



FIBON

YELLOWPAPER

MAY 2022 - 44 PAGES - 10 MONTHS

Contents

1. EXECUTIVE SUMMARY	5
2. GLOSSARY	6
3. FIBON PLATFORM	9
4. FIBON ECOSYSTEM	12
5. FIBON CAPABILITIES	13
5.1 CUSTOMER IDENTIFICATION	13
5.1.2 Address	14
5.1.3 Identification Number	15
5.2 CUSTOMER DUE DILIGENCE	15
5.3 ENHANCED CUSTOMER DUE DILIGENCE	15
5.4 RISK SCORING	16
5.5 USE CASE: FIBON ONBOARDING	17
5.5.1 INSTALLATION	17
5.5.2 CREDENTIAL REGISTRATION	18
5.5.3 CREDENTIAL PRESENTATION	18
5.6 USE CASE: PROOF OF VIRTUAL ASSET OWNERSHIP	19
5.7 USE CASE: CHAIN SCORING	19
6. FIBON TOKEN	20
6.1 TOKEN PROPERTIES	21
6.2 CROWDSALE MECHANICS	22
6.3 BUDGET ALLOCATION	22
7. THE ROAD AHEAD	24
7.1 ROADMAP DRAFT	24
7.2 COMPETITION	24
8. FIBON ARCHITECTURE	26
8.1 BLOCKCHAIN TECHNOLOGY	26
8.1.1 SMART CONTRACT	26

8.1.2 CONSENSUS MECHANISM	27
8.1.3 BINANCE SMART CHAIN	28
8.2 MULTI-SOURCE IDENTIFICATION PROTOCOLS	29
8.2.1 PHYSICAL CREDENTIALS	29
8.2.2 VERIFIABLE CREDENTIALS	30
8.2.3 CORE PROTOCOLS	32
8.2.4 MULTI-SOURCE AUTHENTICATION PROTOCOLS	32
8.2.5 USER AUTHORIZATION PROTOCOL	33
8.2.6 DISTRIBUTED DATA EXCHANGE PROTOCOL	34
8.2.7 CRYPTOGRAPHY AND SECURITY MODULES	37
8.2.8 SECURE MULTIPARTY COMPUTATION	38
8.2.9 FULLY HOMOMORPHIC ENCRYPTION	38
8.2.10 ZERO-KNOWLEDGE PROOFS	40
9. THE TEAM	40

1 EXECUTIVE SUMMARY

The rapid growth of the financial industry led to an increased demand for regulations, especially while performing risk assessments and fighting financial crimes. Mandatory customer due diligence (CDD), know your customer (KYC), risk assessment and anti-money laundering (AML) processes are becoming more complex and intertwined between financial technology partners (FinTechs) and regulatory technology partners (RegTechs).

Conducting KYC/AML operations is time-consuming and costly. Furthermore, these procedures do not support user control over their private data, and lack of interchangeability results in pursuing redundant KYC/AML checks.

Fibon is a dedicated multi-layer blockchain-based platform that enables end-users, financial institutions, FinTechs, RegTechs, and also centralized/decentralized cryptocurrency exchange platforms to pursue KYC, CDD, and AML procedures in a timely and cost-effective manner.

Fibon platform provides standardized, transparent, and privacy-enhanced KYC/AML checks while conforming to European Unions' directives such as AMLD 5 and AMLD 6. Also, through the integration of self-sovereign identity technologies into the platform, Fibon lets users manage their data, monitor processes, and regulate who has access to their data.

The entities in the Fibon ecosystem will be able to share sensitive KYC/AML information securely by their role as integrators between multiple blockchains and identity providers. This naturally leads to performing KYC/AML processes without redundancy.

In order to properly maintain the dynamics of the ecosystem and fulfill business, FIBON utilizes Fibon currency. Fibon cryptocurrency will be used for conducting payments between service providers and consumers.

2 GLOSSARY

Anti-Money Laundering (AML)

Anti-money laundering policies cover the necessary processes for supporting to preventing money laundering and terrorist financing.

Credential

A credential is a set of one or more claims made by the same entity. Credentials might also include an identifier and metadata to describe properties of the credential, such as the issuer, the expiry date and time, a representative image, etc. to use for verification purposes, the revocation mechanism, and so on. Credentials may be issued both in physical and/or digital form.

Customer Due Diligence (CDD)

Customer due diligence (CDD) is the process of evaluating your customers' backgrounds to determine their identity and the level of risk they carry. .

Customer Identification Phase (CIP)

Customer identification phase is the first step that involves collecting and verifying an entity's credentials provided within both AML and KYC procedures.

Enhanced Customer Due Diligence (EDD)

Certain customers, such as politically exposed persons (PEPs), pose a much higher money laundering risk and so require enhanced CDD measures such as obtaining additional customer identification materials, establishing the source of funds or wealth, closer scrutiny of the nature of the business relationship or purpose of a transaction, implementing ongoing monitoring procedures.

FIBON Token

A blockchain-based token that can be used as a general means of payment within the Fibon ecosystem.

Homomorphic Encryption

Homomorphic encryption refers to a class of encryption methods that Rivest, Adleman, and Dertouzos considered as early as 1978 and that Craig Gentry first built in 2009 and that can be performed directly on encrypted data without access to a secret key. The result of this calculation remains in encrypted form and can be revealed by the owner of the secret key at a later time.

Initial Coin Offering (ICO)

ICO is a type of crowdfunding, or crowdsale, using cryptocurrencies as a means of raising capital for early-stage companies.

Know Your Customer (KYC)

Know your customer check refers to verifying the credentials (physical or digital) presented by an entity are legitimate and evaluating the risks of doing business.

Smart contract

Smart contracts are computer programs that are hosted and run on a blockchain network. Each smart contract is made up of code that specifies predetermined conditions that, when met, produce results. By running on a decentralized blockchain rather than a central server, smart contracts allow multiple parties to reach a common result in an accurate, timely, and tamper-proof manner.

Secure Multi-Party Computation (SMPC)

Secure Multiparty Computing (MPC or SMPC) is a cryptographic protocol that distributes a calculation process among several parties, each participant achieving the result and at the same time keeping their inputs

secret.

Selective Disclosure

Selective disclosure is the ability of a verifiable credential owner to select a subset of the claims from the verifiable credential to share with a verifier, without revealing the rest.

Verifiable Credential

A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as cryptographically secure digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.

Zero-Knowledge Proof (ZKP)

A zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without providing any information apart from the fact that the statement is indeed true. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

3 FIBON PLATFORM

The financial industry aims to fix excessive operating costs and poor customer experiences at KYC, due to the difficulty of accessing accurate data and keeping up with increasingly stringent regulations and complex, inefficient processes. Allowing an improved, safer, more transparent, and faster process to implement regulatory compliance procedures such as KYC/AML, due diligence, and risk assessment would open up new opportunities for companies that operate with virtual currencies, financial institutions, banks, intelligence companies business and new ones. Markets are the working market participants, new ICOs, and end-users.

Fibon is a multi-tier blockchain-based distributed platform that enables end-users, FinTech and RegTech partners, and government agencies to track CDD, KYC, and AML processes in a standardized, transparent, and privacy-friendly way. Of course, Fibon supports all forms of identities and credentials, including physical, unreadable, physical machine-readable, and digital. In addition, Fibon implements the standards of the European Union's 5th and 6th AML guidelines (AMLD5 and AMLD6).

Fibon strives to be the most secure and transparent KYC/AML platform with the lowest transaction fees. With Fibon, KYC processes become safer, faster, and cheaper thanks to its KYC/AML toolkit. Fibon has different goals for different participants;

- Provide simple, secure, and robust KYC/AML services for individuals;
- Support FinTechs and RegTechs with customer onboarding, KYC, and AML procedures;
- Ensure compliance with centralized and decentralized crypto exchange platforms to implement;

In a nutshell, Fibon provides the following benefits.

- FinTechs can get rid of excessive fees most of the time by sharing individual verification information with each other without compromising privacy and regulations.
- RegTech companies that have a variety of knowledge about KYC/AML processes can access demanding customers in a platform that allows them to earn FIBON tokens.
- End users will earn tokens for their participation in the Fibon platform. This scenario allows users to control who accesses their data under what conditions. Moreover, they can verify them to demanding entities without having the burden of rerunning the process.

Fibon removes the biggest challenge of KYC, manually sorting unstructured data, which results in a time-saving and much less error-prone process. Using Fibon's KYC tools removes the need for internal resources that are dedicated to manual KYC checks or identity verification.

Fibon will also take place in the ecosystem and offer KYC/AML, risk scoring, personal background checks, notary services, web monitoring, peer-to-peer identity services, and blockchain screening solutions. This enables effective credential verification by taking advantage of AI-driven liveness detection, facial recognition, and automated data extraction from government-issued identity documents. More concretely, Fibon has various benefits for each of its partakers:

1. **Individual Users.** Fibon aspires to be the most secure and transparent KYC/AML platform. Fibon will be available to users via Fibon's website or mobile applications, and they will be awarded FIBON tokens for providing personal information.

2. **FinTechs and RegTechs.** With its use cases specifically tailored for banks, corporations, and transfer companies, Fibon offers KYC/AML services that are safer, faster, and less expensive. Fibon assists FinTechs in performing customer onboarding while adhering to regulations.

3. **Cryptocurrency Exchange Platforms.** Cryptocurrency exchanges, like other financial institutions, implement KYC/AML procedures and controls. Countries and regulatory bodies began to take action to protect the cryptocurrency market. As a result, cryptocurrency exchange regulations are becoming stricter. Fibon's goal is to ease the burden on the cryptocurrency exchange platforms while interacting with the RegTechs and regulatory authorities.

4. **Cryptocurrency Projects.** The cryptocurrency industry places a premium on business reputation. It is critical to understand the risk of the companies with which you have a relationship. They can easily understand vendor and third-party risk, as well as the source of wealth, using Fibon's enhanced data to prevent money laundering. With Fibon, cryptocurrency projects can automate their anti-money laundering (AML) processes. They can also integrate their core system and reduce manual labor.

4. FIBON ECOSYSTEM

Fibon is a public, multi-layer blockchain-based platform with smart contract capability and has its own token called FIBON. Fibon enables customer due diligence, know your customer, anti-money-laundering, and many other processes to be operated in a standardized, transparent, and privacy-enhanced way.

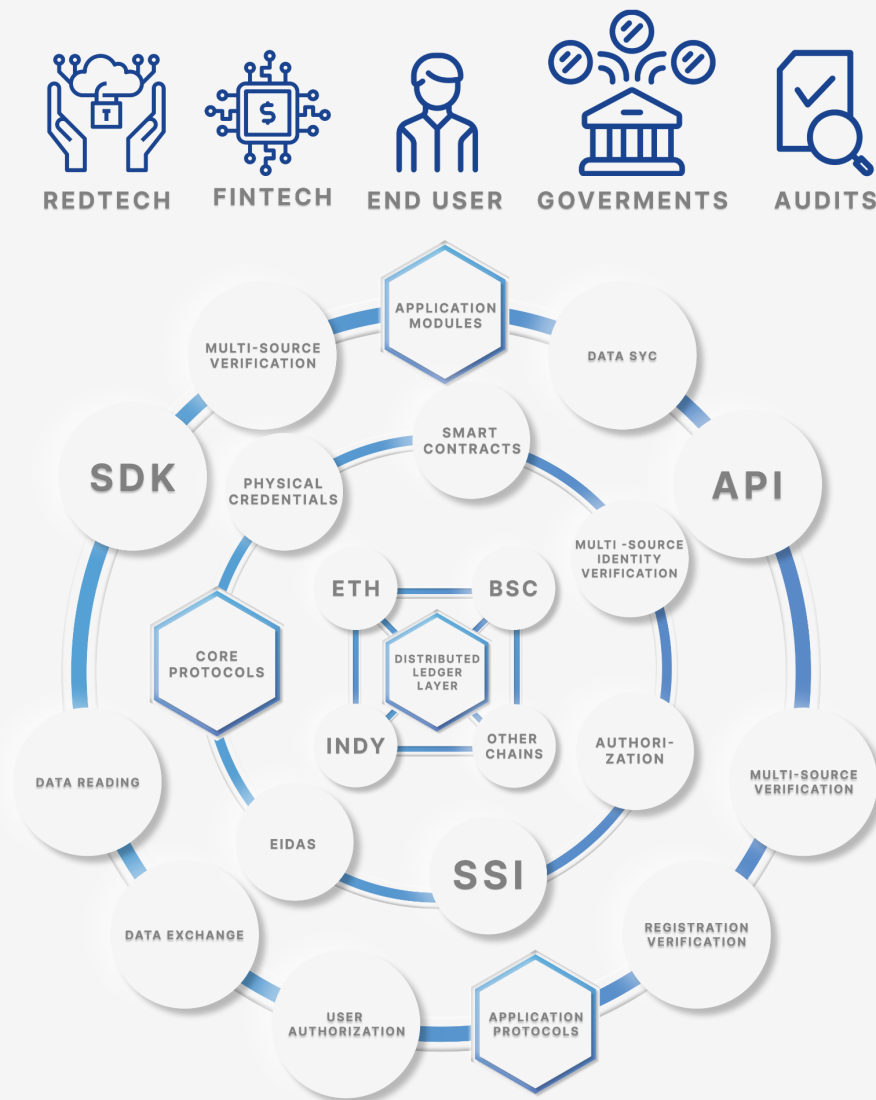


FIGURE 1: FIBON TOPOLOGY

In order to incentivize participating nodes and end-users, and enable RegTechs offering KYC/AML services to get paid for their work, the FIBON token will be utilized. In this way, Fibon nodes are paid via transaction fees for keeping the Fibon ecosystem up and running, financial institutions will send FIBON tokens to the smart contract as a payment for the services that are offered by the RegTechs, and end-users who share their information required for KYC/AML processes beforehand will be rewarded by FIBON Tokens.

Fibon ecosystem components can be seen in Figure 1. A brief explanation of the components is described below:

- RegTech Partners offer their services (KYC/AML checks, risk assessment, scoring, etc.) via smart contracts.
- FinTech Partners interact with the smart contracts of RegTechs to use their services.
- Decentralized Identifiers (DID) and related DID-based protocols as a service help to manage and verify identity information offered by SSI service providers.
- Fibon blockchain is the fundamental platform hosting the smart contracts that enable various services, in addition to the transactions.
- Blockchain Application Programming Interfaces (APIs) enable analyzing various other blockchains both as a whole and/or identity/address-based and create input for Fibon KYC/AML Services.
- Fibon End Users can interact with the system through Fibon mobile application so that they get to manage their documents, credentials, and FIBON tokens.

5. FIBON CAPABILITIES

In general, an AML and KYC process can be illustrated as given in Figure 2.

5.1 CUSTOMER IDENTIFICATION

The Customer Identification Program (CIP) is the initial stage of the AML review process, and it entails gathering and validating the new customer's information as well as the forms of evidence of identification that they supplied along with the KYC form.

confirmed. If the individual does not have a physical address, he or she can offer any of the following:

- Army Post Office box (APO);
- Fleet Post Office box (FPO);
- Residential or business street address next to him.

5.1.3 Identification Number

- This is usually the social security number, the Taxpayer Identification Number (“TIN”), or the Individual Taxpayer Identification Number (“ITIN”) for a person in the United States.
- For non-US citizens, this will be a passport number and country of issuance, an Immigrant Identification Card number, or a number and country of issuance of any other government-issued document demonstrating nationality or residency and carrying an image.

If the customer is a non-individual (“business entity”):

- For a legal entity in the United States, this is generally an Employer Identification Number (“EIN”) obtained from a legal registration document.
- If foreign corporations do not have an identity number, an alternative government-issued document proving the existence of the business or validation through a government-sponsored source or other reputable sources must be acquired.

5.2 CUSTOMER DUE DILIGENCE

CDD is the process of gathering relevant information about a client’s profile and evaluating it for potential money laundering or terrorist financing concerns. Following completion of CDD, the client may be assigned a risk score based on the risk he or she may bring to the firm. Risk ratings can take the form of classification, such as “low risk” or “high risk,” or a quantitative number generated from a risk matrix based on a set of criteria. A risk rating assists a firm in determining how and when to apply suitable checks, treatments, and controls based on the amount of risk. This concept, also known as the risk-based approach, enables a firm to allocate resources more effectively to areas that demand greater attention.

5.3 ENHANCED CUSTOMER DUE DILIGENCE

ECDD is a scenario in which the client has been determined to pose a high risk to the firm. The basic procedure of carrying out ECDD is to get senior management approval

before entering into a connection and to take reasonable steps to identify the source of wealth and the source of money. Customers/transactions with a greater risk include, but are not limited to

- Politically Exposed Person (PEP);
- Customers who are positively identified to have adverse profiles on watch lists;
- Terrorists;
- Non-face to face account opening;
- Correspondent accounts;
- Customers located in high-risk locations.

5.4 RISK SCORING

The client base and business relationships should be evaluated in order to determine the inherent money laundering risk of a business division, unit, or business line. A variety of customer kinds, industries, activities, professions, and enterprises, as well as other characteristics such as client relationship length, can raise or decrease money laundering risks. Customer type, ownership, industry, activity, profession, and/or business may all be utilized to stratify the client base and identify characteristics of client risk.

Depending on the division, unit, or business line under consideration, some or all of these criteria may be applicable. Each client type is given a risk score based on the amount of ML risk it is predicted to carry. The volume of clients that fall under each client type should then be determined/estimated for the business division, unit, or business line in the issue. This information can be used to determine what portion (%) of each business unit, department, or business line's client types are rated according to the risk classification, e.g. low risk versus moderate risk versus high risk versus higher risk, in order to determine the overall inherent client risk.

The risk-categorization strategy used by a financial institution should be properly defined. A table of inherent risk score examples for different client types and inherent risk ratings are in Table 1 and Figure 3, [5].

5.5 USE CASE: FIBON ONBOARDING

5.5.1 INSTALLATION

User installs FIBON Wallet, generates ed25519 private-public key-pair and an address

FIGURE 3: CLIENT RISK RATING

Client 1 - Persons	Rating
<u>Individuals</u>	
- HNV	High
- Retail	Low
- Other	Moderate
<u>Entities</u>	
Publicly Held Companies	
- Recognized Stock Exchange	Low
- Not Recognized Stock Exchange	Moderate
Privately Held Companies	
- Operating Company	Low
- Non-Operating Company	Moderate
- Bearer Share Company	High
<u>Government Entities</u>	
- Domestic	Low
- Medium Risk Country	Moderate
- High-Risk Country	High
- Higher Risk Country	Higher
<u>Financial Institutions/Banks and regulated Brokers</u>	
- Recognized Stock exchange and Compliant Country	Low
- Partially Compliant and not Compliant Country	Moderate
- Not Recognized Stock exchange and not Compliant Country	High/Higher

* Note: a four-point rating scale is used within the above example and can differ depending on the rating scale chosen.

TABLE 1: STANDARD INHERENT RISK RATING

FI Type/Business Unit/Business Line	Inherent ML Risk Rating
Asset Management	Low to Moderate
Brokerage	Moderate to High
Commercial Banking	Moderate to High
International Correspondent Banking	High
Credit & Other Card Banking	Low to Moderate
Investment Banking	Low to Moderate
Retail Banking	Moderate to High
Wealth Management/Private Banking	Moderate to High

5.5.2 CREDENTIAL REGISTRATION

1. User and Fibon KYC Broker establish a secure channel;
2. The user presents his physical credentials and address to Fibon KYC Broker;
3. A Fibon KYC Broker operator verifies the user's physical credentials;
4. Fibon KYC Broker operator signs the hash of the user's documents, and saves Users' addresses and signed hash to KYC smart contract.

5.5.3 CREDENTIAL PRESENTATION

5. User and FinTech consumers establish a secure channel;
6. The user sends physical credentials and his address to FinTech Consumer;
7. FinTech Consumer calls the KYC smart contract with the user's address;
8. If no signed hash is returned by the smart contract, then the Credential Registration scenario is followed by User and FinTech Consumer/ Fibon KYC Broker, depending on the FinTech Consumer's choice;
9. Else, FinTech Consumer gets the signed hash, and computes the hash on the given documents, verifying the signature.

5.6 USE CASE: PROOF OF VIRTUAL ASSET OWNERSHIP

The most naive way to prove possession of a cryptocurrency address is for the owner to send a small amount of cryptocurrency to an address chosen by the auditors to demonstrate control of the assets and the respective address. While this process certainly works, it lacks a deeper understanding of how cryptocurrencies work, and furthermore, it causes unnecessary transactions and the resulting fees.

Every time someone tries to make a transaction with a cryptocurrency asset, they must present a signed transaction that proves to the network that they actually have the private key and therefore the owner of the funds that can be spent through the address. If a common wallet software is used, the exact process will remain mostly hidden from the user. In addition to signing expense transactions with the owner's private key, one can also sign any message with the private key.

The concept of ownership of cryptocurrencies can be divided into control and rights. To demonstrate control of a cryptocurrency, you can move it or sign a message (that is, demonstrate that you know the key). However, there is this fundamental risk that many people can control a cryptocurrency (for example, if two people know the private key) without the legal claims associated with this cryptocurrency. During a financial audit, you will not only need to prove to your auditor that you have a private key, but also that you are the legal owner of the assets in your custody. If a client only has a handful of addresses, the auditor can edit them manually. Since each requires some time, documentation, and reports to validate, the costs increase with the number of addresses. Interestingly, there is a standard in the world of cryptocurrencies that was created by the Bitcoin Enhancement Proposal 32, in which people who need many Bitcoin addresses can link them into a so-called hierarchically deterministic Wallet (HD Wallet).

5.7 USE CASE: CHAIN SCORING

Blockchain and its complementary technologies created many business cases that can have revolutionary impacts. However; these opportunities also made way for money launderers, illegal activities, and funding of terrorism. The decentralized architecture of blockchain enables illegal financial transactions without the knowledge of authorities and it makes it harder to track both source and destination of the transaction. These drawbacks

force national authorities to take action and detect criminal activities.

As stated in [2], Financial Action Task Force aims to determine criminal activities and identify suspicious actions related to virtual assets. These kinds of studies show how important it is to distinguish suspicious transactions from regular ones. For this purpose, Fibon has a use case dedicated to evaluating blockchains and creating analysis reports for its customers. In its role of integrating different partakers related to business into the ecosystem, Fibon also allows and welcomes third-party chain analysis and scoring platforms such as Scorechain[8] and Chainalysis[7].

In order to fulfill the requirements of authorities, Fibon ecosystem implements chain scoring functions. Fibon's risk-based approach can be summarized as below;

- **Transactions:** These cases includes indicators such as suspicious transaction volumes, immediate deposits and withdraws between trading platforms, converting assets multiple times;
- **Transaction Patterns:** Patterns like depositing large investments on trading platforms and trading total amounts in a short period of time create suspicions;
- **Anonymity:** When an individual uses any form of anonymity (such as mixing and privacy coins) these activities are detected and reported by Fibon;
- **Source of Wealth/Funds:** If a transaction came from suspicious sources such as gambling or mixing addresses, these actions are also flagged as red.

6. FIBON TOKEN

Just like many cryptocurrency projects, Fibon is designed to have an economic model designed around its use cases. As can be seen in the Fibon Capabilities section, Fibon has many use cases. Since these use cases need incentives to create and store, any partaker should be encouraged by our ecosystem in order to sustain itself. In this section, we will discuss FIBON token and its part of the Fibon ecosystem.

The maximum supply will be 5 billion tokens. The distribution of tokens can be seen in Table 2. Fibon requires tokens for both maintaining the dynamics of the system and fulfilling business needs. Our ecosystem combines multiple entities and participants that

transact in the system. As a result, many different transaction types and incentives are needed. FIBON token provides liquidity between service providers and consumers. Moreover, FIBON token creates motivation to become network nodes so that they can receive transaction fees and support the network's decentralized architecture. Transaction types and fees can be examined in our yellow paper.

TABLE 2: FIBON TOKEN DISTRIBUTION

	Number of Tokens	% out of Total Token Supply
Total FIBON Token Supply	5,882,000,000.00	100.00%
Unlocked Coins	972,410,000.00	17.00%
Locked Coins	4,909,590,000.00	83.00%

6.1 TOKEN PROPERTIES

The key properties of FIBON token can be summarized as below:

- Tokens that will be sold during Initial Coin Offering phase will be used for development and marketing purposes;
- End users will be rewarded tokens by sharing their identifiers with Fibon thus creating attraction to the ecosystem. These tokens can be used for use cases such as KYC/AML processes;
- Fintech companies need to store some amount of tokens in order to use Fibon ecosystem functions. These functions can be KYC/AML processes, end-users or business user's identification processes, risk scoring of a customer, chain analysis report for an address, for example;
- Since Fibon project builds itself on Binance Smart Chain, every transaction requires some amount of transaction fees. This feature is also needed for malicious behaviors such as denial of service attacks.

6.2 CROWDSALE MECHANICS

There will be three ICO phases in total and how many tokens will be distributed during ICO phases are given in Table 3.

TABLE 3: ICO DETAILS

ICO Phases	Number of Tokens	% out of Total Token Supply	Bonus %	Price per Token (in USD)	Cliff Period (months)	Vesting Period (months)	Date
ICO 1	58,820,000.00	1.00%	-	TBA	0	0	TBA
Bonus for ICO 1	26,420,000.00	0.45%	44.92%	-	3	12	
Total ICO 1	85,244,000.00	1.45%					
ICO Phases	Number of Tokens	% out of Total Token Supply	Bonus %	Price per Token (in USD)	Cliff Period (months)	Vesting Period (months)	Date
ICO 2	44,000,000.00	0.75%	-	TBA	0	0	TBA
Bonus for ICO 2	17,420,000.00	0.30%	39.59%	-	6	12	
Total ICO 2	61,420,000.00	1.04%					
ICO Phases	Number of Tokens	% out of Total Token Supply	Bonus %	Price per Token (in USD)	Cliff Period (months)	Vesting Period (months)	Date
ICO 3	25,176,000.00	0.43%	-	TBA	0	0	TBA
Bonus for ICO 3	11,000,000.00	0.19%	43.69%	-	12	12	
Total ICO 3	36,176,000.00	0.62%					

Total ICO coin allocation (including bonuses): 182,840,000

6.3 BUDGET ALLOCATION

The tokens that are released to the market will be utilized as explained in Table 4.

TABLE 4: BUDGET ALLOCATION

Unlocked Coins	Number of Tokens	% out of Total Token Supply	% out of Unlocked Coins	Cliff Period (months)	Vesting Period (months)
Shareholders	268,700,000.00	4.57%	27.63%	0	36
Pre-launch Sale	58,820,000.00	1.00%	6.05%	3	3
ICO 1	58,820,000.00	1.00%	6.05%	0	0
Bonus for ICO 1	26,424,000.00	0.45%	2.72%	3	12
ICO 2	44,000,000.00	0.75%	4.52%	0	0
Bonus for ICO 2	17,420,000.00	0.30%	1.79%	6	12
ICO 3	25,176,000.00	0.43%	2.59%	0	0
Bonus for ICO 3	11,000,000.00	0.19%	1.13%	12	12
Liquidity Provision and DEX	346,550,000.00	5.89%	35.64%	0	24
Marketing	44,000,000.00	0.75%	4.52%	0	36
Research & Development	50,000,000.00	0.85%	5.14%	0	6
Strategic Partnerships	21,500,000.00	0.37%	2.21%	6	24
Total	972,410,000.00	16.53%	100.00%		

Detailed description of the budget allocation:

- **ICO Phases:** ICOs eliminate a lot of paperwork and are fast and easy crowd-funding resources. With ICO's, Fibon will be able to proceed into the next phases quickly;
- **DEX and Crypto Exchange Platforms:** Accessibility of the native token is an important step. Therefore FIBON token will be released on DEX and traditional crypto exchange platforms;
- **FIBON Website Trade:** Users will be able to buy FIBON tokens easily right from Fibon's official website;

- **Early Backers:** For the investors that join the ecosystem before the ICO is conducted and the token is launched;
- **Marketing:** Tokens are reserved for sales and marketing programs. They will act as a utility token for the acquirement of services;
- **Shareholders:** These tokens will be provided to shareholders and the investors that choose to invest in Fibon project long-term;
- **Research & Development:** Token reserved for the core team and external partners that join the ecosystem and participate in the development and maintenance of FIBON;
- **Strategic Partners:** Tokens reserved for the partnering institutions that adopt FIBON and use our technological base to run their business operations and promote FIBON to a wider audience.

7. THE ROAD AHEAD

7.1 ROADMAP

The roadmap and milestones of the project can be seen in Table 5.

PHASE 1

- Fibon MVP
- Smart Contract Development on Binance Smart
- Smart Contract Security Audit
- Defining KYC / AML Structure Scope
- KYC allowlist integration research
- Multichain compatibility research
- Defining Tiers: Acquire and lock platform tokens to improve user's tier
- Defining early unlocking of tokens will be subject to early "unlock penalty" burn
- Defining distribution of token at the end of the sale

PHASE 2

- Enhancement of Phase 1 features
- Scaling of the platform enabling further growth
- Bug fixes;
- 'fibon.io' Website Launch
- Early Backers Period
- Fibon Goes Live on Binance Smart Chain

PHASE 3

- IOS/Android Mobile Application Release
- ICO 1, ICO 2, ICO 3
- Fibon Ecosystem V1 Goes Live (KYC / AML Basic V1)
- Fibon Pass V1. (IOS/Android Mobile Application)
- Fibon Bridge;
- Dapp Development
 - Wallet integration
 - Backend/smart contracts interaction
 - Multichain compatibility

PHASE 4

- Fibon Listing at Coin Markets
- Fibon Listing at Decentralized Exchanges (DEX) and Decentralized Autonomous Organizations (DAO)
- Reward System & LP Acquisition
- Beta Version of Fibon Ecosystem V2
- Fibon Ecosystem V2 Goes Live (KYC / AML Features)
- Platform Automation
- Fibon Engage-To-Earn
- Platform Automation

PHASE 5

- Fibon Chain V1
- Plug and play automated tools for projects
- Engage-to-earn - tools to track how much community members engage and contribute
- Ability to raise multiple rounds with programmable assets
- NFT & Asset holdings for high-levels - can be used for entry into projectability for Metaverse and other projects to Fibon NFT collections with raise Media, Entertainment, Sports and Esports holdings
- DAO Research and Development
- Fibon Governance
- Fibon DAO roll out

PHASE 6

- NFT Experiences & Metaverse
- Media and Entertainment
- Sports and Esports
- Real Estate and Insurance
- Small Business & Startups - Secure, fast and anonymous Accounting and Bookkeeping
- Retail Industry - Supply chain Management
- ID Centric Ownership & Copyright Verification
- Healthcare and the Life Sciences
- Defi for Institutions

7.2 COMPETITION

- **AMLT.** The Coinfirm AML/CTF Platform and its AMLT Network aim to build the global standard for AML/CTF enabling transparency for cryptocurrency and blockchain-based transactions.
- **Shyft.** Shyft Network is a public blockchain protocol designed to aggregate and embed trust and validation into data stored on public and private ecosystems, and networks with and without permissions. By facilitating bridging across datasets with silos, Shyft allows for layering of context on top of data, ultimately turning raw data into meaningful information.
- **Ontology.** Ontology Network is a blockchain/distributed ledger network which combines distributed identity verification, data exchange, data collaboration, procedure protocols, communities, attestation, and various industry-specific modules, including KYC and AML procedures.
- **Chainalysis.** bills itself as the top provider of AML/CTF software for Bitcoin, claimin Collaboration with global financial institutions and Europol. Chainalysis protects the integrity of the financial system by providing data analysis, visualization, and actionable intelligence. According to publicly accessible information, Chainalysis focuses solely on the development of data analysis tools for the Bitcoin blockchain. Chainalysis has not been found to deliver automated, structured AML/CTF risk reports.
- **Scorechain.** offers its Profile as a supplier of a Bitcoin analytics Platform, helping firms to create regulatory compliance procedures for Bitcoin operations, conduct forensic analysis, and improve consumer engagement for Bitcoin enterprises. According to publicly released materials, Scorechain solely gives simplified statistics on the risk of Bitcoin transaction counterparties.
- **Elliptic.** identifies illegal behavior on the Bitcoin blockchain and provides their services to top Bitcoin firms and law enforcement organizations. According to publicly released materials, Elliptic concentrates on fraud investigations and exclusively offers services linked to the Bitcoin blockchain. Fibon has found no evidence that Elliptic is offering simplified AML/CTF services.

8. FIBON ARCHITECTURE

8.1 BLOCKCHAIN TECHNOLOGY

8.1.1 SMART CONTRACT

Since its adoption in a blockchain, smart contract become a vital part of the technology [1]. When combined with distributed ledger concept, smart contract becomes able to solve most of the trust requiring business cases. It eliminates the need for a trusted third party, replacing it with a decentralized consensus mechanism.

Initially, Fibon ecosystem consists of three smart contracts that are needed for the ICO phases of the project.

- **Fibon Token:** This is the main contract that operates ICO processes and stores necessary data. Its methods cannot be reachable directly so it can be called from Fibon Proxy and Fibon Admin only. All ICO distributions are defined in the constructor. Some ICO distributions are frozen funds and they are stored and controlled in the 'frozenAddressList' property. It has two inherit classes such as IERC20 and IERC20Admin to supply equality with Fibon Proxy and Fibon Admin contracts.
- **Fibon Admin:** This contract will be used for administration and ICO processes. It has a similar structure to Fibon Proxy that is used for only redirection to Fibon Token contract. It contains ICO transfer operations.
- **Fibon Proxy:** Customers will contract through Fibon Proxy contract and this contract will not change in the future. Even if the main contract will change, a proxy contract will be the same so customers do not need to change anything to reach their assets. Fibon Proxy is used for only redirection to Fibon Token contract.

Fibon ecosystem will not be limited by these three contracts. In order to fulfill its requirements, many other smart contracts such as KYC/AML related use cases, risk scoring, chain scoring, etc. will be added. These contracts' detail will be given after the use cases in Section 5 is complete.

8.1.2 CONSENSUS MECHANISM

Blockchain is defined as a distributed decentralized network providing immutability, privacy, security, and transparency. Despite the fact that there is no authority to validate transactions, every transaction on the blockchain is considered secure and verified. The mechanism that makes it possible is the consensus protocol. A consensus algorithm can be thought of as a procedure that allows all participants of the network to reach a common agreement on the state of the blockchain. That is, when a new block is added to the blockchain, it is agreed upon by all the nodes in the blockchain.

Proof Of Work Proof of Work requires participants to mine a block and solve an increasingly difficult problem in order to ensure the mined block is valid. Each of the mined blocks ensures that the miner receives a certain amount of currency. The specified algorithm may be determined by the number of participants and the current difficulty level of the computational problem. The main disadvantage of Proof of Work is the waste of resources spent by miners to mine a new block of information. The expenditure is in the form of electricity spent by miners, which taxes not only the miner but also puts strain on the power network. Computing methods are used to solve a problem that could have been better used to solve many other scientific, astronomical, and medical problems. It should be noted that if the miners can secure a 51 percent or greater stake, they can easily tamper with the network, rendering them insecure.

Proof Of Stake Proof of Stake, on the other hand, works by giving the user with the most stakes the ability to exploit. The miner gains credibility and assurance that he will not tamper with the ledger by having the highest stakes. Having the most (or more than most) stake makes the miner want to maintain the ledger's credibility and thus avoid fraudulent transactions. Proof of Stake mechanisms has been shown to be ineffective for large-scale use cases because they are not scalable, making them more appropriate for a private network setup.

Delegated Proof of Stake The Delegated Proof of Stake (DPoS) mechanism is a consensus mechanism that aims to implement block-level verification. The primary distinction between the DPoS and PoS consensus mechanisms is that the block billing nodes are chosen in a different manner. Each node holding the token is a candidate node in the DPoS consensus mechanism, and each node chooses several agents by voting. The proxy

nodes generate and verify nodes in turn according to a predetermined schedule. There is no mining process that consumes power under this mechanism, which greatly reduces the number of nodes involved in block generation and verification, as well as the time required for consensus.

Conclusion Proof of work blockchain implementations have significant issues with escalating energy consumption and have been shown to be quite unsustainable. Bitcoin, in particular, is a major example, with it being noted that the total energy consumed by all miners across the Bitcoin miner community would be greater than the annual energy consumption of some developed European countries. As a result, pure proof of work systems should be avoided if at all possible. However, pure proof of stake has low and inconsistent reliability, as well as low fairness, which is major concerns. They also have significant security flaws, limiting their use to a very limited private implementation and limiting the widespread adoption of these systems. Delegated proof of stake is an extension of proof of stake that extends and secures the proof of stake. Delegated miners mine the blocks in a delegated proof of stake, and some of them must sign the created blocks to make it valid. This, to a large extent, resolves the flaws of the proof of stake mechanism. Based on our study, we have determined that the best network option for Fibon is Binance Smart Chain (BSC). It implements the most secure and effective consensus algorithm, which is delegated PoS with proof-of-authority.

8.1.3 BINANCE SMART CHAIN

Binance Smart Chain (BSC) is a blockchain network designed for the execution of smart contract-based applications. It uses the Ethereum Virtual Machine (EVM) to run Ethereum-based apps. To achieve network consensus and maintain blockchain security, BSC combines delegated PoS with proof-of-authority (PoA). PoA is well-known for its ability to block 51% of attempts and its tolerance for Byzantine attacks. As we mentioned in the previous sections, this methodology is far superior compared to normal PoW, PoS and DPoS. In this architecture, validators are elected to take turns confirming transactions on the network and are tasked with producing blocks in a PoA way, which takes their stake and reputation in the community into account. Binance Coin (BNB), BSC's native coin, is being staked to contribute to network security and vote on community governance protocols. This

consensus model also enables BSC to attain block times of roughly three seconds, putting it ahead of networks that still use complete proof-of-work (PoW) systems. It is important to note that BSC is not a layer two or off-chain scaling solution. It's a self-contained blockchain that could continue to function even if Binance went offline. Since BSC is EVM-compatible, it is interoperable with the vast universe of Ethereum tools and DApps. This is among the main reasons why Fibon is on BSC.



FIGURE 4: VALID PASSPORT



FIGURE 5: VALID ID CARD

8.2 MULTI-SOURCE IDENTIFICATION PROTOCOLS


8.2.1 PHYSICAL CREDENTIALS

A credential is a document that shows a qualification, competence, or authority granted to an individual by a third party with relevant or de facto power or presumed competence to do so. Most nations' fundamental ID systems were based on physical records such as national ID cards, birth certificates, passports, residency addresses, and even utility bills. Digital advancements have resulted in the digitalization of physical credentials, which now incorporate magstripes, barcodes, and/or chips that allow them to be utilized in a digital context. Below there are some sample physical credentials that can identify a person.

8.2.2 VERIFIABLE CREDENTIALS

Verifiable claims are used to demonstrate certain characteristics of an entity. They can be stored, transmitted, and verified by any entity as data units. A claim consists of metadata, claim content, and the issuer's signature, with the content consisting of any data.

***** SAMPLE FILE *****



CITY OF KIRKLAND UTILITY BILLING
123 5TH AVENUE
KIRKLAND, WA 98033-6121
Pay by Phone - 1-855-498-9970
To pay online: <http://kirklandwa.gov/payments>
Utility Billing Customer Service: 425-587-3150
utilitybilling@kirklandwa.gov

BILL DATE	DUE DATE
3/3/21	4/2/21

PREV. BALANCE	PMTS./CREDITS	CUR. CHARGES
272.87	-272.87	278.78

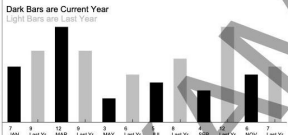
CUSTOMER	ACCOUNT NO.	TOTAL DUE
JOHN SAMPLE	999999	286.19

ADDRESS: 123 5TH AVENUE

BILLING CYCLE	SERVICE	AMOUNT
12/1/20-1/31/21	RESIDENTIAL WATER BASE	43.14
12/1/20-1/31/21	RESIDENTIAL WATER CONSUMPTION	15.51
12/1/20-1/31/21	RESIDENTIAL KING COUNTY SEWER	90.66
12/1/20-1/31/21	RESIDENTIAL SEWER CONSUMPTION	43.52
12/1/20-1/31/21	1-3S GAL CART	55.80
12/1/20-1/31/21	Effect of RES Gbg Utility Tax	5.86
12/1/20-1/31/21	Effect of RES Svr Utility Tax	14.13
12/1/20-1/31/21	Effect of RES Wtr Utility Tax	7.85
12/1/20-1/31/21	KING COUNTY HAZARDOUS WASTE RESIDENTIAL	0.88
12/1/20-1/31/21	KING COUNTY HAZARDOUS WASTE RESIDENTIAL	0.35
12/1/20-1/31/21	12/21/2020, EXTRA BAG, BOX OR CAN, EXTRA, 1 UNITS	6.71
12/1/20-1/31/21	12/21/2020, EXTRA BAG, BOX OR CAN, EXTRA, 1 UNITS	0.70
	Current Charges	278.78
	TOTAL DUE	286.19

***** SAMPLE FILE *****

Dark Bars are Current Year
Light Bars are Last Year



Meter Number	Prev Read Date	Curr Read Date	Prev Read	Curr Read	100s of Cu Ft
6548467	10/22/2020	1/8/2021	336	343	7

This bill includes garbage services provided during Dec, 2020 and Jan, 2021. You will see two different King County hazardous waste charges reflecting one month at 2020 rates and one month at 2021 rates.

ACCOUNT NO.	BILL DATE	DUE DATE
999999	3/3/21	4/2/21

"KIRKLAND CARES" DONATION

I enclose _____ with my utility payment as a donation to "Kirkland Cares". This donation will be used by Hopelink to assist our neighbors in need. (Tax Deductible)

SERVICE ADDRESS	BILL PERIOD
123 5TH AVENUE	12/1/20 - 1/31/21

KIRKLAND CARES DONATION	ENTER AMOUNT PAID	TOTAL DUE
	\$	286.19

Make checks payable to City of Kirkland.
Please include account number on your check.

***** SAMPLE FILE *****

ELECTRONIC SERVICE REQUESTED
1D00009 1 AV 0.398 AUTO SCH 5-DIGIT

JOHN SAMPLE
123 5TH AVENUE
KIRKLAND WA 98033-6121

CITY OF KIRKLAND UTILITY BILLING
123 5TH AVENUE
KIRKLAND, WA 98033-6121

FIGURE 6: VALID UTILITY BILL

A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as cryptographically secure digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.

Lifecycle

There are three types of entities associated with a verifiable claim: the issuer, the holder, and the certifier. The following five operations are included in the life cycle of a verifiable claim:

- **Issuance:** Any entity can make a verifiable claim about another entity's attribute. A university, for example, may provide a student with their transcript by issuing a

verifiable claim. When using a verifiable claim, a validity period can be specified. When the validity period expires, the claim automatically expires.

- **Storage:** Verifiable claims can be issued as public or private claims. In Fibon, public claims are stored in a distributed ledger, whereas private claims are typically stored on the entity's client and managed by the entity;
- **Presentation:** The owner of the verifiable claim can choose who sees the claim and what information is displayed without jeopardizing the claim's integrity;



FIGURE 7: FIBON VC LIFECYCLE

- **Verification** Verifiable claim verification does not need to interact with the claim issuer, only the issuer's ID should be used to obtain the public key information from the Fibon distributed ledger. You can then use the public key to verify the digital signature of the claim;
- **Cancellation:** The issuer of the demonstrable right has the option to cancel its right before it expires. The claim that has been canceled cannot be validated.

- **Anonymous Claim:**

When a claim is made, the claim owner normally exposes the entire content of the claim to the verifier. However, in some cases, the claim owner may not want to expose specific claim content to the verifier. In light of this, Fibon provides anonymous verifiable claim technology to protect its users' privacy.

Anonymous Claim technology solves the problem of concealing the holder's identity while issuing and presenting a claim. An entity receives two verifications of their claim from two different verifiers under the anonymous claim protocol.

Even if the two verifiers conspired to leak the information they possess, they would be unable to determine whether the information they received came from the same entity. When making an anonymous claim, the issuer does not need to provide the original claim to the verifier; only a zero-knowledge proof is required.

The verifier can validate the claim's authenticity by running a validation algorithm with the issuer's public key, certificate, and an assertion of the certificate's attribute values, such as "age>18" AND "resident of Istanbul." All of the attributes of the anonymous claim are included in the public information, which is divided into three parts:

- the name of the attribute,
- the type of the attribute,
- the value of the attribute.

Attributes accept a wide range of data types, including strings, integers, dates, and enumeration types. The cryptographic data primarily consists of the owner's master key and the issuer's public information digital signature.

During the presentation of the anonymous verifiable claim, the owner demonstrates to the third-party verifier that he possesses an anonymous claim from an issuer. They can selectively expose some attribute values while hiding others. Furthermore, they can show that some hidden qualities satisfy certain logical assumptions.

8.2.3 CORE PROTOCOLS

Fibon ecosystem consists of many different use cases and key elements. This section will briefly explain some of the protocols that are beneficial for the system

8.2.4 MULTI-SOURCE AUTHENTICATION PROTOCOLS

Multi-source authentication differs from traditional single-factor authentication systems. Fibon can provide entities with multi-source authentication systems that integrate external identity trust source authentication and entity endorsement in Fibon. Not only can an entity provide information about who they are, but they can also provide information about what they own, what they want, what skills they have, and other aspects of their identity in order to create a comprehensive identity portfolio. The following two methods are part of the multi-source authentication protocol:

- **External trust certification:** With a self-signed verifiable claim, Fibon binds the ID to an external trust source. Any entity can validate an entity's identity by validating the external trust source associated with the ID. The trustworthiness and acceptance of external trust bound to the ID determine the trustworthiness of an entity's authentication.
- **Authentication inside the Fibon ecosystem:** Fibon entities can also authenticate each other by issuing claims to each other.
- **External Trust Certification:** External trust certification will be using the self-introduction method:

Self-Introduction

Users bind trust using social media, e-banking, and other existing trust systems. The concept is pretty straightforward: first, the user adds a proof address from an external trust source to Fibon. The user then provides a credible declaration on the proof address in the following format:

- Claim creation and expiration time;
- Claim content: including the claim type, ID, social media type, social media username, etc;
- Signature: a public key already contained in the ID. When a third party needs to validate the user's external identity, it first reads the certification address of the user's trust source in Fibon, then goes to the address to acquire a verifiable claim, and finally verifies the verifiable claim.

8.2.5 USER AUTHORIZATION PROTOCOL

The user has complete control over their data. Any data access or transaction involving the user must be authorized. As a result, we developed a set of user authorization protocols to protect users' data privacy. The protocol performs asynchronous and verifiable authorization using verifiable claims, and it supports delegated authorization and fine-grained access control.

Roles

The following are the default roles in user authorization protocols:

- **User:** The entity that owns a resource and has the ability to grant access to it.
- **Resource Requester:** The person or entity who wishes to obtain user data or other resources.
- **Resource Provider:** The service provider who provides data or other resources to the user.
- **Authorization Server:** the server that receives and processes authorization requests, as well as provides users with delegated authorization service.

Authorization

After completing registration, the user can access the authorization server and configure the resource's access control strategies. An access authorization request is initiated by the resource requester. The requester will then receive an authorization certificate, which can be used to request data from the resource provider if the authorization condition is met.

8.2.6 DISTRIBUTED DATA EXCHANGE PROTOCOL

Data caching, data use without user authorization, and data copyright protection are some of the drawbacks of centralized data exchange. Fibon proposes a Distributed Data Exchange Protocol (DDEP) that specifies a set of protocol specifications for data transactions between entities. To protect both parties' equity in the transaction, a

middleman acting as a “guarantor” is introduced into the agreement’s transaction process to ensure the settlement process is handled securely and smoothly. The intermediary is in charge of holding the buyer’s funds and transferring them to either the seller or the buyer based on the final trading result. It is fair and secure because the middleman is responsible for the final settlement of the transaction. It operates on a distributed ledger contract with public and decentralized management features to ensure that it can play the role of intermediary effectively.

Roles

The following are the primary roles in the distributed data exchange protocol:

- **Data requester:** Data agencies/businesses/individuals interested in purchasing data.
- **Data provider:** Agencies/companies/individuals who want to sell raw and processed data. The data must comply with local government laws and regulations.
- **User-Agent:** This role is in charge of interacting with users in order to meet user authorization requirements for data transactions. User agents can be diverse (enterprise OA systems, internet platforms, or even simple SMS gateways), but they must be fully implemented as defined in the user license protocol of the application protocol framework.
- **Data owner:** The data subject, which can be institutions/businesses/individuals.

Secure Transaction

Smart contracts provide centralized third-party assurance services for trading activities, allowing for a secure and smooth transaction process that protects the equity of data requesters and providers.

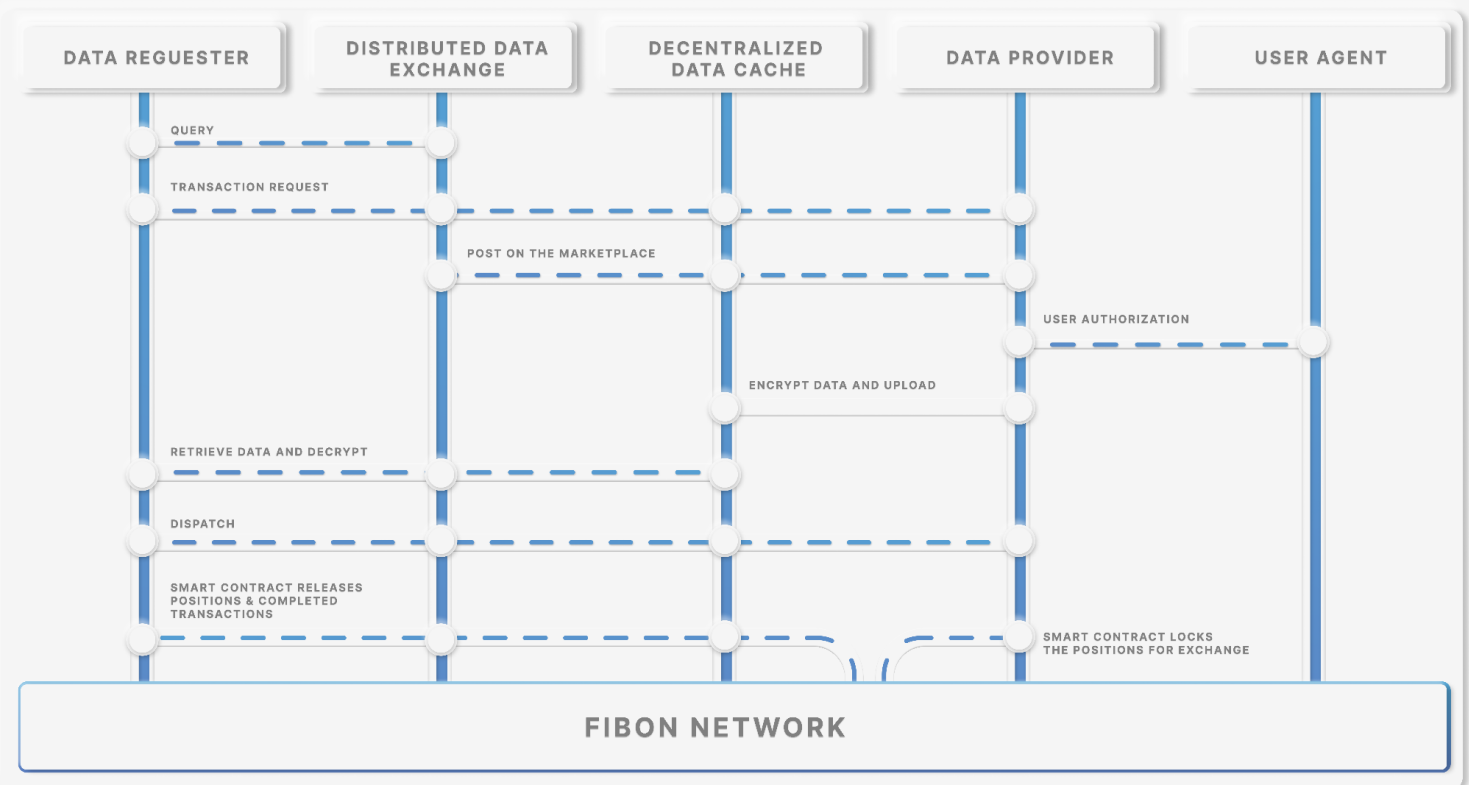


FIGURE 8: FIBON DATA EXCHANGE

The following is the process for implementing the secure smart contract transaction:

1. The data provider enters a pending order and writes the product information, which includes the resource ID, data characteristics, the provider's account, the price, and other features, and the contract waits for a requester to initiate a transaction.
2. The data requester transfers the specified amount to the contract, and the contract verifies that the amount transferred meets the sale requirements.
 - a) If it passes, the contract becomes funds-locked;
 - b) If the check fails, the transferee receives an error message and the transaction status reverts to its previous state.
3. After the data is provided by the provider, the contract confirms and specifies an expiration date. If no other action is taken before the contract's validity period expires, it automatically enters the settlement process (step 5);
4. The requester confirms the contract after receiving the data;

5. The contract transfers the funds to the provider's account and waits for the next transaction.

Data Exchange Process

1. Marketplace transaction preparation

Data provider publishes their product on the marketplace. Then, all there is left to do is wait for a data requester to find it. This can be done via browsing, searching, and filtering properties of the Fibon Network;

2. Transaction request

After locating the data they want to purchase, the requester confirms the identity of the provider using Fibon. Before initiating the transaction request, the requester deposits funds to the contract address, sends a purchase data request to the provider, and attaches the user authorization information. The request contains, but is not limited to, transaction and ID information;

3. Authorization

The data provider accesses the User Agent and initiates an authorization request after receiving the request from the requester. At this point, the User Agent can authenticate the requester's identity via Fibon on demand and perform authorization in accordance with the access control policies provided in advance by the Owner. If the Owner does not specify an access control policy, the User Agent requests authorization from the Owner. The transaction should be terminated if the authorization request is rejected;

4. Uploading data

The data provider generates a one-time session key using the symmetric-key algorithm supported by the requester, encrypts the transaction's data and data characteristic values, and sends the ciphertext to an intermediate storage system, such as IPFS;

5. Locking position

The data provider invokes the smart contract in order to verify the funds deposited by the requester. If the amount entered is correct, the position is locked until the transaction is completed or canceled. In the meantime, the provider encrypts the session key with the

requester's public key and sends it to the requester via a secure channel;

6. Receiving data

After receiving notification of the smart contract event, the requester retrieves the ciphertext from intermediate storage, decrypts it with the session key, calculates and verifies the plaintext's characteristics, and proceeds to step 6 if the verification is successful;

7. Transaction confirmation

When the data trade contract is completed, the contract funds are transferred to the account of the data provider. The mechanism for handling exceptions: The exception handling mechanism can be tailored to specific business scenarios. For example, if the data is not confirmed by the requester within the specified time frame, the provider can instruct the contract to unlock the funds, or the smart contract can unlock the funds automatically;

8.2.7 CRYPTOGRAPHY AND SECURITY MODULES

Naturally, cryptographic algorithms and protocols play a very crucial role in the Fibon platform. Apart from the basic cryptographic primitives such as hash functions and digital signatures, Fibon builds its trust and privacy enhancement models onto the following advanced cryptographic protocols.

8.2.8 SECURE MULTIPARTY COMPUTATION

Secure Multiparty Computation (MPC) protocols allow a group of entities to interact and compute a common function of their private inputs while revealing only the output and date back to 1982[9]. In conventional cryptographic tasks, the security and integrity of communication or storage are assured by cryptography and the adversary is assumed to be someone other than the participants. However, MPC protocols aim to protect the privacy of the participants from each other.

Since the late 2000s, and certainly from 2010 onwards, the domain of general-purpose protocols has shifted to increase the efficiency of the protocols to address practical applications. More and more efficient protocols have been proposed for MPC and MPC can

now be used in various real-life scenarios. It is especially realizable for problems requiring only linear sharing of the secrets and local operations with little interaction between parties, such as privacy-preserving bidding and auctions, distributed voting, private information retrieval, and sharing of signature/decryption functions.

In order to gain a better understanding, suppose that Alice, Bob, and Charlie work in the same company and want to know the highest of their salaries without revealing their salaries to each other. If there were a trusted third party, they would disclose their salaries to that party and get the highest value in return. Secure multi-party computation protocols aim to do the same but without a trusted third party. The three exchanges messages with each other, their salaries remain secret, and in the end, they only learn the maximum salary amount. The most basic properties that a multi-party computation protocol should guarantee are

- **Input privacy.** The messages that are sent during the execution of the protocols do not reveal any information about the private data of the participants other than the information that could be inferred from seeing the output of the function.
- **Correctness.** Any proper subset of colluding parties that share information or deviate from the protocol should not cause honest parties to output a false result. Correctness property can be attained in two ways. Either the honest parties detect this situation and abort the protocol, or they are guaranteed to compute the correct result.

8.2.9 FULLY HOMOMORPHIC ENCRYPTION

Homomorphic encryption is a revolutionary domain of cryptography that allows computation on encrypted data. The data remains confidential while it is processed, and decryption of the output corresponds to the result of operations as it was performed on the plaintext. In a world of distributed computing and heterogeneous networks, it is a valuable skill that data can remain confidential while in an untrusted environment.

The concept of homomorphic encryption was proposed by Rivest, Adleman and Dertouzos in 1978[6] and it gained a lot of attention due to its numerous applications in the real world. Until 2009, there were some limitations on the operations to be performed on the encrypted data. Either only addition or multiplication was allowed or the number of

operations was limited. In 2009, Gentry came up with a solution [3] that removes this constraint, and since then there has been tremendous interest in this area, regarding the improvement, implementation, and application of the scheme.

There are three types of homomorphic encryption; partially homomorphic encryption, somewhat homomorphic encryption, and fully homomorphic encryption. Partially homomorphic encryption (PHE) allows only one operation (addition or multiplication) to be performed on the ciphertext an unlimited number of times.

A somewhat homomorphic encryption scheme (SHE) supports both addition and multiplication but the number of times these operations can be applied is bounded. Fully homomorphic encryption (FHE) on the other hand, allows both addition and multiplication on the cipher text with an unlimited number of times. Although it is still in its early stages, the goal of fully homomorphic encryption is to allow anyone to perform operations on the encrypted data without access to the secret key.

Fully homomorphic encryption is useful in many areas and greatly improves privacy. It can be used for securing the data stored in the cloud, data analysis without putting data privacy at risk, and improving privacy on blockchains. With fully homomorphic encryption, the smart contracts running on the blockchain can process private data without knowing the actual data.

Users can provide encrypted entries along with a simple ZKP that shows that the ciphertexts are well-formed and certain relations regarding plaintexts hold. The nodes verify the proof and run the smart contract with the encrypted data. The user does not have to stay online during the calculation or provide complex ZKPs confirming the correctness of it.

8.2.10 ZERO KNOWLEDGE PROOFS

A zero-knowledge proof or zero-knowledge protocol is a mechanism that is used to prove that a statement is true without revealing any information other than the statement is true. There are two parties involved in the protocol. The prover is the one that creates the proof and the verifier verifies the proof. One can simply prove a statement by revealing it, however proving a statement without revealing the statement or any other information is a challenge. The concept of the zero-knowledge protocol was proposed by Goldwasser, Micali, and Rackoff [4] in the 1980s. It gained a lot of popularity in the blockchain community with zk-SNARKs and Bulletproof.

A zero-knowledge protocol must satisfy three properties:

- **Completeness.** If both parties follow the protocol, then the verifier accepts the proof.
- **Soundness.** No cheating prover can convince an honest verifier that a false statement is true except with negligible probability.
- **Zero-knowledge.** A verifier does not learn anything from the presented proof other than the fact that the statement is true.

In the blockchain, zero-knowledge proofs are particularly useful for confidential transactions, self-sovereign identity, and privacy-preserving smart contracts.

9. THE TEAM

To accomplish our mission, we formed a team of professionals who when combined with the existing work experience, have long years of managerial roles in corporate finance of multinational corporations, banking and investments on a global level, stock market trading, international business law practices, high tech business solutions, and its implementation just to name a few.

Duke A.

Equity and Investment

Director

Vladimir Prelevic

Business Development Officer

Corporate finance & business strategy

Orhan S. Dayıođlugil

Chief Operation Officer

COO, Innovative solutions Designer / Project Maker / Team Leader. Consultant for major VCs and top e-business and digital projects.

Ahmet akmak

Chief Technology Officer

CTO, Information Security and Blockchain Engineer, Applied Cryptography, and Security Protocols. Currently working on decentralized reserve currencies at an international DAO in *Silicon Valley*.

Ömer Faruk Zorlu

Fullstack Blockchain Developer/ R&D Team Leader

CPO, Participated in *NATO's Information Technology* development projects during the period between 2013 and 2016. Experienced in highly complicated full-stack development with a proven track record in designing and developing websites, blockchain programming, embedded systems, networking, and managing databases. Currently working with IBM, Redhat, and top technology brands worldwide especially based in Silicon Valley.

Nathan Boomsma

Head of Design - UX Lead

A visionary professional who is adept at combining marketing initiatives with design technologies. Performed re-design works for *Microsoft, Apple, Mercedes, and Porsche*.

Bünyamin Atik

BC Development Team Lead

Engineering graduate and Product Development manager in the High-Tech industry, Telecom, and Financial technology sector.

Cem Başgül

Marketing Director

Ex-CMO of Vesbo France, International Business Development & CCM

Zeynep Altınok

DeFi Advisor

Founder of DigiFox and the DataDash YouTube Channel with over 473.000 Subscribers, Paratica brand ambassador.

REFERENCES

- [1] Vitalik Buterin et al. "Ethereum white paper". In: *GitHub repository 1* (2013), pp. 22–23.
- [2] Financial Action Task Force. *Virtual assets red flag indicators of money laundering and terrorist financing*. 2020.
- [3] Craig Gentry. "Fully Homomorphic Encryption Using Ideal Lattices". In: *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*. STOC '09. Bethesda, MD, USA: Association for Computing Machinery, 2009, pp. 169–178. ISBN: 9781605585062. DOI: 10.1145/1536414.1536440. URL: <https://doi.org/10.1145/1536414.1536440>.
- [4] S Goldwasser, S Micali, and C Rackoff. "The Knowledge Complexity of Interactive Proof Systems". In: *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*. STOC '85. Providence, Rhode Island, USA: Association for Computing Machinery, 1985, pp. 291–304. ISBN: 0897911512. DOI: 10.1145/22145.22178. URL: <https://doi.org/10.1145/22145.22178>.
- [5] Wolfsberg Group. *The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions, and Bribery & Corruption*. 2015. URL: <https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%5C%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf> (visited on 10/18/2021).
- [6] Ronald L Rivest, Len Adleman, Michael L Dertouzos, et al. "On data banks and privacy homomorphisms". In: *Foundations of secure computation* 4.11 (1978), pp. 169–180.
- [7] *The blockchain data platform*. Sept. 2021. URL: <https://www.chainalysis.com/>.
- [8] *Trust provider for crypto markets AML compliance cryptocurrencies*. URL: <https://www.scorechain.com/>.
- [9] Andrew C. Yao. "Protocols for secure computations". In: *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*. 1982, pp. 160–164. DOI: 10.1109/SFCS.1982.38.