BitCAD

加密智能平台

新商业时代

*“每一个我们的设想都是从其他设想，想法和积累的经验（通过直接互动以及第三方中介获得）中建设而来。”—— Vlad Mitrofanov，BitCAD 首席执行官*

## 简介

BitCAD —— 是一种基于 Ethereum 区块链的多用途智能平台。 BitCAD 用户在交易双方之间创建可靠，可靠的关系，从而消除商业伙伴之间的不信任，不可靠性和不可预测性。

该智能平台的使命在于为无缝衔接商业和计算机技术提供场地。 BitCAD 将帮助用户自动化日常商务流程，在全球和本地寻找商机，实现即时价值交易，并在不可靠的环境中解决争议。

由于区块链技术的发展，BitCAD 取消了金融和法律中介的介入，使得用户能够通过与世界各地的合作伙伴协商和交易，从而自动形成更加灵活的供应链。

本白皮书以提高商业流程效率，灵活性和现代化为目标，介绍了使用 BitCAD 的基础知识，优势，实施的挑战以及实际应用建议。

# 1 BitCAD 区块链——未来的全球商业平台

区块链是分布式账本，现在主要被认为是金融服务领域比特币的组成部分。它提供可信资产和交易的分布式系统，而无需中央信任许可。

对于制造商及其供应商或物流合作伙伴来说，块中的单独交易可能包含原材料或成品的账单，其来源证明，执行操作质量或交货地点和时间的指示。在每种情况下，信息可以由合作伙伴进行存储，验证，共享和更改，而不需要花费时间和担忧谈判正式合同的延迟或者需要复杂的文书工作，例如银行的信用证或运输提供商的债券。

与传统的供应链不同，这些文件和合同由每个合作伙伴的采购，会计或法律部门维护。在一个区块链中，这些元素存储在许多分散的节点上。他们的隐私和诚信由“矿工会计师”（miner-accountants）而不是交易对方或银行等第三方维护。

BitCAD 提供了一个简单的智能合同和 DAO 构造函数，同时使得双方能够制定条款和条件，并确保合同的可执行性和对方身份的可信度。这种分布式信任系统在短期内降低交易成本，但这只是开始。从长远来看，它将会驱动更多灵活的价值链，“实时价格”技术，与商业伙伴更密切的合作，以及与物联网（IoT）的快速整合。

## 1.1 在 BitCAD 中的区块链应用

现代商业流程的低迷，交易双方之间的信任缺失以及与官方机构关系摩擦的加剧，加速了公众对简单，快速和易于访问（无需中介）的交互式环境的需求。

BitCAD 即为基于该需求的平台。

商业活动必须耗费大量的时间，金钱和努力来进行谈判，沟通和文书工作来克服缺乏信任的问题。以下三个关键功能就是 BitCAD 的变革力量所在：

•分散的诚信和信誉。 BitCAD 为用户提供快速并且低成本的信任，基于任何财务或交易关系中的双方的身份和声誉。这不仅降低了与已知合作伙伴交易的成本和时间，而且缩短了建立新业务关系所需的时间和成本。它还扩大了供应商和客户的全球范围，提高了从原材料运输到维修服务全过程的综合效率和灵活度。

•内置货币激励措施，以确保区块链中每笔交易和资产的安全。这不仅允许块链技术能够用于交易，而且可用作在多个价值链之间实现记录，跟踪和监控所有资产功能的注册管理机构和库存系统。这些安全信息包括从原材料到正在进行的产品的知识产权信息，如产品规格，采购订单，保修召回或任何货币或合同等。

•利用基于规则的智能来执行商业功能的能力。块链可以创建智能，嵌入和可信任的程序代码，让参与者将条款，条件和其他逻辑构建到合同和其他事务中。它允许商业伙伴自动监控价格，交货时间和其他条件等信息，并实时协商和完成交易。这降低了交易成本，最大限度地提高了效率，并允许制造商以不同的方式使用数据。

BitCAD 如何改变现代业务流程：

•智能合同：它将采用在区块链上运行并由整个区块链网络执行的计算机程序的形式。其程序代码 —— 合同的条款和条件不能更改，因此提供了完全的信任（过去的流程要求精细的控制和审计流程）。区块链合同不仅可以包含与实体合同相同的细节水平，还可以做一些常规合同不能执行的任务：执行谈判价格和监

控库存水平等。通过自动化、动态地跟踪供应链，库存水平和价格，这又一次代替了昂贵的手工工作，以实现降低成本和最大化利润。 BitCAD 可以将“任何一处到任何一处”市场的愿景变为现实。

•智能设备和产品：例如，考虑一种已经注册在平台上的智能自动售货机。我们能够跟踪其库存和现金状况。该机器不仅在需要补货时发出补货订单，而且可以在没有人工参与的情况下以最优惠的价格找到所需的产品或者完成订购和支付。

BitCAD 的优点：

•用户进行交易的门槛低。

•智能合同中参与者表现的“声誉”赋予表现最佳的用户要求额外费用的权利。

•智能设备可以取代某些人工交易，如我们的自动售货机的例子。

•物联网的设备可以与智能合同进行通信，以跟踪智能合同的状态。例如，智能集装箱可以自动出售其过剩产量。

•使用加密货币更快的结算。

BitCAD 的功能：

•追踪审计：实时追踪 BitCAD 中每个领域的情况，为货物流动提供了关键的证据，为“实时价格”开辟了新的机会。

•实时谈判：智能合同持续查询不同平台上的所有节点，以获得最佳的定价，交货时间和其他条款和条件。

•供应链可视性和可追溯性：例如通过生产记录，可以跟踪是否有缺陷的商品被

制造出来。

•链接物联网大数据：轻松跟踪和验证物联网数据，为企业提供更多更好的产品数据，从而提高质量。

•产品开发中的知识产权管理：使得安全得共享知识产权更容易，更廉价。

### 1.2 BitCAD 的管理：多利益相关者模型

BitCAD 是一个社会福利组织。其工作人员运营智能合同系统，协调标识符的分配，授权行业代表，并倾听致力于维护 Smartnet 安全、稳定和可互操作的全球志愿者的心声。BitCAD 致力于促进竞争，以及帮助开发 Smartnet 政策。

BitCAD 的核心决策就是所谓的“多利益相关者模型”。该分散化系统使得个人，行业，非商业利益和政府都保持在同等水平线上，而不同于传统的自上而下的治理模式，即政府做出政策决策。BitCAD 使用的多利益主体方法允许基于社区的共识驱动的决策，秉承着无国界，多边且对所有人开放的主旨。

BitCAD 最重要的特征是在每个重要决策之前进行公开的公开讨论，无论是在运营（预算，发展战略），技术（安全问题）还是行政方面（修订关键政策）。

公开讨论将按照以下程序进行：

•每个问题讨论时间不少于 21 天。

•在评论期后，回复期同样不少于 21 天。

•如果在评论期间没有收到实质性评论，则不会开始回复期。

•在回复期间，只有收集的意见将被解决，新的讨论场所将不再可用。

虽然 BitCAD 董事会具有批准或拒绝政策建议的最终权力，但业务组织有责

任向董事会提出有利的政策建议。

全球 BitCAD 社区是主要的自我教育驱动。每个参与者都可以直接参与平台的开发和推广，同时有机会创建本地的 BitCAD 组织。BitCAD 的最终目标是每个国家都至少有一个实体。 BitCAD 的理事机构包括董事会和具有完全包容性及透明度的咨询委员会，如图 1 所示。

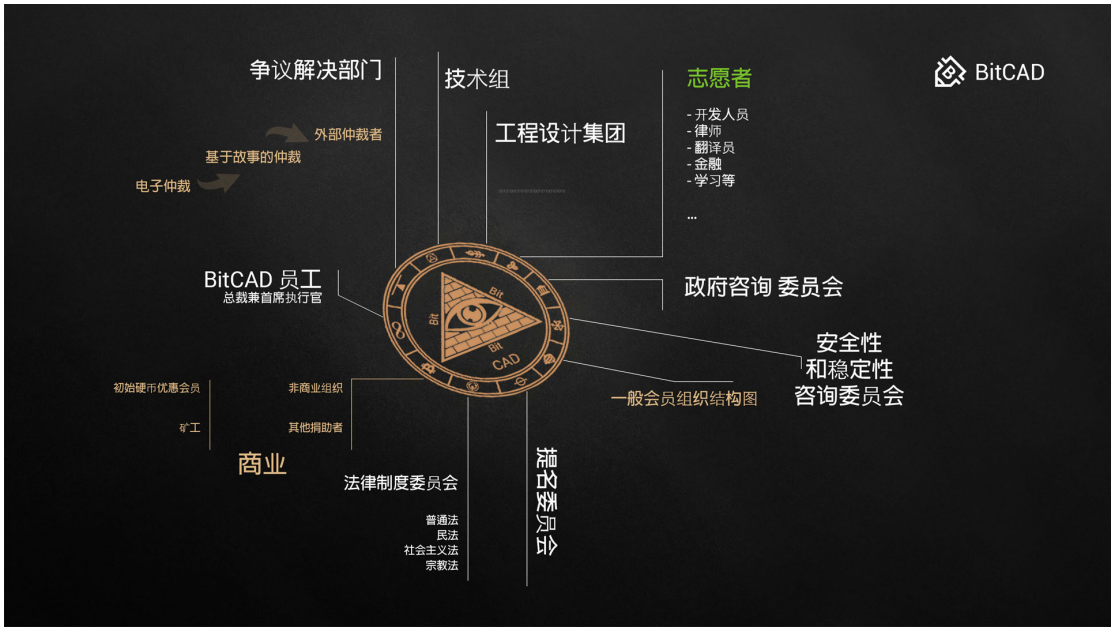



图 1：多利益相关者模型 BitCAD

BitCAD 的董事会

BitCAD 的董事会是一个负责政策制定和日常平台管理的跨国机构，由 16 名有投票权的成员（包括 BitCAD 总裁）和 5 名无表决权的代表组成。

4 个有投票权的成员由商业支持组织 Business Support Organizations (BSO)任命。 法律系统委员会 Law Systems Committee (LSC)和 At-Large Advisory Committee (AAC)相应选举了两位和一位有投票权的成员。 其余 8 名

有表决权的成员由提名委员会投票得到。

无投票权的成员由政府咨询委员会 Governmental Advisory Committee (GAC)，安全和稳定咨询委员会 Security and Stability Advisory Committee (SSAC)和技术组和工程设计小组任命。他们在决策过程中提供技术咨询。

提名委员会 Nominating Committee (NC)

NC 包括志愿者组织的领导。它选举了一些官员（其中包括 8 名投票委员），网络普通用户咨询委员会 At-Large Advisory Committee 的一些成员以及商业支持组织 Business Support Organizations (BSO)，法律系统委员会 Law Systems Committee (LSC)的代表。

业务支持组织 Business Support Organizations (BSO)

BSO 是代表各种领域专家的包容性社区，负责制定全球性政策，并将政策传递给 BitCAD 董事会批准。它提供了交流重要信息和讨论全球问题的平台。

BSO 委员会是一个由商业业务支持专家组成的团队，负责监督所有 BSO 活动，开发平台的总体政策，并向 BitCAD 董事会提供咨询。 一旦当选为 BSO 成员，投票委员身份即被理事会正式批准。

BSO 委员会包括 18 名代表。其中 15 名代表由 BSO 社区（每个地区 3 名）投票决定，其余 3 名由提名委员会任命。

网络普通用户咨询委员会 At-Large Advisory Committee (AAC)

AAC 是 BitCAD 的核心机构，代表 BitCAD 用户的核心利益，并向董事会提供影响个人用户的政策和活动。

AAC 领导层由提名委员会任命的 5 名成员和 10 名由社区选举产生的成员组成（每个地区 2 名）。 NC 任命的 5 名成员也必须代表世界的五个地区。


政府咨询委员会 Governmental Advisory Committee (GAC)

GAC 在各种公共政策活动中宣传 BitCAD，特别是当本地法规与 BitCAD 的政策和活动出现差异的情况下。

GAC 由地方政府和跨国组织的指定代表组成。政府和其他机构将能够向 BitCAD 请求 GAC 会员资格。

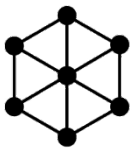
GAC 是一个由共识驱动的组织。 GAC 不会像联合国一样达成一致意见而作出决定。如果出现不能解决的分歧，委员会将所有意见通知董事会。


法律制度委员会 Law Systems Committee

LSC 是一个咨询委员会，负责解决与国际法律制度有关的问题，包括智能合同的标准化和通用数字法律语言的发展。LSC 还将任命 2 名投票委员会成员。

23 名委员将从法律领域的高级专家中抽取出来，并分为上下两院（类似英

国议会模式）。一个院将代表行业，另一个院将代表独立企业和非营利组织。这种制衡机制将防止任何主要成员控制委员会。



安全和稳定咨询委员会 Security and Stability Advisory Committee

SSAC 是由工程师，科学家和安全专家组成的咨询委员会。该委员会使平台免受外部和内部的攻击。

SSAC 成员由董事会任命。任何用户只有在通过严格的筛选过程后才能够进入任命名单。

跨国志愿者社区 Multinational Volunteer Community

BitCAD 志愿者社区是平台领导力的主要驱动力。每个志愿者（或一组志愿者）都可以参与 BitCAD 的开发以及政策、程序和商业模式的建议活动。积极和有创造力的志愿者将能有机会加入 BitCAD 的各个委员会和组织的行列。

BitCAD 将欢迎具有广泛技能的志愿者参与：开发，法律，翻译，会计，营销等。BitCAD 将创建一个教学在线平台，使得新进入的学习者可以快速获取新技能或有效应用现有技能。

BitCAD 员工

BitCAD 工作人员负责执行和实施由 BitCAD 社区开发并由 BitCAD 董事会采用的政策。 BitCAD 员工是从会计，人力资源到技术支持和工程的各个领域的专业团队。

Tectum

Tectum 是 BitCAD 的“孪生”项目，旨在通过 API 促进 BitCAD 的全球整合，并致力于创建一个分散的市场。

Tectum 将会大力向市场推出智能合同。 这将有助于 BitCAD 的用户在已在的交易平台上购买商品，寻找和密封商品，解决物流问题并优化商业流程。

Tectum 目前已经在俄罗斯和中国成功运营。 Tectum 的目标是在符合当地法律的前提下，在每个国家开放其认证中心。这样不仅可以让居民提高在海关和税务局的服务体验，还使其与金融机构和市场互动更容易。

## 2 智能合同——促进业务流程的更好方式

在 1996 年，尼克·萨博（Nick Szabo）将一个智能合同描述为“以数字形式呈现的承诺，包括各方在这些承诺中履行的协议”。虽然自此支持智能合同的技术发展很迅速，关于智能合同核心的定义依旧没有定论。

智能合同通常部署在区块链（尽管其他平台也可能作为托管场所）。在一个块状视图中，智能合同程序逻辑位于“块”内。块是一个软件生成的容器，能

够将信息与特定智能合同捆绑在一起。这些消息可以充当智能合同编程逻辑的输入或输出，并且可以指向其他计算机代码。

### 2.1 合同的语义

我们的部分任务是考虑合同的语义建构——即合同的“意义”是什么？它有不止一个意思吗？合约该如何解释？我们从简单的语义框架开始，并将法律合同视为有两种：

1. 操作语义：这是合同的操作性解释，它来源于对当事方采取的确切行动的考虑。因此，它涉及合同的执行过程。

2. 指称语义：这是整个合同的非操作性的法律解释（或“意义”），包括其所有明显的组成部分和引用的任何其他法律文件。这是律师阅读合同时对合同的意义。

这两个语义不考虑合同的不同部分 —— 它们都是对整个合同的解释，但是具有不同的目标。一个合同可能包含几个文件，同时这些文件受批准的过程可能很复杂。即使是非常简单合同的指称语义可以非常大和复杂，然而相比之下，操作语义可能很简单，同时易于自动执行编码。

操作语义决定了合同的成功执行。如果出现争议，则合同的指称语义通常会规定接下来会发生什么 —— 即在当事方权利和义务的范围内，规定在一方部分履行或不执行情况下应采取哪些补救措施。

法律合同的大部分通常用于当执行存在问题时来界定各方的义务和责任。有时，严重违反合同所采取的行动能够被精确表达。然而，事实并非如此，争议解决可能需要长时间的谈判解决，仲裁或法庭诉讼程序。

此外，重要的是要认识法律的重要作用。所有人需要了解包含在“文件的四个角”内的合同是不现实的。律师将在执政法律的范围内阅读和理解合同——即每份法律文件必须根据其规定或推定的管辖权的相关法律（公司法，消费者法等）进行解释。因此，该法律文书的语义也必须被理解。值得注意的是，法律问题不仅涉及指称语义，还涉及到操作语义——例如，由于政府实行的制裁，某些国家之间的交易可能是非法的。

鉴于这种支持金融工具的法律合同的语义框架，我们可以从智能合同的不同角度得出：

•智能合同代码主要专注于执行，因此只有在执行代码中的操作语义才与其相关。然而智能合同同时考虑了法律合同的指称语义和操作语义，然后执行其操作语义（可能通过智能合同代码）。

### 2.2 更智能的智能合同

通常根据不可阻挡的计算机分布式网络来描述“防篡改”执行。无论恶意行为，断电，网络中断，自然灾难或任何恶意事件，技术意义上都不会失败。有了这样一个系统，假设软件代理一旦启动，就不能停止。对于真正“不可阻挡”的软件代理，代码必须体现为能够采取适当的行动来回应可能发生的各种动态（如另一方没有足够的资金来执行所需的付款）。在正常系统中，软件代理可能会中止同时执行错误或不履行的一方将以传统方式执行。但是在不可阻挡的“防篡改”版本中，所有这些可能性都必须预先确定并且采取适当行动。因此它们不再被视为执行错误或不履行的一方，而是系统的预期状态。

虽然有些机构正在积极追求“防篡改”的智能合同代码，但我们倾向于采

用传统法律手段执行的智能法律合同，其原因包括：

•在强制执行“防篡改”网络共识的系统中，将不会存在“执行覆盖”规定。一旦作为智能合同代码启动，协议就不可能改变。但是，动态变化的协议规定是很常见的。例如，允许信誉良好的客户延迟支付利息几天，或允许付款 假期，或允许统一结算利息。除非事先对每个可能的变化进行编码，否则在防篡改系统中都不可能实现。

•通过网络共识强制执行只适用于在网络控制下执行义务或行使权利。然而，物理世界中的对象和行为不太可能完全受到网络的控制（如果有的话）。

•涉及付款的智能合同代码将需要发布抵押品才能完全实现自动化。抵押品的这种锁定将导致杠杆作用的大幅度下调，并将流动性拉低市场。市场可能会变得更加稳定,但市场参与者将强烈抵制杠杆作用的下调和随之而来的市场下滑。

### 2.3 智能合同构造和模板

BitCAD 的智能合同以标准化模板为基础，提供了一个框架用以提供支持金融工具的法律协议。它使用参数将法律散文连接到相应的计算机代码，目的是为智能法律合同提供法律上可执行的基础。它还有助于自动执行合同，并在发生争议的情况下直接链接相关的法律文件。

通过识别用来指导智能合同代码的可执行行为的关键参数（在本文中称为“执行参数”）来增加复杂的法律文档 —— 智能合同代码为能够通过输入执行参数来控制的标准代码。

在这里，我们将探讨实施智能合同模板的设计环境。我们发现其范围很广泛

且有许多潜在可行的设计决策。因此，我们建议，应该开发一种新的域名专用语言来支持智能合同模板的设计和实施。这种语言的发展已经在进行中。我们称这种常见的电子法律语言 LawTech 或“CLACK”（增强合同知识的通用语言）。

目的是与广泛的执行平台进行衔接。智能法律合同可以在分布式分类帐（如 Corda，Ethereum，Hyperledger 等）上运营的软件代理人执行。

### 2.3.1 模板和参数

模板是由标准机构发布的法律文件的电子代表，例如 International Swaps and Derivatives Association (ISDA)。模板包含合法散文和参数，其中每个参数都有一个身份（一个唯一的名称），一个类型，并且可以（但不需要）具有一个值。协议源于模板，但在谈判过程中可以定制法律散文和参数。签名协议中的所有参数的值是必需的。

协议是一个完全实例化的模板（包括任何定制的法律散文和参数）。在这个阶段，由于交易对手的谈判，法律散文和参数的定制是很常见的。我们也观察到，协议由多个文件组成，例如与各种附件（例如附表）和信用支持文件（例如信贷支持附件）的框架协议（例如主协议）。因此，协议的法律散文将从模板中得出，但不一定需要相同。同样的是，协议的参数将从模板中得出，但也不一定相同。

导出一组执行参数可能由于这三个因素而变得复杂：

1. 执行参数通常嵌入在法律散文中——这些参数的识别最初将通过视觉检查进行，并由图像用户界面辅助。

2. 在协议（和模板）中确定为“参数”的一些值可能不具有操作影响，因此不

应包括在一组执行参数中。

3. 在第一个文档中给定参数的名称，再在第二个文档中赋值，并在第三个文档中使用（以商业逻辑）是可能的。虽然参数不需要在模板中被赋值，但它们必须在已签署协议中被赋值。所有协议的参数值都是合同的关键部分，因为它们直接反映了各方之间的商业关系以及执行参数对合同的影响。

### 2.3.2 智能合同建设者的设计环境

现有法律文件模板中的大多数参数具有简单的类型，如日期，数字等。这些是“基本”或“原始”类型。例如，图 2 说明了主协议中日期的识别。 一旦被高亮和注释，该参数的名称（“协议日期”），类型（“日期”）和值（“16—Mar—2016”）将被传递到可执行代码。


图三

法律散文中的日期被高亮，且通过注释以表示一个简单的参数是被允许的。参数名称为“协议日期”，键入“日期”，值为“2016 年 3 月 16 日”。

不需要将参数限制为基本类型。更复杂类型的值（如列表），也同样需要转移到可执行代码。

将参数传递到可执行代码是必要的，因为我们需要使用标准代码。例如，理论上每个交易可以产生全新的代码，同时在这种情况下不需要参数。参数的数量以及这些参数类型的复杂度通常会随着代码变得更为通用而增加。

除了具有基本类型和更复杂类型（如列表）的参数之外，参数也可以是包含

对其他参数名称的引用的表达式。除非表达式中定义了其他参数名称，否则表达式是有效的函数。在函数作为参数传递的地方，这被称为“高阶”参数，接收代码被称为“高阶”函数。

参数的使用不仅可以用于支持更大程度的代码标准化。在未来，我们可能会看到越来越多的使用正式结构化的表达式嵌入在法律散文中。如果法律散文中的所有商业逻辑都可以用算术或逻辑表达来代替，如上一节讨论的高阶参数，那么法律散文的歧义将会减少，法律散文翻译成执行参数的错误也会减少。这种将正式逻辑运用到法律散文中的过程需要正式结构才能在法庭上获得接受，并且可以被接纳为双方目的的证据。

图 3 说明了我们对未来智能合同模板中参数的复杂性及其在智能合同模板中的作用如何演变的看法。


图 3 法律散文和参数的演变

执行参数在将来可能变得更加复杂，从简单的基本类型参数演变而且还包括更复杂的高阶参数。在未来，如果在参数中使用的商业逻辑的编码能够被律师和法庭接受，那么它可能会替代相应的法律散文。

在前面的小节中，我们观察到，由于对标准化代码的诉求，将参数传递给可执行代码是必要的。这对于效率原因很重要。否则不同的智能合同必须为每个不同的交易构建，测试，认证和部署。如果可以将代码标准化为调用代码的参数，效率会大大提高。

这因此驱动了对代码通用性的需求。我们可以通过传递更多的参数和/或更复杂的参数（具有更复杂的类型）来实现。然而，尽管使用标准化和更通用的代码能够获得收益，但是仍然存在每个银行目前管理其独有代码库的问题。如果智能合同代码能够统一（即共享），则可以只需建立，测试和认证一次，然后即能被每个交易对手使用。

一个可能的进化路线可以建立在使用通用效用函数的基础上 —— 所有交易对手已经接近相同。

### 2.4 未来工作：合法智能合同的通用语言

一个很好的例子是从合同到执行直接处理方式的潜力。目前，律师起草法律合同，然后由其他律师团队进行谈判和更改，然后运营人员检查合同文件和/或其他材料，以确定执行参数，然后却传递给可能已经写过的代码。

这引发了几个问题：

•我们可以绝对确定合同的含义吗？所有各方是否真的同意合同的含义，或者它们各自对合同的含义有什么不同的理解？

•我们可以确定操作人员已经确定了所有执行参数吗？我们可以确定已经确定的那些参数确实与操作有关吗？我们可以肯定他们的名字，类型和价值观被准确地转录了吗？

在将参数传递给代码并运行代码之后，我们可以确定代码将忠实地执行合同的操作语义吗？它会在所有情况下这样做吗？

解决方案是开发一种正式语言用于书写法律文件即合同文件。文件中的语义需要清晰，同时执行参数可以自动识别并传递给标准化代码（或者可以生成

新代码)。这种正式语言会：

1.从精心设计的计算机编程语言中获得一些重要的特点，例如清晰易懂以及组合路径，使得任何条款的含义可以在不阅读文档其余部分的情况下被明确推导出来

2.易于使用。在这种程度上，律师可以使用这种形式而不是使用传统的法律语言来起草合同。

前者在学术界和其他领域已经受到重视。相比之下，后一方面可能是更大的挑战。另一个挑战是，以类似计算机语言编写的这种合同是否可以在法庭上被接纳为对双方意图的真实和忠实的表示。签字和篡改证明文件的问题很容易解决，但法院是否接受这种合同中短语的含义的定义并不明确。这个问题可以通过两种方式解决：

1.作为第一步，该语言能够产生更“自然”的法律风格的文件版本，从而可以在法庭上受理。

2.最后，对特定领域语言和法律的进一步研究可能导致新的形式主义，从而能够在法庭上受理。

由于这种复杂性，我们有动力定义一种通用语言，以支持在智能合同模板的设计空间中得到不同的解决方案。

最初，该语言将有助于规范不同的设计选择和原型的构建。一般来说，语言应尽可能灵活尽可能能够被广泛应用。初步的要求草案如下：

•它应该同时为法律散文和参数提供支持。

•它应该支持不同的内部结构化格式，如 XML。

•它应支持各种格式执行参数的输出，如 FpML。

•它应支持包含多个文件的合同。

•它应该管理从单个模板（和模板层次结构）实例化的多个协议。

•它应允许在一个文档中定义参数，在第二个文档中被赋值，并在第三个文档中使用参数。

•它应该支持多种参数类型，包括高阶参数。

•它应该支持越来越多的标准化和共同的代码共享。

•它应该支持多个执行平台。

•它应该支持与法律散文的充分互动和对法律散文的自动化。

•它应该支持合同的数字签名，加密标识的构建，以及使用该标识作为智能合同参考和恢复的认证标志。

CLACK 语言被指定作为原型来支持智能合同模板。后续步骤包括完全确定文档内和文档间的参考，包括歧义和冲突解决策略，高阶参数中表达式的语法和语义等。

未来有很多问题亟待解决。 我们在本文中已经探讨了一些这些问题，但是我们将带来更多疑惑：是否有可能对金融合同进行直接处理，并且能够充分信任自动化执行合同的操作语义？ 当然，这需要与律师，标准机构和金融服务业合作的学术界的大量工作。

## 3 智能预言——连接现实

智能预言提供了一种简单，灵活的方式来实施“智能合同”，它编码业务逻辑，法律和其他约定的规则。智能预言建立在预言或者提供给智能合同外部世界状态信息的实体的基础上，并将信息收集与合同代码执行相结合。在这样的系统中，规则可以用任何编程语言编写，并且合同可以与任何接受加密签名命令的服务进行交互。这包括但不限于密码安全网络。

一些智能合同系统，包括 Bitcoin 的内置系统，是被严格确定的。为了与现实世界进行交互，这些系统依赖于外部系统提供的称为“预言”的加密签名。

预言是对世界状态进行声明的受信任的实体。由于对于签名的验证具有确定性，确定性的智能合同能够对（非确定性的）外部世界作出反应。

### 3.1 从预言到智能预言

智能合同和预言的概念已经存在了一段时间。几个早期的设计（包括比特币）依赖于在共同网络内执行合同，这就要求其执行具有确定性。在本文中，我们的目的是展示将合同执行融合于智能预言，能够极大程度地简化系统。

最近，加密货币的产生和盛行激发了对人们智能合同的兴趣。基于数学的货币网络为智能合同提供了重要的基础：有价值的数字资产可以通过使用加密签名来进行传输。协议中的资产由公共/私人密钥对标识的帐户所有。当交易携带只能由帐户的私钥的持有者产生的加密签名时，付款才能实现。智能合同可以创建这样的加密签名，因此被指定为任何类型的数字资产的部分或唯一所有者。

不幸的是，加密货币开发人员发现设计一个同时包含强大的智能合约语言和共识系统的系统是非常具有挑战性的。比特币脚本允许在比特币网络上编码和执行简单的逻辑。然而，编码高级逻辑和执行不受信任的代码已被证明更为复杂。

我们认为，可以通过安全可信的方式实施强大的智能合同，同时不会增加现有共识网络的复杂性。

执行不受信任的代码应与共识数据库和跟踪及转移资产所有权的其他服务分离开来。分离的合同系统可以处理不受信任的代码执行，并通过加密签名与共识数据库进行交互。这些签名已经是协商一致的协议原生的，所以不需要修改。从共识网络中分离合同存在额外的好处，即合同可以同时与多个网络以及几乎任何类型的在线服务进行交互。这意味着单一的智能合同可以与 Bitcoin 和 Ripple，基于网络的服务（如 PayPal，Google，Ebay 等）或甚至其他互联网协议（如 SSH，LDAP，SMTP 和 XMPP）进行交互。

如果合同执行与现有系统分离，代码应该在哪里运行？这就是智能预言进来的地方。

对于智能合同的大多数提议（即使是像 Bitcoin 这样的共识网络内部的合同），都取决于独立实体通知反映外部世界状态的合同。只有在满足特定条件的情况下，比特币合同通过将签名引入网络，才能依靠于“预言”来证明来自外部世界的事实。智能预言进一步将将不可靠的代码执行加入预言中。智能预言是信任或半信任的实体，可以提供有关外部世界的信息，并执行缔约方同意的

守则。

### 3.2 实施智能预言

智能预言的实施可以采取许多不同的形式。在下面的章节中，我们将介绍一些我们认为对于大多数（即使不是全部）的智能预言。也就是说，关键组件是：安全识别代码，沙箱代码，智能 API，合同托管和计费模型以及合同客户端。

一旦缔约方已经同意其安排条款，他们必须将规则转化为代码。双方必须检查拟议的守则，并确保其代表他们同意约束条款。同样重要的是，他们可以轻松地验证上传到智能预言的代码是否准确。这就是使用模块的确定性代码编译，散列和代码重用的地方。

合同的所有各方都有很大的利益，以确保最终的机器可执行代码代表合同所有方都认同的逻辑。对于编译语言，这意味着源代码必须与可重复的过程一起共享，以将其编译为机器代码，例如使用 Gitian。对于解释语言，分享源代码就足够了。无论哪种方式，参与者同意智能合同执行的最终指示是至关重要的。

加密安全散列是识别商定的二进制文件或源代码文件的便捷方式。散列函数将任意数量的数据作为输入，并产生一个短的，固定长度的字符串。出于实际目的，这种“散列”可用于任何文本或数据的唯一标识。

尽管可能不是必须的，但我们建议使用防碰撞散列函数。这意味着试图找到具有相同输出散列的两个输入是不切实际的。使用相同散列的两个工作代码是非常困难的，即使使用只有第二个代码存在防图像的散列函数。但是，如果

有人可以使用相同的三裂创建两个不同的合约，那么会导致严重的问题。因此，我们建议使用同时防图像和防碰撞的散列函数。

传统的合同通常都有共同的“样板”元素，智能合同也没有什么不同。任何智能预言系统都可能提供某种形式的代码重用，这能够同时增加方便性和安全性。

许多合同将相对简单易懂的逻辑建立在众所周知的和广泛使用的模块之上。模块可以包含基本功能，例如连接比特币或其他系统的机制。他们还可以包括更高级的功能，如标准拍卖，托管或债券实施。这个逻辑很可能得到许多独立方的广泛使用和验证。

智能预言概念的核心是用户能够就合同的代码达成一致，然后将其上传到受信任的第三方来执行它们。智能预言必须能够安全地执行不受信任且有可能是恶意的用户代码。预言必须保护自己的系统和正在运行其他合同的完整性。

智能预言最灵活的部分之一是计费系统。它能允许缔约方支付执行智慧预言的费用。计费系统完全与核心系统设计分离开来，以接受他们选择的任何付款方式，无论是信用卡还是比特币。结算费用也完全取决于工作人员。

智能合同是目前在技术，商业和法律领域的前沿技术。智能预言将将现实世界的信息与沙盒代码执行环境结合在一起。它独立于现有的分布式网络，如比特币和 Ripple，并且可以与任何基于互联网的服务（包括所有分布式共享数据库）进行交互。将不受信任的代码执行与分布式网络分离可以降低其复杂性，从而提高两个系统的安全性。

智能预言为开发商，企业家和法律及金融专业人士开辟了新的可能性。以前

法律合同需要冗长反复的过程，但是如今可以由智能合同自动翻译成代码。智能合同具有赋予人们更大的权力来建立更公平，更实惠和更有效的法律制度。这也是实现梦想的最简单的方式之一。

## 4 争议解决

争议解决部门是一个包括三个阶段的自动化过程领域。其由电子技术和故事为基础的仲裁组成，或独立和公正的雇佣人员，能够解决有关 BitCAD 和组织管理层决策方面的问题和投诉，以及员工、董事会或社区对参与者的不公平情况。

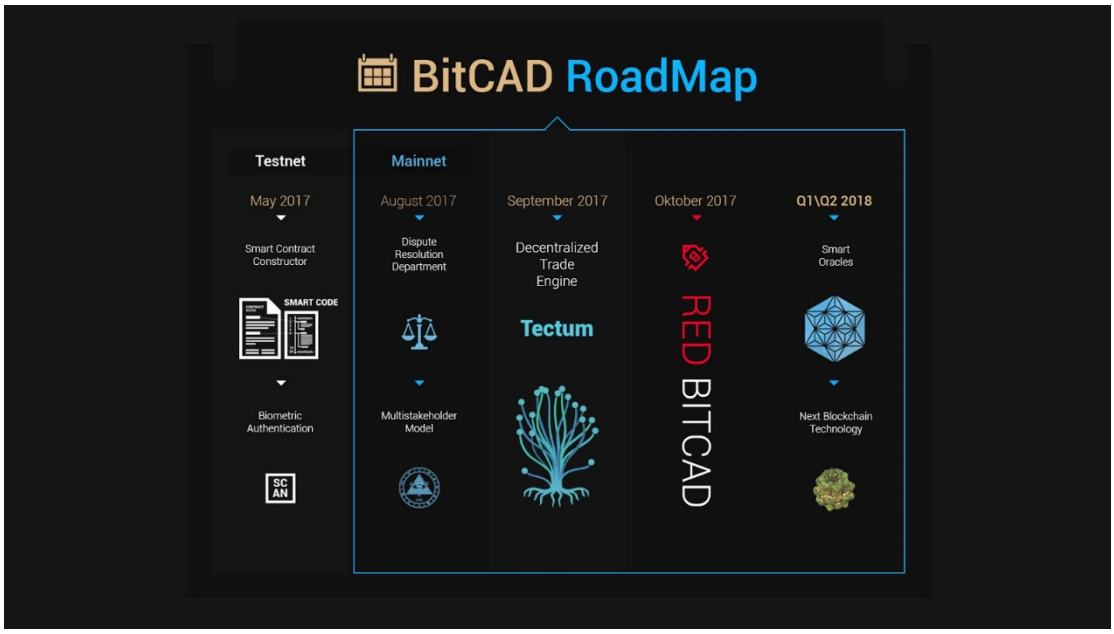
电子仲裁是一种基于互联网技术的全面自动化的争议解决方法。我们可以应用电子仲裁来解决 BitCAD 平台内的所有问题 —— 从包括消费者争议到人际纠纷及冲突。电子仲裁具有很大的解决电子商务冲突的潜力。新的代码模型是嵌入式的，同时代码能够根据交易方的行为和整个交易过程中的交互历史来评估各方。当各方不同意该决定时，他们可以通过自愿随机选择的形式在线解决冲突。

以故事为基础的仲裁是一个权力下放法庭的典范。其中有一个法官被随机选取坐镇权力下放的司法系统中。历史记录和所有文档能够由各方通过提供必要的私钥来单独打开。在某些情况下，只有当各方有私钥时，才能提供双方谈判的加密视频录像。其具体情况取决于开始谈判的初始条件。

监察员是 BitCAD 系统中一名独立，公正和中立的人员，对本指南中描述的 BitCAD 和支持机构的决策，行动或延迟的问题有公正的判断。他是公平的倡导

者。监察员调查这些投诉和企图解决所有的问题。我们强调调解是解决问题的主要手段。所以监察员经常会在各方之间进行调解。但是其没有权力作出，改变或撤销政策及行政人员或董事作出的决定。监察专员有权调查这些事件，并能够使用调解等解决技术来解决这些事件。仲裁法庭，私人律师和国际顾问都有资格作为监察员签约。

## 发展路线图




May 2017 —— Testnet 发布

•生物识别

•智能合同和 DAO 的构造者

2017 年 8 月 —— Mainnet 发布

•争议解决部

•多利益相关者模型（BitCAD 的自治系统）

## 2017 年 9 月

•分散贸易动力 Tectum（应用和 API 的推出）

## 2017 年 10 月

•Red BitCAD（该平台将要启动，任何人或公司都可以在平台上开展和开发业务、使用功能，包括声誉跟踪器。）

•Dark BitCAD（平台与 Darknet 社区合作）

## Q1 / Q2 2018

•智慧预言

•下一个区块链技术（基于分形数学，机器学习和量子密码学的实验技术。采用超级计算机建立业务逻辑和虚拟业务生态系统。）

# 术语表

## 区块链

区块链是一种分布式分类帐，用于持续检查每个交易或数据输入的安全性和完整性。由哈希值链接的块和通过工作证明（或替代的验证算法）激励的块为分块式的信任在块链中提供了基础。

虽然在金融服务领域最为人所知，作为一个基础架构，可以在各方之间实现可信赖的金融交易，而不需要像银行这样的第三方，它可以用于任何行业，以实现更快，更便宜的交易，并支持更灵活不可能的供应链。

## 业务流程

业务流程是各种类型任务的复杂多层次组合，旨在创建某种产品（或服务）及其市场整合。即使是单一产品的单一组成部分也可能涉及无数交易，包括报价请求，传输采购订单和工程变更通知。每种交易类型可能需要不同的金融和监管中介机构，以及双方之间的自身合约和信托关系。凭借立即和低成本的信任保证，BitCAD 可以通过允许任何用户立即找到并开始关系来释放破坏性创新。

## 智能合同

1996 年，尼克·萨博（Nick Szabo）将一个明确的合同描述为“一套数字形式的承诺，包括各方对这些承诺履行的协议”。

换句话说，一个聪明的合同是一个协议，其执行是可自动化和可执行的。由计算机自动化，虽然有些部分可能需要人工输入和控制。可以通过法律强制执行权利和义务或防篡改执行。

## DAO

DAO（权力下放自主组织）是经济合作的新范式。与传统公司不同，DAO 是分散的（它没有所有者，更倾向于横向治理结构）和自治（金融交易记录和计划规则保持在一个块，由整个社区维护）。 DAO 中的大多数业务流程都是自动化的，并通过称为智能合同的计算机程序编码的规则执行。

## 实价

BitCAD 的签名功能，可实时监控在线或实体店中任何产品的价格。这个未来的技术依赖于泛滥的无处不在，以便在全球范围内收集可靠的市场数据。

实时价格数据是市场分析师的天赋，也是客户的福音，使他们能够监控现实价格，而不是投机计划。

## SMARTnet 服务

互联网 2.0，互联网发展的下一个阶段是以权力下放网络和全球智能合同为一体的标志。