5IRECHAIN: A Sustainable Proof of Stake Consensus Mechanism

Vilma Mattila, Prateek Dwivedi, Pratik Gauri, Jamshed Memon, Samiran Bag, Alvin Reyes

5irechain

Abstract. 5irechain aims to become the first layer-1 protocol to develop a sustainable and for-benefit ecosystem based on the sustainable development goals (SDG) defined by the UN. Our proposed consensus mechanism considers sustainability as one of the most important components of the consensus mechanism. Other than sustainability we also aim to curtail favouritism or cartelization in the proof of stake consensus mechanism where nodes can delegate their stake or nominate the nodes of their choice, which helps these nodes being selected for the creation of blocks.

Our block assembler nodes are selected based on multiple factors, including the reliability score, stake, randomized voting and sustainability score(Environmental, Social and Governance). In order to promote the competitive position of smaller holders on the network, the reliability score, randomised voting and sustainability score weighting provides the level playing field to all nodes to an extent. This helps in providing more equal access to all nodes participating in the creation of the blockchain. We also aim to introduce the concept of nested chains, which will enable the 5irechain nodes to create simultaneous blocks and thus providing scalability to the chain. The nodes will be grouped together based on latency and throughput to build and manage smaller chains. These independent chains will then be merged into 5irechains and their reliability, integrity, and authenticity will be measured through joiner blocks, which are being introduced as blocks of blocks instead of blocks of transactions.

1 Introduction

The market cap of cryptocurrencies trading today is approximately 3 trillion dollars and it has more than doubled since last year. There are well over 6000 different coins and tokens trading on cryptocurrency exchanges today. The underlying structure of these cryptocurrencies is based on blockchains – a data structure that works as a decentralized ledger where the transactional record is kept in a secure and transparent manner.

There are two layers of protocols that are the building blocks of blockchain technology. The layer 1 protocols refers to protocols that build the blockchain itself, while layer-2 protocols refers to the technology that operates on top of blockchain or layer-1 protocols [4]. E.g. Bitcoin [9], Ethereum [3], Litecoin [16] etc. are the layer-1 protocols, while tokens like SAND, DAI, CHR etc are layer-2 protocols built upon Ethereum.

5irechain is introducing sustainable proof of stake (SPoS), a new consensus protocol. SPoS is a new consensus algorithm that incorporates a new weighing mechanism that adds to the overall proof of stake (PoS) weight. This new weighing mechanism is based on 5ire's sustainability factors which enable and drive the development of solutions that brings forward Sustainability, Technology & Innovation using blockchain technology to build the 5th industrial revolution.

2 Literature Review

Blockchain technology, as its name implies, is the chain of blocks of transactions [8]. Each block is connected to the previous block through a cryptographic hash of the block. This is to protect the integrity of the block and create a chain of events for the others to traverse through. Its name is synonymous with the popular cryptocurrency bitcoin[4]. However, at the time of writing we have thousands of blockchain based coins and tokens trading on different exchanges ranging from decentralized finance(Defi) to Play to earn games to digital art [11]. One of the most important aspects of blockchain is not blockchain itself, but the distributed nature of the blockchain ledger that makes it attractive to investors and end users [13]. Blockchain itself would be useless if there was a central authority managing it, because it would just be another database holding the transactions just like relational databases. The involvement of the community in running and managing the network without the involvement of central authority is what makes the blockchain technology attractive.

Due to the distributed nature of the blockchain where the network participants maintain a copy of the transaction ledger, it is important that all participants have the same copy of the ledger at a given time or at least majority of them and transactions are verified before adding into the blocks. This is where a consensus protocol plays an important role [7]. Bitcoin [9] uses the proof of work(PoW) as its consensus protocol. The concept of PoW was inntroduced by Cynthia Dwork and Moni Naor in early 1990. They were initially designed as a means to combat email spam. Later, Nakamoto [9] used them in the design of Bitcoin's consensus protocol. In PoW the nodes also called miners compete for creating the next block and miners creating it first will get the reward in bitcoins as a mining reward. However, in order to create the block each node needs to show proof of work, which is essentially mining or finding the right nonce. A nonce is a piece of single-use code which yields a unique hash, or distinguishing code, for the block when the nonce is added into the block along with transactions. Miners add to the block by iteratively checking many nonces until they find an appropriate nonce that matches the search criterion. Finding the right nonce can consume a substantial amount of resources and energy and literature suggests that adding a single transaction in a bitcoin block consumes energy equivalent to what 21 households in the USA consume in 24 hours [7]. This is where altcoins, a term used for cryptocurrencies other than bitcoin, started developing their own consensus protocols that don't require mining.

Proof of Stake (PoS) protocols aim to solve the problem of massive energy usage by the Bitcoin network by replacing computational power with staking. In a PoS based consensus mechanism, blocks are assembled by validator who own large quantities of holdings in the form of cryptocurrency. PoS systems do not incentivise extreme amounts of energy consumption, rather in these systems, validators get to assemble a number of blocks in proportion to their stake. Cryptocurrencies that use PoS as their consensus protocol, tend to structure their incentive schemes in a way that discourages attackers by making attacks less profitable for validators. Due to their reduced power consumption, PoS based cryptocurrencies are often regarded as "green coins". Due to its green nature, it is speculated that Bitcoin will eventually adapt to PoS as its consensus protocol [6]. In 2012, Peercoin [11] became the first cryptocurrency to use a PoS based consensus protocol. Ethereum 2.0 [3] is the major upgrade of the Ethereum network where it is moving away from the proof of work consensus to proof of stake(PoS). Similarly, Polkadot [1], another popular cryptocurrency, also uses nominated proof of stake (NPoS). In NPoS based cryptocurrencies, there are two types of actors in the network, namely validators and nominators. Validators are nodes that validate blocks, maintain parachains and guarantee finality. Nominators are actors that back validators financially with their stake. When validators earn some reward by producing blocks, nominators receive some part of it in exchange for the financial backing. In NPoS based systems, both validators and nominators are required to have their stake locked as collateral. If a validator ever shows negligent or adversarial behavior towards block validation, backing nominators are susceptible to penalty. This provides an incentive for the nominator to select validators wisely as they are liable to forfeit their stakes if the validator he supported acts maliciously.

3 Consensus Protocol

5irechain is introducing SPoS, a new consensus protocol. SPoS is a multifactor consensus protocol where a node is assigned weights based on Stake, Reliability, randomised voting, sustainability score (Environmental, Social & Governance) and previous nomination. We believe that SPoS provides certain advantages over its adversaries. These advantages are over and above the advantages that proof of stake(PoS) consensus mechanism provides over proof of work (PoW) consensus mechanism. Nodes getting the maximum weight will be selected for the assembly of the blocks for next 12 hours when the process of selecting the next nodes will start again. Table 1 outlines the factors along with the corresponding weights they carry.

It is to be noted that we have made these weights flexible and we are developing our product in such a way that we can change these weights based on how balanced our algorithm is in the selection of nodes. We still believe that a node having higher stake should get the higher priority, but stake should not be the

Factors	Weight
Stake	50%
Randomised Voting	20%
Sustainability Score	20%
Reliability Score	10%
Previous Nomination	-2%

Table 1. Assignment of Weights

only criteria of selecting the node, because we believe that this discourages the participation of nodes with smaller stake or nodes, which cannot coerce other nodes to nominate them. We also want to reward the loyal nodes, which are always there and hold the stake for a longer period of time. Similarly, ESG compliance further rewards the nodes for being there for the benefit of the society as whole.

Following are the key features of the consensus mechanism.

1. SPoS uses multifactor weights to select the nodes for the assembly of the block.
2. Randomized voting carries 20% weights, which ensures that nodes having the lower stake can still be selected for the assembly of the block. This essentially helps us curtail the cartelization of the network where nodes can create a nexus among each other by nominating or delegating their stake to favourite nodes each time.
   Nodes, i.e.: nominators, provide votes to potential assemblers that have chosen to compete with each other for the right of assembling blocks. These votes carry 20% of the weights associated with a node. We use the e-voting scheme introduced in Cramer R., Gennaro R., Schoenmakers B [5] to conduct this vote. In this scheme, there is a set of nodes called 'Tallying Authority'(TA). Any node can offer to become a member of this set. However, a node needs to deposit some tokens in order to be eligible for becoming a member of this set. The members are denoted as $TA1, TA2, \cdots$ etc. The members of the tallying authority jointly produce a public encryption key which is broadcast across the network using a threshold encryption technique. This is done by means of Shamir's secret sharing scheme [12]. The set of tallying authority consists of n members such that any $t < n$ of them is sufficient to decrypt a message. A node uses this public key to encrypt her vote. The node also produces non-interactive zero knowledge proof of the well-formedness of her encrypted vote. These encrypted votes and zero knowledge proofs are broadcast across the network. An encrypted vote is accepted only if the zero knowledge proof

validates the correctness of the encrypted vote. Then anyone can use the homomorphic property of the encryption scheme to add the encrypted votes. Once this is done, the members of the tallying authority can jointly decrypt the tally and provide a non-interactive proof of the correctness of the tally. As stated before, decryption requires only t of the n members of the 'tallying authority'. The entire process of voting has been depicted in Figure 1. Once the tallying is done, all participating nodes who were members of the tallying authority can be compensated with tokens.

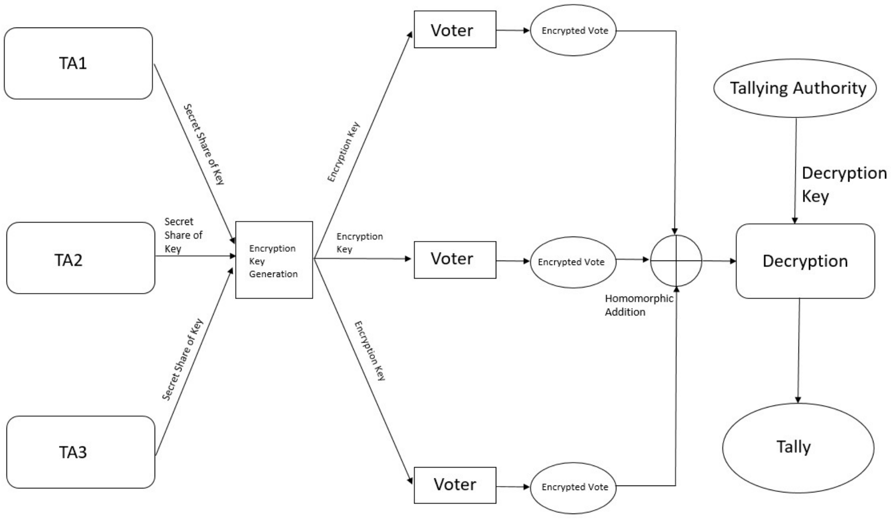

Fig. 1. The election process

3. Nodes are assigned the reliability score based on the amount of time nodes have been online at the time of voting, the duration they have held the stake, the successfull block creation in the give time slot and the blocks attested. This incentivises the participation in the network.
4. The proposed consensus mechanism takes into account the sustainability score, which consists of environmental social and governance score organizations or individuals running the nodes.

   Initially, these scores will be assigned by us depending upon credible inputs obtained from trusted authorities. Later, when the 5ire ecosystem stabilizes, there will be a decentralized mechanism to assign and update the sustainability scores. We shall have a mechanism to allow nodes to periodically provide sustainability scores for organizations/individuals. These scores will be in encrypted format. These encrypted scores will be added up using the homomorphic property of the encryption system, and then jointly decrypted by a set of trustees. The sustainability score can be directly inferred from this decrypted tally. A set of trustees can be selected from the network on the basis of stakes or reliability. These trustees will oversee the process of computing the sustainability score of organizations/individuals.

5. Probability of being selected as assembler reduces by 2% after each epoch . This is not permanent and after fixed number of epochs.

At 5ire our aim is not to punish the nodes with higher stake, but to provide a fair share of opportunity to the nodes with lower stake in order to encourage more nodes to participate in the network. This is why stake still carries 50% weight.

3.1 Reliability Score

5ire gives reliability score to nodes is equally based on:

- Age: Age of node or the time node has been online during the last 14 epochs(7 days). This will be determined through taking into account the number of successfull blocks created by the node during the allotted time slot and number of blocks attested.
- Stake: This will be determined by How long a node have held the stake for.e.g. if node1 has been online all the time during the last 14 epochs and has held the same or higher amount of stake the node will get the maximum reliability score.
- Block assembly: Successful block assembly will give a node more probability to be elected as assembler again. Failure to create a block when the slot is assigned to a node will not only result in less reliability score, but it will also lower the stake due to slashing
  itemize

3.2 Randomised Voting

Concept of randomised voting has been introduced in 5irechain to provide a better alternative to nominated or delegated voting. We believe that nodes should be rewarded and punished based on individual basis and not on collective reward and punishment basis. Therefore, in randomised voting nodes will use a pseudo random voting algorithm to vote for the nodes randomly and then will attest the blocks created by those nodes. This will help us curb the coercion where nodes can persuade the other nodes to vote them in return for better return on their stake. We believe that this coercion promotes cartelisation of the network where nodes keep voting for the same nodes and get more share in block creation than the stake they represent.

Nodes are rewarded and punished based on their individual acts, because it is possible that a block creating nodes gets compromised and creates a fraudulent block. PoS algorithms are typically programmed to punish all the nodes who voted for this fraudulent node even though it was not their fault, because it is possible that a node can get compromised by a malware. Therefore 5irechain will only slash the stake of fraudulent nodes and not of those who voted for the node as votes are random. Stake of voting nodes will only be slashed if they also attested the fraudulent block, because in this case it will be certain that it is a collusion.

3.3 Sustainability Score

One of the multiple factors that help us select the assemblers is the sustainability score. It is a score based on the environmental, social and governance (ESG) index of an organisation. 5ire will use proposals where nodes will submit their sustainability report based on our template. 5ire ESG nodes will evaluate the sustainability report and will assign the weight on a Likert scale to each of environmental social and governance factors. We will be using template to collect the data from the stakeholders who want to participate in the network. Our template will evaluate the ESG compliance of the stakeholders and assign appropriate scores. Our multi-factor consensus algorithm will use this score along with the reliability score, stake, and randomized voting to select the list of assemblers for the duration of 12 hours. Table 2 lists the factors that we will be using for the evaluation of ESG score.

Environmental	**Social**	**Governance**
Energy Sources	Formal Contract/ Minimum Wage	Diversity
Certification(ISO 4001)	Anti-Discrimination Policy	Breaches
Waste Management	Data Privacy	Illegal Practices

Table 2. ESG Factors

4 Slot Allocation

In the current consensus mechanism, selection of assemblers is done on the basis of weights calculated from various parameters concerning a node or a group of nodes. Let us assume that there are n nodes $U_1, U_2, ..., U_n$ who are in the race of becoming a block-assembler. The weights of these nodes are $w_1, w_2, ..., w_n$ respectively. These are the top nodes in terms of weight. Let us define $a_0 = 0$, and $a_i = \frac{\sum_{j=1}^{i} w_j}{\sum_{j=1}^{n} w_j}$, for all $i \in [1, n]$. There are s slots in an epoch that needs to be distributed among these n nodes. Now, for each slot $c \in [1, s]$, generate a random number x_c in the range $[0, 1]$, allocate it to the node U_k, such that $x_c \in [a_{k-1}, a_k)$. This protocol can eliminate cartelization and will also ensure that the nodes get a fair share of opportunity to produce the blocks. The probability of a node getting a slot will directly be proportional to her weight. However, this will ensure that one node does not get to assemble all the blocks in the same epoch. In order for generating random numbers x_c, for all $c \in [1, s]$, we can use the following technique. All nodes participating in the race of becoming assembler may be asked to provide commitments to a random number. They can provide this information at the same time while locking their stakes. Later, they can open the commitments. Now, these committed numbers can be fed into a pseudo-random number generator to generate a sequence of random fractional numbers in the range [0,1], which can be used to allocate slots to the winning nodes. Table 3 shows how a sequence of 3255 slots can be distributed among winning nodes depending on their weights. There are 20 nodes that were chosen on the basis of their weights. Each of them is allocated a number of slots proportionate to its own weight.

Weight of Node	No. of Slot
14.6008	242
6.14162	94
14.1688	180
11.6192	210
11.537	172
7.38233	112
12.4074	181
12.4253	182
5.33839	84
10.2473	178
12.8699	214
3.93118	59
14.5396	215
12.857	226
17.2614	249
4.89747	79
17.0301	271
12.9548	211
3.1547	43
1.56364	33

Table 3. Caption

5 Nested Blocks

Nested-Chains 5irechain addresses the issue of scalability by maintaining parallel chains. These chains are created on the need basis depending on the load on the network. However, once a chain is created it will continue adding blocks, until the chain is synchronised with the 5irechain using a joiner block. Figure 1 shows the structure of the nested-chain. The nested chains not only support the scalability in the blockchain, but it also enables us to support creation of parallel chains without adding new nodes (Assemblers, Attesters/voters, ESG Experts). This essentially means that nodes will be running multiple parallel chains on a single node, but as a separate process. 5ire will use the scheduling algorithms to make sure the maximum utilisation of the nodes. Therefore, unlike the conventional blockchains where nodes will sit idle and wait for their turn to create the block, the nodes in the 5ire ecosystem may get turns to create blocks into another parallel chain in the nested-chain. The nodes in all the parallel chains will be selected in a similar way i.e. based on their weights (Reliability Score, Stake, ESG score and Randomized voting).Figure 2 shows the diagram of how blocks will be structured.

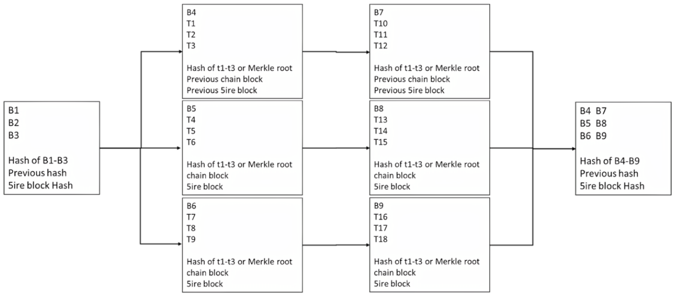

Fig. 2. Nested 5irechain

5.1 Transaction Pools

5ire ecosystem supports multiple chains that may branch out from the main chain and can progress separately only to be merged again in the future. This repeating process of creating smaller chains and merging them forms the base of the 5irechain and its scalabilty. In order to support this, the ecosystem uses multiple transaction pools. There is one transaction pool per chain having a unique serial number. A transaction is included in exactly one of these transaction pools. If there are n transaction pools, then a transaction tr will go to one of these pools depending upon the first $\log n$ bits of the hash value of public key of the sender in tr. That is to say that, if the numeric value of the first $\log n$ bits of the hash value of the public key of the sender in tr is k, then the transaction tr will go into pool k. Let, there be n distinct transaction pools. These pools have numbers between 0 and $n - 1$. When a new transaction T_x appears, it goes to the pool $F(T_x) \in [0, n - 1]$. Here,

$$F(T_x) = \sum_{i=1}^{\lceil \log n \rceil} 2^{\lceil \log n \rceil - i} \cdot I[256 - i]$$

and,

$$I[255:0] = \texttt{SHA-256}(PT_x)$$

Here, PT_x is the public key of the transaction sender.

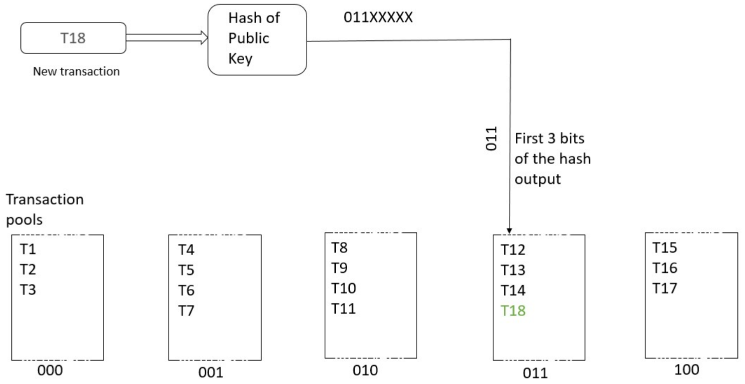

Fig. 3. Inserting Transactions into Multiple Transaction Pools

The process of adding transactions to transaction pools has been depicted in Figure 3. In this figure, there are five distinct transaction pools having ids between 000 and 100. A new transaction $T18$ appears in the network. First, the public key of the sender of the transaction is hashed using a standard hash function, e.g. SHA-256. Then the first three bits of the hash output is chosen. The transaction goes into the pool whose id matches the first three bits of the hash output. In Figure 3, the first three bits of the hash output is 011, hence, the transaction $T18$ is added to the pool 011. Figure 3 shows how the transactions will be stored in different pools based on the starting bits of the hash of transactions. This will allow us to validate the concurrent blocks without having overlapping transactions.

6 Block Verification

In every epoch, a group of nodes are selected for block assembly. These nodes are selected in a decentralized manner depending upon their total weights which are calculated from several parameters. The 5irechain ecosystem assigns slots to these nodes. Let us consider that in an arbitrary epoch, n nodes are selected for block assembly. These nodes are denoted as $V_1, V_2, \ldots, V_n$. The block scheduling algorithm allocates one slot of the epoch to exactly one of these nodes. Let us assume that in a particular slot j, a node V_i, $i \in [1, n]$ is assigned the task of block assembly. All other nodes $V_k, k \in [1, n], k \neq i$ perform as block attesters. Hence, the block assembled by V_i needs to be attested by at least η nodes from the set of attesters, that is, $\{V_k : k \in [1, n] \setminus \{i\}\}$. If at least η of the attester nodes attest the block assembled by V_i, it is accepted into the blockchain. In 5irechain, an epoch consists of many consecutive slots that are allocated to the nodes selected for block assembly. A particular node assembles the block for a particular slot, and all other nodes serve as attesters for that particular slot. This way all the nodes serve as both block assemblers and block attesters in an epoch. At the time of locking the stakes, each participating node selects a random $x_i \in_R \mathcal{Z}_p$, and computes $X_i = \texttt{SHA-256}(x_i)$. Each node V_i publishes X_i along with other transactions that enables participation in the race. Once the winning nodes are selected, they publish the values of x_i. Then all the x_is from the winning nodes are merged to yield a combined random number α. This α is used to allocate slots to the nodes using the block scheduling algorithm. This is shown in Figure 4.

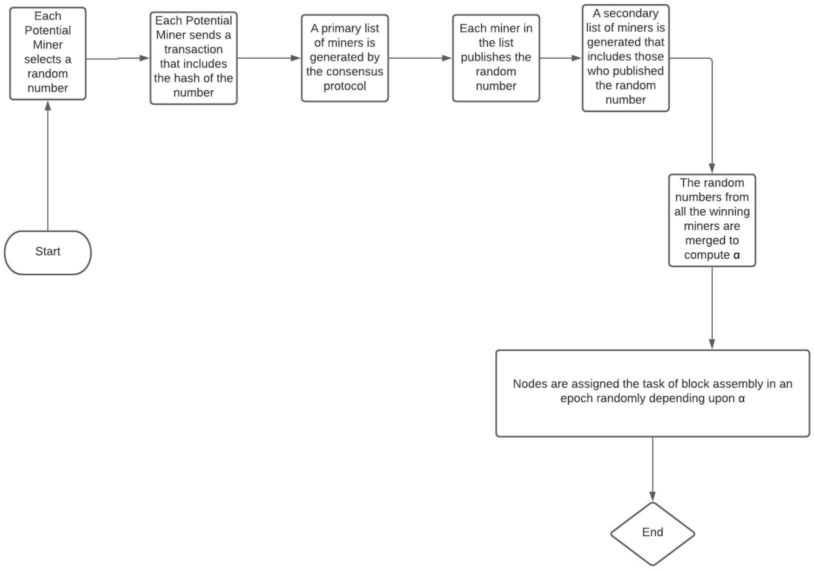
Each Potential Miner selects a random number
Each Potential Miner sends a transaction that includes the hash of the number
A primary list of miners is generated by the consensus protocol
Each miner in the list publishes the random number
A secondary list of miners is generated that includes those who published the random number
The random numbers from all the winning miners are merged to compute α
Nodes are assigned the task of block assembly in an epoch randomly depending upon α
Start
End

Fig. 4. Selecting nodes for verification of blocks

7 Hardware Root of Trust

5ire ecosystem ensures that all the nodes in the blockchain ecosystem establish a certain level of trust. We are introducing a hardware based root of trust based on Trusted Platform Module(TPM). A TPM device will allow the 5ire nodes to remotely attest the devices for any malicious code. TPM contains a key pair called Endorsement Key(EK). This is burned inside the TPM device at the time of manufacturing and even the manufacturer does not know the private key as it is generated inside the TPM device using a random seed. EK cannot be used directly to sign any piece of data, rather it is used to generated another key pair called the attestation key(AK). AK can be used to sign attestation data inside the TPM device. This data is stored into platform configuration registers(PCR). It is the hash of applications that start when the node starts and can help us identity malicious applications running on a node. 5ire blockchain will ensure that all the block assembling nodes participating in the network are running the similar applications when boot. 5irechain remote attesation architecture can be seen in 5. In a decentralised environment it is important that all participating nodes agree with the result of remote attestation of node, however everynode performing attesattion of every participating node will be a time and resource consuming job. Therefore, nodes in 5irechain will generate a collective challenge nonce to perform attestation of node. The process can be described as:

1. All nodes($N1, N2...Nn$) other than the proving node will generate a challenge nonce ($CN1, CN2...CNn$) and send it to proving node for generating a fresh attestation claim.
2. Proving node will generate $\oplus(CN1, CN2...CNn)$.
3. Proving node will ask TPM device to digitally sign freshly generated hash with current PCR values.
4. TPM will generate $Signature(hash(pcrvalues), \oplus(CN1, CN2...CNn)$
5. Proving node will send $Signature(hash(pcrvalues), \oplus(CN1, CN2, CNn)$ along with actual challenge nonce sent by nodes ($CN1, CN2...CNn$) to be added to blockchain.
6. Challenging nodes will $verify(Signature, hash(pcrvalues), \oplus(CN1, CN2, CNn))$ by generating the new $\oplus(CN1, CN2...CNn)$ to make sure that right challenge nonce was signed by the TPM

This claim will be valid for a fixed period, after which nodes will need to re-verify the state of node to other nodes on the blockchain. If a node is running malicious application or application that was not running when the node was setup then challenging nodes can agree to remove the node from the network and slash the stake.

8 5irechain in Post-Quantum Age

Blockchains rely on asymmetric key cryptography algorithms, namely Elliptic curve digital signature algorithm(ECDSA) for wallet addresses, signing

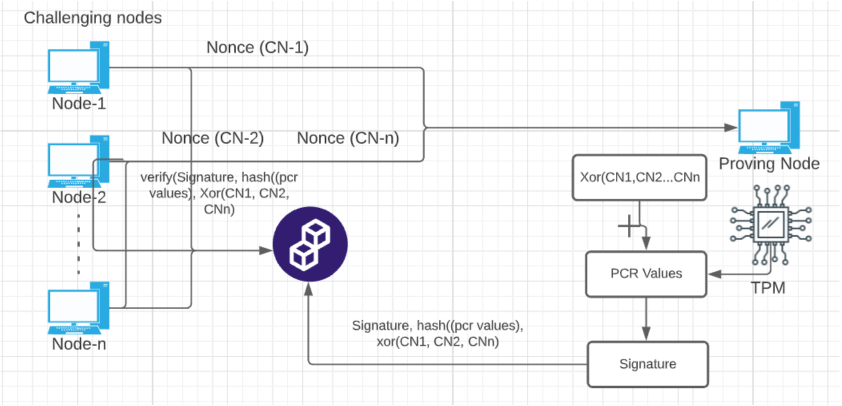

Fig. 5. 5irechain Remote attestation Architecture

transactions and validating new blocks. Therefore, one can say that existence of the blockchain is dependent on security of asymmetric key cryptography. ECDSA is based on a mathematical problem called discrete logarithm problem(DLP) [10]. Use of elliptic curves is being done in public key cryptography for a long time now. This is mainly because on a general elliptic curve there is no known sub-exponential algorithm to solve the discrete logarithm problem[15]. Lets fix a prime p. Let a, b be nonzero integers $(modp)$. The problem of finding x such that $a^x \equiv b(modp)$ is called the discrete logarithm problem (DLP).

It is believed that quantum computers with certain number of Qubits will be able to solve the discrete logarithm problem. An adversary can use Shor's quantum algorithms to attack these mathematical problems that underlie the public key cryptosystem. However, the most pertinent question is the amount of resources required for a quantum computer to break the cryptosystem. According to study done by Microsoft [10] a quantum computer would require 2330 logical qubits to be able to solve the elliptic curve discrete logarithm problem(ECDLP). At the moment IBM possess the quantum computer with most Qubits. It recently revieled the quantum chip with 127 Qubits [2]. IBM is currently in process of introducing the first ever chip with over 1000 Qubits by 2023. If successful, it will be the step closer to achieving the 2330 qubit chip required to solve the ECDLP problem.

Peter Shor[14] presented two polynomial time quantum algorithms, for each integer factorization and discrete logarithm in the finite field of prime order. Shore claims that a large enough quantum computer can break all existing public key cryptosystems using his proposed algorithms. Shor's algorithm proceeds as follows. First, two registers of length $n+1$ qubits are created and each qubit is initialized in the $|0>$ state. Then a Hadamard transform H is applied to each qubit, resulting in the state:

$$\frac{1}{2^{n+1}} \sum_{k,l=0}^{2^{n+1}-1} |k,l\rangle \tag{1}$$

Next, conditioned on the content of the register holding the label k or 'l', we add the corresponding multiple of P and Q, respectively

$$\frac{1}{2^{n+1}} \sum_{k,l=0}^{2^{n+1}-1} |k,l\rangle \rightarrow \frac{1}{2^{n+1}} \sum_{k,l=0}^{2^{n+1}-1} |k,l\rangle|[k]P + [l]Q\rangle \tag{2}$$

the third register is discarded and a quantum Fourier transform $QFT2n+1$ on $n+1$ qubits is computed on each of the two registers. Finally, the state of the first two registers – which hold a total of $2(n+1)$ qubits is measured. 5irechain aims to introduce a quantum safe protocol. We will introduce the quantum safe public key cryptography protocols for digital signature of transactions and block validation. We will introduce a hybrid digital signature algorithm based on elliptic curve(existing standard) and lattice based cryptography(quantum safe cryptography) to sign the transactions and validating the blocks. This will us keep financial and personal data of our customers safe from the advance cyber attacks in the age of quantum computers.

9 Proof of Identity

Most identification systems have massive, centralized databases with millions (if not billions) of records. These centralized datapage are highly valuable targets for hackers because of their sheer size. They are quite easy to steal and utilize because of the personal information they carry. Because the incentive for a successful breach grows exponentially in proportion to the number of identities in the database, it becomes increasingly vulnerable to attack as a database becomes larger. Furthermore, as opposed to many segmented, decentralized databases, a single big database generally indicates a single point of failure. Typically, centralized identity systems are maintained by a single party, which then utilizes third-party processors to access and handle the databases and data – frequently without enough controls and supervision making the databases even more vulnerable to data breaches.

Our approach to solving this is by using identity models that have spanned from blockchain technology - Self-Sovereign Security Model and Unique Digital Credentials using NFTs: people should be at the core of their identity management process (SSID). With ProofID, a blockchain-based SSID implementation with matching keys kept in a digital identity wallet, we may move away from traditional paper-based document systems and towards a digital identity with privacy, security, transparency, and individual rights.

5ire's ProofID is an identity system built on an open platform consisting of a technology stack with a free and open source identity wallet for the identity owner, a marketplace with real products and services available at launch, a JSON-LD (machine readable) protocol, connection to 3rd party identity micro services which comply with KYC laws and regulations.

ProofID overcomes the limitations of centralised identity systems, helps achieve compliance with the most comprehensive national data protection laws and KYC regulations, and returns ownership and control of identity data to the individual – the user – while providing tangible utility for the PID token through real world products and services.

9.1 How ProofID Works

On a personal device, a new user would simply download the ProofID Wallet program. On the device, identity data is saved locally. This information can be backed up to another device or a personal backup service. The ProofID wallet is empty when the user first downloads it. A public/private key pair (also known as a ProofID) is the first item a user needs to place in this container. This ProofID will serve as the user's digital "pen," allowing them to sign papers with their unique digital signature. Because the private key is only known by the identity owner, anytime this digital signature is used, it helps to verify and confirm the owner's identity to inquiring parties (without the need to present in person) anonymously and securely.

ProofID has a lot more to offer than just a login and password. Each ProofID is unique to the person who owns it. When a username/password combination is saved in a third-party database, a ProofID user will never disclose their private key; it will always be kept private. No one, even the ProofID foundation, would know that this was the user's container or that the ProofID number even existed at this point. It was generated entirely by the user and was not issued by any other organisation. This is exactly what self-sovereignty entails. ProofID may now be used in conjunction with identification proofs to obtain attestations from appropriate verifiers such as notaries, government agencies, and so on. The user is eligible to purchase items and services in the ProofID marketplace after they have attested identity claims contained in their digital wallet (covered in detail below). ProofID users must first make identity claims in order to take use of the products and services offered in the ProofID marketplace. The user's qualities (e.g. nationality, date of birth, occupation, etc.) are recorded in text fields as identity claims (JSON-LD blobs). Photos or scans of papers may be saved to save time manually typing data into these text boxes, and optical character recognition will automatically interpret the information, making the procedure much easier. These proofs of identification are only required to meet standard KYC documentation requirements. ProofID's digitally signed attestations will eventually replace identification documents as we know them. The next stage in the procedure is to receive attestations for the identity claims that have been generated. Affidavits can also be saved in the ProofID wallet. These attestations are machine-readable, digitally signed identification assertions that can be valid for a set period. Users' claims may be signed by verifiers or appropriate authorities such as utility companies, notaries, banks, passport agencies, hospitals, driving licence authorities, and immigration. These claims might be signed in such a way that just the most basic information is disclosed. In other words, the identity owner can only tell the asking party what they need to know. For example, a user may simply demonstrate that they live in a specific nation. Alternatively, a person may be able to demonstrate that they are above the age of 18" without divulging any further information. These identification traits are limitless and may include everything from "professional investor" to "entrepreneur." The owner of the identification will be able to pick which information to share with any reliant party. The number of different types of identity claims that may be verified is practically limitless.6 shows the data flow diagram of ProofID.

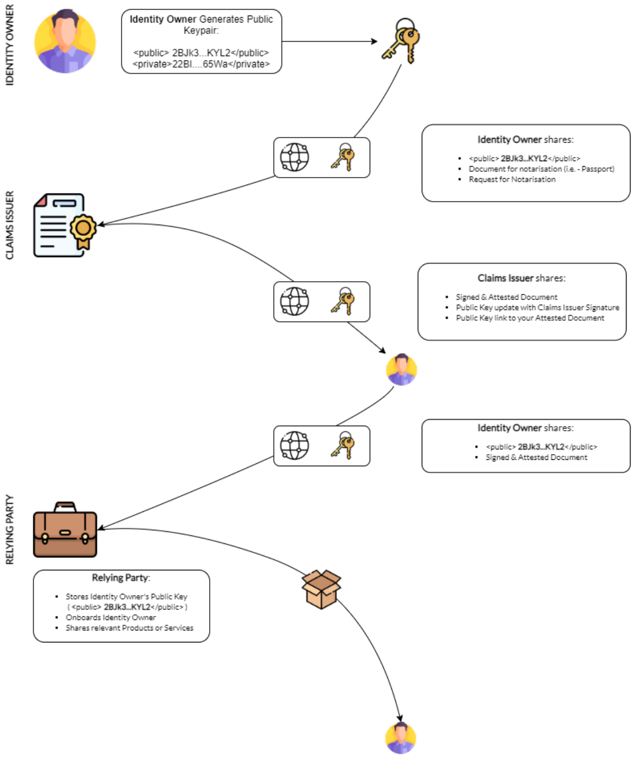
IDENTITY OWNER
Identity Owner Generates Public Keypair:
<public> 2BJk3...KYL2</public>
<private>22BI....65Wa</private>
Identity Owner shares:
<public> **2BJk3...KYL2**</public>
Document for notarisation (i.e. - Passport)
Request for Notarisation
CLAIMS ISSUER
Claims Issuer shares:
Signed & Attested Document
Public Key update with Claims Issuer Signature
Public Key link to your Attested Document
Identity Owner shares:
<public> **2BJk3...KYL2**</public>
Signed & Attested Document
RELYING PARTY
Relying Party:
Stores Identity Owner's Public Key (<public> **2BJk3...KYL2**</public>)
Onboards Identity Owner
Shares relevant Products or Services

Fig. 6. ProofID Workflow

Data is saved on a device (under the owner's control, like how papers are now stored at one's home or workplace), and the owner can authorise a third party to acquire particular data when they wish. This may be accomplished by confirming a notice on the device in question. This feels comparable to "linking" a Facebook account for authentication. Instead of travelling to Facebook's servers to acquire personal data, a user will approve requests from their personal data store, giving them granular control over what information is shared.

It is safer for both the identity provider and the dependent party to reduce the quantity of data that has to be given. The identity owner does not communicate superfluous or sensitive information, and the receiver is not required to keep it. This aids in both security and adherence to privacy laws in various jurisdictions.

5ire aims to use ProofID as one of the weighted factors to allow nodes with smaller stakes to assemble more blocks. This is because ProofID establishes a layer of trust on the node in the network. ProofID will also be used for 5ire wallet where 5ire will link identity of the user with the wallet and enable users to access funds through identity or phone number associated with the account.

References

1. Polkadot: Vision for a heterogeneous multi-chain framework. 2016.
2. Philip Ball. First quantum computer to pack 100 qubits enters crowded race, Nov 2021.
3. Vitalik Buterin. Ethereum white paper: A next generation smart contract & decentralized application platform. 2013.
4. Yongle Chen, Hui Li, Kejiao Li, and Jiyang Zhang. An improved p2p file system scheme based on ipfs and blockchain. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 2652–2657, 2017.
5. Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. In Walter Fumy, editor, *Advances in Cryptology — EUROCRYPT '97*, pages 103–118, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.
6. Marie Huillet. Bitcoin will follow ethereum and move to proof-of-stake, says bitcoin suisse founder. `https://cointelegraph.com/news/bitcoin-will-follow-ethereum-and-move-to-proof-of-stake-says-bitcoin-suisse-founder`, April 2020.
7. Ezra Kaplan. Cryptocurrency goes green: Could 'proof of stake' offer a solution to energy concerns? `https://www.nbcnews.com/tech/tech-news/cryptocurrency-goes-green-proof-stake-offer-solution-energy-concerns-rcna1030`, May 2021.
8. Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7:117134–117151, 2019.
9. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.
10. Martin Roetteler, Michael Naehrig, Krysta M Svore, and Kristin Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 241–270. Springer, 2017.
11. Fahad Saleh. Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies*, 34(3):1156–1190, 07 2020.
12. Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, nov 1979.

13. Virinder Sharma, Victor Orindi, Ced Hesse, James Pattison, and Simon Anderson. Supporting local climate adaptation planning and implementation through local governance and decentralised finance provision. *Development in Practice*, 24, 05 2014.
14. Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.
15. Nigel P Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of cryptology*, 12(3):193–196, 1999.
16. Ikuya Takashima. Litecoin: The ultimate guide to the world of litecoin, litecoin crypocurrency, litecoin investing, litecoin mining, litecoin guide, cryptocurrency. 2018.