Whitepaper Binary

AUDIT-PROOF CHAIN

Binary Chain is the ultimate platform for ensuring security, transparency and efficiency in the cryptocurrency world. We are committed to protecting investors and DApps creators through decentralized audit processes and constant project monitoring. Binary Chain is opening the door to interoperability with the traditional financial world by implementing the ISO20022 standard. This integration simplifies the adoption of blockchain technologies for financial institutions and improves transaction efficiency.

White Paper Summary

Introduction

1. **Security, the pillars of Binary**
   - **1.1** Audit of smart contracts
   - **1.2** Detective, periodic audit of contracts
   - **1.3** Treasury
   - **1.4** ISO a secure way to interoperate between institutions

2. **Consensus mechanism**
   - **2.1** Chain DPoS
   - **2.2** Reward system
   - **2.3** Introduction Users involved in the block validation process
   - **2.4** Validators
   - **2.5** Delegators
   - **2.6** Minimum Hardware Requirements

3. **Governance**
   - **3.1** Introduction
   - **3.2** Voting Proposals
   - **3.3** Voting power, the actors involved in the decision-making process
   - **3.4** Voting process

4. **CVP contract validation protocol**
   - **4.1** Introduction
   - **4.2** Audit Community
   - **4.3** Prerequisites for submitting contract
   - **4.4** Name List
   - **4.5** Contract Submission
   - **4.6** Audit Process
   - **4.7** Deploying the contract
   - **4.8** SFC

5. **Developing on Binary, IDE**
   - **5.1** Introduction
   - **5.2** Tokens NFT
   - **5.3** Models
   - **5.4** Gears

Introduction

In the past, as was the case in the very early stages of the Internet in the early 2000s, fraudsters were widespread within blockchain systems. They exploited errors, security flaws and, most importantly, users' limited understanding of the technology. However, it is important to note that, as has happened in the past with the Internet, blockchain has also become a powerful tool for innovation and financing. For example, ICOs (Initial Coin Offerings) have proven to be an effective means of fundraising when used correctly and transparently. ICOs, despite facing a growing proliferation of fraudulent projects lacking audit and transparency, have demonstrated their potential when managed in a legitimate and compliant manner. These innovative funding tools have the power to catalyze resources for legitimate blockchain projects, allowing them to develop and thrive. However, past lack of regulation has opened the door to problematic situations, including bogus projects and scams, which have undermined trust in the cryptocurrency environment and caused significant backlash in the markets.

In recent years, however, thanks to multiple efforts by national and nonnational regulators, it has been possible to give legal form to this technology. Thanks to the contributions of various experts in the Blockchain landscape to date it is possible for an institution, government, bank and company to integrate the said technology within their business model.

In recent times, we have seen a growing explosion of interest in and adoption of Blockchain technology. Many companies, institutions, governments and public bodies such as the European Union are taking an interest in Blockchain technology to develop high-impact technology solutions for many production processes. The CDP through the PNRR has allocated a €300,000,000 fund to start-ups working in the Blockchain field, this is just one of the big investment plans at the national level. To date, blockchain technology is being used in a variety of sectors such as supply chain, gaming, finance; the one constant among all these applications is security. Binary saw the need for secure solutions within the market and took initiative to develop a technology suitable for this type of market. Although Binary offers a high degree of security one of the fundamental concepts of blockchain as well as decentralization is preserved.

Security, the pillars of Binary

1.1 Smart contract audits

Binary Chain, adopts rigorous technical verification protocols through decentralized audits, ensuring security and reliability for hosted projects. We actively collaborate with a specialized community to preserve the integrity of Smart Contracts and decentralized applications. Through this thorough approach, we ensure safe and efficient operation.
The Contract Validation Protocol (CVP) and Scam Free Contract (SFC) certificate offered by Binary are essential tools. These ensure minimal exposure to fraudulent tokens or contracts, avoiding the pitfalls of trap contracts or the like, safeguarding users from possible deception. The goal is to create a registry of distinctive names, preventing ambiguities and misleading similarities between legitimate projects and possible scams.
These approaches emphasize our commitment to a protected and trusted environment within the Chain, protecting users and helping to build a network that repels fraud and code hacks.

1.2 Detective, periodic verification of contracts

Recognizing the challenge of identifying scam projects, we are committed to ensuring thorough verification of every project hosted on our platform. We are introducing a crucial role: the Detective. Randomly assigned Detectives will review projects in the chain on a quarterly basis. Their task will be to analyze project management, budgets, collaborations and other possible sources of risk.
Once the analysis is complete, the Detectives will have to write a detailed report with evaluations and considerations of the project. If they detect a possible threat, they can temporarily block the license and submit the report to the DAO, leaving it up to the community to decide the fate of the project.
To become a Detective, applicants must stake 5,000 binary Coins and pass an audit by trusted Detectives. The Detectives will be tasked semi-annually with conducting a thorough state-of-the-art review of each DApp in the chain. This critical process involves a thorough analysis of each dApp's functionality, reliability, and adherence to security standards. Following this assessment, Detectives will be compensated based on the volume of staking assigned by the DApp in question, in line with our incentive system, which aims to ensure ongoing commitment to the security, integrity, and reliability of the ecosystem.

1.3 Treasury

It is the native contract that represents the treasury, and contains the funds that guarantee the chain its lavish funding for developments over time. These funds can only be disbursed after approval by Governance, which we will discuss later. To provide a higher level of security, the Treasury balance will be divided into two distinct categories:

1. **Liquid Funds:** These funds will be available for immediate disbursements upon approval by Governance. They represent a ready-to-use resource to address situations of need or emergency. They are a key element in ensuring flexibility and responsiveness in serving Governance.

2. **Reserve Funds:** These funds will constitute the chain reserve and will be subject to a release procedure that requires a waiting period of 10 days from the initial request. Only after completion of this release phase do the requested funds become liquid funds and can be used according to the regular procedure.

This structure is an essential pillar of security because it prevents unauthorized access or potential misuse. In the event of a Governance attack, these funds will remain protected until the unlocking process is carried out, within the next 10 days. Finally, introducing a treasury within the project proves to be a winning move from a strategic point of view because it can be used in different contexts such as developments, liquidity issues and incentives; it is like an internal insurance for the project.

1.4 ISO a secure way for institutions to interoperate

In the rapidly evolving world of blockchain technologies, the adoption of the ISO 20022 standard is an important step toward alignment with traditional financial institutions. This standard, set to become mandatory for all institutions in the traditional economy by 2025, still remains largely underutilized in the blockchain environment. Binary Chain, realizing the importance of adapting to this standard, has planned to implement the ISO 20022 format directly into its protocol. This integration will enable greater interoperability with existing financial systems, simplifying the adoption of blockchain technologies by financial institutions and improving transaction efficiency for end users. The ISO 20022 standard represents a global standard for the exchange of financial data, particularly for payment services. The main objective is to standardize and harmonize financial data flows on an international scale, providing a universal language and process model for payment and reporting communications. The goal of Binary Chain is to create a blockchain ecosystem that complies with international standards, facilitating institutional

financial transactions and promoting a secure, transparent and regulatory-compliant environment. The implementation of the ISO 20022 standard underscores Binary Chain's commitment to remain at the forefront of blockchain technologies. This initiative aims to ensure that cryptocurrencies become more accessible and secure for users and financial institutions. Binary Chain, in addition to providing treasury support for stablecoin and CBDC, plays a key role in ensuring the integrity and security of data within its ecosystem. The involvement of the audit community, which ensures data integrity and security, is an important piece in making Binary Chain a benchmark for financial institutions seeking efficiency, security and transparency in operations. Binary Chain's adoption of the ISO 20022 standard demonstrates a tangible commitment to complying with international standards, promoting transparency and security in the blockchain environment.

2. Consensus mechanism

2.1 Chain DPoS

Binary Chain is based on the Delegated Proof of Stake (DPoS) consensus mechanism, a robust decentralized infrastructure designed to facilitate the adoption of DApps by businesses. Engineered for a high number of transactions per second, this blockchain network offers minimal fees and reliability.
The DPoS system requires a minimum staking of 50k binaries dedicated to the staking process (the minimum participation rate may change over time) to participate in the block validation mechanism. The higher the staked amount, the greater the probability of being selected as a block validator, allowing you to acquire a greater quantity of fees and block rewards compared to the other validators in the chain.
The staking process involves both Validators and Delegators. The latter elect their representatives for block validation through staking and, in return, receive a portion of the block rewards allocated by their delegates.
The security and integrity of the system are preserved by the requirement of controlling 51% of the binary coins in staking to perpetrate fraud, making it economically unfeasible and costly. Any attempt at fraud would result in the confiscation of the collateral of the involved Validators, sent to the Treasury contract, thus deterring potential corruption of the system from the outset.
Participation in the staking process, either as Validators or Delegators, constitutes the DAO community, whose decision-making power is proportional to the amount of coins in staking relative to the total. In later sections of the white paper, the functions and responsibilities of the DAO will be defined in detail.

2.2 Reward system

For each transaction made on the chain by any User, whether it is moving coins from one address to another or initiating a smart contract, a fee is recognized to the validator who validates the block in which said request is fulfilled. Of these fees the validator receives 93%, while the remaining 7% is deposited in the Community Treasury.

In addition to the fees at each block, block rewards are also generated, which vary annually in the following order:

Year	Yearly Unlock	Emission	Total end of the year	Coin for block
0 (instant)	80000000			
1	10400000	13,00%	90400000	0,6595636733
2	9944000	11,00%	100344000	0,630644343
3	9030960	9,00%	109374960	0,572739726
4	8749996,8	8,00%	118124956,8	0,5549211568
5	8268746,976	7,00%	126393703,8	0,5244004932
6	7583622,227	6,00%	133977326	0,4809501666
7	8038639,56	6,00%	142015965,6	0,5098071766
8	8520957,934	6,00%	150536923,5	0,5403956072
9	7526846,175	5,00%	158063769,7	0,477349453
10	7903188,484	5,00%	165966958,2	0,5012169256
11	8298347,908	5,00%	174265306,1	0,5262777719
12	6970612,243	4,00%	181235918,3	0,4420733284
13	7249436,732	4,00%	188485355	0,4597562616
14	7539414,201	4,00%	196024769,2	0,478146512
15	7840990,77	4,00%	203865760	0,4972723725
16	6115972,8	3,00%	209981732,8	0,3878724505
17	6299451,984	3,00%	216281184,8	0,3995086241
18	6488435,544	3,00%	222769620,3	0,4114938828
19	4455392,407	2,00%	227225012,7	0,2825591328

Block rewards cease to be issued after 150 mln binaries have been issued.

Distribution of block rewards will take place according to the following formula:

$$[(BlockRewards - TreasuryFees) * 2^{-1}] * (DelegatorStake / TotalStake)$$

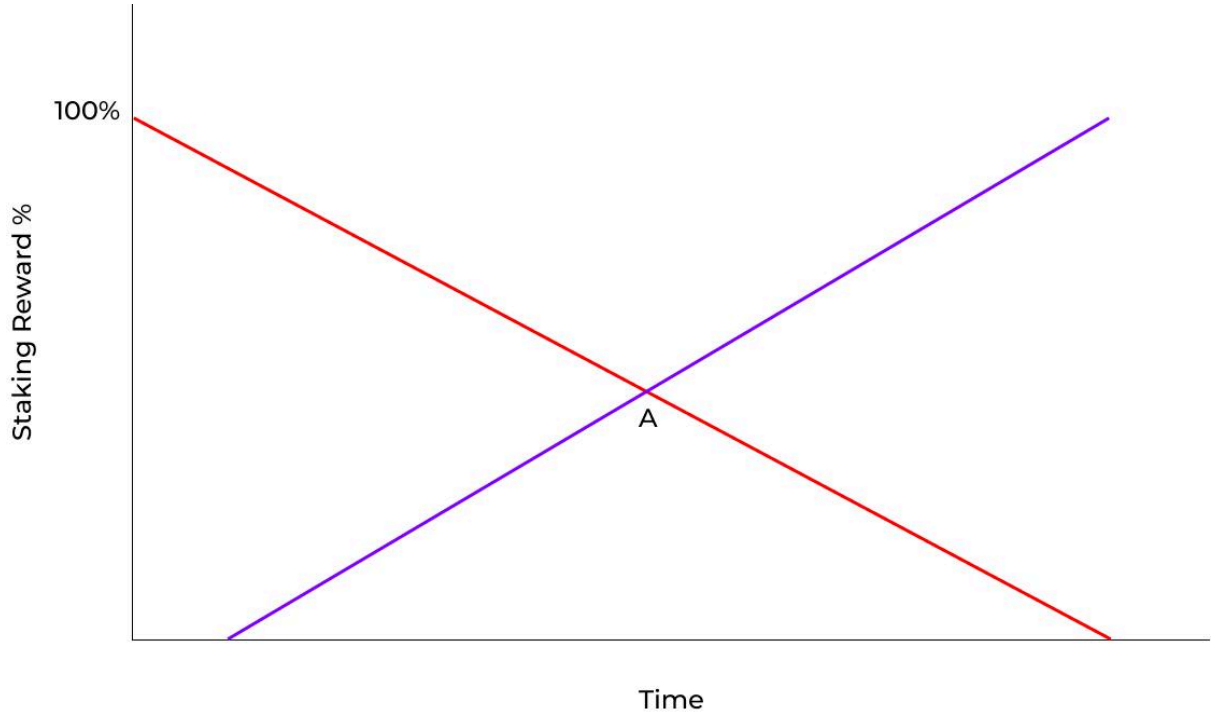
BlockRewards = block rewards collected after the block is closed by the validator
TreasuryFees = commission as a percentage is currently 7%
DelegatorStake = delegator stake
TotalStake = total delegator stake delegated to the validator

As indicated in the formula, half of the rewards go to the validator. The remaining half is divided among all its Delegates in proportion to their participation stake.

Gradually the rewards assigned to validators such as block awards will be accompanied by the fees that each activity in the chain produces, consequently, upon reaching the maximum supply of tokens, 100% of the APR will be made up of commissions.

This model is made possible by the structure of the chain which allows organic growth and is always aimed at decentralization but still limited.

Below is a graph representing the decreasing percentage of block rewards in red and the increasing percentage of commissions that will make up the final reward for staking in purple; point A represents the moment in which the percentage of commissions awarded as a reward exceeds the new token issue.



2.3 Introduction Users involved in the block validation process.

All those who own binary coins and interact with smart contracts by performing transactions or simply staking, are the Users in the chain. Users are a key element of the chain, who take different names and tasks based on the role they play within the Binary Chain, specifically this section will examine Validators and Delegators.

2.4 Validators

Validators are those who verify and approve user transactions, making them immutable within the shared registry. They are responsible for the integrity and security of the chain and for ensuring the accuracy of approved transactions.
To ensure this, Validators are incentivized by gas fees paid by users who wish to approve a transaction, the transactions in question may be of a different nature such as contract interactions or a simple exchange between users.
In addition, the chain to recognize the crucial work done by Validators gives them rewards generated by the staking mechanism that performs a dual function, creation of new coins and remuneration of the Nodes.
To become a Validator, as already mentioned in the part of the consensus mechanism, a minimum stake of 50k binary coins is required.

2.5 Delegators

Delegates are the users of the chain, who delegate their stake to one of the Validators. The Validator to whom staking is delegated by the Delegates is appointed a Delegate, who has the burden of conglomerating the total staking of the Delegates into one so as to participate in the chain validation process.
The continued staking of Delegates will strengthen the Delegate's position by increasing their ability not only to become or remain a Validator, but also to close the block more often by collecting higher fees and rewards.
Delegates receive a share of the blocks rewards generated by their Delegate in proportion to the stake made.

2.6 Minimum Hardware Requirements

To participate in the chain validation process, actors in the role of Validator, in addition to meeting the minimum participation rate must offer the network computational power and shared log storage within a node. The node setup process from a software perspective will be shown within the following documentation.
When it comes to the minimum hardware requirements they are explained by the following table:

Nome hardware	**Minimum required performance**
CPU/Processore	**4 cores**
Ram	**32GB**
SSD	**1 TB**
Internet	**25+ MBit/s in download**

3. Governance

3.1 Introduction

Binary is a public and decentralized blockchain that offers high security standards, enabling its users to deploy and interact with smart contracts in a secure and decentralized environment. Decentralization is made possible through an advanced governance system, comprised of key network actors that contribute to the blockchain's high growth potential.
Governance is the democratic process that allows stakeholders (Validators and Delegators) to make changes to the Binary protocol through voting. This decision-making model allows every user to participate in the voting process without any barriers to entry and to express their own opinions. In the current governance structure of Binary Chain, which already includes the control and administration of native contracts and the supervision of the Audit Community, we propose the addition of a decision-making mechanism for the revision and updating of the minimum staking requirements. This new element is introduced during the epoch cycles, designated periods for the discussion and voting on such proposals.
In this context, foundations and stakeholders will have the opportunity to submit proposals for modifying the staking requirements, following a transparent and democratic process. These proposals will be discussed within the DAO community, where all stakeholders can actively participate in the discussion and voting, with their vote weighted according to their staking share. The decision made through this voting process, if approved, will be implemented in the network, ensuring that the governance structure is not only robust but also adaptable to the ever-evolving

needs of the Binary Chain community. This integration emphasizes the importance of flexibility and responsibility in the decision-making process, maintaining order and coherence with the existing governance system.
Moreover, the DAO has the ability to request additional staking from developers of DApps or protocols in case of suspicious activities on the chain. This mechanism acts as a deterrent against potentially harmful actions and protects investors. In situations where a project shows irregular movements or anomalous behaviors, the governance can require the developer to increase their staking, thereby providing greater security and protection for the community and investors involved in the project. This measure strengthens the developers' responsibility and maintains the integrity of the network.
Governance can interact with many contracts and choices related to the chain that will constructively influence the foundations of the project. Binary offers a democratic infrastructure where everyone can participate and play different roles, respecting the cryptographic parameters that ensure the correct functioning of the chain. Initially, the chain will be governed by a single administrator address, but with the introduction of Governance, the power will pass into the hands of the community.

3.2 Voting Proposals

Network participants to express themselves can access a dedicated forum, which allows them to bring up considerations with respect to different topics. After an initial moment of discussion, the proposal is formalized and then moves to the voting period of the DAO community.
Proposals can be of three different types:

1. **Set Native Params** allows parameters of native contracts to be modified, such as Treasury in times of need/need from the chain for an important reason the DAO can step in and distribute a portion of the funds made available within Treasury.
2. **System Contract Deploy** provides the ability to upload a smart contract to the blockchain with specific conditions, for example, an agreement that will pay a developer to create the new Binary site. This procedure allows the contract to be proposed to be uploaded directly to the mainnet.
3. **Code Changes** consists of proposing changes in the core, formalized as descriptive text (which will then have to pass the development phase), or as an already reworked protocol to be activated by validators.

To officially submit a proposal and take it to the voting stage, staking of 500 binary coins is required. This staking acts as a safeguard against invalid or unwanted proposals, helping to prevent spam.

The user submitting the proposal has two options for initial staking. The user can commit the full amount requested, immediately starting the voting phase. Alternatively, the user can stake at least 10 percent of the requested amount, or 50 coins. In this case, the process begins with the deposit phase, which can last up to a maximum of 7 days.
If at the end of 7 days the required amount is not reached, all collected coins are sent to the common fund (Treasury), and the proposal does not enter the voting phase. However, if the required amount is reached by the deadline, the collected coins are returned to all stakeholders at the end of voting on the proposal. This mechanism helps to ensure an efficient governance process based on active community participation.

3.3 Voting power, the actors involved in the decision-making process

Each individual who participates in the staking process in order to ensure the security of the Binary Chain protocol obtains the right to vote within the community. The decision-making power of each participant is directly proportional to the percentage of coins put into staking, relative to the total assets committed by all stakeholders. In other words, the greater the amount of coins a stakeholder decides to commit, the greater the weight of his or her vote within the Binary Chain DAO community.

3.4 Voting Process

The process of voting on a proposal is done according to the following logic:

1. The 500 binary coins needed for voting to begin are collected.
2. 7 days of voting begins. All participants of the DAO community can cast their vote according to one of the following options:
    a. Yes: in favor
    b. No: against
    c. Veto: against

Veto voting represents a form of voting that can be activated in emergency situations within the DAO. In the event that the DAO community finds itself under a potential attack or significant threat, participants have the ability to use the powerful tool of Veto Voting to override the proposal that was being voted on.

For a proposal to be effectively annulled, at least 30 percent of all votes cast must be Veto votes. In the event that this percentage is not achieved, the proposal will stand, and the decision will be implemented as intended. However, in this eventuality, there

will be an important consequence: all coins that have been staked by participants who cast Veto votes will be subject to confiscation by the protocol. The confiscated coins will be transferred to the Treasury of the DAO, thus helping to ensure the continuity and stability of the community.

3. After 7 days the votes are counted, the proposal passes if all the following conditions are true:
    a. Quorum meets at least 35% of total stakeholder votes
    b. Veto votes reach less than 30% of total votes
    c. Yes votes reach a majority (50% + 1 vote).
4. Proposal:
    a. PASS. The changes are applied and the staked coins of the Veto voters are transferred to the Treasury.
    b. NOT PASSING. The proposal closes and the staked coins of the Veto voters return to the owners.

4. CVP contract validation protocol

4.1 Introduction

The chain has been constructed so that contracts cannot be deployed until they pass the control protocol called CVP (Contract Validation Protocol) as well as approval by the Audit Community. The system of control and verification of future contracts being deployed within Binary's chain offers an unprecedented security guarantee. Binary is building a secure infrastructure for developing DApps and interacting with them.
Contracts that pass all verification steps receive the green light the moment the contract receives the on-chain guarded SFC license, which confirms its integrity.
Binary's goal as a basic element of the chain is to minimize the risk of creating fraudulent contracts or those with possible bugs within the code base.
Despite high security standards guaranteed by the architecture of the system and the actors involved, all those who wish to develop on the chain can do so by meeting certain conditions.

4.2 Audit Community

The Audit Community is a group of experts in the field of DApps that is a key pillar for the proper functioning of the system, ensuring an inclusive and participatory approach

- **Seekers** can review contracts and express their views in the comments section. To become community Seekers, the stake of 100 binaries is required as anti-spam collateral. The most active Seekers will be offered to become Hunters, following the procedure described later, but skipping the evaluation step.

- **Hunters** are tasked with reviewing contracts and deciding approval or non-approval based on democratic voting. As a reward for their work, Hunters chosen according to a probabilistic model, receive a reward from the project they go to review.

  To become a Hunter as a first step requires staking 5k in binary coins. When the stalking is done, the Candidate must pass an evaluation by the community Hunters. The Candidate is paired with one of the procedures of the ongoing contract verification. Together with the other Hunters, Candidate must submit a technical report of the analyzed contract. The Hunters will evaluate the Candidate's competence based on the correctness and accuracy of the analysis indicated in the technical report. The evaluation ends with voting where the majority of votes decide the fate of the Candidate.

4.3 Prerequisites for submitting the contract

1. The Contract wishing to join the ecosystem must inherit the functions of the Binary Base Contract, which acts as a controller, enabling timely interventions in contract management in emergency situations, for example, if suspicions emerge that the project may turn out to be a scam. Binary Base Contract includes features that allow Governance to freeze the contract so as to protect investor funds tied to the project or, in extreme cases, remove it from the chain altogether.
2. File and contract names must be identical and adhere to a specific length in terms of characters. Numbers are allowed, but no special characters. However, when dealing with internal names, such as those used for token contracts, the name must exactly match the name of the contract. Also, the "name" parameter in token contracts must be set as a constant. Further details on this will be provided in the next section on "Name List."

4.4 Name List

This registry guarantees developers the exclusivity of the contract/project/token name, thus preventing registered copies from potential fraudsters. All contracts during the subscription phase until the review process, must pass automatic verification on the availability of the name.

The Dapp name is also used as the name of the contract file, which in turn must be identical to the contract name within the file, respecting these guidelines:

1. If it is a single word just use this as an example:
    a. contract Binary { }
2. If there are multiple words in the name then the words should be separated with the underscore as in the example:
    a. contract Binary_Chain { }

4.5 Sending the contract

To initialize the checking process you need to go to the Deploy for Review section and perform the following steps:

1. Connect your wallet.
2. Upload the contract with the .sol extension.
3. The system asks you to confirm the Dapp name extrapolated from the contract name.
4. You are asked to pay an amount that varies depending on the size of the contract. Each 100 bytes of the contract is equivalent to 45 binary coins. These funds will be used to pay for the work of the Hunters dedicated to the process of auditing the code proposed in the contract.
5. The contract is ready for auditing. The user can check the progress of the auditing process in the appropriate section "Contracts On Audit.

4.6 Review process

After the contract is submitted for audit, it becomes public in the contract list. The parent chain's internal selection protocol randomly selects an odd number of Hunters to perform the contract audit, based on the size of the project being audited. Hunter selection is done using the following formula:

$$HunterPos_n = HashFunc(ContractHash \,||\, Coinbase \,||\, BlockNumber \,||\, HunterAddr_n) * HunterAudits_n$$

For each participant called "Hunter," a unique value called $HunterPos_n$ is created using a hash function called $HushFunc$. This hash function requires several parameters as input:

- $ContractHash$: This is the hash of the contract that will be submitted for review.
- $Coinbase$: This corresponds to the Validator address of the current block in the blockchain.
- $BlockNumber$: This represents the number of the block within which the review request is present.
- $HunterAddr_n$: This is the address of the Hunter participant involved in the review.

After applying the hash function to these inputs, the result obtained is multiplied by $HunterAudits_n$. This value represents the amount of data or bytes that the Hunter participant has audited in the previous 30 days, that is, during a period covering 1,296,000 blocks. The final result of this operation, called $HunterPos_n$ indicates the priority of a Hunter participant in being selected to conduct the audit. This calculation is performed for each Hunter within the protocol, excluding those who are already engaged in different audits. For the selection of the Hunters who will conduct the audit, those with the lowest $HunterPos_n$, values are chosen, as it represents a higher priority. The selected Hunters are responsible for performing all necessary audits of the contract and to make their final judgment through a voting process. This approach ensures a fair and random selection of reviewers and provides an additional layer of security in the Binary Chain contract audit process. After performing a preliminary phase to identify the workforce, the mandatory 10 days begin for analysis by Hunter and Seeker, who conduct research and debate on various topics. The discussion topics are public, but can only be commented on by members of the Audit Community and the contract owner himself; all other users will only be able to interact passively with the audit process. No votes are accepted from Hunters at this stage to avoid hasty and one-sided decisions. After the first 10 days of verification have passed, the following day, the Hunters selected in the previous phase are allowed to cast their votes for or against the contract. The voting phase has a fixed duration of 1 month, to ensure a steady flow. However, in case a more comprehensive audit of the project requires additional time and a majority of the Hunters specializing in the specific audit are in favor of extending the evaluation period, it is possible to vote to extend the duration, up to a maximum of an additional month. This process allows for a more thorough and accurate analysis of the project before making a final decision. Voting results are calculated once all the Hunters

selected to audit the project have cast their votes. The contract is approved if there is a majority of votes in favor. In addition to the vote, the Hunters are required to publish a detailed report on the audit conducted, supporting their vote with a solid thesis. These audit reports will be made public and attached to the Scam Free License (SFC) certifying the Binary Chain contract. Finally to pick up on the in-depth discussion within the chapter regarding governance, it may in certain cases directly affect the fate of the contract in question.

4.7 Contract Deployment

Once the voting process ends successfully, the user who initially submitted the contract for review will see a "Deploy" button appear in the "Contract on Audit" section below the contract. This button is a key element of the process, as it allows the user to upload the contract to the blockchain. However, it is important to note that only the original user who has submitted the contract for audit can use this feature. This ensures that control of the approval process remains in the hands of the user who created the contract, increasing the security of the process. To proceed with the deployment, the user will need to click on the "Deploy" button and then confirm the action via their wallet. Once the transaction has been confirmed, the contract is uploaded to the blockchain and will receive the SFC license. This deployment process is designed to be as simple and secure as possible. The goal is to ensure that only the user who created the contract can deploy, thus preventing any abuse or manipulation. In addition, obtaining the license SFC confirms that the contract has passed a rigorous review process and meets all security and reliability requirements. This provides users with greater confidence in using contracts on our platform.

4.8 SFC

The Scam Free Contract (SFC) License is an official license issued by the chain to contracts that have passed Audit Community approval. This license is not just a simple permit, but a certificate of security and reliability that provides users with a number of crucial pieces of information. These include the address of the contract owner, the address of the contract itself, the hash of the contract, and the Audit Community approval ID, among other relevant information.

```
82
83      struct SFC {
84          bool status;
85          uint256 uuidLicenceSFC;
86          uint256 uuidAudit;
87          bytes32 contractHash;
88          string contractName;
89          address contractAddr;
90          address deployerAddr;
91          uint256 firstLicenceIssueDate;
92          uint256 expiringDate;
93          Data[] history;
94      }
95
96      struct Data {
97          address authority;
98          uint256 date;
99          Action licenceAction;
100     }
101
102     enum Action {Emitted, Expired, Extended, Paused, Retreated}
103
```

Struct SFC is the structure that contains all the information regarding the SFC license of one of the contracts:

status - indicates the validity of the license. TRUE valid, FALSE disabled.

uuidLicenceSFC - unique identifier of the SFC license.

uuidAudit - unique identifier of the Audit. Allows retrieval of all on-chain and off-chain data of the Audit. Example: who were the Hunters who audited, how they voted, their final project report, etc.

contractHash - hash of the code verified by the Hunters during audit.

contractName - name of the contract on the chain.

contractAddr - address of the contract on the chain.

deployerAddr - address of the one who was authorized to deploy after audit.

firstLicenceIssueDate - indicates the date the first license was received. It also indicates the date the contract was deployed to the chain.

expiringDate - expiration date of the license. It can be extended by staking a specified amount of binary coins, which will be used to pay the chain Detective.

history - contains the history of what had happened with the license since it was issued on the chain. This parameter is an array composed of elements called Data. Each Data must contain following three parameters:

- **Authority** - indicates who performed the action on the license
- **Date** - indicates when the action had been performed
- **Action** - indicates what had been performed.

Each SFC license is uniquely associated with the cryptographic address of its holder in the form of SBT, ensuring that only authorized addresses can interact with the associated smart contracts.

1. Secure Interaction with DApps: SFC license holders have the exclusive privilege of interacting with their Dapps on Binary Chain, ensuring intervention only by verified and trusted developers.
2. Multi-sign-like mechanism: It works like a multi-signature system for smart contracts, requiring approval of the address associated with the SFC license to perform critical actions.
3. Traceability and Accountability: Every interaction with a smart contract via the SFC license is recorded and traceable, ensuring transparency and accountability.
4. Renewal and Maintenance: Requires annual renewal with verification and maintenance of security standards, ensuring the resilience of the Binary Chain against threats and vulnerabilities.

Thanks to the license and the data it contains, those who interact with the contract and the owner themselves can carry out interactions with it without having to worry about the security of the code. This license is valid for one year. To maintain the validity of the license for another year, the project must fulfill a specific annual requirement: the staking of binary coins. These funds play a crucial role in supporting the activities of the Detective, an actor that acts as an additional layer of overall security for the protocol. The role of the Detective is crucial in maintaining the integrity of the ecosystem. These professionals conduct periodic reviews of projects, ensuring that they comply with all regulations and do not pose a threat to users. If suspicious or potentially harmful activities are found, Detectives are empowered to intervene and report the problem to Governance. Finally, the SFC license is more than just a permit. It is a symbol of security and reliability, an attestation to users that the project has been carefully examined and approved by experts in the field. With its annual validity and staking requirement, the SFC license ensures that projects continue to meet security standards over time, helping to create a safer and more reliable environment for all users in our chain.

The following metric should be used to calculate due staking:

Each category of those highlighted gives a score ranging from 1 to 6 depending on the answer given.

Volumes in $ per day: 0-500k 500k-1m 1m-5m 5m-10m 10m-15m up to 15m

Volumes in txs: 0-5k 5k-20k 20k-100k 100k-500k 500k-1m up to 1m

Community active channels: 1-3 3-5 5-7 7-9 9-11 up to 11 number

Number of smart contracts: 1-5 5-10 10-15 15-20 20-25 up to 25

Number team members: 1-3 3-6 6-10 10-14 14-20 up to 20

Market cap: 500k-1m 1m-5m 5m-10m 10m-30m 30m-50m up to 50

Number dex/cex: 1-3 4-6 6-10 11-15 16-20 up to 20

Number of detectives assigned according to score obtained

7: 3 detective

8-12: 4 detective

13-15: 5 detective

16-18: 6 detective

19-21: 7 detective

22-23: 8 detective

24-26: 9 detective

27-29: 10 detective

30: 11 detective

31: 12: detective

32: 13: detective

33: 14 detective

34: 15 detective

35: 16 detective

36: 17 detective

37: 18 detective

38: 19 detective

39: 20 detective

41: 20 detective

41: 20 detective

42: 20 detective

Example: Dapp X

Volumes in $ per day : 0-500k **500k-1m** 1m-5m 5m-10m 10m-15m up to 15m

Volumes in txs: 0-5k **5k-20k** 20k-100k 100k-500k 500k-1m up to 1m

Community active channels: 1-3 3-5 **5-7** 7-9 9-11 up to 11 number

Number of smart contracts: 1-5 **5-10** 10-15 15-20 20-25 up to 25

Number team members: 1-3 3-6 **6-10** 10-14 14-20 up to 20

Market cap: 500k-1m 1m-5m **5m-10m** 10m-30m 30m-50m up to 50

Number dex/cex: 1-3 4-6 **6-10** 11-15 16-20 up to 20

Total points: 17

Detectives needed: 6

Annual renewal cost: $9,000

Each detective receives $500 per investigation knowing that there will be three reports per year for each DApp, we have to multiply the number of detectives by the number of reports multiplied by $500 or $9,000 in this case.

5. Developing on Binary, IDE

5.1 Introduction

The IDE for Binary is designed to be a powerful and innovative development environment that greatly simplifies the Smart Contract creation process. This tool offers two modes of writing code: a traditional one and an intuitive "drag and drop" mode using plugins and add-ons.
Smart Contracts created with this IDE can run on both local and remote EVMs, allowing developers to test and submit their contracts for review to the Audit community. Once approved, these contracts can be uploaded to the blockchain.
The IDE is designed to simplify the work of developers, whether they are industry experts or beginners. To further facilitate the process, the IDE includes a dedicated marketplace for the distribution of plugins and add-ons, divided into three categories.

5.2 Token & NFT

Tokens and NFTs collect everything that can be useful in developing one's own token, starting with the basics and working up to the most complex things.

5.3 Models

Models offers several ready-to-use models. Data storage contracts, accounting, payments, lotteries, etc.

5.4 Gears

Gears is the category that contains codes that cannot be included in the previous categories. These are elements that, properly combined, will be able to become apps with unique functionality.

All plugins in the marketplace can be created by developers, who can choose to contribute to the technological growth of Binary or to monetize their work. In fact, when publishing the plugin, the developer can decide whether to distribute it for free or for a fee.
In summary, the IDE for Binary is a comprehensive development environment that offers a wide range of tools and resources to simplify and streamline the Smart Contract development process. Whether you are an expert or a beginner, the Binary IDE is designed to help you implement your projects efficiently and effectively.