5IRECHAIN. A SUSTAINABILITY-DRIVEN FIFTH-GENERATION BLOCKCHAIN

Pratik Gauri[#1], Prateek Dwivedi[*2], Vilma Mattila[#3], Zakaria Salek[#4]

5ire Organization

[1]pratik@5ire.org
[2]prateek@5ire.org
[3]vilma@5ire.org
[4]zakaria@5ire.org

***Abstract*—No one can deny the benefits achieved through technological advances. However, the growth rate and momentum of the fourth industrial revolution raised questions about the directions it is leaning toward and about the lack of control over it as it is wrapped in a for-profit paradigm that only focuses on maximization and economic profit while ignoring sustainability and service of humanity.**

On the other hand, Blockchains have demonstrated an impressive ability in bringing people to consensus and unity of purpose. Nevertheless, present-day state-of-art and implementations face many challenges regarding scalability, security, speed, interoperability, future-proof, and lack of governance.

5irechain is a fifth-generation blockchain that aims to bring a paradigm shift from a for-profit to a for-benefit. 5irechain implements sustainability by design while it ensures democracy and governance, interoperability, high transactional throughput, strong security guarantees, and forkless upgradeability.

1. INTRODUCTION

Blockchains have a significant amount of utility over several fields. However, despite the technological and economic advances, blockchain ecosystems are wrapped in a for-profit paradigm where the human factor is missing. The image of the future is eclipsed with incertitudes, as this absence of the service of humanity at the base layers of blockchains leaves the logic in the code without guidance by design. This paradigm focuses on gains and maximization of profit with no sustainable futurist vision being implied. Our resources are limited. We cannot afford unwise and uncontrolled technological growth. Thus we need to bring back control and guidance over this growth towards the service of humanity.

5irechain is a fifth-generation blockchain that will bring a shift in paradigms from a for-profit to a for-benefit by embedding sustainability and social impact inside the 5irechain runtime logic and ensure that the activities which are aligned with the United Nations 17 Sustainable Development Goals either on-chain or in the real world are highly incentivized with the cutting-edge multilayered Proof-Of-5ire reward distribution engine. All of this while assuring Democracy between all the participants and Governance for the purpose of bringing union and for ensuring the longevity of the 5irechain sustainable vision.

The goal of 5irechain is to embed the for-benefit paradigm inside the runtime logic of the blockchain thus ensuring that sustainability is how the agreed-upon consensus mechanism operates. Only by having this change in the core of the blockchain, we can ensure that the upper logic and activity will follow. 5irechain is able to achieve this purpose while wrapping it in an architectural framework with strong guarantees.

- **Sustainability by design.** 5irechain's main goal is to create a user-centric sustainability-driven ecosystem and it is able to achieve this by having sustainability deep inside the 5irechain reward distribution mechanism and runtime logic. Thus making sure that sustainable participation in the network or in the real world is highly incentivized.
- **Security.** The cutting-edge technology that is used to build 5irechain plus the Nominated Proof-Of-Stake scheme allows 5irechain to have strong security guarantees that other older blockchains lack.
- **Upgradable scalability.** 5irechain is able to achieve high transactional throughput and it enables the migration of real-world use cases that need high scalability promises on-chain.
- **Governance and Democracy.** Older blockchains have no governance procedures and this has led to chain maximalism, 5irechain sophisticated and transparent governance mechanism allows everyone to democratically participate in the network and propose changes.
- **Future-proof and Forkless upgradeability.** By being a cutting-edge blockchain based on WebAssembly. 5irechain is able to upgrade its runtime logic without hard forking. These upgrades are enacted through the 5irechain governance mechanism.
- **Interoperability.** 5irechain has the ability to interoperate with a variety of blockchains. Enabling cross-blockchain transfers of any type of data through bridges.

2. Architecture

2.1. Architectural Overview

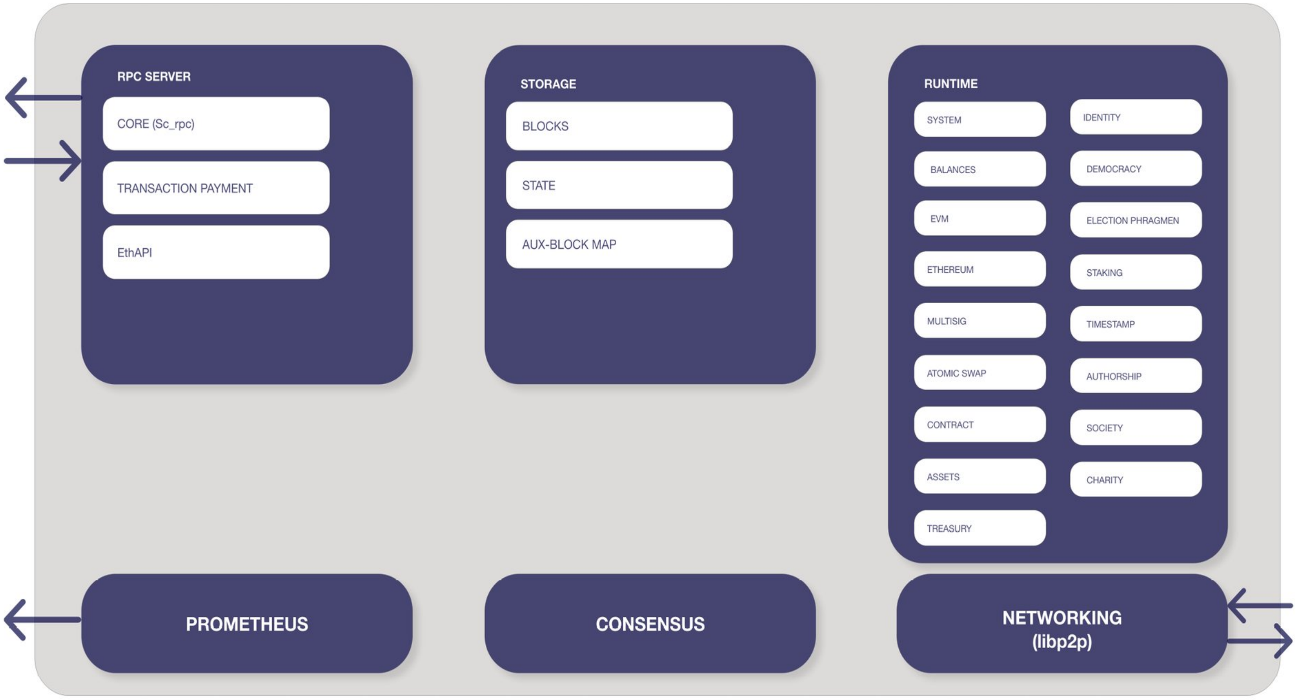

Figure 1. a high-level overview of 5irechain architecture.

2.2. Consensus

Consensus is a method of reaching agreement over a shared state. For the state of the blockchain to continue to build and move forward, all nodes in the network must agree and reach consensus. It is what permits synchronization between decentralized nodes. Moreover, we can see the importance of consensus engines as the primary media for reaching agreement over a shared state between all of the nodes, giving an objective view over the current state. Recent blockchain projects have chosen to substitute the inefficient Proof-of-Work component of Nakamoto's consensus protocol with Proof-of-stake, a scheme where the frequency of validators block production is proportional to their holdings instead of their computational powers that bring forth environmental issues plus a possibility for the construction of maximalist cartels. Proof-Of-Work with Nakamoto consensus consumes an incredible amount of energy with no provable finality and no mechanism to resist cartels constructions. Therefore PoS-based blockchains invite the formation of pools on-chain and allow stakeholders to elect validators that represent them.

2.3. Hybrid Consensus

5irechain is using what is known as hybrid consensus, combining BABE and GRANDPA for block production and provable finality respectively, allowing fast block production and higher levels of security. By our sustainable vision, the 5ire reputation mechanism allows universal and canonical guidance for the network and the real world activities, and direct those activities toward a for-benefit focused paradigm, in which appealing to the 17 United Nations Sustainable Development Goals is highly rewarding for all the actors, while maintaining speed and transaction throughput better than any standard Proof-Of-Stake scheme and high levels of security and efficiency never attained by neither PoW's nor PoS's, All of this in the most human-focused sustainable way where bringing value to existence is highly incentivized.

2.3.1 Block production

2.3.1.1 BABE

Blind Assignment for Blockchain Extension (BABE) is a slot-based block production mechanism, giving a set of active validators. *BABE* assigns slots according to the evaluation of a verifiable random function. On every slot, all authorities try to generate a random instance of the *VRF*, and based on a comparison between a threshold that is proportional to their stake and the *VRF* value generated by each authority, a producer of the current block is chosen. Moreover, in order to achieve democracy, a proof of the *VRF* execution is used by the other participants to be sure of the slot claim [14].

2.3.2 Finality

To trust public ledgers, we need to ensure that it has reached consensus on a particular block. In other words, we say that we have reached finality. First-generation blockchains do not consider finality as a priority. In such blockchains, users are not deterministically sure that their transactions are finalized. Thus we say that a Nakamoto style *eventual consensus* is only able to achieve a *probabilistic finality.* Furthermore, it would take tens of minutes.
To be able to achieve a *deterministic finality*, a finality gadget must be added to the logic of the blockchain, in which a set of voters vote on a particular block and when a threshold of ⅔ voters agreement is achieved, then a block is considered final [7].

2.3.2.1. GRANDPA. a Byzantine Finality Gadget.

GHOST-based Recursive Ancestor Deriving Prefix Agreement (GRANDPA) is the finality gadget used in our multi-layer consensus algorithm. *GRANDPA* provides block finalization by working on rounds, and each round has a set of $3f + 1$eligible voters, $2f + 1$ are assumed to be honest. Validators vote on a block they consider final once ⅔ of authorities decision is taken, they reach an agreement on the chain state rather than on blocks, thus speeding up the finalization even in the most adversarial environments or in bad networking conditions, which make it a potent base layer for building the 5ire sustainable engine [8].

2.3.3. Fork choice rule algorithm

Chain forks generally occur when multiple blocks reference the same parent block. Solving such a temporal inconsistency is a must in order to have a globally agreed-upon canonical chain. A fork choice rule is designed to select the most consistent chain. Some referenced examples of such algorithms are the longest chain rule and the *Greedy Heaviest Observed SubTree (GHOST)* rule. Combining *BABE* and *GRANDPA*, the fork choice in 5irechain is built on the chain with the most primary blocks [12].

2.4.Bridges

5irechain will make heavy use of bridges in order to communicate with other blockchains in order to ensure interoperability and openness. So with the integration of such mechanisms, 5irechain is going to be compatible with other blockchains like Ethereum or any other blockchain, specifically substrate-based blockchains. Thus opening a tremendous stream of on-chain data to be treated and this will lead to rich application logic on top of 5irechain.
The bridging methodologies that will be used with 5irechain are generally.

- **Smart contract bridges**. The compatibility with non-substrate blockchains, 5irechain will implement smart contracts bridges.
- **Substrate bridges.** The compatibility of 5irechain with substrate blockchains is seamless through the bridge pallet.

3. Actors

3.1. Nominator

Nominators are actors who provide sustainability and security to 5irechain by electing validators and by staking the 5ire tokens. Holders that cannot afford running and maintaining a node are highly motivated to become nominators and earn income by electing validators of their choice and share block production reward with them. Nevertheless, they need to choose wisely from the set of available validators as those with higher reputation are more rewarded, not those who have more at stake [13].

3.2. Validator

Validators are one of the major actors in 5irechain, as they are the ones that participate in the verification and in the production of blocks according to our consensus mechanism, and according to their activities appliance with our sustainable vision that is based on the proof of 5ire, they are highly incentivized to be for-benefit driven and to bring impact to the world.

3.3. Council

The *Council* is an on-chain entity that is an assembly of elected actors; it consists of a fixed number of actors. One of the main tasks of the council is to control the way by which the

treasury funds are spent. It also held responsibility for governance tasks such as proposing sensible referenda, canceling malicious referenda, and electing a technical committee. The proposals made by this entity require a majority voting in order for this to go into governance and become motions. The Council members have the right to exercise a *veto* [13].
The council has the right to *cancel* malicious referendums if the two-thirds majority agreed upon the danger of such a referendum execution or if it does not appeal to the global vision of 5irechain, which is sustainability and donation-oriented mindset. Additionally, the council has the right to blacklist harmful proposals. The election of the council members is held by the democratic sequential Phragmén method.

3.4. Technical committee

We choose to adopt the Polkadot vision for the main chambers of governance. The global architecture of the technical committee is composed of members that have demonstrated a good knowledge of the 5irechain workflow and runtime [13]. Also, it welcomes technical teams that are building on the same for-benefit paradigm vision as we do.
The technical committee has the ability to submit emergency proposals, such proposals are prioritized and supported by the council as they are usually based on urgent updates to the runtime and suggested bug fixes of the code.

4. PROOF OF 5IRE IN-DEPTH

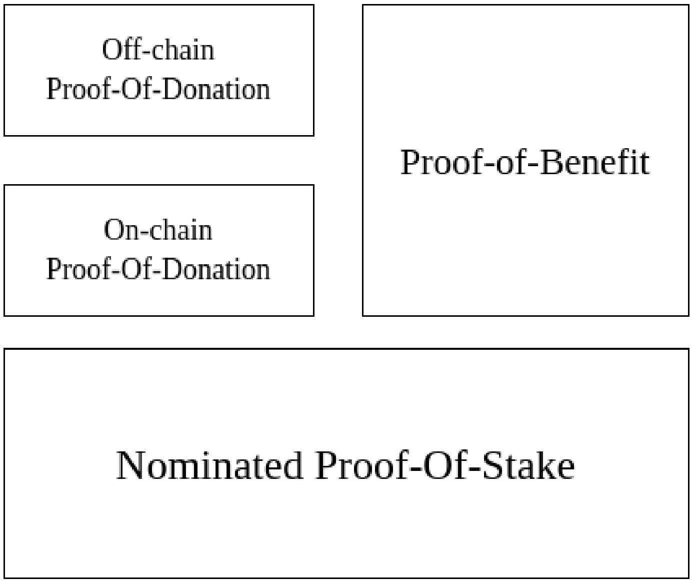

Figure 2. Proof of 5ire Components.

4.1. Nominated Proof-Of-Stake (NPoS)

Within 5irechain, we choose to adopt a cutting-edge variant of PoS called Nominated Proof-of-Stake, a powerful validators selection mechanism that includes high-security guarantees, fair representation of all the actors, scalability, and efficiency by design. A democratic approach where everyone can become a validator candidate or a nominator approving and backing validators. It is highly recommended for them to back up validators with a good reputation as they will be able to collect higher rewards, whether it is block production rewards or transaction fees. The higher reward for electing validators that their activities are applying to the 17 United Nations Sustainable Development Goals, thus bringing a paradigm shift from a for-profit to a for-benefit, and also validators that generate the most positive social impact by building a history of social and environmental driven donations gains more reputation thus more rewards. Moreover, electing validators that have a low reputation will only promise lower to negative economic returns [15].

4.1.1. Staking

The 5irechain staking mechanism is based on the Nominated Proof-of-stake (NPoS) scheme for the selection of the validator set, the next block authors, and for the distribution of rewards. Our multi-layer staking mechanism is designed with sustainability and positive environmental and social impact without forgetting the role of having a history of donation and charity on the reward distribution.

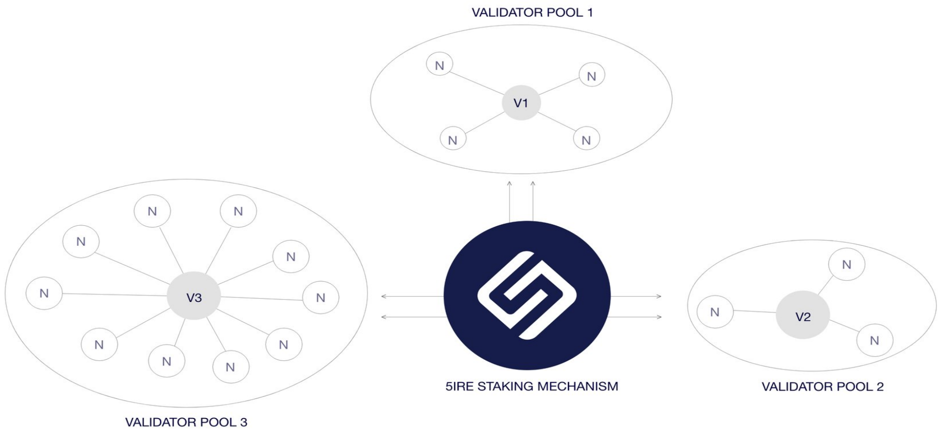

Figure 3. The 5ire Staking Mechanism

- *Base layer.* The payment system in our staking mechanism distributes validators' rewards equally regardless of the stake backing them (Validators-Nominators stake) for their participation in block authoring in the BABE block production scheme or in guaranteeing finality of transactions in the GRANDPA finality gadget. Noting that each validator is backed by a set of nominators with their stakes. Upon an *era* (which is a predefined period where NPoS base layer rewards are distributed), rewards are distributed to validators based on their collected era point which adds a probabilistic component to the reward distribution, generally, an era is 24 hours but can be modified by governance.

- *Sustainability layer.* In 5irechain the global approach is that any entity that has proven a sustainable behavior, not just on-chain, but also regarding its off-chain day-to-day activity is rewarded for taking such a for-benefit paradigm as essential to its activities. For this reason, additional rewards are distributed to validators proportional to their 5ire score calculated by registrars audits and submitted to the treasury, upon a budget period which is chosen to be seven days, the voted upon reward proposals are then distributed to the validators that achieve higher 5ire scores based on their appliance with the Proof-of-benefit (PoB) and Proof-of-Donation (PoD) of the 5ire score reward distribution mechanism.

4.2. Proof-Of-Benefit (PoB)

At the core of our revolutionary, cutting-edge staking mechanism, the democratic proof-of-benefit scheme exists as the median by which the validators are rewarded based on a score that presents a measurement of the amount of benefit such a validator generates for the planet. Our approach is a must for the world. Thus bringing value and positive impact has never been as rewarding as when on-chain and off-chain activities are done on 5irechain. The rewards are proportional to the commitment of network actors to the 17 Sustainable Development Goals (SDGs). For this reason, we choose to incentivize the validators that empower our sustainable vision highly, for example, a validator that is proven to be helping in achieving quality education or taking urgent action to combat climate change and its impacts is more rewarded than the one who does not. Thus we achieve sustainability by design.

The process by which the score of a validator is determined is based on audits made by trusted and democratically elected Reporters that perform audits on the giving active validators, this is done by submitting a proposal, and if enough votes are gained, the reward is then distributed to the concerned validator from the 5ire treasury.

For decentralization purposes, all the users not just audit reporters have the right to submit spending proposals toward beneficiaries that are proven with a for-benefit mindset. Only proposals that are in accord with the 5ire sustainable vision are accepted. And beneficiaries are not only limited to validators, everyone that brings meaningful impact not just to the 5ire ecosystem but to humanity and the world by activities conforming to the 17 Sustainable Development Goals (SDGs). Proof-Of-benefit uses the Treasury for its rewards distributions.

A second approach for rewarding actors that have sustainable best practices is through on-chain sustainability indexes that are build based on off-chain data that help

Process of reward distribution

There are three ways of submitting For-benefit spending proposals. We will go through them by ascending priority.

The first approach is by creating a proposal through the 5ire portal treasury tab, and the submission of a `proposeSpend` extrinsic and specifying the beneficiary address and the deposit of a bond which is a small percentage of the requested amount, the existence of the deposit bond, this amount is burned if the proposal is rejected, or refunded otherwise. Note that there is no possibility for proposals revocation, they are either accepted or rejected to make sure that registrars and the public alike announce proposals only when they are sure and that they will hold responsibility for this action.
After the submission process, the mechanism will automatically take the required bond deposit. Since proposals have no metadata it's up to the proposers to explain the reasons in the main 5ire community mechanism that will be chosen later. When the proposal is successfully submitted, the council members start a *motion* about it so it might be accepted or rejected, when a threshold of majority members is attained the decision is taken. The threshold is to be determined after a successful launch of 5irechain, generally three-fifths for accept motions and one-half for rejection motions.

The second approach is through a *Tipping* system. Tips can be suggested by anyone, not just audit registrars. There is no definite value for tips; their value is determined as the average median of all the tippers' suggested values. For the first implementation of 5irechain, generally, the tippers are the same as the Council members or a subset of them, but in the near future, Council members and tippers are going to be separated gradually until they become independent subsets. When more than half of the tippers endorse a tip value, the proposal enters a closing phase and the median of the ripped values are considered for payout. Tips generally contain the beneficiary address plus a *reason* argument which is generally a UTF-8 encoded URL pointing to the explanation and the audit report on the 5ire general public communication and publication of the audit report platform that would be determined later. The proposer of the tip is required as for general proposals to place a small bond deposit and he is rewarded with a finder fee which is paid out from the total amount of the tip.

The third approach and is the most convenient and prioritized Proof-Of-Benefit reward distribution mechanism through the adoption of Polkadot's *bounties* spending mechanism, Since there are limitations on the council members capabilities and expertise on judging and curating all of the proposals relative to each one of the 17 Sustainable Development Goals (SDGs) even if individual council members might have the expertise, probably the majority won't and also the council member might become overwhelmed with proposals. The process of curating and judging proposals might be delegated to *Curators.*

Curators (Audits Reporters). are experts on each one of the 17 Sustainable Development Goals (SDGs), they can be defined as addresses with control over a portion of the treasury. And their expertise makes them worthy of judging the audits submitted by registrars and users spending proposals alike on each topic or goal. When an audit registrar submits a bounty proposal, they define the Curator with enough expertise in the audit domain of expertise. When the proposal passes the Council members select the Curators, and those Curators need to make a deposit in order to take the position, this mechanism assure punishment when malicious or erroneous behavior is coming from the Curator but if they make a successful judgment, the deposit is transferred back plus a part of the audit reward. The Curator reward is included in the audit estimated payout and specified by the proposer as a Curator fee to incentivize them to take the task and invest with their energy and expertise and the judgment of the audit [13].

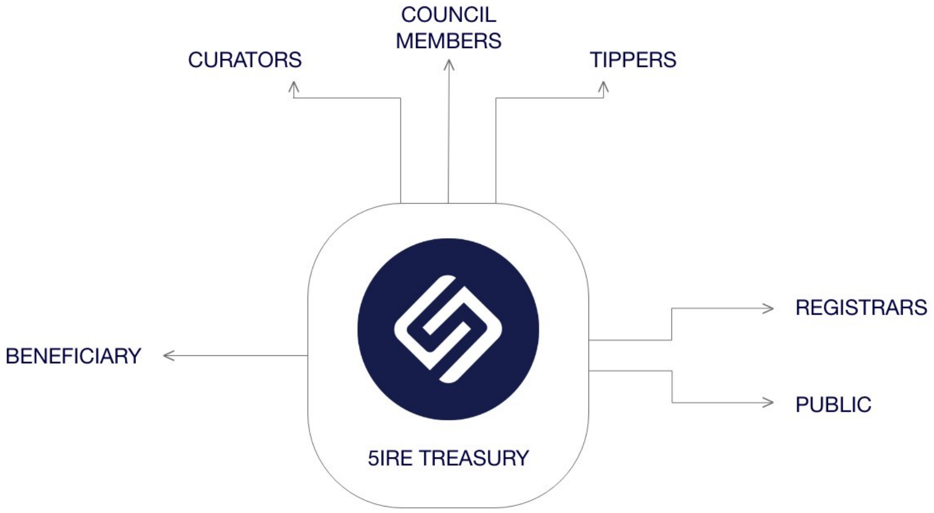

Figure 4. Process of audit-based reward distribution

4.3. Proof-of-Donation

The 5irechain sustainability reward distribution mechanism has another layer that focuses on rewarding charity-oriented activities. These activities can be either on-chain or in the real world to formalize and implement this part of the scheme we devise the tracking and rewarding of charity behavior to two main parts. An On-chain Proof-Of-Donation and an Off-chain audit-based Proof-Of-Donation which is analogical to the mechanism deployed in the creation of the Proof-Of-Donation but different in terms of the specified set of objectives and body of work.

4.3.1. On-chain Proof-Of-Donation

The on-chain Proof-Of-Donation is based on the substrate charity pallet which represents a charitable organization that collects funds into a self-contained pot that is controlled by the pallet itself and allocates the funds to charitable causes and what makes it suitable for the implementation of the on-chain Proof-Of-Donation are two useful concepts .

- **A shared pot of funds controlled by the pallet itself.**
- **Absorbing imbalances from the runtime.**

Instantiation of the charity pallet

The Charity pallets account is controlled by the pallet itself, not a specific user cryptographic key pair to avoid potential misuse of a pot controlled by someone.

Receiving Funds

Charity can receive funds in two main ways [6].

- **Donations.** Users can donate to the pallet, and users that have a good history of donations gain a strong reputation thus having more potential on receiving rewards based on the on-chain Proof-Of-Donation.
- **Imbalances.** Charity can also receive funds by absorbing imbalances created in the runtime. This is making 5irechain sustainable by design. *Imbalances* are created when 5ire tokens are burned or minted. Charity's objective is to collect funds through *Negative Imbalances* that are triggered when slashing of a validator happens, transactions fees, or when other pallets inside the runtime burn funds as a part of an incentive-alignment mechanism.

4.3.2. Audit-based off-chain Proof-Of-Donation

The Audit-based off-chain Proof-Of-Donation is analogical in the design to how Proof-Of-Benefit works as an audit-based process but different in terms of the specified set of objectives and body of work, in the Proof-Of-Donations the objectives of audits are about tracking the history of the off-chain donations of the subject beneficiary based on real-world data. The workflow is similar to the Proof-Of-Benefit.

5. GOVERNANCE

As we have chosen to be a substrate chain taking advantage of the cutting edge technology of the parity rust based framework for the creation of our next-generation blockchain because of features that are needed to fulfill our democratic vision and this technology allows us forkless upgradeability, so any voted upon runtime logic modification can be achieved without needing to hard fork the network causing destruction and divisibility instead of power and union and most importantly staying loyal to the sustainability and for benefit prior goal of the network. In order to achieve this, we took advantage of Polkadot's highly sophisticated governance mechanism that allows continuous evolving in accordance with the assembled stakeholders. Where the commandment of the network is in favor of the majority and made by them, this canonical universal governance system is highly suitable for the 5irechain network. Thus we choose to adopt it to ensure that the sustainable for-benefit paradigm is always maintained and in a democratic way. To make this possible, we bring to use Polkadot various novel mechanisms, including a revolutionary state-transition function stored on-chain and defined in *WebAssembly,* a platform-agnostic intermediate language, and *referenda* with a dynamically adjustable threshold that defines the meaning of *super-majority* [13].

5.1. Mechanism

In order to bring network modifications to life, the governance mechanism composes the will of the *Public* (token holders) and council together as administrators of the network upgrades decisions, no matter who made a proposal, this latter must go through a *referendum* to let any active actors of 5irechain weighted by stake vote on a decision.

5.1.1. Referenda

Referenda is an inclusive stake-based voting mechanism, a composition of *referendums,* where each referendum has a *proposal* that is a function call in the runtime with high privileges. Such functions have the power to even change the entire code that defines the runtime logic of the chain [13].
Referendums are procedural votes. The reason for this lay in the notion of a *Problem* as defined in complexity theory. Where a problem is a generic question that contains parameters and variables, when instantiated, we obtain an instance of the problem. It is shown that most of the problems can be formalized as an equivalence of a decisional problem which can be answered in a binary way. Thus referenda are defined as discrete events in time with a fixed voting period, and the only voting options are “Yes” or “No”.
The ways referenda can be started with are.

- Publicly submitted proposals.
- Council-based proposals.
- Technical Committee-based emergency proposals that have been approved by the council.

6. TREASURY

The notion of a *Treasury* is highly important for the 5irechain logic. It is at the heart of the for-benefit paradigm as it is the primary media to distribute incentives to the network actors who apply to the proof-of-benefit by respecting and investing in the achievement of the 17 SDGs and also for the proof-of donation part of our consensus and staking mechanisms where rewards are distributed for the identified actors that spend for charity or investing in the proposed projects that are democratically voted upon, the only project that brings benefit to humanity will get chosen, and such actors that have gained a reputation based on their historical donation register are going to be rewarded by the treasury.

6.1. Definition

The Treasury is defined as a pot of funds that are collected in many ways such as transaction fees, donations, slashing, inflation, Etc. The main spending way of such a mechanism is by the making of spending proposals when approved by the council and after the waiting period *"budget period"* ends they get distributed to the concerned actors [6], and for us, in 5irechain the proposals and spending are directed toward a for-benefit paradigm to ensure that the actors that work more for humanity and sustainability are the most rewarded by our staking mechanism and to ensure the funding of the actors and project that brings value and thus leading the 5th industrial revolution where bringing sustainability and support for the 17 Sustainable Development Goals (SDGs) is more profitable than acting against this paradigm. Thus achieving and motivating sustainable actions by design. The duration of the budget period is adjustable according to the governance, so we make sure that the distribution period is democratically chosen. a default budget period value will be defined in a way that assures that the 17 SDG registrars have enough time to do the audits.
When token holders want to propose a spend from the treasury, they must put a reserve deposit of a small percentage of the proposed spend, which is returned if the proposal is accepted or slashed if rejected.

6.2. A fusion between the Treasury and the sustainable Proof Of 5ire mechanism

This democratic vision was enabling the creation of the for-benefit paradigm. This is our adopted solution combined with the governance mechanism to bring to life our sustainability vision, thus formalizing the problem of rewarding the actors on-chain. This fusion is based on specific actors, where elected and trusted *Registrars* that held the identity of the validators and their reputation-based audits performed by the registrars toward each validator who has already being judged by a registrar, this later perform an audit on validators that assign a 5ire score to them based on their appliance with the 17 Sustainable Development Goals (SDGs) and a detailed audit is submitted to the *5ireassembly* for further discussion and if accepted and the proposal period ends rewards are distributed to the validator that deserves, the reward is proportional to the 5ire score assigned to the validator. The same for the proof-of-donation, where the reward is based on the history of donations that the validator made.

6.3. The funding of the Treasury

The Treasury can be funded by .

- ***Inflation.*** In 5irechain, the staking ratio is chosen to be xx%, and with an inflation rate of xx%, those ratios are very important for the network, and any deviation from them will make a proportion of this inflation go to the Treasury. To give a clear image of this, imagine our staking ratio to be 60%, and the inflation rate is 5%, then if 60% of the token distribution are staked, then the totality of the inflation goes to validators as rewards, and if it is less or greater than the staking ratio, some of the remaining tokens go to the Treasury.
- ***Transaction fees.*** While the totality of each block's transaction fees goes to the validator authoring the block, the remaining portion goes to the Treasury.
- ***Slashing.*** The penalties made to misbehaving validators while active cause him to lose a part of his staked tokens. The slashed tokens go to the Treasury with a reward going to the actor that reported the misbehaving of the validator.

7. IDENTITY

We chose to adopt the substrate identity mechanism that allows users of the chain to couple pieces of information to their on-chain accounts and submit a request in the form of judgment to a registrar. The definition of identity is one of the main mechanisms that allow our 5ire score mechanism to work, for this reason, we make sure that it is a democratic and functional scheme so we can know information about actors such as validators and they are highly motivated to set an identity for two main causes, the first one is they will gain a good reputation, so nominators can put trust on them, the second one is that validators with an identity gain advantage in the 5ire score mechanism and in earning rewards based on audits.

7.1. Registrars

Registrars are important network participants that have mainly two functions, the first one is making sure of the identities, the second function is doing audits on identifiable accounts. So they are a core participant in the 5irechain network, for this reason, the voting mechanism ensures that the chosen registrars are liable and trustworthy. Anyone can become a registrar by submitting a proposal to Democracy with a preimage hash of the submitted pieces of information. Registrar can set up a fee for their services, for example, identity provider type of registrar can put the reasonable amount for this services, and the registrars that perform audits can make higher fees for the service, as this is a complicated ongoing process that determines the amount of reward that will get distributed to the audited validators.

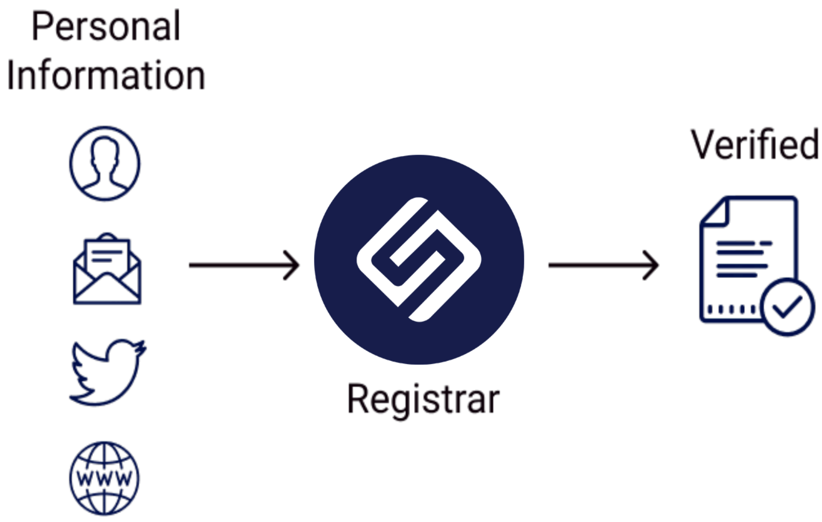

Figure 6. Identity Registrars

7.1.1. Judgments

Substrate chains use the *judgment* notation to describe the request action users take in order to validate the injection of their information on-chain, so the judgments are made by registrars.
Validators are required to pay judgment fees to registrars, whether it is an identity judgment or an audit judgment. Logically the fees for the audits are higher than the ones concerning identities. In order to make the process more declarative and transparent, we introduce the notion of *confidence levels* that are used when registrars provide judgment toward an entity that might select a level of confidence in their attestation [16].

- **Unknown.** Meaning that no judgment has been made. It is the value by default.
- **Reasonable.** Meaning that the provided information is reasonable, but there was no performing of in-depth verifications by a registrar (e.g. Audits, donation history, formal KYC process).
- **Known Good.** The registrar has performed an audit and has certified the correctness of the provided pieces of information.
- **Out of Date.** Meaning that the provided pieces of information used to be Known Good, but now they are considered as outdated.
- **Low Quality.** The pieces of information have low quality, this is generally done by a performance of a poor audit, but they can become up to date and modified.
- **Erroneous.** Meaning that the provided pieces of information are erroneous or hide malicious intent.

As we mentioned earlier, 5irechain is based on trust and reputations, including registrars, as they will gain more trust by performing proper and reasonable audits about validators appliance with the sustainable development goals laid down by the United Nations. Solid shreds of evidence should back such audits.

8. DEMOCRACY

5irechain makes heavy use of the substrate democracy pallet to handle the administration of stakeholders voting. The Democracy pallet launches a referendum from a proposal that it takes from the queues and repeats this process every *launch period,* defined in the runtime. Any *referendum* can be a simple majority in which a/2 +1 vote to a yes or no to decide the outcome. To be able to achieve Democracywe utilize the Phragmén election Method [16].

8.1. Sequential Phragmén Method

Validators election

The election of validators is based on a Phragmén method derivative which is called the sequential Phragmén method heavily used in a nominated Proof-of-Stake scheme based on their stake and the stake of the nominators that backs them. At its heart, this algorithm tries to calibrate the variance of the weight between validators.

Justified Representation

The Phragmén method is one of the interpretations of *Non-Partisan Proportional Representation*. It was named after Edvard Phragmén. This method came to resolve a candidacy problem giving a set of candidates, a fixed number of seats that have less cardinality than the set of candidates against a set of giving voters, the voters have the ability to give their votes to any subset of the candidates set excluding the empty set, and the set of all candidates [16].

UNORDERED PHRAGMÉN METHOD**.** As described above, the Phragmén method is an iterative method that portrays an election scenario where a set of candidates compete against each other in order to win seats and achieve this by voting. Let us discuss the situation where voters have the same voting weights, which is not the case in a blockchain scenario. "Basic Phragmén" was first described by Brill et al. in their paper "Phragmén's Voting Methods and Justified Representation". Seats are given sequentially until the election achieves the number of seats. Each group of an equivalent ballot is given a place number, which is a non-negative rational number, this number is the fractional number of seats elected so far by these ballots; it is always assured that the place numbers are always equal to the number of the allocated seats [3].

WEIGHTED PHRAGMÉN METHOD. In blockchain, candidates usually do not have the same weight (Stake). In our voting models (validator selection, governance voting), elections are weighted proportionally to voters holdings (tokens). Thus we see a bias in the voting power. The weighted phragmén method allows us to achieve a justified representation of all the participants, this way, we achieve democracy by allowing minorities participation while preserving the freedom of choice [16].

9. SMART CONTRACT

9.1. Overview

A Smart Contract is a procedural and executable program containing a set of functions and states that runs on top of a blockchain while residing at a specific address on the blockchain storage as an account, they have balances and the ability to send transactions. What makes them different from the traditional contracts is the fact that their execution is not controlled by anyone.

5irechain will provide two smart contract virtual machines that will be added to the runtime with the intention of creating its own *WebAssembly* targeted smart contract that will come with its own embedded domain-specific language in the near future.

9.2. EVM Smart Contracts

5irechain will integrate the *Frontier* EVM execution environment for its Ethereum compatibility layer that will allow the execution of EVM bytecode to be natively executed on top of 5irechain. So developers can easily migrate their Ethereum Dapps to 5irechain with minimal to zero modification, and they will still use the same Ethereum-based tools and frameworks. 5irechain will support Solidity, Vyper, and any other language that compiles to EVM bytecode. Plus support for all of the already existing Ethereum RPC methods. So Developers are guaranteed a seamless migration of Dapps to the sustainable For-benefit 5irechain network.

9.3. Wasm Smart Contracts

5irechain will also provide the ability to execute WebAssembly smart contracts that are designed for correctness and efficiency in mind. More precisely 5irechain will integrate the substrate Rust-based embedded domain-specific language called ink! That will allow the execution of the inherently safe, fast, and secure Rust smart contracts on top 5irechain runtime logic. This integration will make use of the Contract Pallet already provided by the substrate framework.

10. USE CASES

10.1. E-governance

One of the most discussed innovations in blockchain technology is smart contracts, which allow the execution of business logic on-chain. They open the door for a whole new paradigm like the permission to create digital assets where smart contract uses embedded logic by defining a canonical interaction way for those digital tokens to interact and function (e.g represent voting rights or a stake in protocol revenue), one of the powerful features of smart contracts is that they are tamper-proof mechanism meaning than no external counterparty can tamper with the terms and the logic embedded on them, they are a form of law described as code on-chain. They can become the new form of multiparty business automation [1].

One of the main goals of 5irechain is to become a governance framework that proposes a strategic pathway that enables interoperability between off-chain digital legacy systems and governmental infrastructures with blockchain technology, thus enabling a marriage between the two currently distinct fields and bringing the powerful features of blockchain to legacy systems. The adoption of blockchains by organizations has pointed to the integration and interoperability between blockchains and other systems as one of the most promising use cases of distributed ledger technology and yet the most challenging one [2].

Through the integration of the 5ire ecosystem with an off-chain worker oracle mechanism will enable a whole new shift in how legacy systems work where the processing of citizens and users claims can become verified through 5irechain and be assured of the *non-repudiation* of the whole process of claiming and verification.

The benefit of the interoperability between legacy systems and the 5ire Ecosystem.

- **Governance by design.**
- **Transparency and accountability.**
- **Sophisticated document control systems.**
- **Reducing corruption and error by using smart contracts.**
- **Elimination of inefficient intermediaries and introduction of data validation through off-chain oracle systems.**
- **Strong security guarantees. Confidentiality, Integrity, authentication, and Non-Repudiation.**

Potential use cases for legacy systems, government, and the public sector.

Agricultural insurance. Present-day mechanisms used by the insurance systems for issuing and validating claims and payout processes are respectively inefficient and time-consuming, and we think that this is the main reason for index-based insurance not being adopted by smallholder farmers despite their benefits in providing social protection for farmers affected by floods and natural catastrophes in the hope of reducing the impact they suffer as a result.

5irechain provides a smart contract index insurance that brings automated instant payouts to the insured farmers, and with the help of a decentralized oracle network system, 5irechain eliminates the need for intermediaries assessment in case of natural catastrophes through automated data feeds [1].

Identity Management and Self-Sovereign Digital Identity Aggregation. 5irechain will give legacy systems, governments/enterprises workers, and citizens the opportunity of owning their self-sovereign identities while still permitting the verification of credentials on-chain. Nowadays, digital legacy management tooling encounters severe security, scalability, and elasticity issues. 5irechain identity management's vision is to give back the right of owning identities for citizens and users alike. A self-sovereign approach where identities reside on the user side while maintaining a cryptographical process of issuing and verifying credentials and information contained on them without revealing other sensitive data. Our powerful mechanism is conforming to the W3C standard that defines *decentralized identity* as a globally unique persistent identifier that does not require a centralized registration authority; instead, it is cryptographically issued and verified. However present-day decentralized identity systems are very fragmented and form isolated frameworks with no means for interoperability, making the existence of a universally unique decentralized identity management system very challenging, such a dream is very promising for various scenarios like borderless credential verifications, network actors reputation in an on-chain governance and credit lending. 5irechain not only aims to become a decentralized identity standard implementation but also aims to solve this system's fragmentation with a built-in identity aggregation mechanism for other decentralized solutions and legacy systems.

5ire identity guarantees .

- Decentralization. The process of claiming and issuing is an on-chain process.
- Democracy. The 5ire score instantiation and registrars are tracked by the sustainable 5ire democratic governance mechanism that is based on the Phragmén method.

The 5irechain-based self-sovereign digital identity management system can form the basis for many governmental tracking and validation services.

- **Verification of academic credentials and validation of professional qualifications.**
- **Electronic healthcare records and vaccination tracking.**
- **Become a middleware for the collection of payroll taxes.**
- **Management of student loans and innovation grants.**

We can mention other use cases like .

- **Land Registry and land-title transfers.**
- **Intellectual property protection and digital rights management.**
- **Voting.**
- **Healthcare.**

5IRE725 and 5IRE735. A Self-Sovereign Identity Standard For 5irechain. As one of the 5irechain principle components is identity, plus being a DID aggregator and having selfsoverignity at the runtime, we leverage 5IRE725 to fastly create their own identity management system on top of 5ire. 5IRE725 describes proxy smart contracts that can be controlled by multiple keys or by a 5IRE735 associated standard to add and remove claims to a 5IRE725 identity smart contract.

Society 5.0 and Smart Cities. According to the United Nations data booklet "The World Cities in 2018", By 2030, 60 percent of the world population will live in cities. And as cited in the booklet, understanding the key trends in urbanization is crucial to the implementation of the *2030 Agenda for Sustainable Development,* including Sustainable Development goals. This increase in the urbanization rate of growth surely can bring economic benefits. Yet this includes high risks of environmental and social problems. Thus we see a considerable need for wrapping this growth rate in a for-benefit sustainable operating model instead of a destructive for-profit paradigm.
The G20 Global Smart Cities Alliance and FY 2020 Japan smart city project have shared a framework of common principles for the implementation of *Smart City Technologies* that should be highlighted for blockchain utilization in building smart cities of the future [4].

- **Define a clear and sustainable vision.**
- **Interoperability.**
- **Formulate regional organization/initiative**
- **Scalability and Future-Proof.**

5irechain main goal is to lead the 5th industrial revolution by bringing a shift in the network activities and shareholders toward the service of humanity, the missing factor in all existing frameworks of interaction. In order to answer this question we tried to dive deep into the technological aspect of the business models and tried to embed the missing human factor and sustainability in the core of the technology itself. Thus bringing control and sustainability in the runtime logic of our blockchain and consensus mechanism in order to serve humanity, not technology. 5irechain is the missing point in providing an implementation of the framework of G20 Global Smart Cities Alliance common principles [4] to build *Smart City 5.0*.

- **Sustainability and service of humanity by design.**
- **Interoperability by bridges and cross-chain communication.**
- **Governance and Democracy by design.**
- **Scalability through hybrid consensus and future sharding of the network.**
- **Future-Proof by Forkless upgradeability of the runtime logic.**

10.2. Defi 5.0 . User-centric decentralized finance

Decentralized finance on top of 5irechain will provide the possibility of existence to various financial applications and services in the most sustainable way with its user-centric vision that does not include intermediaries. 5irechain purpose is to make sustainable Defi accessible to the unbanked people and ensure that financial services are working in a for-benefit paradigm. 5irechain will host a variety of applications and services alike.

Financial services on top of 5irechain are superior to their centralized counterparts across the following primary features.

- **Permissionless.** No one is in charge of the services and everyone can participate in the ecosystem with no privileges for certain parties.
- **Censorship Resistance.** No central party is able to reverse the order of transactions or bring *repudiation* about the global state of the system that is shared among all users that have an objective view over the global state. Also no one can shut down the service.
- **Trustless.** Users don't have to put trust on a central party, Trust is distributed among all the actors and the network with no one having the ability to be of a particular privilege on the trust providence part.
- **Programmable.** Developers have the ability to leverage all the previously discussed properties while being assured about the creation of upper logic on top of 5irechain by creating rich smart contracts either by using the EVM for the ethereum style of smart contracts or the more advanced and efficient WebAssembly smart contracts based on a Rust eDSL language.
- **Efficiency.** Open financial services on top of 5irechain are controlled by code instead of inefficient intermediaries and middlemen, thus gaining speed and lowering costs of the creation in traditional markets.
- **Sustainability.** The financial interactions in 5irechain are driven by sustainable actions. This unprecedented approach ensures the creation of money markets that are aligned with sustainable development, not against it like traditional markets.

5IRE-20 Tokens and NFTs. 5irechain will support all the existing token standards like 5IRE-20, 5IRE721, 5IRE777, and 5IRE1155. You can create your own tokens or migrate your already existing tokens.

Liquidity Bridges. With 5irechain you can wrap existing tokens and transfer liquidity from blockchains like Ethereum to 5irechain.

Automated Market Makers. With 5irechain, you can create AMMs and DEXs that take advantage of the 5irechain ecosystem and the interoperability aspect of 5ire, DEXs on top of 5irechain can process a great amount of transactions because of the speed and efficiency of the cutting-edge technology underlying 5irechain.

Stablecoins and Money Markets. You can create sustainable solutions that hedge against volatility and help users earn interest on their holdings, while creating rich ecosystems on top of 5irechain that make use of *Algorithmic Stablecoins*.

Global Liquidity Aggregator. 5irechain can act as a liquidity aggregator from centralized and decentralized liquidity pools and Defi protocols.

Sustainable Staking and Yield Farming. You can participate in the Proof of 5ire mechanism and earn attractive APY while bringing value and benefit to humanity.

Sustainable DAOs. Users are encouraged to create DAOs around sustainability and the service of humanity. And the complex account types offered by 5irechain can help in the creation of complex DAO hierarchies and governance mechanisms for the control of a multi account shared wealth.

Decentralized insurance. 5irechain aims to make insurance automated, cheaper, faster and transparent. So coverage is more affordable. 5irechain aims to build out coverage from users that are not able to afford either the complexity or the cost of traditional insurance systems. We aim to help smallholder farmers against droughts and floods, women who are running small businesses, and everyone that was previously excluded from traditional insurance.

Quadratic funding. 5irechain is a community-driven project that is backed up by the community, 5irechain aims to use the quadratic funding model for fundraising projects on top of 5irechain, this has the potential to improve the way we fund all types of public goods in the future. This fundraising model makes sure that the projects that receive the most funding are the ones that have a special demand, the projects that stand to improve the lives of the people and bring sustainability to the table. The quadratic funding model follow those steps.

- The donated funds are collected in a matching pool.
- A sequential round of public funding starts.
- Everyone can signal their demand for a certain project by donations.
- When the round is finished, the funds in the matching pool are distributed to projects, the projects that have unique demand end up with the highest amount from the matching pool.

5ire Bonds. 5irechain is taking a unique approach in Defi space that allows stakeholders to stake a particular project tokens for prefixed lock-up periods and farm a different project tokens. The 5ire Bonds will be initially deployed on Ethereum and Binance Smart Chain.

ZK-Rollups & ZKswap. Based on the "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge." Proof and commitment scheme, 5ire chain aims to develop its own ZK-Rollups based layer-2 solution for great amounts of scalability will work in the creation of its first ZK-Rollups based layer-2 DEX with the AMM model.

Predetermined Spending Wallets. With the integration of withdrawal rate limiting, holders can make use of wallets that are limited in their spending capabilities over a fixed period of time. This kind of wallet is very suitable for large amounts of holdings in the case where it is stolen or compromised. You can make sure that the amount of transfers that can get out from the wallet are fixed over a period of time, thus giving you time to safely pull the funds back to a primary wallet.

Atomic swaps. Atomic swaps are one of the main building blocks for smarter transactional logic, basically it is a mechanism that enables the exchange of one asset to another without any use for intermediaries. It creates automated, self-enforcing rules that execute specific opcodes or a series of transactions to reach a finality without the need for middleman assurance of trust

Multi-signature Account and Wallets. being based on Substrate we have access to the rich accounts hierarchies and definitions and we are able to create highly sophisticated DAO and governance systems based on building blocks like proxy accounts and multi-signature-accounts that are a common way to share the ownership of a wealth over multiple accounts, this comes handy when institutions and associations need to claim a shared ownership over an account that represent them**.**

Self-sovereign DID Wallets. 5irechain thinks highly of DIDs and credential verification where users have full control over their identities. DID wallets will allow sophisticated recovery modes for users and organisations alike, and also it will let users add additional permissioned options over the 5irechain permissionless blockchain. This will create a delegation mechanism and inheritance to be applied over funds owned by a wallet. Additionally with verifiable credentials users can perform identity checks like KYC/AML without revealing other sensitive informations and can also attest for hedge fund subscription or for government backed stable coins.

Colored Coins. 5irechain colored coins are a class of method that can be used for ephemeral exchange of value as a representation and a management tool for real world assets. Their native nature makes them very powerful for many real world use cases and for flash loans. As their native nature gives strong security guarantees. To give a brief example of their use, let's imagine a real world asset that has an ephemeral nature as tickets for theater. 50 tickets can be represented as 50 colored coins at a certain timing. They are very powerful in their representation of ephemeral values.

Strong Consumer Authentication Wallets. this is a highly recommended procedures for securing sensitive fund transfers, where a controller is setting a whitelist of authorized payees, this is helpful for governmental accounts and banking authorities to make sure that only certain addresses are allowed to receive the funds and thus avoiding critical phishing attack that triggers the human in actions like emails phishing attacks and hijacks.

Supply Chain and Transactional Clawback Escrow. In 5irechain the finality and validity is fast so transactional throughput is high, so for sensitive fund transfers we recommend to use the transactional clawback escrow as a mechanism that adds a threshold period where funds are transferred after they have been sent, this way senders can lower the risk of address typo errors, so there is a timing for the transaction to be passed and checked with a possibility of a Clawback, this period can be short or long, a use case that can have a heavy use of this mechanism is supply chain where there is always incertitudes and error between buyers, shipping companies, and suppliers.

United Nations Sustainable Development Goals (SDGs) As Indexes. 5irechain will work on the tokenization of the 17 SDGs and bringing them on-chain for the purpose of making the for-benefit paradigm more promising by taking advantage of the 5irechain transparency and accountability features and the sustainable reward distribution.

11. Conclusion & Perspectives

5irechain is a sustainability-driven blockchain with reputation-based mechanisms. In the near future, 5irechain aims to become an ecosystem that focuses on positive impact and invites other blockchains and projects on top of 5irechain to adopt this vision and innovate in the way they utilize those mechanisms.

5irechain highlights many building blocks that can be combined to further create tools and schemes that are going to make the shift from the fourth industrial revolution to the fifth. We invite Stakeholders, Developers, Legacy agencies, and users alike to be creative in the way they are using 5irechain and the way they will interact with the ecosystem.

5irechain is focused on improving its sustainability rewards distribution, interoperability bridges, and identity management systems as they are key components for 5irechain. 5irechain is focusing on the implementation of the self-sovereign DID Aggregation mechanism. Also in the near future, 5irechain aims to have its own eDSL Wasm smart contract language and will furthermore add features through governance. 5irechain

References

[1] Gartner Top 10 Strategic Technology Trends for 2020, October 2019. https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/ (link as of 25/11/20).

[2] Forbes, The Five Ingredients of Blockchain Interoperability, February 2019. https.www.forbes.com/sites/richardgendalbrown/2020/02/13 the-five-ingredients-of-blockchain-interoperability/?sh=6df1b2e958a1 (link as of 25/11/20).

[3] Svante Janson. phragmen’s and Thiele’s election methods. 2018

[4] Cross-ministerial Strategic Innovation PromotionProgram (SIP), Smart City Reference Architecture White Paper, March 31, 2020

[5] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, “High-speed digital-to-RF converter,” U.S. Patent 5 668 842, Sept. 16, 1997.

[6] Official Documentation for Substrate Blockchain Developers, Substrate Developer Hub. https://substrate.dev/

[7] Christopher Copeland and Hongxia Zhong. Tangaroa. a byzantine fault-tolerant raft. http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf, 2016.

[8] Alistair Stewart, Eleftherios Kokoris-Kogia . *grandpa. a Byzantine Finality Gadget. June 19, 2020*

[9] Vitalik Buterin. Ethereum. A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper, 2013.

[10] Gavin Wood. Ethereum. a secure decentralized generalized transaction ledger. http://gavwood.com/paper.pdf, 2014.

[11] Satoshi Nakamoto. Bitcoin. A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008

[12] Webassembly. http://webassembly.org/, 2016.

[13] Gavin Woods. Polkadot. a vision for a heterogeneous multi-chain framework. https://polkadot.network/PolkaDotPaper.pdf, 2016

[14] Handan Kilinc Alper, BABE Blind Assignment for Blockchain Extension protocol. https://research.web3.foundation/en/latest/polkadot/block-production/Babe.html

[15] Alfonso Cevallos, Nominated Proof-of-Stake. https://research.web3.foundation/en/latest/polkadot/NPoS/

[16] Alfonso Cevallos, Alistair Stewart. A verifiably secure and proportional committee election rule. 27 April 2020