Whitepaper

Re-engineering Technology Interconnectivity

Table of Contents

1. Blockchain

A blockchain can be perceived as a four-dimensional continnumum that has three horizontal layers including transaction and blocks, consensus, computing interface, and governance on one vertical layer.

1.1 Transaction and Blocks

As the lowest level layer, marked exchanges have slandered among all hubs, and blocks are created by full hubs. This is the establishment of blockchain where moving of advanced resources (in this manner the innate qualities) and record security are accomplished through crypto natives like elliptic bend signature, hash capacity, and Merkle tree.

1.2 Consensus

The center level layer shows the distributed idea of the blockchain, where all hubs inside the organization arrive at agreement on all inner states on-chain by means of strategies like Proof of Work (PoW), Proof of Stake (PoS) and their variations, and so forth. The agreement layer influences adaptability the most. PoW is normally thought to be less versatile when contrasted with PoS. Also, this layer intensely impacts security as far as two-fold spending and different assaults centered on changing the blockchain states in an unforeseen manner.

1.3 Computing Interface

The initial two level layers structure the state of a blockchain while Computing Interface layer is basic to make a blockchain helpful, which includes extensibility. For example, shrewd agreement has been carried out by Ethereum to empower programmability where one could depend on the appropriated "world computer" for executing the particulars of an agreement. Sidechain, along with blended mining, has additionally been grown seriously to help programmability. Second-layer protocols like the Polygon , state channel have been created to expand the adaptability of a blockchain at this layer. What's more, apparatuses, SDKs, systems, and GUIs are additionally critical to ease of use. The Register Interface layer gives designers the ability to create decentralized applications (DApps), a fundamental piece in making the blockchain helpful and significant.

1.4 Governance

Similarly as with organic entities, the best blockchains will be those that can best adjust to their surroundings. Expecting these frameworks need to advance to endure, the underlying

configuration is significant, yet over a long sufficient timeline, the systems for change are generally significant, which is known as the upward layer administration.

There are two basic parts of administration:

• Motivator: Each gathering in the framework has its own impetuses. Those impetuses are not generally 100% lined up with any remaining gatherings in the framework. Gatherings will propose changes after some time that are worthwhile for them. Systems are one-sided towards their own endurance. This generally shows in changes to the reward structure, money related arrangement, or perceived leverages.

• Coordination: Since it is far-fetched all gatherings have 100% motivating force arrangement by any means . The capacity for each gathering to facilitate around their normal motivating forces is basic for them to influence change. A main consideration is how much coordination should be possible on-chain (e.g., votes to the principles of a framework like Tezos , or even roll back the record if greater part partners don't like the change) versus off-chain (like Bitcoin Improvement Proposition (BIPs)).

1.5 Models

Blockchains can be sorted as missioned and requested of relying upon how it is worked. For instance, Bitcoin is missioned implying that anyone can make a location and start cooperating with the organization, which is "fabricate trust from trustless". Interestingly, the requested of blockchain is a shut and checked biological system where the entrance of every member is characterized and separated dependent on job, which is "fabricate trust from less trusted". There are advantages and disadvantages to each approach. Not withstanding, this load of contemplations reduce to essential plan compromises among trust, adaptability, calculation, and intricacy. For instance, Bitcoin and Ethereum are blockchains assembled on top of trustless hubs since versatility is unequivocally wanted. Thus, either part of calculation is required (on account of PoW) or a more refined agreement system is required.

2. Internet Of Things

The Internet of Things (IoT) is evolving as an expression of society's interconnecting network vision. However, It is only the start of a bigger movement. The quantity of associated IoT gadgets is expected to develop by 21% every year, ascending to 30 billion by 2025 , and the worldwide market of IoT is relied upon to develop from 389 billion USD in 2020 to 1.6 trillion USD by 2025. Although venture specialists and invigorated buyers support IoT as the following modern revolution, there are three major issues preventing the widespread development and implementation of IoT.

2.1 Scalability Problem

Most of IoT gadgets are associated and controlled in a concentrated manner as of today. IoT gadgets are associated with back-end foundations on open cloud administrations or on-premise server homesteads to send information and get control orders. At present, the size of IoT is bottlenecked by the adaptability and flexibility of these back-end foundations, servers, and server farms. The generously high working cost of running the size of IoT is probably not going to be covered by the benefit from selling gadgets.

2.2 Lack of Privacy

IoT is relied upon to empower mass support of end-clients on strategic administrations like energy, portability, lawful and popularity based solidness. Protection challenges start from the way that IoT associates with the actual world aberrant and programmed ways. Also, the measure of information gathered will increment significantly when it increases.

A few of the normal security dangers, as listed are:

1. Recognizable proof: Partner a (industrious) identifier, e.g., a name and address or a alias of any sort, with a person;

2. Restriction and following: Acquire a singular's area through various implies;

3. Profiling: Order data dossiers about people to induce interests by relationship with different profiles and information sources;

4. Protection disregarding network: Passing on private data through a public medium and in the process uncovering it to an undesirable crowd;

5. Life cycle changes: Gadgets frequently store enormous measures of information about their own set of experiences all through their whole life cycle that could be spilled during changes of control in a gadget's life cycle;

6. Stock assault: The unapproved assortment of data about the presence, attributes of individual things, e.g. Robbers can utilize stock information to really take a look at the property to figure out a protected opportunity to break in;

7. Linkage: Connecting diverse recently isolated frameworks with the end goal that the blend of information sources uncovers (honest or mistaken) data that the subject didn't uncover to the recently confined sources and, above all, didn't have any desire to uncover. This load

of normal protection dangers are because of information spill at the gadget level; or, information spill during correspondence; or, all the more regularly, information spill by unified networks.

2.3 Functional Values

Most existing IoT arrangements need significant worth to be created. "Being associated" is the most utilized offer. Nonetheless, essentially empowering network doesn't make a gadget keen or helpful. A more noteworthy part of the worth that IoT produces comes from connection, participation, and in the long run independent coordination of different technologies. A couple of good analogies are that singular cells collaborate to fabricate multi-cell creatures, creepy crawlies fabricating social orders, people assembling urban areas and states. By participating, this load of people join to construct something that has more value worth than their own. 85% of heritage gadgets need capacity to associate or help out one another because of similarity issues. The information sharing for business and functional bits of knowledge is almost inconceivable.

3. Benefits and Challenges of Blockchain and IoT

Detecting and discernment, change and transmission, and handling are the embodiment of most smart things on this planet. For IoT, while the detecting and discernment layer is unexpectedly dispersed, the last two are not for the time being, which is the root for most adaptability, protection and extensibility issues. We imagine blockchain innovation, as the spinal cord and sensory system of IoT, as the best possibility to address the previously mentioned IoT-explicit issues.

3.1 Benefits

By embracing blockchain innovation, IoT promptly profits by the accompanying angles on account of blockchain's properties including decentralization, Byzantine issue resistance, straightforwardness and changelessness.

3.1.1 Decentralization

Decentralization liberates clients and gadgets from controlled and predictable observation, along these lines to some degree tending to the protection concern forced by brought together gatherings who corner the market and attempt to see each part of client/gadget for their own advantages, e.g., promoting. Decentralization, under the setting of crypto economy, likewise designates "versatility" that is frequently characterized as "how much a framework can adjust to responsibility changes by provisioning and de-provisioning assets

in an autonomic way, to such an extent that at each point in time the accessible assets match the current interest as intently as could be expected". A blockchain and the fundamental crypto-economy can be planned in a manner that is sufficiently flexible and savvy enough for IoT situations and applications. For instance, more blockchain hubs could be turned up if the organization has sufficient calculation errands with enough motivations to perform.

3.1.2 Transparency

Blockchain gives cryptographic confirmations that the information secured on the chain is continously prompt and permanent, which can be helpful in numerous situations, e.g., anchor conditions of the IoT world on the blockchain for the reason of inspecting, authentication, criminological investigation, verification and approval.

3.1.3 Programmability

Bitcoin accompanied essential programmability to permit an exchange to succeed provided that the basic content is executed effectively. This programmability can be and ought to be reached out to IoT gadgets, some of which as of now just have basic and hard-coded rationale that can't be additionally customized once delivered.

3.2 Challenges

3.2.1 Native Privacy Is Not Enough

Local protection ensures from the blockchain can just assist with tending to the security torment point in IoT to the extent that it holds information on the chain instead of incorporated servers, utilizing pseudonymity. In any case, in case a gadget's alias at any point connected to its personality, all that it could possibly do under that alias currently be connected to it.

3.2.2 Heavy Operations

In the IoT world, numerous gadgets are considered as feeble hubs since they are:

• Unequipped for performing PoW-based mining because of the force and calculation requirements;

• Not ready to store huge amounts of information (e.g., gigabyte level, not referencing terabyte-level and petabyte-level) because of the force and capacity requirements;

• Not ready to confirm all exchanges by handling the entire blockchain;

• Not ready to associate with peers constantly, contingent upon its uptime and availability quality.

4. IOTEN Design and Architecture

4.1 Design Principle

IOTEN means to turn into the security driven and versatile sensory system for IoT. To accomplish this and to address the previously mentioned difficulties, our engineering configuration has the accompanying standards.

4.1.1 Separation of Duties

Straightforwardly associating all IoT hubs into one single blockchain is a fantasy that can't become valid. Other than the way that diverse IoT applications require in a general sense diverse capabilities of a blockchain, facilitating each IoT hub on one blockchain makes it fill quick in size and calculation, and at last become too heavyweight for some IoT gadgets. All things considered, partition of obligations ensures each blockchain cooperates with a particular gathering of IoT hubs, and, simultaneously, collaborates with other blockchains when required. This is practically equivalent to the web – heterogeneous gadgets first structure an intra-associated bunch, intranet. More modest intranets can additionally shape a bigger intranet, which in the end associates with the foundation of the web and speaks with one another. "Division of obligations" typically makes an even framework to augment both productivity and protection.

Each blockchain has various utilizations and applications and ought to be planned and streamlined toward various headings. For instance, a blockchain that is committed to transferring exchanges between its subchains don't have to have complete contract running on top of it; one more blockchain that associates gadgets in the equivalent trust zone ought not think often about value-based security to an extreme.

4.1.2 IoT Friendly

As previously mentioned, the IoT world is brimming with heterogeneous frameworks and hubs, more grounded or more vulnerable as far as their assets of calculation, stockpiling, and force. Since tasks that should be possible by frail hubs can be effectively finished by solid hubs, activities on the chain ought to be planned and enhanced for frail hubs, i.e., tasks ought to be sufficiently lightweight to preserve assets like calculation, stockpiling, and energy.

4.2 Blockchains in Blockchain

IOTEN is an organization of numerous blockchains that are progressively orchestrated, where numerous blockchains can run simultaneously with each other while holding interoperability. In the IOTEN world, the root blockchain oversees numerous blockchains or subchains. A subchain associates with and interfaces with IoT gadgets that share something in like manner, e.g., they have a comparative useful reason, work in comparative conditions, or offer a comparative degree of trust. On the off chance that a subchain doesn't work well, e.g., being assaulted or encountering programming bugs, the root chain is totally unaffected. Likewise, cross-blockchain exchanges are upheld to move worth and information from subchains to the root chain or from one subchain to another by means of the root chain.

The root blockchain is a public chain available by anybody, which has three primary targets:

- **Relay** rate and information across subchains in a protection saving way of empowering interoperability among subchains
- **Supervision** of subchains, e.g., punish the reinforced administrators of subchains by bond seizure
- **Settlement and securing** of installments and trust for subchains.

With these characterized destinations, the root chain explicitly centers around adaptability, security protecting capacities and the capacity to coordinate subchains. A subchain, then again, might actually be a private blockchain and depends on the root bind as a hand-off to connect with other subchains. A subchain wants adaptability also, extensibility to adjust to enhanced prerequisites of various IoT applications. A subchain is reasonably run by administrators whose job is dependent upon an adequately high bond being saved on the root chain. Alternatively, the framework permits administrators to choose at least one administrator to represent it with or without additional bond. The administrator goes about as a light customer on the root chain, and a full hub on the sub-chain to seal new Blocks.

4.3 Root Blockchain

The root blockchain utilizes UXTO-based model as Bitcoin and Monero for the following reasons:

• Exchange requesting becomes trifling without the requirement for nonce or arrangement numbers, which places negligible requests on agreement conspires and permits exchanges to be handled in equal;

• Applying existent security saving procedures like ring mark, and z-SNARKs for concealing sender, collector and exchange sum become conceivable.

The root blockchain is made out of hash-connected Blocks, and a Block is created of a header that connects to the past block and a rundown of exchanges. The root chain permits essentially two kinds of exchange: (1) fundamental exchanges including P2PKH, P2SH, Multisig and so forth, and progressed exchanges that empower cross-blockchain tasks like BondedRegistration, Lock, ReLock, Reorg and so on. Approved exchanges are added into a Block that has a unique size, upper-limited by 8MB. A Block is created like clockwork by our agreement plot as point by point in the following segment. The root anchor is intended to be non-Turing complete with the backing of a stack-based content and a rich arrangement of opcodes

4.4 Subchains

IOTEN accompanies a structure for creating and provisioning a custom-made subchain for decentralized IoT applications by typifying low-layer natives like tattle protocol and agreement component. IOTEN subchains utilize a record based model, which is better for following state changes. There are two sorts of records, normal records, and contracts. Legitimate exchanges are added into the Block, which is created by something similar agreement plot as the root chain to accomplish a similar level of absolution to make cross-blockchain correspondence more productive. Subchains either utilize the root chain's token, IOTEN token or characterize their own token. The token characterized by engineers on subchains can be circulated freely by token deals or trading on open exchanged trades. An agreement is upheld by subchains and runs on top of a lightweight and effective virtual machine. Different choices are additionally being investigated. With a private agreement, IoT gadgets associated with the equivalent subchain use the common state in two ways,

• First, gadgets can cooperate with the environment on their subchains' states, e.g., lights turn on and off without help from anyone else dependent on a "clock state" on the subchain;

• Then again, gadgets can change the state on subchains when the physical state changes, e.g., indoor regulator refreshes temperature by means of contract in view of its sensor information.

4.5 Cross-Blockchain Communication

Cross-blockchain correspondence is relied upon to be utilized with high recurrence in IoT applications. There is consistently the requirement for an IoT gadget in a subchain to organize with one more gadget in an alternate subchain. Once more, restricted by IoT gadgets' low calculation and capacity impression, we are inspired to configure cross-blockchain correspondence in a quick and practical manner.

4.5.1 Pegging and block Finality

Pegging is a system for scaling the Bitcoin network through sidechains. It vigorously depends on Simplified Payment Verification (SPV) , and permits Bitcoins to adequately "move" from the Bitcoin blockchain to the sidechain also, back. The fundamental thought is basic: Tokens are shipped off an exceptional location to be secured on the Bitcoin blockchain; when this Lock exchange has been affirmed, one sends Reorg exchange to the sidechain remembering the Lock exchange and verification of incorporation for the type of a Merkle branch. The sidechain utilizes SPV to check the Reorg exchange and, in case it is approved, makes similar measure of tokens and sends them to an ideal location on the sidechain. Starting today, fixing fills in as a crude for practically all cross-blockchain correspondence protocols, e.g., Universe, Lisk, Rootstock. Two separate fixing streams can be effectively coupled together to make the purported Two-Way Fixing (2WP) to make move tokens to and from.

Block finality is the assurance that the new Block produced is conclusive and can't be changed. Block finality impacts the substantial execution of fixing considerably as one needs to delay until block certainty is accomplished (essentially with high flexibility) on the sending blockchain prior to mentioning to Reorg. Most open blockchains like Bitcoin try not to have block finality. The getting blockchain can just get a probabilistic confirmation, e.g., as more PoW diggers affirm an exchange, it is more plausible the exchange has been acknowledged. Using a finishing agreement resolves this issue since the getting chain has affirmation with one Block affirmation on the sending blockchain. For IoT applications, cross-blockchain moving of worth and information is expected to be quick and low fee, which requires a concluding agreement instrument on both root chain and subchains. IOTEN agreement accomplishes instant block finality, itemized in the following segment.

4.5.2 Cross-Blockchain Communication Protocol

We should survey the protocol at an undeniable level . Let’s say person named Mark on subchain 1 wishes to dispatch an exchange to a location named Craig on the subchain 2, and each of the three blockchains utilize a similar sort of token without an exchange expense for effortlessness. Note that by applying fixing gullibly, four exchanges are expected to make a "remote call" from subchain 1 to subchain 2 through root chain, i.e., (1) a Lock exchange

on subchain 1; (2) a Reorg exchange against root chain; (3) another Lock exchange on root chain; and (4) one more Reorg exchange against subchain 2. This interaction demonstrates Craig needs to sit tight for something like 4 Blocks to acknowledge this "remote call", and information this "remote call" conveys should be put away on each of the three blockchains, which makes it slow and costly. We intend to improve this interaction by brushing (2) and (3) into one ReLock exchange, which speeds up the whole cycle as well as tries not to store information on subchain 1 and the root chain.

IOTEN cross-blockchain protocol has the accompanying advances.

1. Each subchain is enrolled on the rootchain by presenting an exchange called Bonded Registration to the rootchain, including its chain name, chain ID, setup, beginning Block, and selection of administrators; This is a one-time process;

2. At the point when Mark wishes to dispatch an exchange to Craig, he starts a Lock (X, H(D), F/T) exchange where X is the quantity of tokens, H(D) is the hash of the information D to be connected, F/T shows the from and to addresses including IDs for the two chains;

3. When the Lock exchange has been remembered for subchain 1, Mark starts ReLock (X, H(D), F/T, S, P) exchange to the rootchain by including X, H(D), F/T, some current details of subchain 1 are indicated as S just as confirmation of-incorporation P that incorporates Merkle parts of ongoing Block headers and Merkle branches demonstrating Lock exchange has been incorporated;

4. The rootchain approves ReLock exchange and acknowledges it by remembering it for the most recent Block, and makes X tokens and secured them an uncommon location;

5. When ReLock exchange has been remembered for the root chain, Mark communicates a Reorg (X, D, F/T, P') exchange on rootchain's organization with X, D, F/T and another confirmation of-incorporation P' that demonstrates the consideration of ReLock exchange;

6. Administrators of subchain 2 become mindful of Reorg exchange, and they approve furthermore, make similar measure of tokens on subchain 2 and send them to address Craig with D related.

4.5.3 Sharing Bandwidth

One potential concern with respect to cross-blockchain correspondence is that a malevolent subchain spams the rootchain or another subchain by sending over a gigantic measure of cross-blockchain exchanges that depletes other blockchains' ability. One way of alleviating

is to let each subchain bid for its portion and "rate-limit" exchanges from a subchain if its standard is depleted.

One can characterize a standard dependent on the extra room inside one Block. Accepting Block size is 8MB greatest, and 4MB is saved for ordinary exchanges occurring on the rootchain, and 4MB is saved for all cross-blockchain exchanges, which is additionally isolated into, say 4096 quantity pieces with every share piece to be 1KB. A subchain offers for n portion pieces (with a specific upper bound) as per the expected utilization by putting down a store corresponding to n. At each round, simply up to nKB can be utilized inside another Block for exchanges from this subchain and each such exchange is charged a "data transfer capacity" expense from the store (to compensate excavators who help to uphold this rule); remaining exchanges are lined up and ultimately dropped when break. The standard distribution could be dynamic as in it gets changes when the rootchain develops, as displayed in Figure 3. On the off chance that one subchain spams others, it wears out its stores at a high speed and in the end loses the quantity. Then again, if one subchain puts down a major store only to hold a major piece of transfer speed without really utilizing it, the rootchain will have a component to discount part of the store dependent on the proportion between the normal number of exchanges per block and the saved transmission capacity, which assists with settling the held transfer speed near the real utilization.

5. Fast Consensus with Instant Finality(DPoS)

5.1 Proof of Work

Proof of work (PoW) is the main driver in arriving at the worldwide agreement of most blockchains, including Bitcoin and Ethereum. PoW makes it computationally hard to build a legitimate hinder and append it to a blockchain. The more extended the blockchain turns into, the harder it is to invert any exchange recorded already by the blockchain. To control the blockchain, an aggressor needs to possess 51% of the entire calculation force of a PoW-based blockchain network.

In spite of the fact that PoW gives an exquisite answer for the worldwide agreement of huge circulated blockchains, it has a few intrinsic disadvantages. The general calculation cost to keep up with the worldwide agreement is a similar expense of the 51% assault. This implies that regardless of whether most of the blockchain members are straightforward, they actually need to utilize a ton of power to keep up with the blockchain, which isn't reasonable for the climate of IoT networks that typically favor energy productivity. Likewise, fair and Block of individual gadgets, processing PoW ordinarily costs a great deal of CPU cycles and memory use, which presents troublesome prerequisites to the equipment assembling and

expenses of installed IoT gadgets. Last yet not rent, PoW doesn't give block finality which is a basic property needed to develop proficient cross-chain correspondence.

5.2 Proof of Stake

Proof of Stake (PoS) was proposed as a proficient option in contrast to PoW for blockchains arriving at agreement, which plans to stay away from the previously mentioned issues of PoW. The fundamental thought of PoS is that a haphazardly picked set of hubs vote on the following Block, and their votes are weighted dependent on the size of their stores (for example staked amount). On the off chance that certain hubs make trouble, they might lose their stores. Along these lines, without computationally concentrated PoW, the blockchain can run considerably more effectively, and can accomplish a monetary solidness: The more stake a member has, the more motivator the hub needs to keep up with the worldwide agreement, and the more uncertain the hub gets rowdy. There are a few public PoS plans and executions, for example, Tendermint that has been taken on by IOTNmerous applications.

5.3 Delegated Proof of Stake (DPoS)

Delegated Proof of Stake (DPoS) refines the possibility of PoS in the way that DPoS permits members to pick a few agents to address their segments of stakes in the organization. For instance, Adam can make an impression on the organization to give Mark the capacity to address her stake and decision in the interest of her. DPoS offers a few advantages for our IoT applications:

• Small players can pool their stakes to have a higher possibility together to take part in block proposing and casting a ballot, and offer the prizes thereafter.

• Resource-obliged hubs can pick their agents, so not every one of the hubs need to remain online to add to agreement.

• Delegates can be the hubs with solid force supply and organization conditions, and furthermore can be picked powerfully and arbitrarily, so we will have a higher by and large accessibility for the organization arriving at agreement.

5.4 Practical Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance (PBFT) was proposed by Castro and Liskov in 1999 as an effective and assault safe calculation for agreeing in a appropriated non-concurrent network. We intend to utilize PBFT for the basic democratic calculation of our DPoS agreement component, since it is a compact and very much concentrated on calculation that gives fast

irrevocability that is basically significant for building a productive and attractive blockchain. As shown in Castro and Liskov's unique paper, PBFT offers both accessibility and security if probably 33% of the organization hubs are broken or pernicious, and the organization cost of PBFT is extremely least, for example around 3% contrasted with an unreplicated network framework.

The average digital currencies dependent on PBFT incorporate Stellar and Zilliqa .

5.5 Randomized Delegated Proof of Stake (Roll-DPOS)

To have a quick and productive agreement system with moment block certainty in the setting of IoT, we join the ideas of DPoS, PBFT and Verifiable Random Capacities (VRFs). VRF was first presented by Micali et al. in [19] and is a family of capacities that can deliver openly irrefutable confirmations for the rightness of their irregular yields. At an undeniable level, our proposed Roll-DPOS has four stages choose up-and-comers, structure advisory group, propose hinder and finish block

- **Elect Candidates**

All nodes in the IOTEN Network could take part in this stage as far as deciding in favor of the board of trustees' applicants. To urge hubs to cast a ballot, the framework ensures the delegates share fashioned awards with their electors. The applicants structure a bunch of in any event 97 representatives; this number will increment in the future to additionally keep away from the centralization of the mining power. When the applicants are chosen, they will be fixed in one age, which is reliable of 47 emphases.

- **Form Committee**

In every cycle, an irregular board of size 11 is chosen from the up-and-comer pool utilizing VRF for making blocks in the following 11 rounds. The thought is to utilize the hash of the block in the last emphasis and the hub's private key as contributions to the VRF to create a Boolean yield showing in case one is chosen as the council part, a need showing one's structure to propose block, and a proof demonstrating one's capability for proposing the Block at a sure round. The utilization of VRF is significant as it gives a non-intelligent way of arranging all representatives for proposing blocks in a decency and secure way.

- **Propose Block**

In each round (which is generally at regular intervals), each board hub proposes another Block and broadcasts it to the organization, along with the need and the verification. Just

the Block proposed by a board of trustees' hub with the most elevated need and has not been proposed in a similar emphasis is considered by different hubs, which is called an up-and-comer block.

- **Finalize Block**

In the equivalent round, any remaining hubs use PBFT to decide in favor of/against the competitor block. If more than 2/3 panel hubs concur applicant Block's validness, it is concluded and is added to the blockchain by everybody in the organization. From that point forward, the proposed block what's more, settle block are executed in the following round; if the current cycle wraps up, one more irregular council will be shaped before the proposed block and finished Block are executed.

5.6 Creating Periodic Checkpoints for Light Clients

In IoT organizations, we expect a great deal of gadgets be light customers, which are the blockchain members that don't record the full exchange history locally. Considering the capacity overhead of the full blockchain, e.g., over 100GB for Bitcoin, many installed minimal expense IoT gadgets might not have the ability to download the full blockchain. Nonetheless, these light customers actually have capacity to rapidly check the accuracy of the blockchain and collaborate with it - the plan is remembered for Satoshi's unique Bitcoin whitepaper [21]. Nonetheless, utilizing PoS rather than PoW has a hindrance for light customers. When checking accuracy of PoS based blockchains, customers need to download a rundown of public keys and marks for block proposers and electors, and the arrangements of Block proposers what's more, electors might change for each Block. Along these lines, when light customers return on the web subsequent to remaining disconnected for some time, the customers might have to download an enormous number of public keys and marks, and afterward confirm every one of them. To moderate this exhibition issue, Vitalik, the creator of Ethereum, has proposed making occasional designated spots on the blockchain, called epochs, for instance each 50 Blocks. Every designated spot can be confirmed dependent on the past designated spot, with the end goal that light customers can get up to speed with the entire blockchain a lot quicker.

6. NETWORK SECURITY

In the organization, there are numerous re-encryption hubs which apply access the board arrangements. Intermediary re-encryption permits IOTEN to part the trust between access the executives and decoding freedoms, without presenting a consistently online consistently confided in substance (like a conventional key administration framework). Excavators never

see plaintext information, or anything which permits them to unscramble the information. They are exclusively answerable for putting away re-encryption keys and applying re-encryption capacities. The primary danger of this model is arrangement between a digger and a peruser of the information. On the off chance that the excavator gives the peruser re-encryption keys for the information, the information can be unscrambled whenever by the information peruser, bypassing any restrictive or on the other hand time sensitive limitations. We balance this danger in more than one way: utilizing split-key edge re-encryption plot Umbral to decentralize trust between various diggers, permitting beneficiaries of the information to demonstrate accuracy or mistake of re-encryption to the next network by including check convention into Umbral, making the convention sensibly pseudo-unknown. Likewise, we apply monetary motivating forces for reasonable activity, depicted in Sec. VII.

The subsequent danger is hubs breaking down (returning phony information as opposed to performing re-encryptions). We settle this issue utilizing a test convention.

The third danger is hubs intriguing with one another to perform half assaults. This danger is generally dangerous for multi-party calculations , (for example, Puzzle). In any case, for our situation the aggressor just gains the capacity to illegitimately apply re-encryption arrangements, not to unscramble information nor to give admittance to a been conceded client admittance to the information.

Preferably, the framework ought to be just about as decentralized as could be expected, but half assaults don't think twice about privacy of the information, very much like half assaults in verification of-work cryptographic forms of money don't enable an aggressor to move reserves.

6.1 Split-key re-encryption

Envision that a re-encryption hub chooses to re-scramble information quickly as opposed to applying restrictive arrangements as trained. A split-key intermediary re-encryption plan can be utilized to tackle this issue.

Rather than one re-encryption key, m-of-m re-encryption keys can be utilized to deliver "re-encryption shares." These offers can be consolidated customer side. A m-of-m plan exists for AFGH encryption. An agreement assault here would require m excavators and the peruser of the information. In any case, AFGH-based plan is helpless against forswearing of administration assault in light of being m-of-m.

An edge based m-of-n plot (Umbral) seems, by all accounts, to be significantly more fitting for this undertaking. This plan likewise can permit an outsider to confirm rightness of re-encryption, which is significant for keeping the hubs legit. The upsides of m and n can be chosen dependent on execution versus security compromises by the customer while re-encryption hubs don't authorize a specific upsides of m what's more, n.

6.2 Pseudo-secrecy

It is profoundly valuable for the security of the framework that re-encryption hubs don't have the idea what it is they are re-encrypting. This keeps them from knowing which re-encryption keys to perform plot assaults on (and attempting to connive with all the organization members is infeasible when the organization is decentralized).

Our convention is at first pseudo-anoynm, for example it doesn't store characters of any member. Right off the bat, the re-encryption plan ought to be key-private. If not, it would be feasible to decide the responsibility for key by emphasizing over sets of all the realized public keys. Also, the re-encryption hub and the beneficiary of the information ought not have a similar identifier for a similar re-encryption key.

This standards out a basic method of putting away a re-encryption key in a key-esteem store while the beneficiary can concoct the key.

6.3 Challenge convention

There is a danger of excavators returning arbitrary numbers rather than accurately re-scrambling information. Since the information is

private, clients of the framework can't distribute this information and their key as verification that the excavator has cheated.

It is inconceivable for a digger to recognize a "genuine re-encryption" and a re-encryption of irregular information. Thus, we can create various "counterfeit" re-encryption keys which are planned explicitly to challenge the diggers. If a excavator cheats, the information and the key for this test aren't related with any private information.

The excavators should show the hashes of information previously, then after the fact re-encryption to the organization. On the off chance that this re-encryption was a test and the excavator has cheated, challengers can introduce a proof that non-delicate keys identified

with this challenge ought to really deliver an alternate re-encryption result, and the digger's insurance store can be granted to the challenger.

The framework ought to likewise deliberately create various "wrong re-encryptions", to boost challengers to work.

Planning a test convention is a complicated issue identified with "reasonable trade" conventions. It requires cautious plan and testing, and Ethereum's Evidence of-Stake (Casper) convention is confronting this intricacy now. It could be conceivable to simply check accuracy fair and square of the encryption calculation.

Extraordinary thought ought to be given to shielding re-encryption keys from spilling. The accompanying test convention is proposed. While tolerating liability regarding a re-encryption key, an excavator hopes to get an expense f over the long haul T, so the proprietor of the information stores f coins. The excavator should likewise set up insurance c which will be relinquish if releases the re-encryption key is spilled.

In the event that a challenger demonstrates that the excavator has released a re-encryption key, the challenger ought to be compensated. In any case, the information proprietor might move the excavator to deceitfully gather the test reward. We make this "selfchallenge" infeasible. If the test has occurred after time t, the challenger will get $\alpha f\, t/T$ coins, where $\alpha < 1$.

The information proprietor for this situation gets $(1 - t/T)f$ coins returned. The security and the remainder of the expense gets seized for the advantage of different members of the organization, with the aggregate sum of $c + (1 - \alpha)t/T$.

There additionally ought to be no impetus for the proprietor of the information to counterfeit test the excavator as opposed to denying the strategy. Along these lines, in a "right" renouncement, the proprietor of the information gets $(1 - t/T)f$ coins back, and the digger gets $c + f\, t/T$ coins, where c is the security which was marked.

6.4 Potential dangers

In a cell phone the board use case (Sec. VIII I), the main thing is to repudiate access from a lost or taken gadget before the information is compromised. Envision a potential assault where somebody takes the gadget and intrigues with the important excavators. In that capacity, it should be absolutely impossible for excavators to recognize a client, as well as the other way around. Another

conceivable assault is a gathering of excavators denying access and requesting extra installment to re-encode. In any case, there is no motivator to do as such since the proprietor of the information can undoubtedly re award admittance to that cell phone. Another conceivable danger is a mining hub keeping re-encryption keys for quite a while past the existence of the approach, sitting tight for somebody to assault the end-client gadget and conspire with the mining hub. To forestall this danger, it is significant that the mining hub can't sort out if the information is significant or not, and a decent way of doing this is to anonymize the information proprietor what's more, the actual information.

Decentralized DRM (Sec. VIII D) expects to be that once content (a document or a piece of video) is unscrambled, it has been ,bought, so access revocation isn't actually an issue. Notwithstanding, if a hub realizes that the substance is extravagant, they might endeavor to move toward the purchaser and request a less expensive cost for the substance, removing the first vender. To forestall this, we ought to anonymize the beneficiary of the information. It would likewise assist with concealing the specific valuing data from the mining hub while as yet permitting it to confirm the vital sum was paid utilizing zk-SNARKs.

At the point when IOTN is utilized to tie down admittance to records or messages, both conceding and denial of access are significant. So full anonymization is profoundly alluring. Potential assaults incorporate beneficiaries of the information paying off excavators to keep approaching after it ought to have been denied and excavators blackmailing expenses from the proprietor when it is basic to renounce access. Anonymization gives off an impression of being a significant piece of making such assaults infeasible.

6.5 Zk-SNARKs

A proof that allows one party to prove it owns certain information without revealing it.

The acronym Zk-SNARKs refers for Zero-Knowledge Succinct Non-Interactive Knowledge Arguments.

They aid in the establishment of trust while interacting in a blockchain and significantly speed up transaction verification while also concealing facts from prying eyes.

The term "zero knowledge" refers to a party's desire to show the truth of a proposition without explaining why it is true.

Before completing a transaction in a blockchain, a user may be required to show that certain requirements are satisfied. They may, for example, need to demonstrate that they have adequate funds to execute a transaction without divulging how much money they have in their wallet.

In a blockchain, Zk-SNARKs are also helpful for verifying one's identity. If Adam wishes to verify Daniel's identity, they can send a secret message to Daniel without telling them what it is and ask Daniel to decode it using their private key. The communication can then be sent back and forth between Daniel and Adam, establishing their identity.

Succinct indicates that the zero-knowledge proof can be confirmed in a matter of milliseconds, even for large-scale program statements. A non-interactive zero-knowledge protocol has little to no interaction between the prover and the verifier. This implies they can only send one evidence to each other. Argument demonstrates that it is only secure for provers with low computing resources, implying that provers with sufficient computational capacity can persuade the verifier of a false proposition. It is difficult for the prover to construct a proof/argument without possessing information.

On the blockchain node, Zk-SNARKs stores just the proof of the transaction, protecting the identity of the sender, receiver, and other transaction data.

7. Token on IOTEN Network

The local computerized cryptographically-got badge of the IOTEN Network (IOTN) is a significant part of the biological system on the IOTEN Network, and is intended to be utilized exclusively on the organization. Before the dispatch of IOTEN mainnet, the symbolic will exist as an BEP20 viable token on the Binance blockchain, which will be moved to a token on the IOTEN mainnet when the equivalent is dispatched.

IOTN is needed as virtual crypto "fuel" for utilizing specific planned capacities on the IOTEN Network (like executing exchanges and running the conveyed applications on the IOTEN Network), giving the monetary motivating forces which will be burned-through to urge members to contribute and keep up with the biological system on the IOTEN Network. Computational assets are needed for running different applications and executing exchanges on the IOTEN Network, just as the approval and check of extra Blocks/data on the blockchain, accordingly suppliers of these administrations/assets would require financial impetuses for the arrangement of these assets (for example "mining" on the IOTEN Network) to keep up with network honesty, and IOTN will be utilized as the unit of trade to measure and pay the expenses of the burned-through computational assets. IOTN will be mineable

for a considerable length of time, with remunerations of the mining diminishing over the long haul dependent on a straight inclination decrease model.

IOTN is a fundamental and imperative piece of the IOTEN Network, on the grounds that in the nonappearance of IOTN, there would be no normal unit of trade to pay for these expenses, along these lines delivering the environment on the IOTEN Network unreasonable.

IOTN is a non-refundable utilitarian utility symbolic which will be utilized as the unit of trade between members on the IOTEN Network. The objective of presenting IOTN is to give a helpful and secure method of installment and settlement between members who communicate inside the environment on the IOTEN Network. IOTN does not at all address any shareholding, support, right, title, or interest in IOTEN Foundation Ltd. (the Foundation), its partners, or some other organization, endeavor or undertaking, nor will IOTN qualifies token holders for any guarantee of charges, income, benefits or venture returns, and are not expected to establish protections in Singapore or any applicable purview. IOTN may just be used on the IOTEN Network, and responsibility for conveys no freedoms, express or suggested, other than the option to utilize IOTN as a way to empower use of and association with the IOTEN Network.

Specifically, IOTN:

(a) is non-refundable and can't be traded for money (or its identical worth in some other virtual cash) or any installment commitment by the Foundation or any partner;

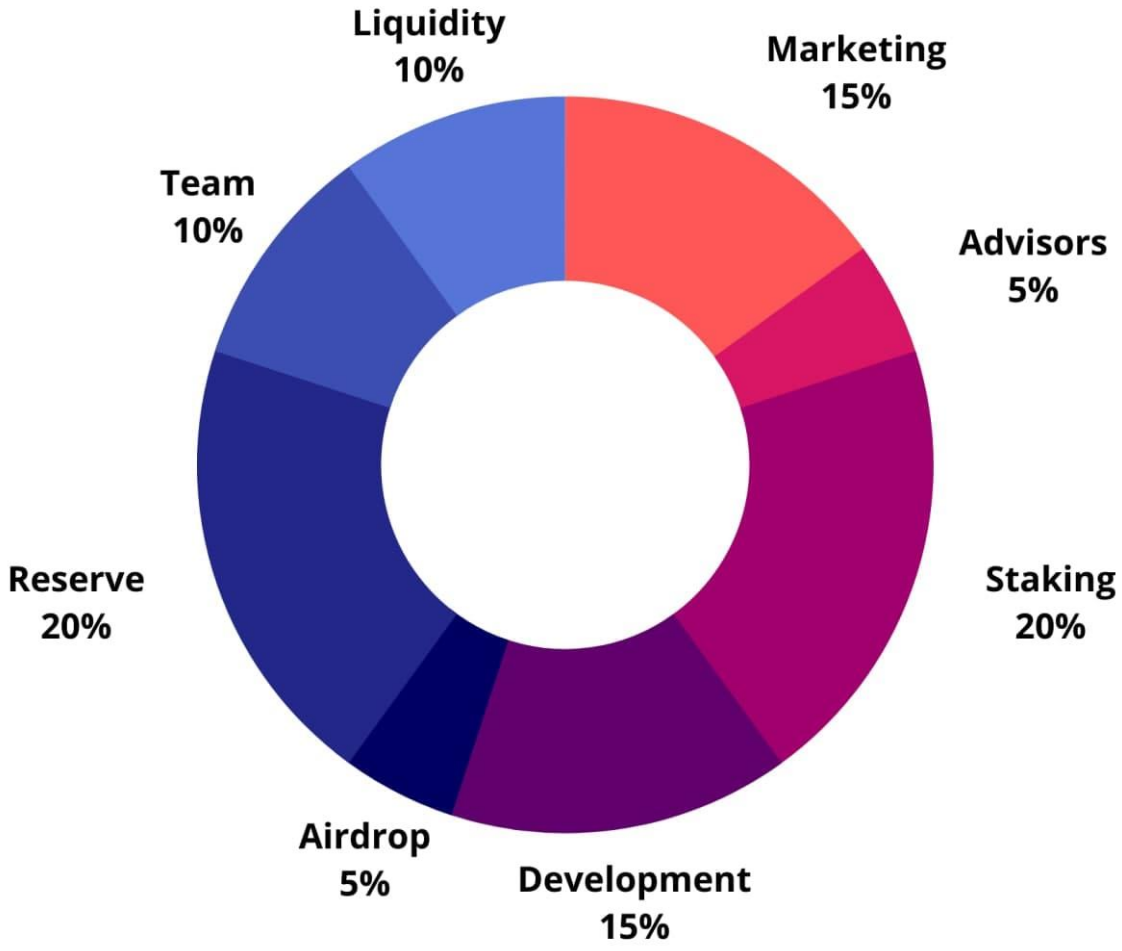
(b) doesn't address or present on the symbolic holder any right of any structure with regard to the Foundation (or any of its offshoots) or its incomes or resources, including without constraint any option to get future income, shares, proprietorship right or stake, offer or security, any democratic, dissemination, reclamation, liquidation, restrictive (counting all types of licensed innovation), or other monetary or then again legitimate privileges or comparable freedoms, or protected innovation freedoms or some other type of investment in or identifying with the IOTEN Network, the Foundation, the Merchant or potentially their specialist organizations;

(c) isn't expected to be a portrayal of cash (counting electronic cash), security, ware, bond, obligation instrument or some other sort of monetary instrument or on the other hand venture;

(d) isn't an advance to the Foundation or any of its offshoots, isn't expected to address an obligation owed by the Foundation or any of its associates, and there is no assumption of benefit; and

(e) doesn't furnish the symbolic holder with any possession or other interest in the Establishment or any of its partners.

7.1 IOTEN Network Tokenomics



Total supply: 10.000.000.000 IOTN

Liquidity - 10%:

These tokens are immediately available as liquidity for the community of IOTEN Network.

Advisors - 5%:

Half of these tokens are immediately available for the current project partnerships to have a solid team and future growth. The remaining 50% of those Advisory tokens are locked.

The locked tokens are being released at the rate of 5% every month, which means all of them will be available for in the next 20 months.

Marketing - 15%:

Half of these tokens are available immediately, as the IOTEN Network needs recognition in the early stages of the project development. The remaining 50% of those Marketing tokens are locked. The locked tokens are being released at the linear rate of 5% every month, which means all of them will be available for marketing purposes in the next 20 months. Marketing is essential for building a strong foundation for the project to flourish.

Staking - 20%:

These tokens will be available for the native staking that will be available by the end of Q1 2022.

Development - 15%:

Half of these tokens are available immediately, as the IOTEN Network needs funds during the early development stages to build a solid foundation. These funds will be used to develop the IOTEN Network and Research on IOTN use cases (Industry 4.0; Shared Economy; Smart Home and etc.) in the upcoming years.

Airdrop - 5%:

These tokens will be distributed to the community shortly after the DEX listing.

Reserve - 20%:

These funds will be used to ensure the IOTEN Network growth in the upcoming years. The locked tokens are being released at the linear rate of 5% every month, which means all of them will be available in the next 20 months.

Team - 5%:

Half of these tokens are available immediately. The locked tokens are being released at the linear rate of 5% every month, which means all of them will be available in the next 20 months.

7.2 IOTEN Network Roadmap

8. IOTEN Powered Ecosystems

The IOTEN blockchain upholds an assortment of IoT biological systems, shared economies, shrewd homes, industry 4.0, independent vehicles, and supply chains, and so forth. The designers upheld by IOTEN incorporate IoT equipment makers, IoT gadget control framework designers, savvy home application engineers, shared economies gadget makers, inventory network information integrators, information publicly supporting merchants, independent vehicles designers, and so forth. This part portrays a couple IOTEN controlled environments.

8.1 Industry 4.0

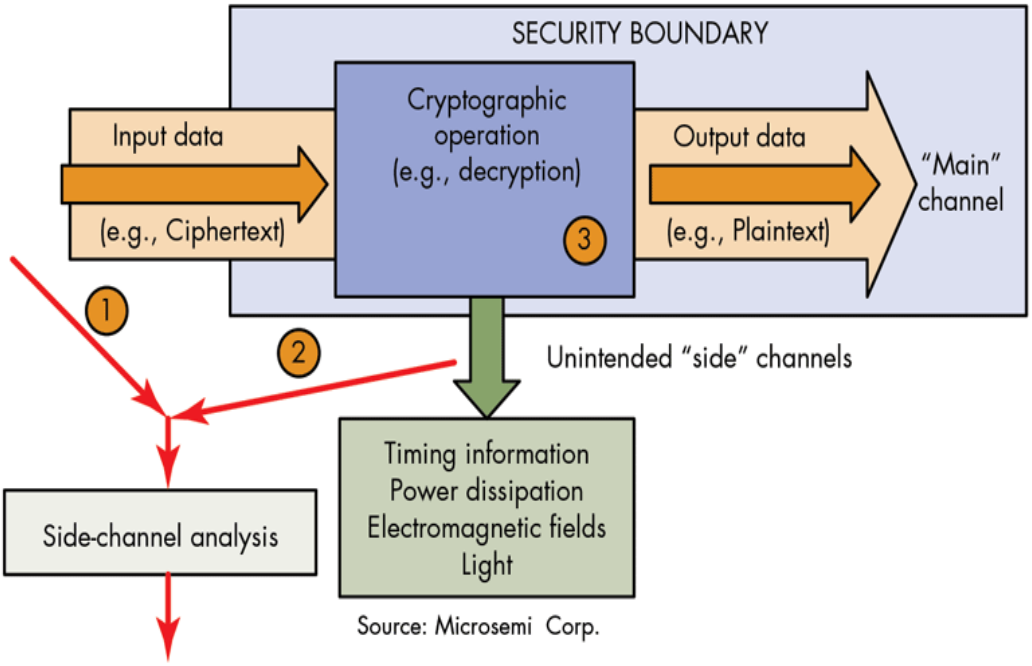
Industry 4.0 refers to the use of automation and data exchange in manufacturing. According to Boston Consulting Group there are nine principal technologies that make up Industry 4.0: Autonomous Robots, Simulation, Horizontal and Vertical System Integration, the Industrial Internet of Things, Cybersecurity, The Cloud, Additive Manufacturing, Data and Analytics, and Augmented Reality. These technologies are used to create a "smart factory" where machines, systems, and humans communicate with each other in order to coordinate and monitor progress along the assembly line. Networked devices provide sensor data and are digitally controlled.

The net effect is the ability to rapidly design, modify, create, and customize things in the real world, while lowering costs and reacting to changes in consumer preferences, demand, the supply chain, and technology. So how are Industry 4.0 and IOT related exactly?

Industry 4.0 uses an Internet of Things, in order to perform digital manufacturing. All devices, robots, simulations, and tools have sensors and provide data. IOTEN Network with its IOTN aim to be the connecting force between all of the technology and entities.

Additionally, no manufacturer is an island as nearly every manufacturer has a supply chain which in turn has its own tools, and its own data, processes, and network. Bringing each of these networks together into a bigger Internet of Things promises to allow the entire supply chain to react more seamlessly to the market. This networked information sharing will help address long standard manufacturing problems like the Bullwhip Effect or tracing quality issues down a supply chain.

Given that both Industry 4.0 and IoT demand linking together previously independent devices and systems, it isn't surprising that a chief shared concern is security. As the trend of using smart devices increases, it will be harder to track breeches and manage all of those devices. Industry is moving quickly to address these security concerns, melding new technologies with standard IT security technologies like network security and encryption.



Another hurdle for both IoT and Industry 4.0 has been the lack of standards. Having a bunch of smart devices is great, but if they all record data in their own format and require their own protocol, integrating them into an automated factory will be cost prohibitive and difficult. Manufacturing giants like Bosch, the Eclipse Foundation, and others have been working on

standard communication protocols and architectures like OPC UA, MQTT, and PPMP. These all aim to help smart devices, including those on the factory floor, communicate with each other and provide common data formats. But more data formats can mean more difficulty in creating one data model.

Two key examples of Industry 4.0 search include

- Product 360 – used to understand all of the components of a product and their fault data.
- Enterprise Search / Knowledge Management – used to ensure that each person from marketing to design to quality control can find the relevant information they need from procedures to specifications to models.

8.2 Shared Economies

As of late, many organizations have zeroed in on shared economies, from rides sharing like Uber/Lyft, home-sharing like Airbnb, bicycle sharing like Mobike, and so forth. They all provide individuals with a superior living comforts.

It is an alternate theme to talk about their plans of action; here we primarily center on their innovative design. Among every single common economy, ride-sharing is the one that can't stay away from a human activity, viz., drivers. It's anything but an IoT-controlled economy. Notwithstanding, later on, when independent vehicle innovation becomes experienced what's more, well known, ride-sharing will be fueled by IoT. All IoT-fueled shared economies share a few likenesses: They all require a lock that can be opened by a store and rental expense. It is entirely conceivable and furthermore effective to control the entire sharing and returning interaction utilizing an IoT gadget. In concentrated world, the economies are controlled by a unified cloud. There are different downsides:

1. A huge store is held by an organization that may not be dependable. As of late, there have been many situations where the organization that runs a common bicycle administration in China can't repay stores to its clients;

2. The common economies are not totally determined by the local area. Many shared things are claimed by an organization. This has caused a misuse of social assets.

3. Because of the unified nature, the client information will be put away and constrained by one organization. There are hazards that either the cloud or the customer can be hacked to acquire client information.

IOTEN, as a foundation, could be used to control these applications without the issues above and make shared economies decentralized and more proficient. Solidly, an IOTEN-controlled shared economy gives the accompanying advantages:

1. Store is totally settled by a savvy contract. With nobody keeping down the cash, returning of the store is constantly ensured. Clients don't need to trust the organization to utilize the help.

2. Each common thing understands its worth and mission in an independent manner. In the biological system, it doesn't make any difference who claims the common things in it. Everybody can claim and add to the environment. The economy can be controlled by the local area. Thus, organizations can assume the part of keeping up with the IoT lock and overseeing the local area. It is a lot lighter plan of action that organizations can quick grow and serve more individuals.

3. Once more, clients don't need to trust the organization to keep up with their information. Their information is kept in the chain with security assurance.

8.3 Smart Home

In the current keen home market, numerous IoT gadget makers are as yet utilizing obsolete advancements to foster their items. They need a lot of advancement work on their cloud. The expense of advancement and upkeep is high, and execution is low. Conveying their items onto the IOTEN blockchain will to a great extent lessen working expenses on designing and distributed computing, and simultaneously, generally increment the presentation of their gadgets. In a basic savvy light model, with cloud innovation, it goes on two outings from client guidance to changing the condition of a light. Makers are not cloud specialists so frequently their administration isn't ideal. The full circle can require one to three seconds. This powers them to utilize cloud administrations by large IT organizations. There are few drawbacks of utilizing these cloud administrations:

1. Makers can't completely control the accessibility of cloud administrations.

2. They need to persistently pay for the cloud administration notwithstanding their one-time charge on selling their IoT gadgets.

3. There are dangers of their cloud, customer side, or intranet being hacked causing client information to be taken or home security issues.

Interestingly, IOTEN blockchain deals with the gadgets locally and interactss with general society chain on the web when important. The public chain is kept up with by the local area.

There is no support cost for IoT makers. IOTEN blockchain has security assurance that can forestall spilling information or control being hacked regardless of whether the intranet isn't protected. As well as permitting IoT makers to convey their IoT gadgets on the IOTEN blockchain, IOTEN will join forces with IoT chip producers to foster IOTEN blockchain-empowered chips to speed up the plan and production patterns of IoT gadgets. IoT producers will just coordinate the chip to get their gadgets upheld by the IOTEN blockchain.

8.4 Identity Management

The developing universe of IoT has affected how Identity and Access Management (IAM) need to work. As far as the personality of things, IAM should have the option to oversee client-to-gadget, gadget to-gadget, as well as gadget to-support/framework. One direct way is to consider IOTEN blockchain as a decentralized PKI framework (because of its permanence) where every element is given a cryptographic character as a TLS declaration and the relating private. This declaration, which will in general be a brief one, is endorsed by the gadget's underlying and seemingly perpetual authentication also, distributed on the IOTEN blockchain (either root chain or subchain). Different entities can access and believe the brief declaration secured on the blockchain, and things would then be able to confirm when they become web based, guaranteeing secure correspondence between different gadgets, administrations and clients, and demonstrating their honesty.

What's more, the inherent and seemingly perpetual declarations for gadgets could be sorted out in a pecking order, similar to the traditional PKI, where parent gadgets could sign kids' testaments. With the pecking order, denying and pivoting declarations becomes conceivable. For instance, if one gadget gets compromised, its parent gadget or regardless of whether grandparent gadget could sign a denial order and send it to the blockchain where the last option nullify the gadget's authentication.

9. Future Research Work

Some continuous and future bearings of exploration to further develop IOTEN are as per the following. Saving computation: There are a few regions toward this path we are effectively researching:

• How to hold private states on the blockchain which can be utilized for registering by a specific gathering of hubs;

• Privacy-safeguarding private agreement where the brilliant agreement can be assessed when its business rationale is secured by encryption. While completely homophobic

encryption and unclear jumbling plans are the sacred goal, in principle, functional proposition like Hawk is promising for the not so distant future;

• Further diminish the calculation and capacity impression of the security saving strategies IOTEN is right now utilizing;

• The quantum-safe adaptation of protection safeguarding methods IOTEN is right now utilizing, for example, quantum-safe ring mark.

9.1 Native NFT Marketplace

IOTEN's NFT Marketplace will be a one-stop shop for all the needs of NFT creators and much more. Currently, the main issue with NFTs is that they are illiquid. IOTEN's proprietary technology solves this issue and brings true opportunity for all artists. Desired amount IOTN will be staked when minting the NFT or can be separately staked for existing NFTs on IOTEN native NFT Marketplace. This will result in providing new or existing NFTs with value in IOTN.

As an example, Alex mints and NFT on IOTEN native Marketplace and simultaneously is asked if he wants to stake IOTN and connect it to the NFT. As soon as NFT is minted, the cheapest the NFT can be sold is set to the staked amount of IOTN tokens. When Mark acquires the NFT from Alex, the owner of the NFT changes and the staked amount is also transferred to Mark. Mark can now un-stake the IOTN from the NFT and separate NFT form the IOTN or he can decide to increase the floor price by staking more IOTN on top of the current staked amount. Staking will be calculated based on the APY at that point in time and during the un-staking the rewards will be distributed.

9.2 TEN Wallet

TEN wallet protects user privacy by generating a custom address every time the user withdraws digital assets or sends them to another wallet. Additionally, TEN wallet uses smart

contracts to hold collective funds in its network to mix the inflow and outflow of cryptocurrencies to mix up transaction data.

As an example, Alex decides to send some tokens to Mark. However he wants to send the tokens in BNB or other cryptocurrency supported by TEN wallet. He can transfer the crypto assets to Mark while being fully private. This is achieved by creating a pool and mixing up the inflow and the outflow from the TEN wallet pool. Additionally, Staking IOTN will provide lower transaction costs for the senders.

States Pruning and Transferring

We are assessing various approaches to securely prune the states put away on sub-chains to decrease the capacity impression since numerous IoT gadgets have restricted capacity. Pressure of Blocks and exchanges is certainly easy pickings. Moreover, moving states from sub-chain to root chain (since the last option is more grounded as far as capacity) in a productive and security saving way is likewise a fascinating subject to examine.

Administration and Self-revising

While IOTEN blockchain offers motivating forces for keeping up with agreement on its records, it doesn't have an on-chain instrument for the time being that flawlessly revises the guidelines administering its protocol and prizes protocol advancement. We intend to lead research on administration and self-revising to address this.

Tree-Structured Blockchains

The current IOTEN is a two-layer blockchain and normally, it ought to be reached out to a tree of blockchains by utilizing procedures like Plasma and Cosmos. The arrangement is to assess these recommendations and upgrade the current plan of IOTEN to ultimately uphold more mind boggling progressive designs.

10 Finality

In this white paper, we presented IOTEN, an adaptable, private, and extensible blockchain committed to the Internet of Things, with its design and center innovations including

1. Blockchains in blockchain to expand versatility and protection,

2. Genuine protection on blockchain-dependent on solid installment code, consistent size ring mark without confided in arrangement

3. Quick agreement with moment certainty dependent on VRF and PoS for high throughput and moment irrevocability, and

4. Adaptable and lightweight IOTEN-based framework models.

11 Acknowledgements

We want to offer our thanks to our guides and counsels and to the many individuals in the IoT, cryptography, and digital money networks for their initial input and helpful ideas.

Interest in an ICO is a high-risk act. Our deal is coordinated to experienced experts acquainted with Blockchain advancements, cryptographic money exchanging, and other monetary instruments, like stocks or forex.

By taking part in this ICO, the financial backer ought to acknowledge the security dangers. The member announces that he knows about the legitimate vulnerability identified with this kind of administration and that he has directed his own assessment of the consistence of the administrations presented by IOTEN Network with material law.

Any individual who purchases IOTN tokens recognizes the task's innovative and financial vulnerability introduced in the White Paper. Accordingly, members know about the absence of plausibility to make any legitimate move against the organization in case of the undertaking's disappointment or non-execution, and the occasion of a decay or even absolute loss of worth of IOTN. The acquisition of IOTN token permits you to utilize the benefits made by IOTEN Network administration.

No other privileges are moved to the symbolic holders. All the more explicitly, the organization's sole liability is to circulate the IOTN tokens under the conditions set out in the White Paper.

During the ICO, the organization can't be considered liable for any of the accompanying:

- Use of the service not in accordance with applicable terms
- Error, failure, malicious activity, or breach of the White Paper by the user, third party or third party controlled service;
- All direct or indirect damages that may occur during the operation: cryptocurrency losses, financial gains or losses, or other damages of this nature
- Loss of control for any reason (loss, hacking, Unwanted disclosure, or technical failure) of users' login details that could lead to fraudulent use of tokens
- Temporary or permanent suspension of the service, for whatever reason, especially at the request of public authorities, judicial authorities, or a third party

- Computer failure resulting in loss of data, including the event of percussion
- Professional activity of users.

References

[1] ITC Blockchain for IoT. https://iotchain.io/.

[2] Ahmed Kosba et al. “Hawk: The blockchain model of cryptography and privacy preserving smart contracts”. In: Security and Privacy (SP), 2016 IEEE Symposium on. IEEE. 2016, pp. 839–858.

[3] HDAC Blockchain for IoT. https://hdac.io/.

[4] Hyperledger Fabric. https://www.ibm.com/blockchain/hyperledger.html.

[5] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[6] Shen Noether and Adam Mackenzie. “Ring Confidential Transactions”. In: Ledger Vol. 1 (2016), pp. 1–18. DOI: https://doi.org/10.5195/ledger. 2016.34.

[7] Proof of stake instead of proof of work. Retrieved January 9, 2018 from https://bitcointalk.org/index.php?topic=27787.0

[7] AB Ericsson. “Ericsson mobility report: On the pulse of the Networked Society”. In: Ericsson, Sweden, Tech. Rep. EAB-14 61078 (2015).

[8] Sanjam Garg et al. “Candidate indistinguishability obfuscation and functional encryption for all circuits”. In: SIAM Journal on Computing 45.3 (2016), pp. 882– 929.

[9] Yossi Gilad et al. “Algorand: Scaling byzantine agreements for cryptocurrencies”. In: Proceedings of the 26th Symposium on Operating Systems Principles. ACM. 2017, pp. 51–68.

[10] Benedikt Bunz et al. Bulletproofs: Efficient Range Proofs for Confidential Transactions. Cryptology e-Print Archive, Report 2017/1066. https://eprint.iacr. org/2017/1066. 2017.

[11] Vitalik Buterin. Light Clients and Proof of Stake.https://blog.ethereum. org/2015/01/10/light-clients-proof-stake/

[12] Adam Back et al. “Enabling blockchain innovations with pegged sidechains”. In: URL: http://www.opensciencereview.com/papers/123/enablingblockchaininnovations-with-pegged-sidechains (2014).

[13] Čolaković, A and M Hadžialić [2018] Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks, 144, 17–39. Crossref, Google Scholar

[14] Alexander Skidanov. Unsolved Problems in Blockchain Sharding, 2018 (accessed October, 2019). https://medium.com/nearprotocol.

[15] Gavin Wood. 2018. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. ethereum.github.io/yellowpaper. Retrieved from https://ethereum.github.io/yellowpaper/paper.pdf

[16] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. Recursive composition and bootstrapping for SNARKS and proof-carrying data. In STOC, pages 111–120. ACM, 2013

[17] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. 2016. A Secure Sharding Protocol For Open Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16. DOI:https://doi.org/10.1145/2976749.2978389

[18] Al-Ali, AR, IA Zualkernan, M Rashid, R Gupta and M Alikarar [2017] A smart home energy management system using IoT and big data analytics approach. IEEE Transactions on Consumer Electronics, 63(4), 426–434. Crossref, Google Scholar

[19] Maksym. "Why and How ZK-SNARK WORKS 1: Introduction & the Medium of a Proof." Medium, 20 July 2019, https://medium.com/@imolfar/why-and-how-zk-snark-works-1-introduction-the-medium-of-a-proof-d946e931160.

[20] Paul Valiant. Incrementally verifiable computation or proofs of knowledge imply time/space efficiency. In TCC, volume 4948 of Lecture Notes in Computer Science, pages 1–18. Springer, 2008.

[21] Alessandro Chiesa, Yuncong Hu, Mary Maller, Pratyush Mishra, Noah Vesely, and Nicholas P. Ward. Marlin: Preprocessing zk-snarks with universal and updatable SRS. IACR Cryptology ePrint Archive, 2019:1047, 2019.

[22] Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser†, Nicolas Gailly, Ewa Syta, Bryan Ford. 2017. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding.

[23] G Maxwell And. 2015. On Stake and Consensus. Retrieved January 9, 2018 from https://download.wpsoftware.net/bitcoin/pos.pdf

[24] C. P. Schnorr. 1991. Efficient signature generation by smart cards. J. Cryptology 4, 3 (1991). DOI:https://doi.org/10.1007/bf00196725