FirmaChain

白皮书

1.2版本

目录：

1. 概述

1.1 知识产权（IP）授权协议的重要性（专利、商标及版权）

互联网的发展让世界进入了信息无边界的时代。对个人、公司乃至国家来说，知识产权（例如专利、商标以及版权等）的保护及其经授权的工业应用已经成为至关重要的竞争力之一。

然而，知识产权保护以及转让履历很难通过当前的技术来追踪，这就导致了全球的 1）知识产权侵权，以及 2）在执行授权过程中的欺诈及滥用问题。因此，我们希望利用区块链技术来检验知识产权及转让，以便公司和个人在授权的过程中得到安全的保障。

1.2 知识产权授权协议引入电子合约的必要性

目前，大多数合同仍秉承传统的书面形式。目前为止，电子签名与文档相关的服务已经陆续问世，电子合约的有效性也已经得到了法律的认可。但是大多数公司仍然沿用书面合同，很多公司并不了解电子文档的便利性。

“我们开始思考，
为什么人们更偏好书面合同？”

时至今日，书面合同比起电子合同更受青睐，且在社会享有更高的可信度，因为书面合同的原本的用途之一是可以作为证据使用。而且提供电子合同的服务方大部分都是中心化的，因此有伪造、信息丢失或黑客入侵导致的机密信息泄露的风险，电子合约看起来比书面合同更加脆弱。

我们可以举几个实际的例子，来重点说明几个问题：

例一：
我最近从一个拥有知识产权（专利）的用户手上购买了其使用权。可我很担心这个用户是不是该专利的真实持有者，毕竟授权方是外国人，也很难确定他有没有曾经授予过其他人专属权。万一第三方在未经授权或逾越授权范围的情况下使用我购买的专利该怎么办？

例二：
A 公司与 B 公司为签订内容发布合同，在执行合同之前一直在交换修订了单词的文档。签订合同当日，B 公司带来的合同草案包括了有关版权保护的附加条款，而此前双方尚未对此进行过讨论。时间有限，而董事长又不在位，场面略显尴尬。尽管负责人未经董事长准许就立刻做了必要的更正，也执行了合同，但类似情况时有发生。

上述例子表明，在知识产权授权协议领域引入基于区块链的电子合同，能够通过其广泛的应用来解决上述包括产权保护以及记录在内的问题，提高签约过程的透明度和效率。

FirmaChain（以下简称“我们”）利用区块链的去中心化特性，提出了可靠的去中心化数据存数方案，来实现以下目标：1）提供电子合同管理服务，以确保交易文件中有关知识产权许可协议的内容的透明性与可靠性；2）（二）从根本上解决核查缔约方和伪造合同的问题；3）利用 DApp，为合同各方制定合理的合同制定程序；4）制作合同的过程中减少资源的利用，化繁为简，降低国际合同的处理成本；并且 5）突破书面合同的限制，带来新的服务。

1.3 信息的去中心化

全世界有数以百万的电脑正长时间运转，但资源仍然未能物尽其用，特别是存储空间以及网络宽带。如果将这些闲置存储空间及网络资源以一定价格租借给他人使用，那么相比起类似文档存储服务，使用者可以以更低廉的价格存储文件，而提供者则可以提供未使用的资源，从中获利。

我们设计了一种去中心化的分布式文件存储系统，利用可靠的存储空间来保护数据的完整性和可靠性。去中心化说明该文件存储系统由每一位参与者直接管理和运营，无需进行中心化管理。

P2P 分布式文件共享系统（例如 BitTorrent）还允许个人在共享数据后，享受上传和文件存储的服务。然而此类 P2P 文件共享系统的基本思路即个人下载的内容与他/她上传的体量需持平。可惜的是，这种系统未能充分激励用户，无法通过奖赏鼓励用户持续上传文件，以维持他们的动力。结果就是 P2P 分布式文件共享系统无法保证文件数量，它们始终有随时消失的风险。

我们利用市场原理来解决上述问题，让用户可以根据自己的需求买卖文件存储空间，各种原因导致文件从系统中消失的问题也可得到解决。而且该系统不要求持续上传文件来获取下载文件的权利，省去了用户的麻烦。

我们将在下文详细介绍 FirmaChain 的关键技术——分散式数据存储系统。此外，我们会在未来即将披露的《FirmaChain 技术白皮书》中对分布式数据存储系统进行的更为详细的说明。

2. 技术

2.1 介绍

FirmaChain 的构建基于以太坊（Ethereum）智能合约的概念，其功能包括参与者之间的合同签署、文件 UID 的上传、各个存储空间的地址的监督以及合同状态的管理。我们在运行服务的过程中获得了许多结果，让我们有了更多有用的见解与提升的空间。我们发现矿工费的增长（gas fee）导致了整体服务成本的增加。再有，用户无需保留基于智能合约所创造的原始合同文件和验证记录。结论就是，把上述责任可委托给验证人就能够提高服务效率、简化服务流程。

从以上分析中可以看出，传统的智能合约协议机制与费用结构并不适合 FirmaChain，而我们的使命则是提供"物有所值"的服务。由此我们得出了最后的结论：要么刺激参与者在区块链网络上使用代币，要么构建一个垂直主网，只有这两种方案才更为符合 FirmaChain 的宗旨。由于开发流程中的其他功能也需要主网，因此 FirmaChain 是基于 Cosmos SDK（利用 Tendermint BFT 协议机制的框架）的专有主网，并启动交换代币的计划。

2.2 概述

主网详细信息如下：

代币	
代币符号	FIRMA
守护程序	Ufirma
小数点位	6
初始供应量	600,000,000 FIRMA (600,000,000,000,000ufirma)

网络	
imperium-0000	测试网
augustus-1	主网

运行环境	
Go	v1.13
Tendermint	v0.32.7
Cosmos-sdk	v0.32.4

2.3 运行机制

合同签署服务在链上的运行机制如下所述：

1. 创建合同：上传合同的详细内容，例如参与者的签名、文件 UID（哈希值）及文件存储端点等。→ 开始

2. **取消合同**：检查上传合同的详细信息→上传所有参与者的签名，同意使合同的哈希值无效→取消完成

3. **确认并验证合同**：确认合同哈希值与所有者地址是否匹配，接受合同文件路径

```
type Keeper struct {
        cdc        *codec.Codec
        storeKey sdk.StoreKey
}

func NewKeeper(cdc *codec.Codec, storeKey sdk.StoreKey) Keeper {
        return Keeper{
```

```
                cdc:      cdc,
                storeKey: storeKey,
        }
}

func (k Keeper) IsContractPresent(ctx sdk.Context, hash string) bool {
        store := ctx.KVStore(k.storeKey)
        return store.Has([]byte(hash))
}

func (k Keeper) IsDuplicateOwner(contract types.Contract,
                                        owner sdk.AccAddress) bool {
        for _, address := range contract.Owners {
                if owner.Equals(address) {
                        return true
                }
        }

        return false
}

func (k Keeper) GetContract(ctx sdk.Context,
                                    hash string) types.Contract {
        store := ctx.KVStore(k.storeKey)
        if !k.IsContractPresent(ctx, hash) {
                return types.NewContract()
        }

        bz := store.Get([]byte(hash))

        var contract types.Contract
        k.cdc.MustUnmarshalBinaryBare(bz, &contract)

        return contract
}

func (k Keeper) InitContract(ctx sdk.Context,
                                    hash string,
                                    path string,
                                    owners []sdk.AccAddress) {
        contract := k.GetContract(ctx, hash)
```

```
	contract.Hash = hash
	contract.Path = path
	contract.Owners = owners

	k.AddContract(ctx, hash, contract)
}

func (k Keeper) SetContract(ctx sdk.Context,
                            hash string,
                            path string,
                            owner sdk.AccAddress) sdk.Error {
	contract := k.GetContract(ctx, hash)

	if k.IsDuplicateOwner(contract, owner) {
		return types.ErrContractDuplicated(types.DefaultCodespace)
	}

	if len(contract.Hash) == 0 {
		contract.Hash = hash
	}

	if len(contract.Path) == 0 {
		contract.Path = path
	}

	contract.Owners = append(contract.Owners, owner)

	k.AddContract(ctx, hash, contract)

	return nil
}

func (k Keeper) AddContract(ctx sdk.Context,
                            hash string,
                            c types.Contract) {
	store := ctx.KVStore(k.storeKey)
	store.Set([]byte(hash), k.cdc.MustMarshalBinaryBare(c))
}

func (k Keeper) GetContractsIterator(ctx sdk.Context) sdk.Iterator {
	store := ctx.KVStore(k.storeKey)
```

```
        return sdk.KVStorePrefixIterator(store, nil)
    }
```

在这种情况下，端点使用存储区块链或防篡改伪造 IPFS，并进行了相应的验证。之后已验证的端点值将转换为以下 JSON 格式，并存储于事务块中。

另外，各个数据以默克尔树的形式进行处理以便管理，服务项目在利用数据时，相关数据会转换为默克尔树形式。Duite（duite.io）采取的便是这种形式。我们为 Duite 服务提供软件工具和指南，Duite 可以通过 FirmaChain 轻松管理数据。利用默克尔树来管理数据的一个优势之一是可以选择性地共享数据。

数据所有者仅记录默克尔树的根哈希。由于默克尔树的性质，虽然有一部分数据会被公开，但使用者提供默克尔证明（包括根哈希），即可验证全部数据的真实性。依靠这种性质，我们便可以在传输数据时将一些敏感的个人信息排除在外。而且使用者可在交易之前，就验证数据的真实性，具体方式就是提供诸如合同创建者签名这种选择性信息（尤其是在接收方提出要求时）。转换后的数据最初会保存在使用者的智能移动终端或电脑的存储空间中。

由于区块链上记录的内容只有原始数据中提取的根哈希，因此加密算法不受任何限制，特别是用于数据的存储及共享时。即使现有的加密方法可能会因为计算能力的提高而变得过时或不稳定，我们仍可以自由部署新的加密方法，无需彻底检查已经记录在区块链上的数据。

```
{
    "value": {
        "msg": [{
            "type": "firmachain/addContract",
            "value": {
            "path":"<https://ipfs.in-
    fura.io:5001/api/v0/cat?arg=QmTF7NerdGZhnDPJj3Yj51gqH18o8kLtgkgtVjMLk1V9tx>",
            "hash": "790e54e8723d7ad9c05b232498c3341e6f4465ec6db9f0449c2ba52fcf9d0569",
            "owner": "firma1ytleandjvn27kcpsfly3d39amw6n2znfpm5eg7"
          }
      }],
      "fee": {
        "gas": "200000"
      },
      "signatures": [{
          "pub_key": {
```

```
                "type": "tendermint/PubKeySecp256k1",
                "value": "AphzfQjmeJtOSczRUmZeqUKMDU4i6BkX9zL7B8HhidV1"
              },
              "signature":"yuHO318uATRuv3bTN6n2EKESWjFi5M9+3JnorGbaV2Zbu.
    pMu6roR7dRtVZ46biAKZ4VhP6YMDbwNpTF5X6wLNA=="
        }],
        "memo": ""
    }
}
```


2.4 firma-cli 使用者手册

firma 和 firma-cli 的安装方法和用户指南如下：

安装 Go

1. FirmaChain 是利用 GO 语言编写的应用程序，构建于 Cosmos SDK 与 Tendermint。
2. 如果您已经下载 GO 程序，可跳过这部分内容。
3. 请点击 GO Download and Install Guide 并下载 Go 1.14 或最新版本的 GO 软件。
4. 建议您安装稳定的 GO 版本。
5. 安装后，必须如下面所示的命令行添加$ PATH 环境变量。

```
bash
mkdir -p $HOME/go/bin
echo "export PATH=$PATH:$(go env GOPATH)/bin" >> ~/.bash_profile
source ~/.bash_profile
```

下载二进制文件

1. 成功下载后开始设置 GO 环境，请务必下载最新版本的 firma 与 firma-cli。
2. 克隆 FirmaChain GitHub，执行 build 命令。

```
bash
git clone -b https://github.com/FirmaChain/FirmaChain
cd FirmaChain && make install
```

1. 如果出现以下错误消息，则设置中可能包含了 LDFLAGS。

```
flag provided but not defined: -L
usage: link [options] main.o ...
make: *** [install] Error 2
```

2. 使用以下命令，将 LDFLAGS 从设置中删除。

```
LDFLAGS="" make install
```

复制二进制文件

1. 为了您使用方便，请在安装二进制文件之后创建 Symlink。
2. 请参考以下命令创建 Symlink。（对象文件夹可能因您的 GO 设置与操作系统而不同。）

```
sudo ln -s ~/go/bin/firma /usr/local/bin
sudo ln -s ~/go/bin/firma-cli /usr/local/bin
```

3. 创建 Symlink 后，请检查 Symlink 的功能是否正常运行。

```
> firma
FirmaChain (server)

  Usage:
    firma [command]

  Available Commands:
    init                Initialize private validator, p2p, genesis, and application configuration files
    collect-gentxs      Collect genesis txs and output a genesis.json file
    gentx               Generate a genesis tx carrying a self delegation
    validate-genesis    validates the genesis file at the default location or at the location passed as an arg
    add-genesis-account Add genesis account to genesis.json
    start               Run the full node
    unsafe-reset-all    Resets the blockchain database, removes address book files, and resets priv_validator.json to the genesis state

    tendermint          Tendermint subcommands
```

```
  export                Export state to JSON

  version               Print the app version
  help                  Help about any command

Flags:
  -h, --help                help for firma
      --home string         directory for config and data (default "/Users/Marutian/.firma")
      --log_level string    Log level (default "main:info,state:info,*:error")
      --trace               print out full stack trace on errors

Use "firma [command] --help" for more information about a command.
```

预建二进制

如果您的环境不允许构建 FirmaChain，或由于其他各种原因而无法构建 FirmaChain，您可预建二进制。请在存储库（FirmaChain Repository）中的 Release 目录中找到预建二进制文件。

1. 支持 Ubuntu（linux）和 macOS（darwin）操作系统。
2. 预构建二进制文件是由 Ubuntu 18.04 和 macOS 10.15 Catalina 所构建。

2.4.1 参与网络

创建新的节点以参与网络。

1. 创建一个新的节点和设置文件。

```
# ex: firma init validator --chain-id=augustus-1
firma init <moniker> --chain-id=<chain-id>
```

2. moniker 必须使用 ASCII TEXT 编写
3. 之后可在~/.firma/config/config.toml 文件中修改 moniker

```
# A custom human readable name for this node
moniker = "<new_moniker>"
```

设置最低手续费（Gas Price）

此设置的目的是防止 FirmaChain 遭到攻击。

1. 请在~/.firma/config/app.toml 文件中将手续费设置为最低值 0.01ufirma。

```
minimum-gas-prices = "0.01ufirma"
```

复制 Genesis 文件

此为导入 FirmaChain 的基本信息的过程。

1. 基本信息包含在 genesis.json 文件中，可以在 FirmaChain Launch 中找到。
2. genesis.json 文件位于~/ .firma / config 目录中。
3. 请参考以下命令。

```
curl https://raw.githubusercontent.com/FirmaChain/FirmaChain-Launch/master/genesis.json > $HOME/.firma/config/genesis.json
```

由于 Launch Repo 尚未披露，因此我们在本文中为 Augus-tus-1 main-net 提供了一个单独的 genesis.json 文件。（韩语版本无）

4. genesis.json download (https://github.com/FirmaChain/FirmaChain-Launch/blob/master/genesis.json)

添加种子节点

区块链是由多个互连的节点组成的网络。为了将您创建的节点添加到网络，您必须找到 Peer。

1. 请检查 FirmaChain Launch 中可用种子节点的列表。
2. 您可以在~/ .firma / config / config.toml 文件中设置种子节点。
3. 在 config.toml 文件中选择以下项之一并进行修改。

```
seeds="<Seed Node1>,<Seed Node2>"
```

```
persistent_peers="<Seed Node1>,<Seed Node2>"
```

启动节点

1. 启动节点十分简单。

```
firma start
```

2. 请检查节点的激活状态。

```
firma-cli status
```

2.4.2 验证者的参与

以区块验证者身份参与 FirmaChain

验证者的角色

1. 运行节点来管理事务日志
2. 验证区块的完整性并生成块
3. 对记录在区块上的合同文件（以电子合同形式）的哈希值进行验证

成为验证者的凭证

1. 目前尚无成为验证者必须要满足的标准。然而新申请的验证者需比现有验证者结合更多的 Firma。

验证者系统设置

1. 硬件要求（所列出的条件会随着网络的发展而变化。FirmaChain 基金会将支持不断变化的硬件要求）
2. 数据中心设施需满足基本电源要求、联网条件、防火墙设置、硬件安全模块和备用服务器。
3. 宽带至少为 5Gbps 网络
4. 具备至少 100Gb 的存储设备

验证者任务

1. 主网常规开发更新过程中，升级软件并修复 bug
2. 参与 FirmaChain 社区治理和所有决策过程

验证者惩罚（罚没 Slashing）

1. **停机时间（Downtime）**：验证者错过块上签名即为停机时间。验证者错过近期 10000 笔交易中的超过 500 笔以上的交易时，则会受到惩罚。停机时间罚没比率是验证者与委托者拥有的总量的 **0.01%**。

2. **双重签名（Dual Signature）**：如果来自 A 链的验证者在 A 链与 B 链相同的两个区块高度上签名（即，A 链和 B 链源自共同祖先），那么验证者将在 A 链被罚没。由于双重签名是极为严重的错误，其发生会让验证者与委托者双方的利益都受到损害。

确认验证者的公钥

```
firma tendermint show-validator
```

创建验证者

请参考以下命令，创建验证者。

请在操作前检查以下项目：

1. 所有块必须同步到节点。
2. 必须在 firma-cli 上注册密钥和账户。
3. 注册验证者时，需最低质押 100 万 Firma。
4. 注册验证者所需的交易费用会从注册账户中扣除。
5. 交易费必须设定为“**自动**”，交易费必须设置为 **1.7** 以上。

```
firma-cli tx staking create-validator \
--amount=1000000000000ufirma \
--pubkey=$(firma tendermint show-validator) \
--moniker=<moniker> \
--chain-id=<chain_id> \
--commission-rate="0.10" \
--commission-max-rate="0.20" \
--commission-max-change-rate="0.01" \
--min-self-delegation=1 \
--gas="auto" \
--gas-prices="0.01ufirma" \
--gas-adjustment=1.7 \
--from=<account_name_or_address>
```

查看我的奖励

FirmaChain 使用 DPoS 奖励机制，个人或实体可以将个人代币质押给注册的验证者来获取奖励。

1. 请参考以下命令来查看我的奖励。

```
firma-cli query distribution rewards <my_address>
```

2. 您可以通过上面的命令查看奖励数量以及您投票过的所有验证者列表。
3. 请参考以下命令来查看对某个具体验证者投票后获得的奖励。

```
firma-cli query distribution rewards <my_address> <validator_pubkey>
```

领取奖励

您可以通过对某个具体验证者身份进行质押或者直接参与网络来领取奖励，。

您无法要求想要兑换的奖励数量，奖励将以总额进行支付。

```
firma-cli tx distribution withdraw-rewards <validator_pubkey> \
--from=<account_name_or_address> \
--gas=auto \
--gas-prices=0.01ufirma \
--gas-adjustment=1.7
```

2.4.3 用作命令行

通过 firma-cli 的命令行界面，FirmaChain 可以查找网络上的注册信息或发送的交易。也就是说，使用 firma-cli，用户以及参与者可以查看他们的钱包余额，转账 Firma 给其他用户或参与者。

1. 在安装和构建 FirmaChain 时，会同时创建 firma-cli 与 firma 二进制文件。
2. 有关安装与构建 FirmaChain 的详细指南，请参考二进制文件章节。
3. 可以在 firma-cli 中使用的 1-depth 命令如下：

```
status      Query remote node for status
config      Create or query an application CLI configuration file
query       Querying subcommands
tx          Transactions subcommands
rest-server Start LCD (light-client daemon), a local REST server
keys        Add or view local private keys
version     Print the app version
help        Help about any command
```

> **在每一个命令的尾端插入'-h'或'—help'，便可查阅功能的简要说明和相应命令的简要用户指南。**

Wallet Creation 创建钱包

您必须在 FirmaChain 上创建一个钱包来转进或转出 Firma。

1. 您可以插入以下命令来创建钱包。

```
firma-cli keys add <key_name>
```

2. 输入密码（8 个或以上字符），完成创建钱包。如果忘记密码或已重置 firma-cli 密钥，您还可以通过助记词来找回。
3. 请将您的助记词保管于线下安全的地方。
4. 请参阅以下内容，利用助记词找回钱包。

```
firma-cli keys add <key_name> --recover
```

5. For other wallet related commands, please refer to the list below.
   有关钱包的其他命令，请参考以下列表。

```
firma-cli keys show <key_name>   // Check the address of a specific wallet.
firma-cli keys delete <key_name>   // Delete wallet from the storage space.
firma-cli keys list   // Look up all list of wallets on the storage space.
```

转出 Firma

以下内容为使用 firma-cli 来转出 Firma 的简要指南。

```
firma-cli tx send <from_key_or_address> <to_address> <amount> [flags]
```

用户必须具备以下信息才能转出 Firma：转出 Firma 的钱包、密钥名称、钱包地址以及要转出的 Firma 数量。 输入金额时，您必须输入 1,000,000ufirma。 （Firma 和 ufirma 之间的换算如下）

- 1Firma 等于 1,000,000ufirma（小数位：6）

LCD (REST API) 激活

1. REST API 服务器可以从 firma-cli 激活。

```
firma-cli rest-server
```

2. 在此命令下，一旦 Shell 会话结束，服务器将变为非活动状态。
3. 建议您在后台执行此命令。
4. LCD 服务器处于激活状态时，无法通过 firma-cli 查询。

搜索已签署的合同（文件）

只有在 FirmaChain 上注册的文件才可以使用哈希值确定其真实性。

1. 请在获取文件的哈希之后，使用下列命令来确定文件的真实性。

```
```

```
firma-cli query contract <hash>
```

更多命令等待您体验。

请在每个本指南中未列出的命令的末尾插入“ -h”或“ --help”，以获取更详细的说明和指南。

2.4.4 用作 RPC

LCD 主机信息

主网：http://lcd.augustus-1.firmachain.org

测试网：http://lcd.imperium-0000.firmachain.org

GET /txs
按高度查看交易

GET /txs/{hash}
按哈希查看交易

GET /node_info
查看已连接节点的信息

GET /contract/{hash}
查看合同哈希值

```
func QueryContractHandlerFn(cliCtx context.CLIContext) http.HandlerFunc {
  return func(w http.ResponseWriter, r *http.Request) {
    vars := mux.Vars(r)
    paramType := vars["hash"]

    res, _, err := cliCtx.QueryWithData(fmt.Sprintf("custom/%s/%s", types.QuerierRoute, paramType), nil)
    if err != nil {
      rest.WriteErrorResponse(w, http.StatusNotFound, err.Error())
      return
    }

    rest.PostProcessResponse(w, cliCtx, res)
  }
}
```

POST / 合同
注册合同

```
type AddContractReq struct {
  BaseReq rest.BaseReq `json:"base_req"`
  Path    string       `json:"path"`
  Hash    string       `json:"hash"`
  Owner   string       `json:"owner"`
}

func AddContractHandlerFn(cliCtx context.CLIContext) http.HandlerFunc {
  return func(w http.ResponseWriter, r *http.Request) {
    var req AddContractReq

    if !rest.ReadRESTReq(w, r, cliCtx.Codec, &req) {
      return
    }

    baseReq := req.BaseReq.Sanitize()
    if !baseReq.ValidateBasic(w) {
      return
    }

    addr, err := sdk.AccAddressFromBech32(req.Owner)
    if err != nil {
      rest.WriteErrorResponse(w, http.StatusBadRequest, err.Error())
      return
    }

    msg := types.NewMsgAddContract(req.Path, req.Hash, addr)
    err = msg.ValidateBasic()
    if err != nil {
      rest.WriteErrorResponse(w, http.StatusBadRequest, err.Error())
      return
    }

    utils.WriteGenerateStdTxResponse(w, cliCtx, baseReq, []sdk.Msg{msg})
  }
}
```

GET /blocks/latest

检索最新的区块信息

GET /blocks/{height}

从指定高度的区块中检索信息

GET /bank/balance/{address}

通过指定地址检索所拥有的 FIRMA 数量

POST /bank/accounts/{address}/transfers

将 FIRMA 发送到另一个钱包

GET /supply/total

当前提供的 FIRMA 总量信息

GET /minting/inflation

查看区块链当前的铸币通胀率

GET /minting/annual-provisions

即将铸造的 FIRMA 的预计年产量

GET /staking/validators

查看有关所有验证者的信息

> 请参阅 https://cosmos.network/rpc/v0.37.9，以获取有关 RPC 的更多详细信息。

2.5 代币经济

```
  let goalBonded = 0.51 // Target Bonding Percentage
  let inflationRateChange = 0.0000001 // Change in Inflation Rate
  let blocksPerYr = 6311520 // Blocks Minted per second
  let inflation = 0.0116428571425 // Inflation Rate
  let max = 0.017 // max inflation
  let min = 0.007 // min inflation
  let totalSupply = 600000000
  let bondedRatio = 11000000 / totalSupply // Current Bonding Percentage (based
on 1 million per validator)
  let bonded = 11000000

  let validator_count = 11 // Number of Validators
  let rateChangePerYr = ( 1 - bondedRatio / goalBonded ) * inflationRateChange //
Annual Fluctuation Rate

  let rateChange = rateChangePerYr / blocksPerYr // Fluctuation Rate per Block
```

```
  inflation += rateChange // Calculate change in inflation rate

  if(inflation > max)
      inflation = max;

  if(inflation < min)
      inflation = min;

  let annual_provisions = inflation * totalSupply // Number of Annual Coin Pro-
visions
  let validator_rewards = annual_provisions / validator_count // Validator Reward
  let rewardPerBlock = validator_rewards / blocksPerYr // Coin Reward per Block
```

代币总供应量会根据以上所计算的通货膨胀率而增加。验证者节点每建造一个区块便会获得 Firma 作为奖赏。

3. FirmaChain DApp：电子合同

3.1 现有知识产权授权协议的问题以及基于区块链技术的解决方案

由于国际合同要求本人亲自执行，因此其中一个合同方需花费大量时间和差旅费。

目前的知识产权授权协议在修改及订立之前都在线上进行传输。然而服务器的中心化结构可能存在伪造和安全漏洞的隐患。不仅如此，使用电子邮件与 Messenger 收发合同时，无法验证对方的身份、权威性以及权利。区块链技术的出现可以解决上诉所有问题。

FirmaChain 与**电子合同**结合了合同的基本因素与区块链技术，旨在使多方合同当事人圆满签订并实施合同。此外，FirmaChain 正在尽全力解决上述社会问题。

基于区块链的 FirmaChain 电子合同在专利、商标和版权（游戏、角色、动画等）等知识产权授权协议中发挥充分优势。此类知识产权授权协议将成为 FirmaChain 建立的新平台的第一类服务目标。

当前的授权协议存在以下问题：

欲执行协议的受让方很难验证知识产权（专利、商标等）的实际持有人（包括独家受让方）。其名称或地址可以在韩国知识产权局出版的官方专利刊物中确认。跨境合同的情况，将知识产权转让已给第三方或进行独家或非独家授权时，想要明确受让方的身份并追踪实际许可方就更具挑战性了。

由于难以确认执行授权协议的人的身份，许可方同样也面临欺诈风险。而且第三方很难了解专利、商标的使用期限以及许可方（包括独家受让方）的完整信息。

例如，购买者在购买产品时，难以确认这种已经注册了专利或商标的产品是否由合法拥有该知识产权的人员生产

就算相关人员拥有知识产权，但签署一份书面协议仍然会消耗大量时间以及费用。所有者想要在其他国家使用知识产权时，同样面临各种实际问题（时间与成本）。跨境汇款、缴税等过程，各方始终都有遭到欺诈的可能，造成不便和困扰。

FirmaChain 为解决上述问题提出了一下解决方案：

1. 用户只要能够访问网络，就可以确认知识产权的详细信息，包括知识产权、所有人以及适用范围（地域范围）。
2. 在整个合同执行过程中进入基于区块链的电子合同，用户因此而能够记录和验证整个合同签署的过程，包括谈判以及收发历史记录等。
3. 经验证的许可方与受让方可以利用电子合同平台（E-Contract）快速执行包括知识产权授权协议在内的线上跨境合同，避开欺诈风险的同时，无需在现实世界里见面处理。
4. 各种灵活功能，包括控制面板、标准合同样式、法律咨询服务匹配以及第三方专业人员审核等，让合同签署变得更加快捷。
5. 知识产权所有者可以在 irmaChain 平台上轻松找到潜在受让方，从而降低成本，促进各种许可协议的执行。

FirmaChain 的解决方案将拓宽国际授权市场，提高相关交易的透明度。

3.2 电子合同和流程控制的需求

人们对书面合同的一成不变的偏好引发了很多社会上的问题。合同文件需要单独保存，十分不便。一开始，双方各 1. 持有一份书面合同，同步任何后续修订内容十分困难，也增加了欺诈的可能性。许多公司通过电子邮件或语音录音的额外措施，配合修改内容的时间，但难于管理。虽然书面伪造是一个无法避免的严重问题，可导致法律纷争，难以预防。为解决这些问题，电子合同开始在社会中崭露头角。

电子合同是一种公司之间数字化的合同协议。具有类似概念的电子文档（《电子交易法》）被认为具有与书面文档相同的法律效力。国内外与商业交易有关的法律规定，电子签名（《数字签名法》）具有法律效力。由此，电子合同也具有法律效力。

目前，电子合同的效率优于书面合同。 然而电子合同仍然未能超越书面合同，成为人们的首选。这是因为电子合同有一些不可避免的问题，例如合同可能会被未经授权的人员签署，系统故障可能导致传输风险等。此外，不够先进的公司表明立场，愿依附传统方式，因此电子合同技术的地位仍然处于被低估的状态，其必要性未得到认可。

FirmaChain 的目标是通过利用区块链的特点，实现电子文件与合同的透明性与可靠性，从而解决当前的问题。

3.3 为什么要使用电子合同?

< 使用电子合同创建并实施合理的合同 >

从先进的现代社会的角度来看，在制定和实施大小合同时，我们使用的是相当原始的方法。比如，我们通过几次电子邮件的传达来收发合同，或者有时在同一天交换合同。有些人在签署合同之前没有正确检查合同的内容，使用不符合法律要求的印章或邮票，甚至因为合同太消耗时间而不签合同便开始工作 。

另外，许多公司签订合同时，由于交易成本高且合同期长，因此他们选择只管理合同内容，包括合同的进度、状态、附加工作以及书面合同修改等。因此合同执行日程变得难以管理。

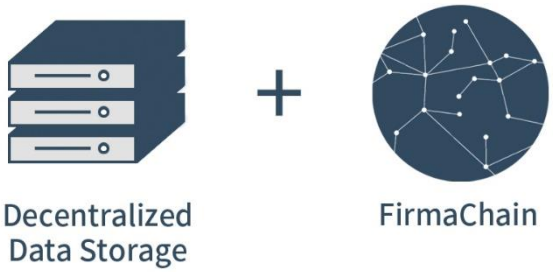
FirmaChain 的电子合同（DApp）通过智能合同和公共链提供透明账本，确保合同的合法性和稳定性。**利用这样便捷与基础的功能来管理合同签署过程，可以提升业务的效率。 此外，它可以合理地解决交易费用问题，将用于合同的货币替换成加密货币。它还可以解决以下具体问题，创建跨国合同时出现的双重征税、海外法人成立以及海外汇款等，从而使人们能够有效地执行其业务计划。**

从上述服务结构中可以看出电子合同将提供多种功能。（电子合同的强制安全参数、标准合同的表单预设、合同编辑和管理）

4. 电子合同的结构

电子合同分为：1）核心层：保存加密合同数据和交易；2）应用层：使用 DApp 创建和管理合同；3）服务层：验证和处理电子合同，并连接核心层和应用程序层。

4.1 核心层（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。支付方式为当地法币币种或 **FirmaChain 的代币(以下简称"FCT")**。若将款项设为当地法币币种时，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。

如果在修改合同时交易金额有任何变化，则新的预存金金额将根据先前设定的存款金额另外汇出或退还。

***散列串(Hash String)**

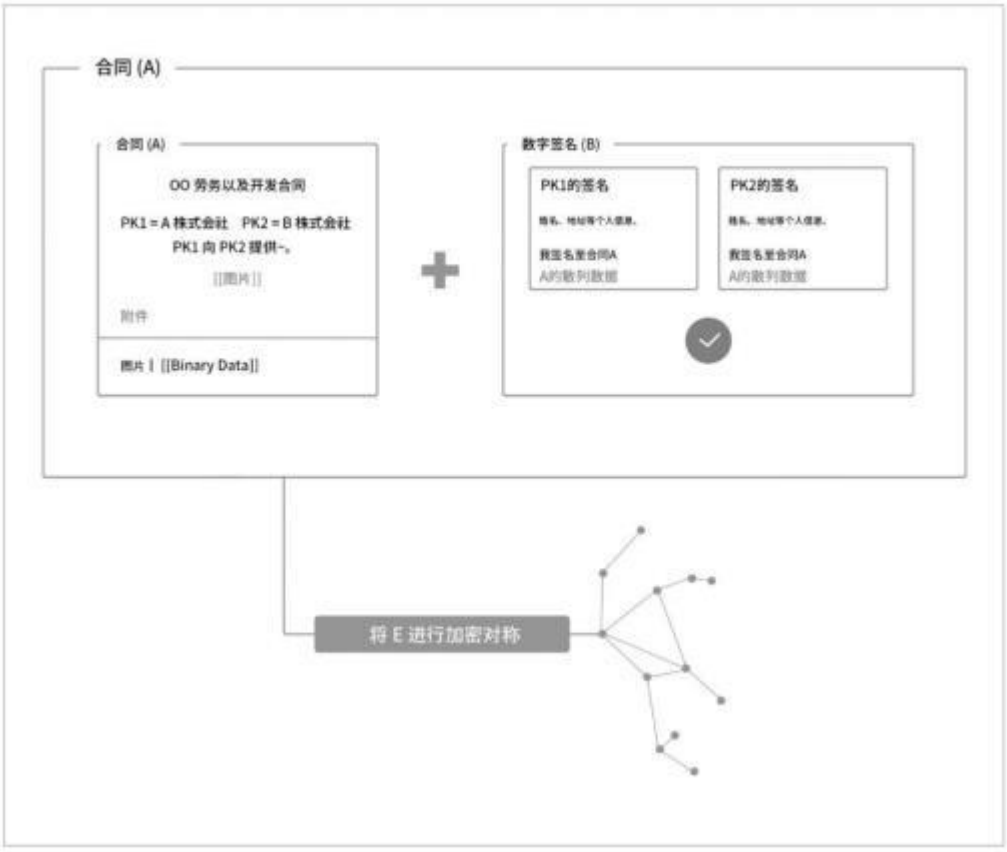
散列串是指利用加密散列函数将任意长度的数据对应至固定长度 的字符串。该函数是单向函数，无法通过散列串获得原版数据，假使 原版数据中出现了极其微小的变动，就会得出完全不同的散列串。这 便于检查数据的完整性 ， 我们将散列串作为 FirmaChain 的电子文件 固有识别数据。将使用的加密散列函数有 SHA256 或 SHA512 等，此 类算法均已通过验证。

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。

implemented.

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。 文档的散列串上载到 FirmaChain 的智能合约中，并实现了合约。

专利许可合同（独家许可）

本合同由 A 有限公司（以下“甲方”）与 B 有限公司（以下“乙方”）之间缔约并签订：

第一条 目的

甲方向乙方独家授予甲方所拥有的以下专利权（以下“专利”），

专利号	No.
发明名称	

第二条 专利的注册

自本协议执行起，乙方可以自付费用注册前条所述的许可书。甲方应配合。

第三条 许可书的适用范围

乙方使用专利的许可范围如下：
1. 地区：韩国
2. 期限：自 20xx 年 xx 月起，共 xx 年
3. 适用类型：制造与销售

……

第十三条 许可费的退款

乙方在任何情况均不退还已收取的许可费。

第十四条 合同的终止

在出现以下任意一种情况时，甲方可以无需通知乙方立即终止本合同：
1. 乙方未及时缴纳许可费；
2. 乙方在无正当理由的情况下，自本协议签署之日起 x 个月内未使用该专利时；或者

…

附件。合同内容

[[image::Binary Data...]]

甲方电子签名：
[[Digital Signature::0GCSqGSZKjeGcjDlb3D...]]

乙方电子签名
[[Digital Signature::DOL5Ulsuulb3DQEISaC...]]

< 加工结束后，加密处理之前的电子合同样本 >

上述样本是加工过的电子文档。该电子文档由包含合同内容的文本数据组成； 例如图像，音乐，录音等的二进制 base64 编码的数据；以及可以随时验证双方电子签名的公钥。

以上样本可能会在合作伙伴律师事务所审查后进行某些修订，以确保电子文档和电子合同的法律有效性。

$A = Contents\ of\ a\ contract$ $E_K(M): Encrypt\ M\ by\ using\ key\ K$

$HASH_A = SHA256(A)$ $S = Secret\ key\ of\ A$

$SK, PK = KEY\_GENERATE()$

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

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

$S1 = E_{SK1}(M1)$

$S2 = E_{SK2}(M2)$

$B = S1||S2$

$W = A||B$

$C_W = E_S(W)$

$HASH_W = SHA256(C_W)$

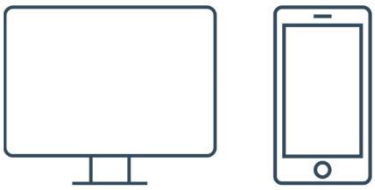
$HASH_W \rightarrow Smart\ Contract$

$C_W \rightarrow Decentralized\ Data\ Storage$

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。

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。 此外，用户可以编辑标准合同并保存他们创建的合同。

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. 发展路线图（Roadmap）

- 业务发展路线图

2021 第一季度

- 扩大市场份额，获得韩国市场的活跃用户
- 与主网节点验证者深入讨论关键术语
- 与韩国其他公司/区块链项目的技术和商业伙伴关系

2021 第二及第三季度

- DONUE营销活动
- 选择最后11家公司作为主网节点验证者
- 开拓中国市场
- DONUE的功能更新

2021 第四季度

- 进行数据驱动的分析，以进行下一个DONUE更新
- DONUE的业务扩展到东南亚市场

- 技术发展路线图

2021 第一季度

- DONUE功能增强
- 扩展主网可用性
- 内化DONUE上的实时数据（IDS和其他主要数据）身份验证

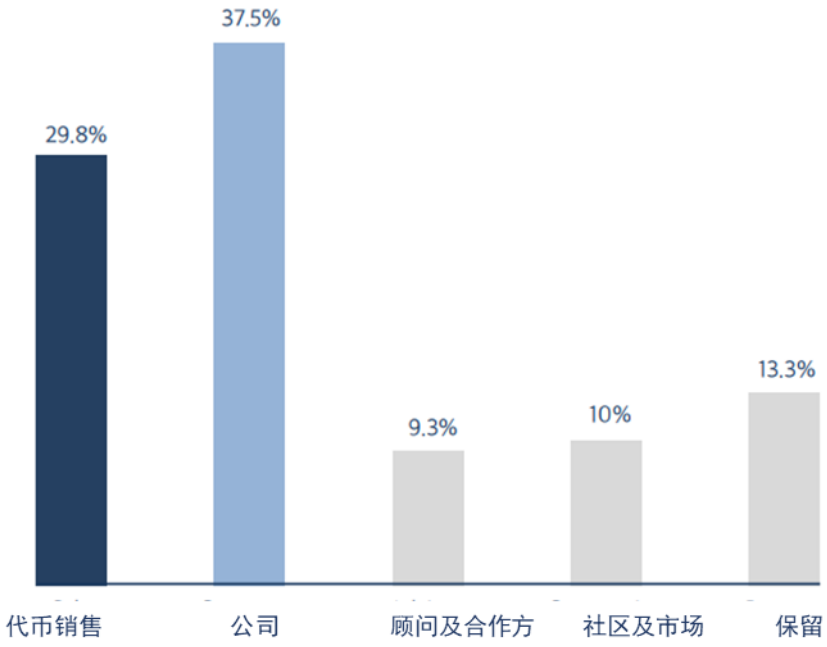
2021 第二季度

- DApp开发
- 主网智能合约的开发与更新

2021 第三及第四季度

- 主网代币交换
- 对主网上的硬分叉实施的评估/审查
- 主网与DONUE之间的网络API集成
- DApp发布
- 开发DONUE SDK

6. 代币分配



* 所有数值为小数点四舍五入的整数

初始发行量：600,000,000 FCT (FirmaChain Token)

总发行量：279,406,275.58 FCT (as of March, 2021)

7. 团队介绍

Young Yoon
首席执行官

Jack Lee
首席技术官

Bullisay Park
首席区块链架构师

Wan Kim
全球业务
中国区负责人

Justin Wee
全球业务负责人

Juchan Park
前端开发人员

Timothy Kim
市场经理

Jason Piao
区块链开发人员

Robert Han
规划经理

8. 顾问

Han Jong Lee

CEO

Goodtimewith.me

Firma–chain的愿景是通过去中心化、透明并且可靠的区块链技术，消除各种复杂问题，实现改革现代社会的基础，即书面合同的目的。

尤其是涉及多国的合同时，我们基于经济增长的技术可以透明、有效地解决国家间双重征税、海外注册、境外汇款和费用等问题。期望通过我们长期的团队合作以及快速、灵活的执行力，将愿景落地。Firma团队邀请您加入我们共同面对挑战，寻求真是。

Hyeonwook Jeong

CEO / Founder创始人

beSUCCESS

在基于区块链的数据存储中仍有很多改进空间，尤其是电子文档和合同的形式。我从早期见证并参与了FirmaChain团队合作。

根据我的个人经验，我相信FirmaChain将持续增长并在将来保持强大实力，因为其团队坚实、发展路线图切合实际 。FirmaChain强大的团队具有开发解决方案的巨大潜力，能够为交易注入更多的创新，并加速其发展。就个人而言，我很高兴能作为顾问加入，并支持该项目的全球扩展。

Guho Son

CEO

Monument Company

Former Managing Director of SoftBank Ventures

Monument 公司

软银创投前任总经理

区块链从金融行业开始一直引领着第四次工业革命，并且被认为是领先的技术。设备数量众多，交易量飞涨，导致传统的基于云的集中式系统出现各种问题，例如系统维护和安全性。

FirmaChain的解决方案将不仅为金融业创造更透明、更安全的解决方案，还将给零售、制造业带来益处，解决社会文化问题，最终为我们的经济带来积极影响。

Jiwook Kim

Attorney at law

Partner at Yoon & Yang LLC

Yoon & Yang LLC合伙人律师

区块链技术依赖网络内参与者的责任与交易验证，它让加密信息去中心化，从而提高透明度和安全性。 FirmaChain利用了区块链的这些特点，制定了基于区块链的电子合同平台。 它可以简化合同程序（草拟合同、谈判、缔结合同），上传到区块链网络的合同由参与网络的人员验证，消除了伪造风险并增加了合同管理的透明度，加强了合同安全。FirmaChain是解决我们在传统合同中遇到的缺点的方案。

9. 合作

战略合作伙伴

finector BLOCORE Hexlant.

Atlas Capital BLOCKLINKER PURSUIT OF PERFECTION Decenter

哈鲁资本 HELLO CAPITAL LIWU Law Group ZBT play games get rewards

生态系统合作伙伴

GoodTimeWith.Me ReviewShare blank.

ACE CONSTRUCTION CO., LTD. freshworks MagNet Blockchain Marketing Agenc

bananatok CERTIK FOUNDATION INSIGHT PROTOCOL

合作媒体

KoreaTechDesk BlockDaily ICORATING BSR

10. 免责声明

请仔细阅读整个免责声明。如果您对即将付诸现实的行动有任何疑问，请咨询您的法律、财务、税务或其他专业顾问。

1.1 法律声明

本白皮书（以下“白皮书”）以当前形式发行，仅用作提供目前构想的白皮书中描述的平台（以下“平台”）和应用程序相关的一般信息，必要时会进行审核和修订。请注意本白皮书所述的工作内容仍在进行，所提供信息仅反映封面所示日期为止的内容。包括与 Firmachain Pte Ltd（以下“公司”）业务运营和财务状况有关的信息，可能在今后进行修改。 我们保留出于任何原因或在任何时候不经通知的情况下更改、修改、添加或删除白皮书部分内容或网站的权利。

(a) 任何人都没有义务就平台固有的代币（即“FCT 代币”以及/或“ FCT 币”或统称“代币”）（定义见上文）的买卖产生履行合同的义务或承担法律约束力的承诺，并且不接受任何依据本白皮书的付款。代币的买卖受具有法律约束力的协议约束，其详细信息将与本白皮书分开提供。如果相关协议与本白皮书有任何不一致之处，应以前者为准。

(b) 对于任何代币的销售，代币发行人/分销商/卖主销售的代币，或代币的购买，本白皮书均不构成任何意见，也不构成部分建议。白皮书所陈述的事实也不构成任何合同或投资决定的基础或与之相关的依据。

(c) 代币并不应当构成一种资本市场产品，包括但不限于根据《新加坡证券和期货法》或任何其他司法管辖区的等效法令所定义的证券、以杠杆外汇交易目的的即期外汇合约、衍生品合约或共同基金中的投资单位。因此，本白皮书不构成，也无意构成任何司法管辖区管辖内的任何形式的招股说明书、简介声明或要约文件，并且不应解释为任何形式的证券要约、商业信托的投资单位、共同基金的投资单位或任何其他形式的投资建议。

(d) 任何代币不得被诠释、解释、分类或当做能使购买者参与或接收来自平台、代币或形式相关的利润，收入或其他付款或回报。 。

(e) 任何司法管辖区如果对本白皮书中所制定的提供虚拟币或代币具有管制或禁止的规定，则不可以复制、发行或本白皮书或部分内容复制，分发或散播本白皮书或其任何部分。

(f) 本白皮书中列出的任何信息无任何监管机构的审核、检查或批准。司法管辖区都没有或计划采取任何此类行动。

(g) 如果您想购买任何代币，不应将代币诠释、解释、分类或视为任何类型的《新加坡证券和期货法》或其在任何其他司法管辖区（包括但不限于）中所规定的资本市场产品，包括但不限于：（a）加密货币以外的任何其他货币；（b）任何实体发行的债权证、股票或股份；（c）有关该等债权证、股票或股份的权利，期权或衍生产品；（d）差异合同或任以保障利润或避免损失为目的或拟定目的的任何合同；（e）共同基金或商业信托的投资单位或衍生产品，或任何其他类型的证券。

1.2 发行与传播的限制

(a) 任何辖区的法律或法规要求都可能会禁止或限制发行或传播本白皮书或其任何部分。如果本白皮书或其部分内容（视情况而定）受到限制，您必须自费寻求法律及其他相关建议，了解该规定，本公司及其代表和附属公司（“分公司”）则不承担任何责任。

(b) 已向其分发或分发本白皮书副本，对其提供访问权限或以其他方式拥有该白皮书的人，不得以任何目的将其分发给其他人，复制或以其他方式分发本白皮书或此处包含的任何信息 。

1.3 免责声明

(a) 公司及及其附属公司提供的代币、平台和相关服务均按"现况"和"现有"为基础。本公司及其附属公司不对代币、平台或本公司提供的任何相关服务的可访问性、质量、适用与否、准确性、充分性或完整性作任何担保，也不作任何明示、暗示或其他方式的陈述；并明确声明不对公司及其附属公司提供的代币、平台和相关服务的错误、延误或遗漏或据此采取的任何行为承担任何责任。

(b) 本公司、其附属公司及其董事、管理人员及雇员不对任何实体或个人作任何形式或意图以任何形式对白皮书中列出的所有信息的真实性、准确性和完整性作出任何陈述、保证或承诺。

(c) 在适用法律和法规允许的最大范围内，公司及其附属公司不应对任何由于您对本白皮书或其任何部分的接受或依赖而产生的或与之相关的间接、特殊、偶发、继发性或其他任何形式的侵权、合同或其他形式的损失（包括但不限于收入、利润以及使用或数据的损失）负责。

1.4 前瞻性陈述的提示声明

(a) 本白皮书中阐述的某些信息包括有关项目的未来计划、事件和预测的前瞻性信息。这些陈述非历史事实，可以被识别为"将"、"估计"、"相信"、"期望"、"项目"、"预期" 或类似的表述。本白皮书中包含的前瞻性陈述也包含在其他公开可用的材料中，例如演讲、访谈、视频等，陈述内容包括但不限于公司或其附属公司的未来结果、业绩或成果。

(b) 前瞻性陈述涉及各种风险和不确定性。这些陈述不能保证将来的业绩，也不应对其过分依赖。如果这些风险或不确定因素中的任何一种成为现实，则公司或其附属公司的实际业绩和进步可能会与前瞻性陈述所设定的期望有所不同。如果情况发生任何变化，附属公司不承担更新前瞻性陈述的义务。根据本白皮书、本公司或其附属公司的网站以及其他本公司或其附属公司制作的材料中所述的前瞻性陈述而行动，然而未能实现前瞻性陈述的内容时，则全部责任由您个人承担。

(c) 截至本白皮书发布之日，该平台尚未完成且尚未完全投入运营。有关平台的任何描述均基于平台将完成且可全面运行的基础上进行的。但是本款绝不应被解释为作出平台将最终完成或完全运行任何形式的保证或保障 。

1.5 潜在风险

通过购买、持有和使用代币，如果其中任何风险和不确定性发展成为公司或其附属公司的实际事件、业务、财务状况、运营结果和前景，您明确承认并假设本款列出的风险 。在这种情况下，您可能会丢失代币的全部或部分价值。 此类风险包括但不限于以下风险：

与代币有关的风险

(a) **可能没有交易该代币的公开或二级市场**

I. 代币旨在用作要在平台上使用的原生代币，并且公司及其附属公司尚未且可能不会积极促进代币的任何二次交易或外部交易。此外，且代币一直没有公开市场，并且未在在任何加密货币交易所还是在其他地方进行过交易。如果代币在加密货币交易所进行交易，不能保证会为代币开发活跃或流动的交易市场，若开发，不能保证其续存。无法保证代币的市场价格不会降到购买代币所支付的价格以下，也不表示市场价格。

II. FCT 代币和/或 FIRMA 代币不是任何中央银行或国家、超国家或准国家组织发行的货币，也不由任何硬资产或其他信贷支持。公司及其附属公司不对代币在市场上的流通和交易承担任何责任。代币的交易仅取决于相关市场参与者之间对其价值的共识，无任何人有义务从代币的持有者（包括代币的购买者）获取代币，也无任保证代币在任何时间都有任意程度的流动性或市场价格。因此，公司及其附属公司不能确保对代币有任何需求或交易代币的市场，也不保证如果代币可以在交易所进行交易，购买代币的价格表示代币的市场价格。

与公司，其关联公司和平台有关的风险

(a) **有限的可用信息**

截至本白皮书发布之日，该平台仍处于早期开发阶段。其治理结构、目的、共识机制、算法、代码、基础架构设计以及其他技术规范和参数可能会随时更新以及更改，恕不另行通知。尽管本白皮书包含与平台有关的当前可用的关键信息，但如公司网站上所声明，可能会不时进行调整和更新。购买者将无法完全访问与代币和/或平台相关的所有信息。 尽管如此，公司预计自行决定在有必要的情况下，不时在公司网站上宣布重要的里程碑和进度报告。

(b) **通过销售代币而产生的数字资产面临盗窃风险。**

尽管公司及其附属公司将尽一切努力确保实施安全措施来安全持有从代币销售中收到的任何加密货币，但不能保证不会因黑客入侵、 挖掘攻击、复杂的网络攻击、分布式拒绝服务或此类区块链地址或任何其他区块链或其他方面的漏洞或缺陷而致使该加密货币遭受盗窃。此类事件可能包括例如变成缺陷或源代码所导致的滥用。在这种情况下，即使完成代币的销售，公司及其附属公司也可能无法接收所筹集的加密货币，并且公司及附属联公司可能无法将筹集的资金用于平台的开发，平台的上线可能会暂时或永久性地受到限制。因此，发行的代币可能不具备价值。除非您专门购买了私人保险为其投保，代币不配备保险。如果代币有任何损失或价值损失，您可能无权追索。

(c) **区块链地址可能受到损害，并且可能无法回收数字资产。**

区块链地址本身应具有安全性。然而如果出于任何原因用于接收购买数量或其他方式的区块链地址受到损害（包括但不限于丢失该区块链地址的密钥的情况），该区块链上持有的资金可能无法回收、分配，并且可能永久无法恢复。在这种情况下，即使成功售出代币，公司及其附属公司也将无法收取筹集的资金，公司及其附属公司将无法将此类资金用于平台的开发，并且平台的实施可能会被暂时或永久限制。因此，发放的代币可能不具有价值。

(d) **平台的成功无法保证，并且公司及其附属公司可能会停止平台的开发、启动和运行。**

I. 代币的价值和需求在很大程度上取决于平台的性能。不能保证平台在启动后会收到欢迎并取得任何商业成功。该平台尚未完全被开发、敲定和整合，在发布

之前可能会进行进一步的更改、更新和调整。此类更改可能会对其预期的用户吸引力产生意想不到的和无法预料的影响，从而影响其成功。不能保证创建代币的过程是持续不断的或没有错误的。

II. 尽管公司已尽一切努力提供了现实的预期，但也无法保证代币销售中筹集的加密货币将满足平台的开发和整合。由于前述或任何其他原因，平台的开发和整合可能无法完成，并且无法保证将启动其系统、协议或产品。 因此，发放的代币可能不具有价值。

III. 可能导致平台的开发、启动或运行终止的其他原因包括但不限于：（aa）加密货币和法定货币的价值出现不利波动，（bb）公司及其附属公司无能力建立平台或确保代币的使用，或解决与平台或代币的开发或运营的技术问题，或商业关系的破裂，（cc）开发或运营期间的知识产权纠纷以及（dd）公司或其附属公司未来的资金需求的变化，以及为这些需求提供资金的融资和资本的可用性。由于上述及其他原因，该平台可能不再是一个可行的项目，可能会被解散或未被启动，从而对该平台以及已发行的 FCT 代币和/或 FIRMA 代币的潜在效用和价值产生负面影响。

(e) **对平台和所提供服务的需求可能匮乏，并影响代币的价值。**

I. 启动平台后存在风险，消费者、商人、广告商和其他主要参与者对平台和服务缺乏兴趣，并且可能兴趣有限，因此可能导致平台和代币无法使用 。这种兴趣的缺乏可能会影响平台的运行以及代币的使用或其潜在价值。

II. 存在可能已经建立的替代平台或以满足类似要求的平台，并以服务现有业务所针对的潜在细分用户。 例如，有些公司的受众为广告公司，这些广告公司寻求购买消费者数据和市场分析。因此，如果竞争导致对平台、服务和代币无法引起兴趣和需求，则平台的运行和代币的价值可能受到负面影响。

(f) **公司及其附属公司可能会遇到系统故障、网络或服务的意外中断、硬件或软件缺陷、安全漏洞或其他可能对公司或其附属公司的基础架构网络或平台造成不利影响的原因。**

I. 公司及其关联公司无法预测或检测到何时会发生黑客攻击、网络攻击、采矿攻击（包括但不限于重复支付攻击、多数采矿权攻击和"自私挖矿"攻击） 、分布式拒绝服务、平台和代币或其他任何依赖以太坊区块链的本公司及其附属公司、平台以及代币所（包括但不限于智能合约技术）中的错误、漏洞或缺陷 。 此

类事件可能包括例如导致其被利用或滥用的编程或源代码中的缺陷。 公司及其附属公司可能无法及时发现此类问题，并且可能没有足够的资源来有效地应对同时发生或迅速连续发生的多起服务事件。

II. 尽管公司及其附属公司将采取对于维护平台及其其他服务至关重要的措施，来抵制对其设备或基础设施的恶意攻击，但无法保证杜绝将来有可能发生的网络攻击（例如分布式拒绝服务），也不保证任何此类安全措施都将有效。任何严重违反安全措施或其他破坏措施，从而导致损害公司及其附属公司的网络或服务（包括平台）的可用性、稳定性和安全性。

与参与代币销售有关的风险

(a) **您可能无法赎回为代币支付的购买金额。**

除非有任何适用的销售条款规定或适用的法律法规规定，否则公司无义务向您退还购买金额。不承诺代币未来的任何性能或价格，不承诺固有价值或持续的付款服务，也不保证代币将具有任何特定价值。 因此，可能无法赎回购买金额，或者需要遵守适用的法律和法规。

(b) **购买、分发和使用代币可能会给您带来不利的法律和/或税收影响。**

I. 加密货币和加密资产的法律性质仍然具有不确定性。在某些司法管辖地区中，代币可能会被视为证券，或者将来可能会被视为某些司法管辖区中的证券。本公司及其附属公司不对代币的分类方式提供任何担保或保证，每个购买者将承担在各自司法管辖区将代币视为证券的所有后果，对其合法性、使用性和转让负责。

II. 此外，对购买或处置此类加密货币或加密资产的税收，可能取决于它们是否被分类为证券、资产、货币或其他形式。由于对代币征税仍处于不确定的状态，因此您必须就购买、获得或遗弃代币而咨询个人税收建议，这可能会给您带来不利的税收后果或税收报告要求。

(c) **购买者钱包相关信息的丢失或损害以及您访问平台的方法可能会对您代币的访问和拥有产生影响。**

如果您丢失平台上创建的唯一个人 ID 和其他标识信息、与购买者钱包或存储该钱包的金库相关的必需私钥，您可能会永久失去对代币的访问和拥有权、保管、托管或引起购买错误。

(d) 由于**区块链存在可能的拥塞，交易可能会延迟或丢失。**

大多数用于加密货币交易的区块链（例如以太坊）容易出现周期性拥塞，在此期间交易可能会被延迟或丢失。个人也可能意图向网络发送垃圾邮件，以期获得购买加密代币的优势。这可能会导致此类情况：进行交易时，区块生产者可能排除您对代币的购买，或者完全排除您的交易。

隐私和数据保留问题。

作为代币销售、验证过程以及平台后续运行的一部分，公司可能会收集您个人信息。个人信息的收集、使用和披露受适用法律和法规以及公司提供的隐私政策的约束，收集到的所有信息将用于代币销售和平台运营，因此，有可能将其转移给公司指定的全球承包商、服务提供商和顾问。除外部妥协外，公司及其任命的实体还可能遭受内部安全漏洞的侵害，从而导致其员工可能挪用、误放或丢失购买者的个人信息。公司可能有必要投入大量财务资源，以减轻因任何违规或损失造成的问题，结清罚款并解决监管部门或政府部门的询问。任何信息泄露或丢失也将损害公司的声誉，从而损害其长期前景。

宏观风险

(a) 全球总体市场和经济状况可能会对公司及其附属公司的运营以及平台的使用产生不利影响。

I. 公司及其附属公司可能会受到总体全球经济和市场状况的影响 出现全球性经济问题时，有可能导致或持续导致整个信息技术产业的放缓。经济疲软可能会对公司及其附属公司的业务战略、经营成果和前景产生负面影响。

II. 平台所依靠的服务器、带宽、位置和其他服务供应商也可能受到经济状况的不利影响，进而可能对公司及其附属公司的运营或支出产生负面影响。

III. 无法保证当前的经济状况极其恶化、长期或反复出现的衰退是否会对公司及其附属公司的业务战略、经营成果和前景以及平台产生重大不利影响。这反过来可能会影响令牌的价值。

(b) **区块链技术、加密货币、代币、代币提供和平台的监管制度仍然不确定，任何变化、法规或政策都可能对平台的开发和代币的使用产生重大不利影响**

I. 代币、代币买卖、加密货币、区块链技术以及加密货币交易所的监管目前处于未能发展或发展之后的状态，很有可能出现迅速的进展。此类法规在不同辖区之间也存在很大差异，因此具有很大的不确定性。不同司法管辖区的各种立法和行政机构可能会在未来采取法律、法规、指南或其他行动，可能会严重影响公司平台的发展和增长、代币的采用和使用或发行、买卖。公司及其附属公司或平台用户未遵守任何法律、法规和规章（其中某些法律、法规和规章可能尚不存在或可能因解释而发生改变）可能导致各种不良后果，包括民事处罚和罚款。

II. 在许多外国司法管辖区中，区块链网络也面临不确定的监管环境。各个司法管辖区可能会在不久的将来颁布影响平台的法律、法规或指令，从而影响代币的价值。此类法律、法规或指令可能给本公司或其附属公司的运营直接带来负面的影响。未来任何法规变更所带来的影响都无法预测，这类变更可能十分重大，并可能严重不利于平台的发展和增长以及代币的应用和使用。

III. 公司及其附属公司可能需要获得许可、许可和/或批准（统称为"监管批准"）的前提下开展其业务，包括创建代币以及开发和运营的业务。然而公司可能无法获得此类监管批准，或者如果相关主管部门出于任何原因未更新或撤销此类监管批准，则可能会对公司及其附属公司的业务造成不利影响。

IV. 无法保证未来有关当局不会对本公司及其附属公司施加更严格的要求，也不保证本公司及其附属公司将能够及时适应不断变化的监管要求。这些其他或更严格的规定可能会限制公司及其附属公司开展业务的能力，并且如果公司及其关联公司不遵守任何此类要求，则可能会面临违规行为。

V. 此外，如果因遵守此类新实施法规而导致成本（财务或其他方面）超过某个范围，或不在维持其商业性、或不再获取管辖范围内对运营的监管批准，并且公司及其附属公司可能会选择终止平台和/或代币。此外，很难预测政府或监管机构如何或是否会修改影响对分布式账本技术及其应用（包括平台和令牌）的法律法规。在诸如上述的场景中，分布式代币可能仅具有很少或没有任何价值。

(c) **可能存在不可抗拒力、自然灾害、战争、恐怖袭击、暴动、民众骚乱、广泛传播的传染病以及公司及其附属公司无法控制的其他事件有关的风险。**

公司及其附属公司可能会由于不可抗拒力、自然灾害、战争、恐怖袭击、暴动、民变、广泛传播的传染病以及不无法控制的事件而暂停或延迟公司代币的的销售和平台的活动。此类事件也可能导致全球市场的经济前景不确定，并且无法保证此类市场不会受到影响，或者无法保证从全球金融危机中复苏。在这种情况下，公司及其附属公司的业务战略，运营结果和前景可能会受到重大不利影响，并且对

代币和平台的需求和使用可能会受到重大影响。此外，如果将来在公司及其附属联公司和平台参与者运营的任何国家/地区爆发此类传染病或传染病，则市场情绪可能受到不利影响，可能对平台及其社区产生负面影响。

(d) **包括代币在内的区块链和加密货币是相对较新的动态技术。除了此处重点说明的风险外，您购买、持有和使用代币还存在其他包括我们无法预料的风险。这样的风险可能会进一步变为本文讨论的风险的意外或结合的以外。**

1.6 无进一步的信息或更新

本白皮书中未包含的任何有关代币、平台、公司或其附属公司业务和运营信息或陈述未曾告知或授权给任何人士。若授权，则不得被视为代表本公司或其附属公司的授权。

1.7 语言

本白皮书可能会翻译成其他语言。如果由于不同的语言的翻译而引起分歧，以英文版本为准。

1.8 建议

本白皮书中的任何信息均不应被视为有关代币、平台、公司或其附属公司的业务、法律、财务或税务建议。您应就代币、公司或其附属公司及其各自的业务和运营咨询您自己的法律、财务、税务或其他专业顾问。您应该意识到可能会在不确定的时间承担购买代币的财务风险。