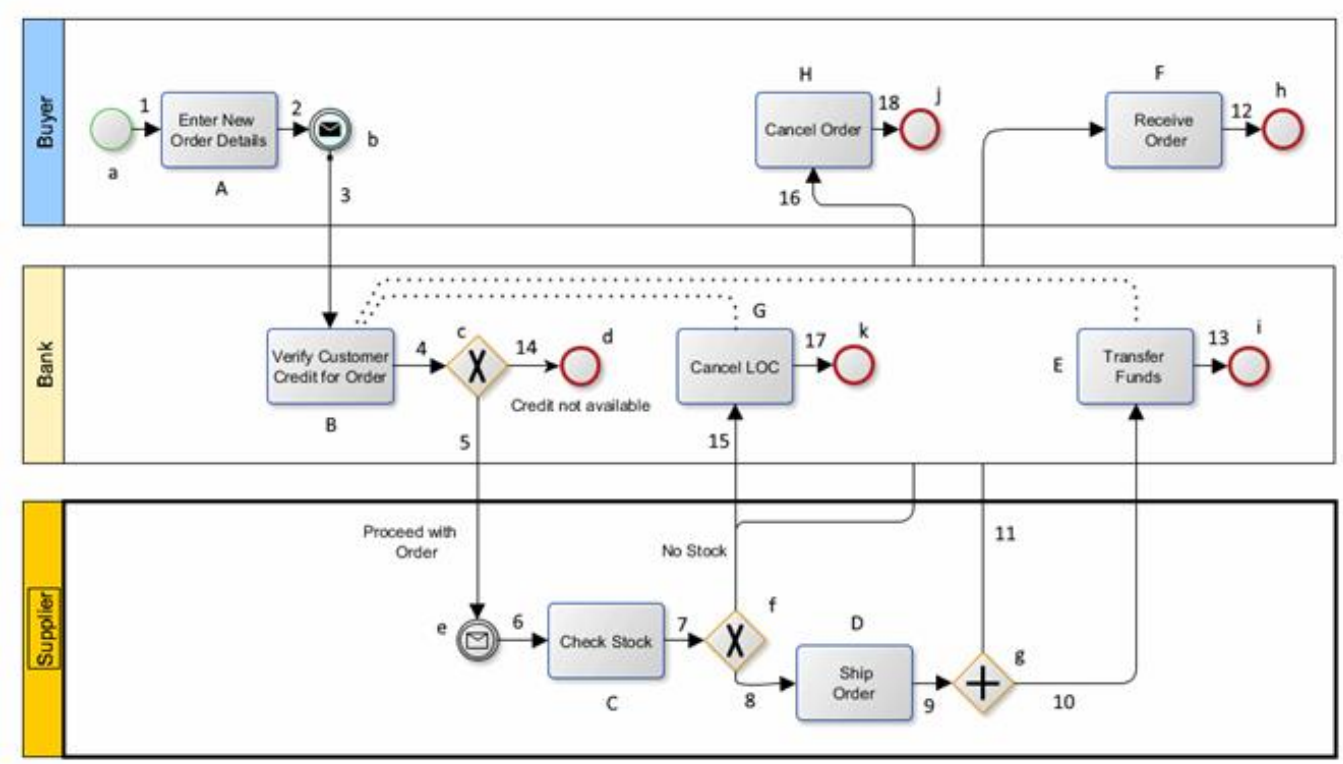
CROS - 跨机构工作流

在CVM内部，每个智能合约都将在一个安全的沙箱内执行，避免了恶意代码所可能造成的系统崩溃，信息泄露或其它任何危害到CVM的后果。CVM在原生操作系统之上有它自己的虚拟操作系统环境。CROS智能合约通常有非常相似的资源需求，CROS虚拟机操作系统通过内存池设计, 几乎完全不需要常见的内存分配和释放动作, 进而也完全不存在内存垃圾清理需求, 所以几乎完全不存在内存抖动现象。除了显著优化了内存使用外，CVM操作系统还可以进行内存块分配，加密密钥永远不会泄漏, 永远不会因为硬件错误发生最近新闻中的“熔毁”和“幽灵”这种类似问题。

作为最后一个安全层，CVM的所有内存都对每一个会话分别进行加密，所以甚至连CVM物理设备的站点管理员也无法提取私有数据，类似于Microsoft Azure区块链技术的工作方式。

为了帮助理解CROS 虚拟机的内部原理，让我们想象以下的基本BPMN跨机构工作流过程。图2描绘了一个典型的跨国商业交易过程，当然为了讨论方便, 这个例子对真实过程进行了很大简化，即使如此，在这个简化模型中仍然有相当多的事情发生，包括为了保证合约始终处于有效状态, 必须能够正确处理多个异常终止条件, 比如说银行绝对不能在发货订单之前转移资金。

CROS - 跨机构工作流



上图并不严格符合BPMN标准。比如 “No Stock”路径并没有使用并行网关符号去分叉到两个独立的路道。虽然对于读图的人来说是清晰的，但语义分析器必须注意到这种情况，自动将并行网关引入其内部表示，以便后续的验证和优化算法功能正常。

由于CROS区块链主要关注状态变化，它并不关心用户输入新的订单时活动A的细节。只是，订单的创建将触发生成一个智能合约，然后自动到步骤B，在那里它必须等待用户输入。合约可以对等待动作设置内置的超时机制, 如果没有，系统会使用默认的超时时间以确保存储资源不被浪费。

有些动作将被自动处理，如E、G、H。因为这些功能可以全自动，不需要用户输入或反馈。CVML代码生成器将根据交易类型对执行模型进行优化，并且可以对智能合约内的各种动作同各种风险和交易处理信心关联起来。这个独特架构设计是CROS平台的一个关键特性，使得CROS在速度，效率和成本方面与其他系统相比具有优势。

CROS将采用多模式费用机制, 避免了以太坊网络使用的所谓“燃气耗尽”的这种有些蹩脚的概念。没有人喜欢碰到这种情况, 一个合约浪费了一个月的时间才从网络中收到失败的反馈然后没有被执行。这会阻碍许多可能的使用案例。CROS支持以太坊类似的费用模式, 即合约用户自愿支付费用金额，同时也支持网络节点以竞价方式争取工作这种标准的费用模式。

6.3 应用场景

场景1：贸易融资

区块链技术可以改变的一个领域就是贸易融资，其历史进程的根源可以追溯到十六世纪的欧洲商人。现状是它通常要求银行针对运输货物发出信用证或其他形式的付款保证（小企业很难以合理的成本获得），同时卖方或出口商也经常碰到付款延期的情况。

CROS将简化全球订购和转移货物的整个过程。一旦订单处理的智能合约模板发布到CROS，新的订单就可以通过Web接口产生。供应商，托运人，海关代理经纪和银行都将有他们可以访问的定制接口，但只显示与他们在整个交易中的角色相关的信息。 CROS能够实时追踪资产，交货时自动发放付款，消除了供应商收不到付款的风险，以及买家汇款后却收不到货物的风险。可以选择一个CROS物联网设备附加到运输的货物之上，它将发回位置数据以及任何其它可能重要的信息，例如温度，震动和振动，是否曾被上下倒放，包装是否打开过等。这大大降低了欺诈，商品被盗或被假冒产品替换等的风险。

通过最大限度地减少国际贸易的支付风险，缺少财务资源的小企业能够与大企业有力竞争，因为大企业所拥有的那些财务资源现在小企业也可以在CROS技术平台上获得了。

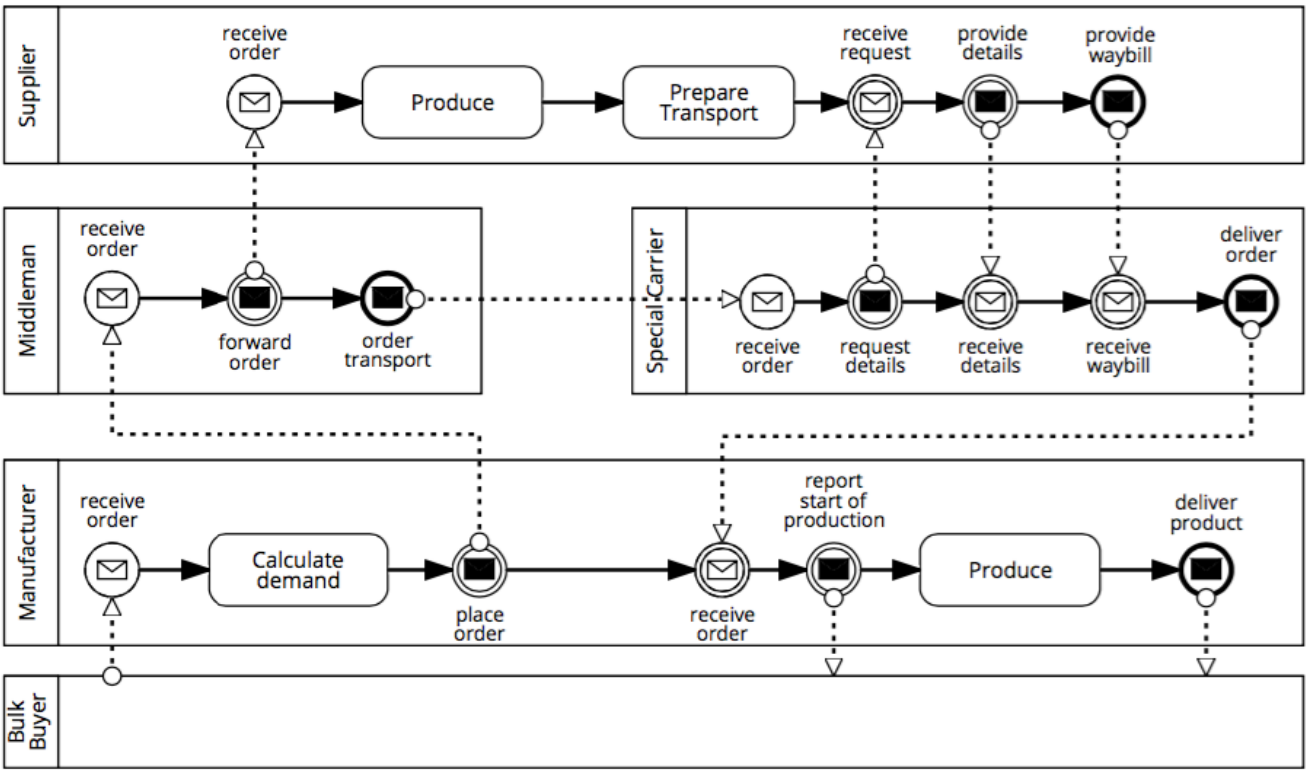
场景2：供应链

现代供应链有数据优势，但是存在信任短板。一直以来机构间缺乏信任，担心商业秘密的泄露，这阻碍了机构间共享信息。反过来，即使分享了信息，别人也不敢全信。CROS平台和它的分布式账本给与资产相关的交易创建了永久的和共享的记录, 因而建立了一个牢不可破的信任链。每个记录都有时间戳，并紧跟着前一个事件。CROS有潜力在三方面突破：可见度、优化和需求。

以下是一个简化的供应链场景，批发商从制造商那里订货。制造商反过来通过一个中间人订原料，原料供应商再通过一个特殊渠道向原料制造商订货。如果没有全局监测, 每个参与者对整体进展的了解有限。这样在发生冲突时很容易造成误解和相互指责。同样，如果你正在同一个新的网上找到的供应商打交道， 你无法核实他是一个在地下室工作的人，或者是一个大企业。

如果通过CROS智能合约操作，那么这些通常会造成跨机构的流程复杂化的障碍就可以被消除了。

场景2：供应链



（1）所有参与者可以审阅CROS不可篡改的公共账本上的可信任的历史信息，找到发生问题的准确根源。这是因为所有的状态变化信息都记录在区块链上。

（2）智能合约可以从全局的角度提供独立的进程监控，只有符合预期的消息才会被接受，并且必须是从登记的相关角色用户送出的。

（3）加密可以确保只有必须公开的数据才会被公开，而其余的数据只对必需它的流程参与者看见。

（4）以可靠方式保证执行的智能合约是可以从CROS流程模型模板生成的，对最终用户基本不费吹灰之力。

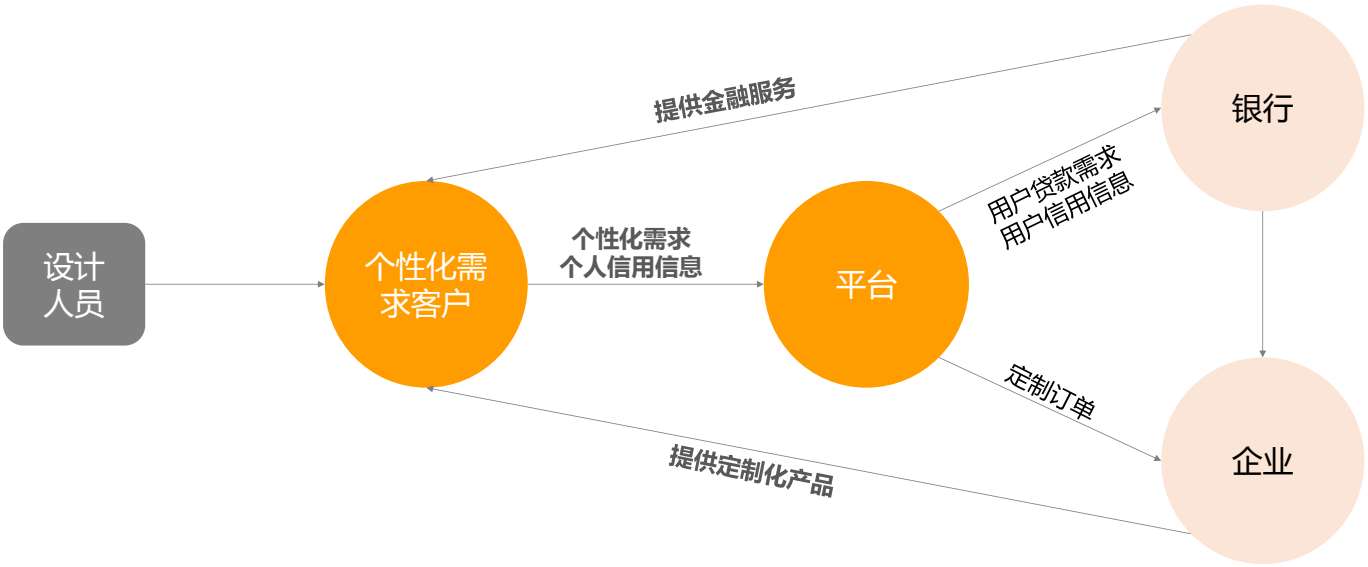
场景3：共享经济

比如这样一个例子，如果需要连接产品设计师，最终客户，金融机构，和制造商一起提供一个定制的产品。一旦客户找到合格的设计师并谈好价格，他们必须一起工作才能完成一套完整的符合要求的设计文档。

然后，客户必须找到一个有实力和可靠的制造商来实际制造产品给他。另外，即使制造商很愿意接受订单，没有银行融资制造商也没有足够的资金来购买原材料，因此他们需要银行的融资。所以制造商要求提前支付保证金以覆盖原材料成本，但客户想使用他的银行授信，结果造成了更多问题和延误。

在共享经济中，相关各方必须付出相当大的时间和精力要么管理文档工作，要么来回转发电子邮件，以及签署和扫描文件，可能还会有冗长的会议，所有这些都可能需要几天的时间来来回回。

有了CROS，我们创建了一个协作生态环境来实现这一目标，避免了所有这些管理的时间浪费。



场景4：保险

区块链技术还可能改变个人保险产品的订制和管理的方式。基于区块链的个人身份识别机制可以被保险企业用来验证索赔, 以及不需要进行很多理赔工作就支付赔偿。

当某人提出索赔时，通常保险企业的理赔员必须出面检查损害或者核实。这造成了调查员和理赔员人数的不足，往往造成延误。CROS区块链可以将相关调查员和理赔员合成认证为一个总池，一家保险企业就可以从更大的人员池中调配资源，加速索赔处理和减少差旅费用。承保方, 调查员和受保方都可以通过CROS区块链安全地处理业务和签署，并降低成本，消除欺诈，提高效率。

很多旁观者和保险企业会特别关注寿险行业, 因为对遗属而言在他们最痛苦的时候登记和确认死讯会相当耗时和折磨。有了CROS驱动的保险系统，通过使用智能合约可以在收到正式的死亡通知后自动处理索赔，给受益人的赔付可以在几天（而不是几个月）内完成。这些功能也可以应用于意外伤害保险，如汽车保险。

CROS Token

07

CROS Token是CROS网络内的唯一正式支付媒介, 被用来支付区块链基础架构的使用。类似于以太坊的Gas模型，CROS的用户也需要为区块链上进行的任何交易“燃烧”CROS Token，这包括：

- 创建一个新的私有企业区块链；
- 在区块链上存储数据（金额要根据数据大小计算）；
- 部署和执行智能商业合同；
- 部署和执行BPMN工作流脚本。

用户可以通过以下方式获得CROS Token：

- 将业务合同模板发布到CROS模板库。其他用户使用合同模板时可以获得收入分成；
- 基于POBV共识算法在CROS主链上挖掘新币；
- 通过在跨机构工作流上提供服务获得Token。

参考文献

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] The Ethereum Team. A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper 2014

[3] Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., Mendling, J.: Untrusted business process monitoring and execution using blockchain. In: Proc. of BPM, Springer (2016) 329347

[4] Dumas, Marlon ; Rosa, Marcello L. ; Mendling, Jan ; Reijers, Ha jo A.:Fundamentals of Business Process Management. Springer, 2013.

[5] García-Bañuelos, Luciano & Ponomarev, Alexander & Dumas, Marlon & Weber, Ingo. (2017). Optimized Execution of Business Processes on Blockchain. .

[6] Murata, T. (1989). Petri Nets: Properties, Analysis and Applications. IEEE Trans Reliab. 51. 541-580.

[7] Wood, G. Polkadot: Vision for a heterogeneous multi-chain framework. https://github.com/polkadot-io/polkadot-white-paper 2016

[8] Redhat. The Drools Business Rules Management System. http://drools.org/

[9] Thomas, S. & Schwartz, E. A Protocol for Interledger Payments. https://interledger.org/interledger.pdf 2015

[10] Kiepuszewski, B., ter Hofstede, A.H.M., van der Aalst, W.M.P.: Fundamentals of control in workows.

[11] Hull, R, Batra, V.S., Chen, Y.M., Deutsch, A : Towards a shared ledger business collaboration language based on data-aware processes. In: Proc. of ICSOC, Springer (2016)

[12] 2. Milani, F., García-Bañuelos, L., Dumas, M.: Blockchain and business process improvement. BPTrends newsletter (October 2016)

免责申明

This is a conceptual document (“Technical White Paper”) describing our proposed CROS blockchain protocol and direction for its network development. It may be amended or replaced at any time. However, there is no obligation to update the Technical White Paper or to provide the recipient with access to any additional information.

Readers are notified as follows:

- **Not available to all persons**: the CROS platform and CROS Token are not available to all persons. Participation may be subject to a range of steps, including the need to provide certain information and documents.
- **No offer of regulated products in any jurisdiction**: CROS Token (as described in this Technical White Paper) are not intended to constitute securities or any other regulated product in any jurisdiction. This Technical White Paper does not constitute a prospectus nor offer document of any sort and is not intended to constitute an offer or solicitation of securities or any regulated product in any jurisdiction. This Technical White Paper has not been reviewed by any regulatory authority in any jurisdiction.
- **No advice**: this Technical White Paper does not constitute advice in relation to whether you should participate in the CROS platform or buy any CROS Token, nor should it be relied upon in connection with, any contract or purchasing decision.
- **No representations or warranties**: No representations or warranties are made as to the accuracy or completeness of the information, statements, opinions or other matters described in this document or otherwise communicated in connection with the project. Without limitation, no representation or warranty is given as to the achievement or reasonableness of any forward-looking or conceptual statements. Nothing in this document is or should be relied upon as a promise or representation as to the future. To the fullest extent permitted under applicable law, all liability for any loss or damage whatsoever (whether foreseeable or not) arising from or in connection with any person acting on this Technical White Paper, or any aspect of it, notwithstanding any negligence, default or lack of care, is disclaimed. To the extent liability may be restricted but not fully disclaimed, it is restricted to the maximum extent permitted by applicable law.
- **Other companies**: The use of any company and/or platform names and trademarks does not imply any affiliation with, or endorsement by, any of those parties. References in this Technical White Paper to specific companies and platforms are for illustrative purposes only.

You must take all necessary professional advice, including in relation to tax and accounting treatment. We hope the CROS project will be highly successful. However, success is not guaranteed and digital assets and platforms involve risk. You must assess the risks and your ability to bear them.

CROS

联系我们

EMAIL

info@cros.network

WeChat

CROSNETWORK

WEB

Cros.network