FirmaChain

白皮书

Version 1.1

目录

1. 概要

1.1 知识产权许可(专利权,商标权,著作权等）合同的重要性。

互联网的发展打开了无国界的信息时代。因此保护知识产权和工业应用的知识产权许可协议不仅是个人竞争力的核心，也是企业和国家竞争力的核心。但是因为现在没有技术力量来追踪知识产权保护和转让的履历，所以存在知识产权侵权和国际知识产权许可合同的欺诈以及全球滥用权利等问题。我们希望实现通过区块链技术能够准确记录知识产权认证和转让，以便安全地保护国际知识产权许可协议。

1.2 知识产权许可合同领域上电子合同的必要性。

现代人在签合同时，依旧秉持着传统的书面签约方式。虽然法律也认同电 子合同的效力，且诸如电子签名以及与有关电子文件的服务陆续问世，但是除了 个别开放的 IT 企业之外，大部分企业尚未意识到电子文件的便利性，仍旧固守原 有的书面签约行使。

于是我们开始思考：
‘企业为什么更偏好书面签约形式呢?’

在合同签署时，比起电子合同，当代社会仍然更信任书面合同。因为书面契约有原 版可做证明，此外，提供电子合同的服务多数存在中心化问题，有伪造、篡改的 风险和数据流失等各种风险因素，难以得到信任。若交易资金规模较大，合同当 事人易产生担忧（如，伪造、删除内容等），签约与生活有密切关系，但当事人 的种种担忧严重阻碍了签约这一形式的发展与进步。此外，在企业进行跨国签约 时，通过海外法人得到的交易贷款税金、转账费、处理费等给合同当事人带来巨 大负担。下面通过几个日常生活中发生的事例来说明这一问题。

事例 1.

我最近从拥有知识产权（专利权）的用户那儿购买了许可证。
但是我怀疑它是否是专利所有者 ， 因为它来自外国用户的购买 ， 而不是国内用户。而且我也特别担心因为很难核实卖方是否也向其他人授予了独家许可。此外 ， 如果第三方未经授权或不公平地使用我购买的许可专利权，我该怎么办？

事例 2.

A 公司与 B 公司计划签署发行合同，直至签约前一天，两家公司还在修改文 档，不断进行磋商。双方签约合同当天，B 公司打印的合同原件上多出了一条不 属于版权保护范围内的内容。因时间紧凑，公司董事长也在场，当时的情况十分 尴尬。幸好工作人员及时修改了内容，没有影响签约，但这种情况随时都会发生。

基于上述情况，在知识产权许可协议领域引入基于区块链的电子合同服务不仅可以提高合同签订过程的有效性，还可以构成合同可扩展性，例如保护知识产权和可追溯性。

FirmaChain 将实现区块链的去中心化，这将保证区块链交易账本的透明性， 通过可信性从根本上解决合同伪造及篡改问题。此外通过 DApp，合同当事人可 履行合理的合同签署程序，利用较少的资源起草合同，通过简化过程减少跨国合 同签署时所需的处理费用，以此来打造解决书面合同限制的合同程序管理服务与 信任度高的分布式数据库。

1.3 数据的去中心化

如今，全球多数的个人电脑都处于开机状态，但并不是每台电脑都在使用 电脑系统资源。硬盘等储存空间与网络宽带就是典型的例子。例如，将剩余的储 存空间和网络服务租借给有需要的用户，可收取适当费用。与其他类似的文件储 存服务相比，用户可以以较低的价格储存文件，而本人又可以将闲置的资源转化 为收益。

如何在保证数据的完整性与可信性的同时，又能提供稳定的储存空间呢？ 考虑到上述几点，我们推出了去中心化的分布式文件储存系统。"去中心化"是 指不存在中央管理储存的机构，而是由参与系统的所有用户进行管理与运营的系 统。因此，所有文件不经过中央机构，而是由个人用户上传、储存，发送给其他 的个人用户。

比特流等点对点分发协议也是通过个人对个人的形式交接数据后上传并储 存文件。但是该类点对点文件分享系统是用户相互转发自己所拥有的文件，只能 下载用户共享的数据。这种方式对于无代价维持种子结点的用户来说，并没有足 够的动力持续上传文件。因此，该用户上传的文件有随时消失的风险，同时无法 保证文件有足够的实用性。

为解决拥有文件的用户因各种理由而消失的问题，我们采取了根据用户的 需求交易文件储存空间的市场系统。在该系统环境下即使不维持上传也可下载文 件。

关于 FirmaChain 的核心技术——去中心化数据储存，接下来将进行详细阐 述，具体内容将在日后公开的技术白皮书中做详细介绍。

2. 去中心化的数据储存

包括以太坊在内的现有大部分区块链平台均能储存数据，但维持区块 链时需要花费更多计算能力，这就要求支付比电脑储存更高的费用。因此， 以储存数据为目而使用时，需要支付近乎天文数字般的费用。

但在大多数情况下用户不需要永久储存文件，而且多数用户不愿为储 存数据而支付高额的费用。因此，若使用去中心化储存库，就可以以合理 的价格在指定的时间内，为用户存储大容量文件。另外，我们打造的结构 具有以下特点，为了加强储存数据的完全性，将额外的信息储存至单独的 区块链网络。

若双方成交时，从用户向挖矿人传输要储存的文件开始，文件存储协 议即成立。在协议期间，挖矿人需持续证明自身在诚实地储存文件，证明 方式以各种验证的理论为基础公开透明地进行。用户与挖矿人之间达成协议内容应该公开给所有用户，内容被包含在 区块内并传播到网络，需接受经过所有网络组员的确认。

2.1 FCT(Firma Chain 代币)

FCT 是使用 FirmaChain 有关服务时所需要的货币，主要用途有以下两 大方面：第一，通过 Firma 网络形成的 DApp 服务使用费；第二，使用 FirmaChain 的去中心化数据储存库时应使用 FDR，FCT 可兑换为 FDR，被 用于存储更严格、更完善的字符串。

我们为提高 FCT 的技术含量在不断努力，我们将构建出符合 DApp 的 转账费和区块回报，还考虑区块传送速度，打造具备无限扩展性的独立区 块。考虑通过太坊虚拟机(Ethereum Virtual Machine，以下简称 EVM) 的智能合同，通过确保技术稳定、已获得验证稳定的以太坊平台，开发可 快速实现商用化的技术 。目前我们采用以太坊的大都会（Metropolis， 以下简称大都会）， 我们的技术人员对以太坊第二阶段的情况进行了细致 的考核，并决定使用以太坊。

为使用以太坊的智能合同功能，FCT 将以 ERC-20 货币的形式发行。用 户可通过 FCT 储存使用 DApp 服务时所需要的信息。与储存期限有限制的 FirmaChain 去中心储存数据库不同的是，使用 FCT 可半永久储存可以区分 信息是否伪造，篡改的状态信息。

但是如果能找到更符合 FirmaChain 需求的区块链平台，我们将通过 相应平台网络发行 FCT。此外，如果有需要也可能独立搭建 FirmaChain 的 网络。为实现服务的稳定开发，我们也考虑使用更多样的区块链平台。

2.2 FDR (Firma 数据回报)

FDR(Firma Data Reward)是在FirmaChain的去中心化数据库中通 用的货币，也是回报。用户为储存文件向挖矿人提供手续费，也就是FDR， 若挖矿人成功储存文件时能获得相应的回报。除存储文件时获得的FDR回 报之外，挖矿人还可以检验区块链生态界参与主体的行动并生成区块，此 时可以获得挖矿的回报。

用户为使用去中心化数据库，可将FCT兑换成FDR。此外，挖矿人可 在这一过程中获利，可使用FDR去使用FirmaChain的几个DApp。

在运行初期，为了保证FCT成功兑换为FDR，在FirmaChain的FCTFDR交换智能合同钱包里，以提前挖矿的方式分配FCT与FDR。用户通过 交换智能合同输入FDR钱包的地址，并转账FCT时，相应额度的FDR将转移到用户的钱包。FCT与FDR的兑换比为一比一，为防止该钱包出现FCT 与FDR不平衡的现象，对每单位时间的交换比例进行限制。

实现区块链生态的稳定运行时，拥有大量FDR的挖矿人或交易所可起 到FCT-FDR交换智能合同作用。但是他们运营的交易所与FirmaChain的 交易所不同，这些交换所未经过验证因此可信度不高，也无法确保交换比 例为一比一，另外还会收手续费。此外，每单位时间的交换比例也没有限 制。

今后根据我们的路线图完善 FirmaChain 的主网后，可实现去中心化 数据库与代币平台的整合，届时有可能实现 FDR 与 FCT 统一。

2.3 文件储存市场

2.3.1 市场与订单

去中心化数据库为用户与挖矿人提供文件储存合同的交易市场。用户 购买订单或挖矿人出售订单时，将在全体网络公开的单一账本中记录该内 容。若符合条件的订单已存在时，两个订单达成交易，在经过双方的确认 与签名之后开始进行文件储存程序。这样，在公开的自由市场上价格由供 需关系决定。

<문件储存市场图示>

2.3.2 订单成交规则

虽然使用单一的账本，但不能对不同的订单同时进行交易。因此，用 户在订购时，可以向挖矿人提出追加要求。相反，挖矿人也可向用户或就 需储存的文件提出附加条件。例如，若用户希望挖矿人更负责任，则可提 出支付担保金的条款。同理，挖矿人为了拒收小规模文件的储存订单，可 设定小文件的规模。

用户与挖矿人可向对方提出各种诉求。如，挖矿人或用户的地理位置、 挖矿人想要的文件储存价格上限、少储存期限等。上述内容将成为电子 合同，详细条件主要根据技术设计，将仅包含去中心化文件分享市场必要 的因素。

这些条件将在网络节点达成交易时进行评估。其中，部分条件由于经 网络正式认可，可确认相应事实，但若用户与挖矿人在非正式形成的条件 下达成交易时，则情况不同。此时，网络节点只评价双方所输入的内容是 否符合条件，而不判断内容是否属实。因此双方应在成交后，亲自确认对 方是否符合条件。

2.3.3 评价系统

用户为更加稳定储存文档，可参考挖矿人的评价。这些行为之所以重 要，是因为某些挖矿人不坚守储存文件的义务，可能会冒被处罚的危险做 出一些会网络带来恶劣影响的行为。虽然不存在正式的评分系统，但用户 可将挖矿人的累计文件储存量、储存失败率、合理的手续费等项目作为根 据，选择参与网络时间更长，并且致力于维护良性生态环境的优质挖矿人， 将文件交给此类挖矿人储存。

但是这些信息无法在区块链网络正式验证 ，用户在成交后签名之前应 再次确认挖矿人的各项条件。这将以额外服务的形式提供，挖矿人的文件 储存记录记载在区块链网络内，因此可供人随时确认，亦可经过计算来确 认有关数据。日后，可在客户程序阶段整合第三方提供的挖矿人评价计算 功能。

2.4 文件储存协议

2.4.1 储存程序

用户与挖矿人成交后，双方将再次确认条件并进行签名。此后将形成 关于分享文件合同的临时钱包，用户的资金与挖矿人的保证金将转移至临 时钱包。用户向挖矿人传输将要储存的文件，在文件传输完成后挖矿人将 文件加密，其后挖矿人将文件复制及加密已成功完成的文件储存证明传输 至区块链。该证明将在文件储存合同期间内持续进行传送。合同成功到期 时，挖矿人可利用证明记录，从临时钱包中将文件储存回报以及保证金转 至自己的钱包。若挖矿人未能及时传从证明时，用户可在区块链传播"文 件储存失败证明"。用户可利用挖矿人的"文件存储失败证明"，可从临 时钱包中将储存文件的回报以及保证金转至自己的钱包。

<成交过程的图示>

2.4.2 退还程序

用户要求退还文件时，可向挖矿人提出退还文件的要求。这时，用户 应向挖矿人支付成交时设定的退还回报金。挖矿人收到文件退还邀请时，应将文件传输给用户。挖矿人可拒绝退 还文件，但拒绝记录将保留在区块链上，以后可能会在用户端得到负面评 价。

2.4.3 文件储存证明

用户向无法确保信任的挖矿人委托文件储存，于是希望在传送文件后 挖矿人能在合约期间内，持续证明安全保管文件。

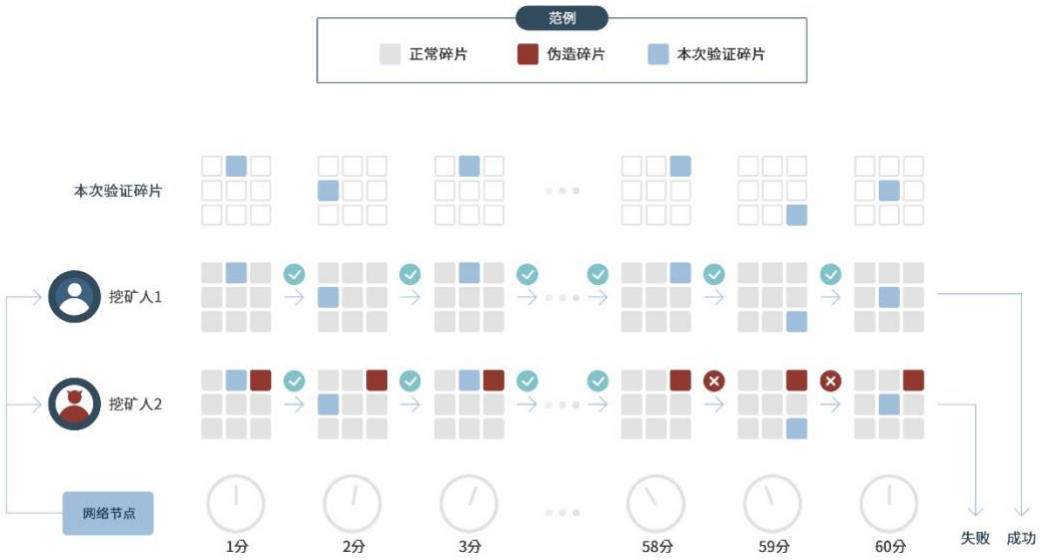
简单的证明方法是，拥有文件的用户向挖矿人要求提供文件内容，并 进行对照。在合约期间内持续对比文件内容，用户就能确认挖矿人正在妥 善储存委托的文件。

但是，随着用户与挖矿人共享的文件增加和文件容量的增加，引发网 络频带过载现象，导致文件验证速度下降。因此，为维持系统要求的低 验证速度， 文档大小将受到限制。

为了解决该问题，用户可要求挖矿人传送随机抽出的文件碎片，再进 行比较。使用该方法的优点在于当交换次数不断累计时，就可以更加确信 确定挖矿人拥有全部文件。

然而，仍存在一些问题。第一，用户需要储存所有文件；第二，用户 需不间断的向挖矿人提出验证要求。除挖矿人之外的多数用户不会 24 小时 启动电脑。第三，若采用上述的验证方式，也不符合用户使用去中心化数 据库的目的。

上述方式的问题在于用户为验证存储文件的完整性，需要与挖矿人保 持联系，同时还需拥有原文件。此外， 挖矿人需要证明持续拥有文件，同 时还需证明不会出现上述问题。在此情况下，满足上述条件的方式就是zkSNARKs。



<证明过程图示>

zk-SNARKs 是"Zero-Knowledge Succinct Non-Interactive Argument of Knowledge"的简称。根据去中心化数据库文件储存证明， 每个单词的含义如下：第一， "Zero-Knowledge(零知识)"是试图验证 的人（用户）完全不拥有证明人（挖矿人）所拥有的文件信息。 "Succinct(简略)"是指无论文件有多大，挖矿人应在短时间内提供证明， 相应证明结果的容量也应极小。"Non- Interactive(无产生互动)"，是指 验证人与证明人同时无需同时在线交流验证 ， 证明人只要在结束证明工作 之后 ， 向验证人传送终验证即可。"Argument of Knowledge(主张知 识)" 是指挖矿人应知道文件的内容。不是用户亲自验证，而是通过随机种子， 在区块链网络中，任何用户都可以验证挖矿人是否拥有文件的方式。

2.5 区块链

2.5.1 订货帐

在文件储存市场，用户或挖矿人产生新订单后将其传播至区块链网络 节点。该订单将注册至单一的订货帐，与全网络节点共享，一个节点收到 的信息将传送至其他所有的节点。若订货帐内的订单未成交时，过一段时 间后，将自动从订货帐中删除。相反，订单成交时将即刻从订货帐消失， 得到用户与挖矿人的签名之后，以交易的形式传播到网络。

2.5.2 交易

交易是指在去中心化数据库上发生的一些行为当中，应记录在账本上 的公开行为。用户与挖矿人成交后，且双方签名时，将形成文件储存交易 合约。挖矿人在与用户达成文件储存协议之后，在储存该文件的期间内定 期形成文件储存证明交易。若挖矿人不履行储存任务，或存储失败时，区 块链的所有用户都可参与，并传播"文件储存失败证明"。用户要求挖矿 人提供文件内容时，将形成文件退还交易，挖矿人应将文件退还给用户。 挖矿人成功满足返回文件的需求或根据文件储存失败与否需要转移FDR时， 用户或挖矿人可记录FDR交易记录，结合前面的交易记录传送至区块链网 络。

2.5.3 交易队列与交易手续费

用户或挖矿人创建新交易后，该交易将传播至区块链网络。已传播的 交易不会立即包含到区块内，而是进入交易队列。交易队列将分享至所有 用户端，一个网络节点接受的交易将转达至所有其他节点。区块挖矿人在 制作区块时参考区块队列。若区块队列积累的数据总规模大于可形成的大区块规模，区块挖矿 人参考区块的形态与交易手续费，形成效率高的交易组合，并将其传输 至区块链网络。

2.5.4 区块

区块数据内部包含许多交易，在每个区块形成周期中，根据自身协议 算法选定区块挖矿人后将进行挖矿。但若在该期间内不存在区块挖矿人时， 无法形成区块。区块挖矿人根据条件在交易队列中选择交易后加入该区块。 新形成的区块将传播至整个网络，并接受所有网络节点的确认。区块挖矿 人将获得区块挖矿的回报，其中包括形成区块的回报，以及区块中包含的 交易手续费。

2.5.5 区块形成协议算法

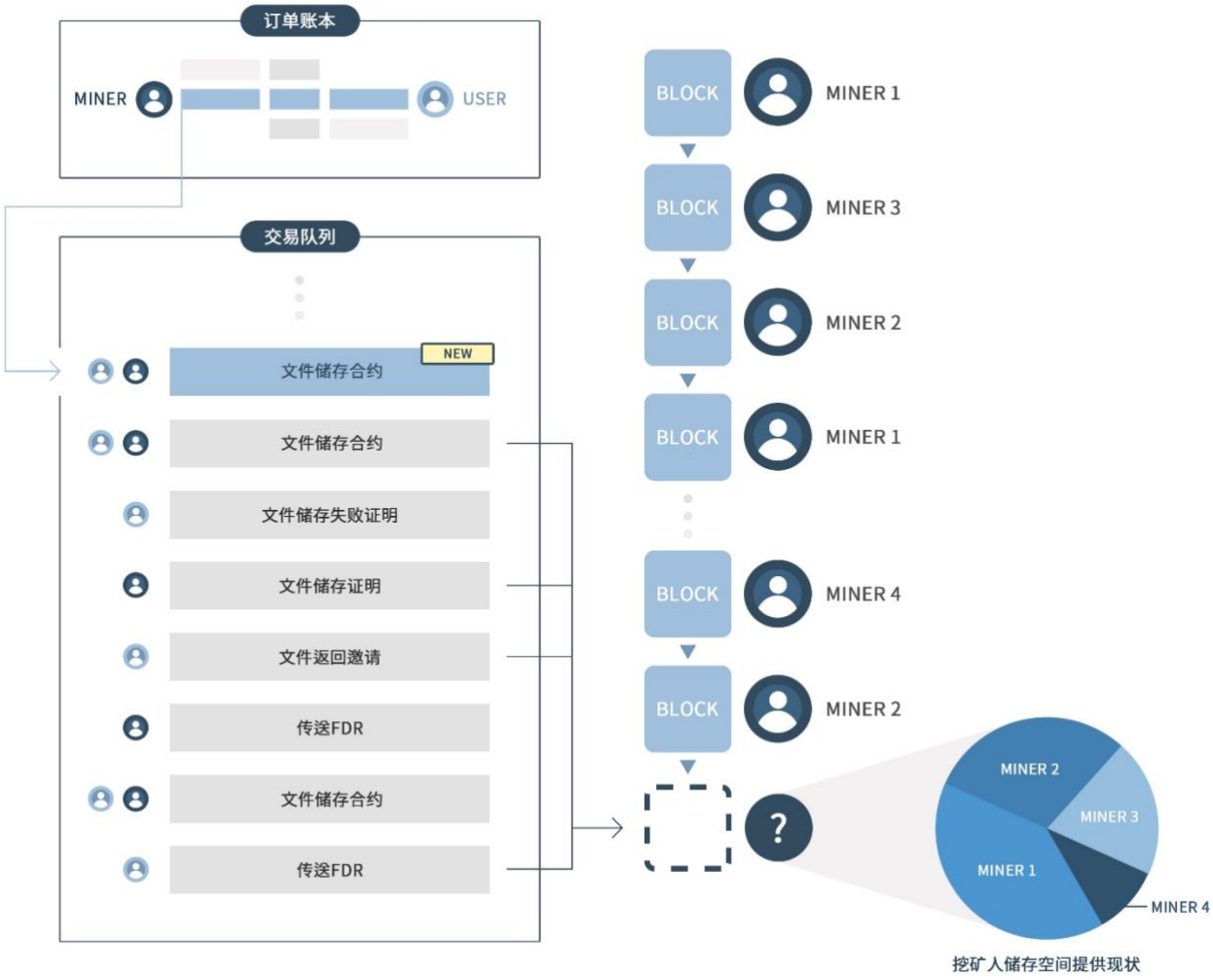
比特币等诸多货币以工作量证明方式(Proof-of-Work)形成区块。工 作量证明方式是指，为形成一个区块，直到获得满足特定条件的加密散列 函数为止，需重复无数次加密工作。因此，越是具备高采矿能力的人越有 可能性挖掘出区块。

此外，也有通过权益证明(Proof-of-Stake)方式形成区块的代币。权 益证明方式是指在区块链网络中，拥有更多权益的人，越是容易挖到区块 的证明方式。例如，根据每个挖矿人的代币持有比率赋予挖区块的机会等， 这是多个权益证明方式之一。

在去中心化数据库中，重要的资源就是储存空间。如果选择工作证 明方式时，不只对挖矿人的储存空间提出要求，同时也对工作能力提出要 求。若使用较好的CPU或GPU时，可以加快数据运算速度，但这不代表空 间容量或质量的提升。去中心化数据库的优点之一就是在进行分布式数据储存时，在工作过 程中运算速度无需超过指定标准。

因此，工作验证方式并不符合我们将要实现的区块链，我们采用的协 议算法为使用达成订单总存储空间的储存空间证明方式（Proof-of-Storage），这可鼓励挖矿人提供更多的储存空间。

以上就FirmaChain的核心技术去中心化数据库的结构进行了简单阐 述，将在接下来的电子合同管理服务中储存利用去中心化数据库签署的合 同。



<区块链图示>

3. FirmaChain分布式应用 ： 电子合同

3.1 现存知识产权许可合同相关问题及运用区块链技术解决问题的方案

在现代人的生活中，合同无处不在，且存在形式多样。由于国际书面合同要求面对面处理合同所以其中一个缔约方必须出国然后才可签署合同。但这种方式会造成不必要的时间金钱浪费。

同时，现有的知识产权许可协议是通过在线电子合同转让然后修改和总结进行的。但是因为服务器是以集中的方式，所以存在伪造和安全风险。.此外，如果您通过电子邮件或聊天工具进行合同签署，没有办法验证对方的身份，资格或不知道对方有没有权利。但是，区块链技术可解决这些所有问题。

为解决上述的社会问题 ，FirmaChain与电子合同将缔结合同的基本 因素与区块链技术相结合，旨在使多方合同当事人圆满签订并实施合同。

此外，专利，商标，著作权（游戏，动画片，卡通）等知识产权许可协议等领域是FirmaChain公司具有区块链电子合同优势的领域。这个领域是FirmaChain的第一个目标。

下面是关于现有知识产权许可协议的问题。

很难确认许可协议的许可人是知识产权的实际所有者（包括独家许可人）。专利局的官方书籍可以识别权利持有人的姓名和地址，但在国际合同中，当知识产权转让或许可给专用被许可人或普通被许可人时，更难以识别承包商并跟踪实际所有者。

此外，从许可人或想要许可知识产权的所有者的角度来看，那些可能是具有欺诈性的，因为他们无法通过网络验证他们想要许可的被许可人的身份。而且第三方很难知道有关专利，商标的有效时间和许可证的所有信息。例如，从购买专利和商标项目的客户的角度来看，无法验证该产品是否是真正的被许可人。

即使您了解经过验证的知识产权所有人，直到签署书面合同为止，也会浪费许多时间和成本资源。对于拥有许可证的许可人,找到想要在其他国家使用自己的知识产权的买家是非常困难的。最后，在国际许可协议签订后，处理海外汇款，税收，费用等问题充满了欺诈风险，不变性，是一个很棘手的问题。

为了解决这些问题，FirmaChain将提供以下解决方案。

1.由于区块链的分布式Ledger性质，如果您使用互联网连接，那么您可以轻松识别个人拥有的知识产权类型，保留期限和位置。
2.如果用基于区块链的电子合同替换现有的合同方法，那么区块链可以透明清晰的记录合同及交易历史等信息完全保证重要消息不被修改。
3. 通过区块链认证的许可人（Licensor）和接受许可证的人（Licensee）无需会面，通过电子合同（E-Contarct)就可以签订国际合同（知识产权许可协议
4. 为了快速而方便的处理国际合同（知识产权许可协议）我们则提供了便利。（仪表板功能，多语言进行实时翻译，提供许可协议标准格式,24/7网上法律咨询及检讨）与我们平台相关的每个国家的专利律师会确保您，速度，安全的注册您的独家许可。
5. 我们的平台不仅帮助许可人快速轻松的找到在其他国家有潜在能力的被许可人，并且可以帮助许可人签订更多及合理的成本的协议。

FirmaChain提供的解决方案将扩大国际许可市场并确保合同的透明度。

3.2 电子合同与程序管理的相关需求

现代社会更偏好书面合同的形式，这导致了各种问题的发生。书面 合同的缺点在于应保管合同文件，合同当事人各持一份合同原件，其后修 改内容时却无法同步更新内容，还易出现伪造书面合同的问题。诸多企业 通过邮件、录音等外部方式保证及时更新合同内容，但这也难以进行精确 管理。伪造合同文书易导致法律纠纷，也无法阻止这些问题的发生。为解 决这些合同中存在的弊端，电子合同应运而生。

电子合同能将企业之间的合同内容数字化，类似的电子文件（电子 文件与电子交易基本法）有着与纸张文件同样的法律效力。韩国以及其他 国家商务法等相关法律也规定，在签约时电子签名（电子签名法）有同等 的法律效力。因此，电子合同也同样有法律效力。

目前电子合同的效率高于书面合同，但无法避免无权利人签合同的情 况、系统障碍导致传送风险提升等问题，因此与书面合同相比，电子合同 并未受到社会的青睐。此外，一些传统企业仍固守传统签约方式，目前电 子合同技术没有真正得到客观的评价，甚至被视为不需要的技术。

FirmaChain 利用区块链的技术特点，致力于打造透明、可信的电 子文件与合同系统，目标是解决现有问题并促进电子合同的普及。

3.2 何谓电子合同？

<利用电子合同撰写、履行合理的合同>

现代社会在不断发展进步，从这一角度来看目前的签约方式颇为传 统。例如，合同当事人通过邮件多次交换、修改合同，有时在签约当天交 换实体合同书时只是粗略地确认便进行合同。有时在没有任何信息的情况 下，使用无法律效力的契印或盖印，或者认为内容过于简单而直接省略合 同。

此外，多数公司进行资金大、周期长的合同时，只通过书面的形式 管理合同进展、额外项目、更改合同等内容，导致难以跟上合同的时间表。

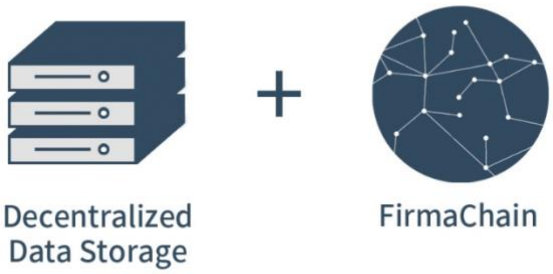
我们将提供利用FirmaChain的电子合同(DApp)智能合同与公链， 保障账本的透明度，确保合同的法律效力与稳定，同时和更加便捷地管理 合同使用需要的功能，提高业务的效率。同时，以加密货币支付合同款项，合理解决转账手续费问题。尤其是在签署跨国合同时，可解决不同国家之 间的双重课税、海外法人建立、海外汇款等问题，更有效地完成业务。

我们的电子合同将具备多种功能，具体内容请参照接下来的合同结 构部分。（ 加强电子签名安全系统、支持标准合同预先布置、提供合同进 展与修改目录等 ）。

4. 电子合同的结构

电子合同分为三大部分。第一，核心层面，此时将加密的合同数据进 行储存后再形成合同交易；第二，应用层面，此时进行 DApp 的撰写、管 理合同；第三，服务层面，此时验证电子合同、进行更改、连接核心层面 与应用层面。

4.1 核心层面 (FirmaChain)



核心层面用于转账款项、分布储存整个合同程序的有限状态、确认电子文 件的完整性、保证该合同数据不会出现被伪造的情况。在不同阶段，合同也会有不同的有限状态，详细内容如下。此外， 实际情况将会比下述内容更加细化。

达成合同

创建合同时，为确认支付方的支付款项能力，在合同双方达成一 致意见的情况下，在款项中预先设定一定比例作为预存金。支付方式 为韩元或 FirmaChain 的代币(以下简称"FCT")。若将款项设为韩元 时，则无需付预存金。

合同写好后，在经过合同双方的审核与确认后，将在去中心化数 据库撰写合同。这时将显示"等待上传"，支付方的货币钱包的余额 超出预存金金额，若有订金类等需要支付的款项时，必须完成支付。 结束该过程后状态将转换为"正在进行"。合同转为进行，在智能合 同上上传包括*散列串的交易记录。此后，所有合同当事人应履行合 同。如果以韩元作为支付手段，不需要 FCT 便可直接在智能合同上形 成交易，以附件的形式出示账户交易记录或转账证明，将相应电子文 件包含至合同即可。

进行合同

进行合同后，在双方同意下以 FCT 或韩元的形式支付交易款项。 在区块链和服务层面确认该支付的内容，并再次确认合同的情况。

结束合同

在支付合同规定的款项后 ，该合同转为"等待结束" ，合同当事 人确认合同内容之后终转为"结束" ，将向接受订单的一方支付款 项。

撤销合同

由于缔约双方的原因，在合同进行过程中会出现被撤销的情况。 但已被上传的合同无法删除，只能额外撰写撤销合同。这时，将在电 子合同记载已被撤销的合同内容，根据双方的协议或合同内容若需要 退款、另外付款时，可根据原来的合同再次签订新的支付合同后解决。

针对因缔约双方的某些原因而撤销合同的情况，相关的技术支持 部分将在接下来的电子合同服务章节中叙述。在合同进行的过程中发 生的事情将被存储在去中心化数据库中，可以随时查看相应数据。

更改合同

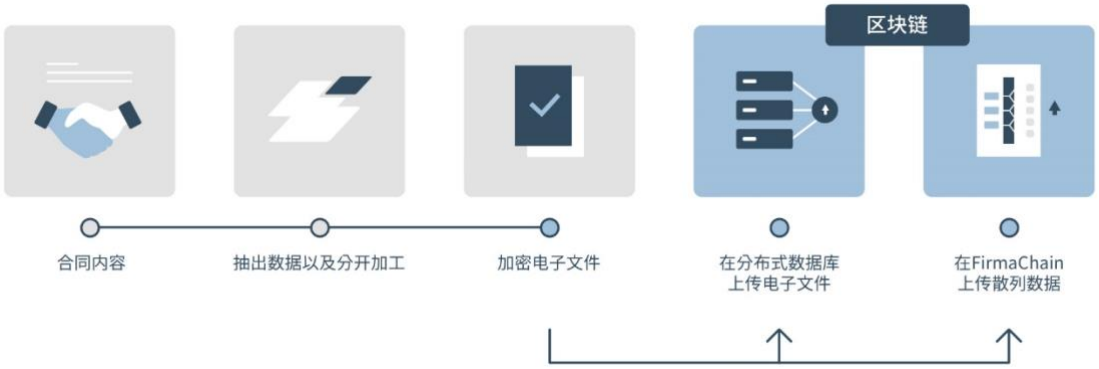
针对合同进行过程中出现的突发性问题，可通过特别协议更改合 同内容。重新创立关于更改内容的特别协议合同后，需经过合同当事 人的确认，该合同将成为在主合同的下属合同。此外，该下属合同的 散列串记录至智能合同，相应内容将上传至在去中心化数据库。若更改合同时款项出现变化，需按照之前的预存金比率存入韩元， 或获得退款。

*散列串(Hash String)

散列串是指利用加密散列函数将任意长度的数据对应至固定长度 的字符串。该函数是单向函数 ，无法通过散列串获得原版数据 ，假使 原版数据中出现了极其微小的变动 ，就会得出完全不同的散列串。这 便于检查数据的完整性 ， 我们将散列串作为 FirmaChain 的电子文件 固有识别数据。将使用的加密散列函数有 SHA256 或 SHA512 等，此 类算法均已通过验证。

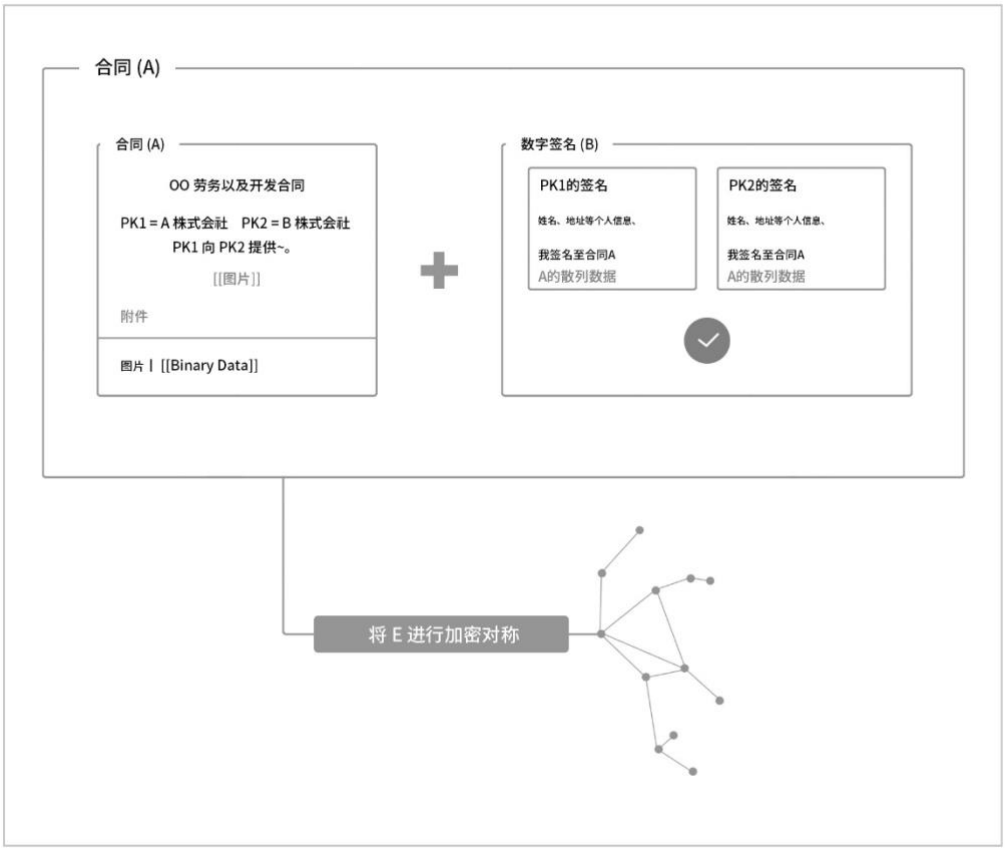
4.2 服务层面(Firma 网络)

Firma 网络起到应用层面的电子合同服务与核心层面之间的加工人、 验证人的作用。合同在电子合同上撰写，为了上传其内容至 FirmaChain，需经过中间加工过程。



加工工作包括在电子合同文件上的文字数据与其他数据（图片、音 乐、录音等），将对此进行加工后，使上传至去中心化分布式数据库。但 建议合同数据仅限使用文字数据。

但是关项合同，除文字之外必须包括一些内容。为此，通过电子合 同支持的 Markdown 语法制作的电子文件转移至 Firma 网络时，将在合 同内容中间的图片或其他附件包括到电子文件当中。此外，*以数字签名（使 用公开密匙方式：如，RSA，Merkle 签名等）代替电子签名。完成加工 后的完整文件将上传至去中心化的分布式数据库。



合同当事人加入电子合同时，将获得一对以 RSA 形式打造的公开密 匙(Public Key，以下简称 PK)与非公开密匙(Secret Key，以下简称 SK)。

在合同部分（A）包括合同当事人的公开密匙。便于理解，假设有两 个合同当事人，将每对（SK,PK）为(SK1,PK1)与 (SK2, PK2)。在数字 签名(B)领域添加各合同当事人个人或商家信息，还加将履行合同 A 条款 的内容，后以各方的 SK 加密。为限于合同 A，信息内包括合同 A 的散列 串。

通过对称密匙系统将整合合同 A 与电子签名 B 的电子文件 E，仅限给 合同当事人发行密匙，上传至分布式数据库。通过电子合同将上传 E 的散 列串，实施合同。

软件开发合同书

[[Public Key::MIGfMA0GCSqGSIb3DQEBAQUAA...]] 是株式会社A的验证密匙
[[Public Key::mJG8wVQZKjeGcjDOL5UlsuusFnCz...]] 是株式会社B的验证密匙
株式会社A(以下简称 “PK1”)与株式会社B(以下简称 “PK2”)关于软件 同:

第一条 (目的)
本合同目的在于“PK1”要求的软件开发委托至“PK2”，规定“PK1”与“PK2” 要的项目。

第二条 (开发范围)
1. ABC应用制作
2. ABC服务器制作

第三条 (款项与支付方式)
1. “PK1”对“PK2”当作本业务的开发劳务费支付总款项 (300,000)FCT
   ⑴ 签订本合同同时合同总额(150,000)FCT
   ⑵ 经过最后检查后7天之内支付总额(150,000)FCT
2. 款项支付方法:“PK1”通过电子服务向“PK2”的钱包地址转账。

附件，合同内容
[[image::Binary Data ...]]

PK1的数字签名:
[[Digital Signature::0GCSqGSZKjeGcjDIb3D...]]

PK2的数字签名:
[[Digital Signature::DOL5UlsuuIb3DQEISaC...]]

<完成加工后加密前的电子文件样本>

上述的例子是加工后的电子文件。该电子文件包括合同内容的文字 数据、文字以外的图片、音乐、录音等组成的二叉数据、以 base64 编码 的数据、随时可以验证合同当事人的数字签名的公共密匙。

以上内容将为 作为电子文件与电子合同的法律证据，根据合作律所的检讨，部分内容将 会更改

$A = Contents\ of\ a\ contract$

$E_K(M)$:*Encrypt M by using key K*

$HASH_A = SHA256(A)$

$S = Secret\ key\ of\ A$

$SK, PK = KEY\_GENERATE()$

$M1 = "Information\ about\ PK1,\ I\ agree\ with\ this\ contract(HASH_A)'$

$M2 = "Information\ about\ PK2,\ I\ agree\ with\ this\ contract(HASH_A)'$

$S1 = E_{SK1}(M1)$

$S2 = E_{SK2}(M2)$

$B = S1||S2$

$W = A||B$

$C_W = E_S(W)$

$HASH_W = SHA256(C_W)$

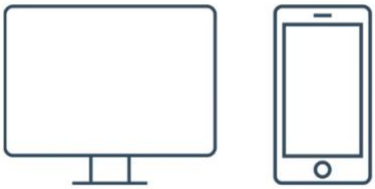
$HASH_W \rightarrow Smart\ Contract$

$C_W \rightarrow Decentralized\ Data\ Storage$

上述公式结合合同内容与数字签名，陈述上传至去中心化数据库的 电子文件制作过程。跟随电子合同开发的进行开发更有效、安全的算法时， 上述内容将会改变。

这些加工过程只限于电子合同内使用。通过 Firma 网络的其他 DApp 根据该服务的特点，可写至多种加工工作算法。根据该合同的效力，可通 过该算法制作许多服务。这将成为制作多种电子文件服务的基础。

4.3 应用层面 (DApp)



电子合同(DApp,去中心化应用)的基本作用是撰写合同，在合同当事 人同意的情况下更改所需要的部分，获得所有合同当事人的确认，在区块 链记录该情况。此外，在以太坊的智能合同代码相联系，在电子合同上进 行关于确认合同情况与更改等所有有关合同的内容。 确认合同书之后可 进行签名，签名之后在电子合同可监督所有与合同过程有关的内容。此外， 可利用在引文提到的有助于立合同以及履行的多数功能。下面讲述该部分 功能。

可使用有助于撰写合同的 Markdown 与视觉编辑

可通过 DApp 立合同。为实现数据的文字化，应根据电子合同规 定的 Markdown 语法所写。为对 Markdown 语法感到困难的用户支 持视觉编辑软件 (WYSIWYG)。 此外，支持之前使用的 doc 与 hwp 等合同文档形式，提供切换功 能。

加强电子签名安全系统

多数电子签名服务直接在数字匡威撰写。但是这容易让其他人代 理签名 ，也无法期待与公认认证书一样的效果。同样 ，书面签名也面 临一样的风险。无论有多大的法律效力 ，若该情况发生 ，无法确认谁 进行签名。用户可登录电子合同后，可利用 Firma 网络提供的数字签 名注册系统。若发生法律纠纷时，通过该系统容易证明。详细内容将 在后面陈述。

支持预先布置标准合同

在电子合同获得法律顾问后，提前拿到合理范围内撰写的多种标 准合同。若与标准合同没有很大差异时，只要更改合同当事人、合同 对象、项目名称、合同款项、日期就可以储存自己写的合同。

分析合同进展与更改内容

通过电子合同可判断合同进展的程度。此外，若合同内容出现更 改时，可添加对该内容进行比较的微分工具一眼判断哪些内容的更改 以及删除。这将帮助合同当事人之间更容易看出所更换的内容。

跨国合同时法律顾问

进行跨国合同时，由于各国的习惯、法律体系的不同，难以立合 同条款。我们将比较各个实例，提供撰写合同时的建议。此外，若交 易规模大或频繁出现交易时，将提供一对一的法律顾问服务。

不仅如此，我们将支持更多签合同时所需要的功能

电子合同网络服务利用 Javascript(ES7 标准)的 Node. js Framew- ork 制作服务器与 ReactJS 库。我们选择 ReactJS，是因为以便合同当事 人进行合同，该库能制作便利性与识别度高的资料。

目前在策划手机服务。主服务在网络进行，手机端可使用合同当事 人之间的对话、关于合同的提示等便利功能。我们将使用 React Native 或使用该平台（iOS、安卓系统）的当地语言制作。

我们以服务过程中开发速度快、稳定、效率高作为目的选择 该技术。

此外，需要合同的所有网站、应用服务当中可利用我们电子合同服 务的核心功能之一。该功能以模块形式利用包括电子合同与签名功能，将 制作 SDK 颁发。此外，将利用 FirmaChain 制作多项电子文件服务。

5. Token Economy

5.1 生态系统

此前的解释一样，Firma Chain 的应用层面 Token Economic 的 E-Contract 服务。由用户客户和提供专业服务的专家组成，你可以子啊上面看到，如果你说明了市场上的交易，那你就会去叙述你的生态系统。Firma Chain 在生态系统中有最基本的货币 FDR 可以通过 Firma Chain 转换为 FCT。你不可以把 FCT 变为 FDR。此外，FDR 是确定 Credibility Score 的计算和 User Reward 的标准，因此使用此服务的主体可以保留不将 FDR 转为 FCT。此选项可用于显示信息提供者的可靠性。

5.2 应用层面 (DApp)补偿系统

5.2.1 Credibility Score

该信息提供者将会得到一个 FDR 的奖励。资讯提供者可以将收到的 FDR 转换为 FCT，但可以计算出 FDR 对 Credibility Score（以下简称 CS）的标识，使服务用户能够确认信息提供者的可信度。您的资讯特供着所持 FDR 值越高，您的咨询提供者所提供的长期服务的可信度就会越高。由于各种服务提供者自然而然地就会偏好那些 CS 较高的咨询提供者，因此，它引导我们对现有的咨询提供者服务，从而能够持续提供服务，对于新的咨询提供者则引导我们不断地积极参与。CS 的计算方式如下：

$$CS_{r,n}(L) = \frac{\sum_{i=1}^{n} L_k(1-r)^{k-1}}{\sum_{i=1}^{n}(1-r)^{k-1}}$$

（r,n 是由各种服务种类决定的常数，L={Li}中 Li 是前 30 天的平均 FDR 的保有量。例如，过去 30 天的平均 FDR 流量。）

5.2.2 服务使用者补偿系统

Firma Chain 提供的第一个 DApp 即，E-Contract 包括建立并签订电子合同，请求法律咨询等服务。用户在使用这些服务时，会得到一个由下列公式决定的 FDR 的补偿。

$$FDR_{a,b,r}(c) = ar^{[log_b c]}$$

$$(a > 0, b > 1, 0 < r < 1)$$

（a,b,r 是由服务种类决定的常数，c 是指在规定的时间内该服务的使用次数）

用户可将获得的 FDR 转换为 FCT，并将其用于 DApp 内各种服务或通过交易实现现金化。或者是保持原样。每个服务在规定的月数内，经过 FDR 净收入之和每月重新计算等级，根据等级可以得到服务使用费折扣等附加优惠。净收入定义为：

$$\text{Net Gain} = \text{Gross Gain} - \text{Converted to FCT}$$

5.3 FDR 与 FCT 的代币循环生态系统

FDR 和 FCT 有密切的联系，但 FDR 和 FCT 没有直接的联系。刚开始的时候，为了补偿生态环境，我们会在用 FDR 交换一部分 FDR 的时候寄存。同时发行与存入的 FCT 同样数量的 FDR 代币。还有 Firma Chain 为了补偿应用层面是 FDR

如果您想要将您获得的 FDR 转换为 FCT 那么将会给您提供额外的 FCT，以便事先交换。Firma Chain 将用户为使用服务而支付的 FCT 的一部分重新存入 FDR 交换使用，并将 FCT 随时随时保持足够的水平存放。

此时，Firma Chain 未将 FDR 可交换大量一次性在市场上流通所产生的副作用最小化，对用户分类，或对整个可交换量，对单位时间内量大可交换量限制为下列公式：

$$CAP_T(D) = \min\left(M - a \cdot \max(0, T - D), \frac{D}{b}\right)$$

$$\left(M, T > 0, b > 1, 0 < a < \frac{M}{T}\right)$$

（D 是 FDR 转换用 FCT 的保有量，T 是 FDR 的总发行量。）

如果您想将全部交换量设定为 CAP/小时，那么您不能将 FDR 交换为 FCT，就不会发生此类情况。但是如果交换代币数量的限制远远为达到用户的期待，那么不能说这个系统正常运行。如果发行数量和生态系统的实现规模有差距，在此情况下，Firma Chain 可以在保留的生态补偿的 FCT 范围内销毁或发行 FDR，以减少其怪理。您可以根据实际情况调整参数来决定您在使用此服务时所获得的 FDR 大小。

6. 路线图

2018

02 FirmaChain 的研究与开发

04 公开 1.0 版的白皮书

11 上市原型的 E-Contract 服务

Q4 上市 E-Contract 服务

2019

Q1 上市运用 IPFS 的电子合同服务

Q2 完成 100 个以上的项目

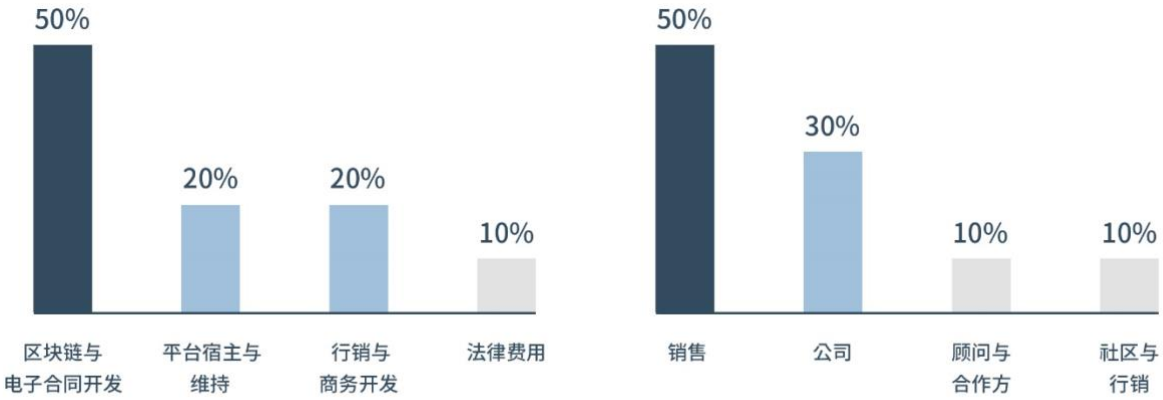
Q3 启动去中心化数据库测试网站 / 上市根据测试网站公开的电子合同

Q4 上市 Firma 网络后完成后续工作

2020

Q1 启动去中心化数据库主网 / 一千件以上 Solution 合同，上市 SDK

7. 代币生成事件



总收行贬模: 600,000,000 FCT (FirmaChain Token)
销售量 : 300,000,000 FCT

没有超过总收行量收行的代币。通过优惠价格招募的以太坊将由于右断图形的领域。 公司拥有的代币将为维持 Firma 区块链系统保管一年。此外，使用本公司代币的群体 不用于审传的代币将可用于扩大 Firma 公司贬模、上市交易卟的空投等行销为目的使 用。

8. 工作团队

尹映寅

代表理事

李侻奎

开叹理事

朴不二世

設計責任

区块链

尹大炫

行销策划总负责

李相潤

海外事业部

美国

芮尙元

社区经理

魏亨旭

海外事业部

印度

金桢完

海外事业部

中国

金聖优

项目经理人

朴镇叙

区块链开发人

朴炳奎

区块链开发人

朴秦星

区块链开发人

朴柱讚

前端开发人员

金多殷

媒体和内容设计师

韩明圭

社区经理

任祥赫

营销

9. 顾问

Ju Young Song

律师

Milbank, Tweed,
Hadley & McCloy LLP

我相信利用区块链技术的智能合同能够简化复杂的合同程序，能够 减少不履行合同时发生的法律纠纷以及强制执行等所支出的费用。 同时，还能广泛应用至多个领域，这将给我们的生活带来翻天覆地 的变化。

FirmaChain能够克服书面合同的缺点，利用区块链的透明性与可 信性进行电子合同管理服务，除减少不履行合同的风险之外，还能 解决履行合同时所支出的时间过长以及费用过高等问题。我相信 FirmaChain能提高智能合同的水平，对于它将给我们这个社会带 来的积极作用，我十分期待！

Han Jong Lee

代表理事

Goodtimewith.me

FirmaChain拥有的前景是以区块链技术的去中心化、透明性、可 信性来创新，现代社会普遍使用的书面合同其实有许多负面影响。

尤其在签署跨国合约时更是问题重重，例如，不同国家间交易时的 双重课税、建立海外法人、海外转账、手续费标准，如今可以通过 透明、高效、经济的技术来解决。我相信FirmaChain能以迅速快 捷灵活地执行能力，以及极强的耐力，终实现未来目标，也相信 他们的真诚态度与挑战精神，我愿与他们一同前行

Jihwan Won

带务理事

KJ DNS

FirmaChain是结合意大利语的签名"Firma"和区块链技术结合 的意思，包括合同在内所有需要签名的文件，都可以通过去中心化 实现公共交易账本创新的新技术。

我们已离开传统的时代，逐渐步 入面向未来的数字信息化时代。在这样的时代里，能够确保个人与 个人用户之间通过大规模分享网络降低信息改变的可能性，保障透 明性与信任度的区块链技术受到欢迎是大势所趋。我期待区块链技 术能够应用到建筑行业，能够改善外包商与转包商之间产生的不公 正估价现象以及篡改合同等问题。2018年我们将迎接信息化时代， 此时此刻，我希望FirmaChain能成为提供颠覆性服务的领军企业。

Hyeonwook Jeong

代表理事

beSUCCESS

以区块链为基础的区块链数据库中，电子文件与合同有很大的发展 前途。我在初期开始就非常看好FirmaChain团队，并且支持他们。

根据我过去的经验，FirmaChain将能不断发展下去，同时还能巩 固自身地位。这是因为他们是一个值得信赖的团队，同时拥有可实 现的现实性目标。我相信FirmaChain的开发团队能凭借过硬的实 力的，发挥极大的潜力，开发出更多电子文件与合同领域的解决方 案。我个人也非常期待能以Firmchain顾问的身份参与其中，希望 能协助他们拓展国际业。

Guho Son

代表董事
Monument Company
前 Softbank Ventures
常务理事, CFO

源于金融领域并迅速发展的区块链技术作为引领第四次产业革命的新一代技术，备受瞩目。通过数以亿计的设备处理呈几何级数上升的交易量的中央集中型云方法应考虑管理、保护等多种问题。

但如果实现了FirmaChain追求的合约过程简化，交易透明，强力保护的话，会给金融领域，甚至给制造、流通、公共服务及社会，文化等设计我们生活的各个领域都将带来积极变化，同时也会带来巨大的经济波及效应和创新。

Jiwook Kim

伙伴律师
法务法人Hwawoo
(股份公司)

区块链技术是以网民的信赖为基础，将检证后的交易和加密的信息保管在分散的总账里，因此可以确保交易的透明和安全。FirmaChain就是把这种区块链的去中心化转嫁到合同中的平台。此平台使得合约过程得到简化，通过区块链网络，当事人可以方便检查流通中的合约，断绝了伪造的可能性，由此可以实现对合约文书进行透明又安全的管理。FirmaChain克服了现存合约文书的缺陷，有望成为确保合约签订、执行，管理过程中的透明度和可靠性的创新型解决方案。

Joonwoo Kang

COO

Hexlant

2018.01 ~	Hexlant COO
2017.01 ~ 2017.08	BuildIT CTO
2014.08 ~ 2017.01	Samsung Electronics Software Engineer

Seongsan Lee

CEO

SPIN Protocol

2018.09 ~	SPIN Protocol CEO
2018.06 ~ 2018.09	Director of Global Sales and Business Development. SOOM -Foundation
2018.02 ~ 2018.08	International Business Development Manager. Minds Lab, Inc
2014.05 ~ 2018.02	Senior Manager, Trade / Investment and Business Development. KOTRA

10. 合作方

战略合作方

区块链生态合作方

新闻

11. 结语

我们 Firma 团队(包括 Firma 公司、股东、公司全体人员、下属公司)撰 写了这本白皮书，旨在为关注我们 FirmaChain 的所有人提供更具体的信 息，其中包括我们工作团队的介绍以及其他详细信息。

也就是说，撰写本白皮书并不是为了邀请各位参与投资，且与此毫无 相关。此外，Firma 团队编写白皮书内容的时间点仅限于现在， 对未来情 况不做保障。

Firma 团队对于本白皮书的内容，不对任何具体情况做出保证，也不 担负任何法律责任。也就是说，Firma 团队不保障以下几项内容：第一， 白皮书内容是否以法律权益为依据，是否侵害第三方权益；第二，白皮书 是否有商业价值或是否有用；第三，白皮书是否能帮助各位达成自己特定 的目标；第四，白皮书内容是否有错误等等。除上述内容以外，在其他领 域均可免责。

若各位在做出决策之前参考本白皮书时（参考白皮书或以该白皮书为 基础的内容）无论盈利或是亏损，所有责任均由各位承担。也就是说，由 于参考本白皮书而导致各位蒙受损失，或是财务上的其他亏损等情况， Firma 团队无需承担任何赔偿、补偿等其他责任，上述内容请各位悉知。