The Neuralium Crypto Token

Neuralium inc.

September 4, 2019

Document Version 0.1.0
(Matching Release: TESTNET Phase I)

Abstract

A new crypto token based on a novel blockchain architecture that was created to do things differently than other existing technologies. The Neuralium is designed to be quantum resistant, protected by a custodian and is intended to be fully universal in order to provide access to crypto tokens for the regular people. It is defined by its ease of use and a much safer, integrated and better supported ecosystem. It supports a fully decentralized peer-to-peer network with democratic transaction selection. It also brings forward an entirely new mining algorithm which is completely green and absolutely fair to everyone.

Contents

1 Introduction

Since the arrival of Bitcoin and the blockchain, so called cryptocurrencies have taken the world of technology and finance by storm. One is now hard pressed to ignore the existence of these technologies and the potential disruption they can still cause the world over. The blockchain is a marvelous idea where the history of activities are permanently etched in time, allowing for a verifiable and trustworthy ledger to be offered and verified by third parties to ensure structural integrity. Cryptocurrencies make use of this method to provide a ledger that ensures the integrity of the transactional activities over time. Combined with a decentralized peer-to-peer network, this became a strong asset for regular users to send tokens the world over near instantly. While this has worked very well up to now, sadly, the existing cryptocurrencies also have their fair share of problems with very serious consequences. In many cases, the existing cryptocurrencies are not sustainable at scale and may cause irreparable damage to the Earth.

The Neuralium has been designed in an effort to create something that is different to what has already been previously done. It is intended to compensate certain short comings of other technologies and to make a token that is fair and usable by all. It also made certain choices in order to offer a safer and more integrated experience to the users than would otherwise be possible with other technologies.

2 Post Quantum Cryptography

Conventional cryptography such as RSA and ECC are essentially based on the difficulty to factorize large prime numbers. This kind of cryptography is by far the current dominant schemes in the world of blockchain today, but it is at risk of being broken by quantum computers in the future. At the time of writing, these quantum computers are nowhere near close to breaking this cryptography, but they are closing in very quickly, and it is only a matter of time until a private cryptographic key can be broken in a usefully short period of time. Once this day arrives, all cryptocurrencies based on these schemes will effectively become obsolete.

The Neuralium makes use of new and innovative cryptography schemes that are designed to be quantum resistant. These algorithms are used in synergy to create a unique ecosystem that will remain viable far into the future. A design choice that was made was to always offer a predominant cryptographic algorithm and an optional backup algorithm in case it was ever needed. This means that if a scheme is ever found to have issues in the future, one can quickly change to the backup scheme without any forking. Here are the various encryption schemes used by their design family.

	Primary	Secondary
Hashing	SHA3	SHA2
Digital Signatures	XMSS & XMSS^{MT}	qTesla
Asymetrical	McEliece	NTRU
Symetrical	XChacha40	AES256

2.1 Structural Hashing

Most of the existing cryptocurrencies perform their structural hashing through the use of Merkle trees. The problem with this approach is that it is relatively simple in the way that it hashes nodes together, and this creates potential issues with its security. It has already been demonstrated that in certain cases, a Merkle tree can have entries swapped and still hash to the same Merkle root. This could in theory allow attackers to corrupt transaction values and still hash correctly to pass cryptographical validation. In the Neuralium, we addressed this issue by using

Sakura trees exclusively. Sakura trees use a much more sophisticated method of hashing trees of hashes together using tail ends and kangaroo hops. This elaborate structure makes it near impossible to swap entries in the tree and still hash to the same Merkle root. It then becomes theoretically impossible to corrupt the structure of the blockchain by changing content.

3 Onchain Accounts

One of the biggest problems of the blockchain is that ECDSA is essentially a single use signature scheme. In theory it can be used multiple times, but every time it is used after the first signature, it becomes easier to break. For maximum security, it really must be used only once. This means that users should create a new key for every transaction that they want to make. This becomes a limitation factor as there is no way to ensure correlation between a users activities over time. It might be fine for anonymous activity seekers, but in truth, even such users are rarely truly anonymous and can mostly be identified by powerful relational analysis software that take into account points of entry and points of exit into the token. For everyone, save a few highly sophisticated users, the anonymity advantage is thus moot, and this scheme results only in limitations with no real advantages.

The Neuralium devised a novel way to use hash-based cryptography in such a manner that allows it to create on the blockchain permanent accounts. Users will publish an account as their very first operation and then from then on, all their transactions will be correlated to this account. The user remains fully anonymous as this account is only a number with no personally identifiable properties, but the account correlation gives the system the ability to perform new types of operations, such as building trust levels, replacing keys, returning stolen funds and restoring wallets for example.

Accounts are created in the following manner. When joining on the blockchain, a user will always begin by creating a special transaction where they will present their account to the chain. This presentation will contain various multi-use cryptographic keys that the user will create and use to validate their activity. For example, one can create a main key and then a backup key. Once an account has been presented publicly, the user is free to create transactions for its assigned account ID and use the keys to confirm identity. When creating a subsequent transaction, the user will tell the other users which account it is using, and in which block to find the published public key. The others are then able to lookup the account, load the public key and validate the message. If the message validates correctly, then we know that this transaction was created by the owner of the previously published account.

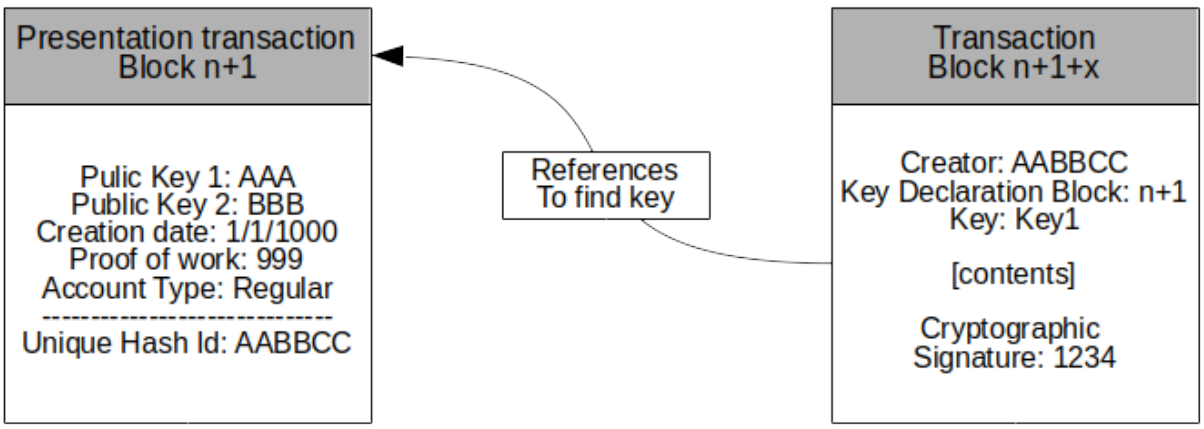

Figure 1: Transaction referencing the presentation transaction for the public key

Over time, keys for an account may need to be changed for various reasons. Users can create key change transactions where they will use a previously published super key to instruct the blockchain of the change. Once this change has been completed, the blockchain is aware of the change and transactions can continue using the new key, which always correlates to the published account id from the presentation transaction.

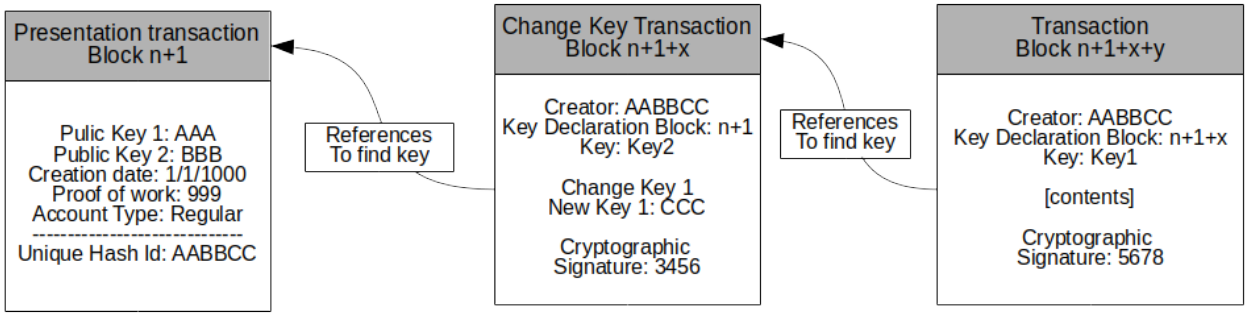

Figure 2: Key changing replacing the presentation transaction as the public key reference

3.1 Key Storage

The Neuralium stores its various account keys in independently encrypted files that are not required for wallet use until the keys are explicitly needed to sign a transaction. This means that a super key can be physically removed from the computer, and only restored if ever needed to change the other account keys. This offers much better overall security since it becomes impossible for hackers to steal a key that is physically not on a computer.

4 Decentralized Peer to Peer Network

The Neuralium is built around a fully decentralized peer to peer network where every node is equal to any other (there are no supernodes in the topography). The communication between the various nodes is ensured by its own custom gossip protocol. The protocol allows for the passing of various message types such as blocks, transactions and so called blockchain messages (signed messages that alert the blockchain members of a transient event that is not saved on the blockchain but rather on an optional sidechain). The protocol is built in such a way that it will batch messages together for optimization and provide an opportunity for a node to determine which messages it wants to receive, and which ones it wants to ignore. This method is used for efficient echo attenuation.

5 Trusted Block Emission

Most cryptocurrencies are built around an idealistic idea of decentralization. It is a nice idea in theory, but in practice in real world scenarios, the problem has proven to be either impossible to truly achieve, or in the interim is made temporarily viable by an order which is based on rules that are ultimately destructive and unsustainable at scale. The root of the problem stems from the inability to trust anyone in a large system of decentralized and individually untrusted nodes. In such a large system, it is not possible for all nodes to talk with all others at all times to coordinate and establish truth, and there will inevitably be bad actors that will want to corrupt the system by using this inability for all to establish perfect truth, and depending on their means, these bad actors can achieve it in various ways. In a decentralized system made

up of a large number of nodes, every nodes vote about its own version of the truth is as good as any other one, and then the problem is to figure out how to keep the overall truth and cull the (hopefully) minorities of liars. Due to this problem to ensure that we can properly exclude the bad actors and keep the good ones, various techniques have been devised, but due to the equality of a large number of nodes with no central head, all of these techniques are based on establishing some common limitation factor to isolate some temporary leaders, which is intended to put the control out of reach of (hopefully statistically insignificant) bad individuals and remain into the realm of the good majority through general consensus. In theory it is a good idea as the majority is essentially trusted to be in good faith, and thus a small number of bad actors will be diluted through the masses and lost in the numbers. In practice though, these very limiting factors can always be co-opted by powerful organizations to gain influence that is not representative to their numbers on the network, at the expense of the general common user. The very same walls erected to keep out the bad guys end up giving these bad guys a disproportionate amount of power at the expense of the more numerous but less influential good guys. The most obscene aspect of this is that most regular users do not realize that they are kept out due to the complexity of perceiving this control and thus erroneously believe their crypto token to be free of influence.

So, while these cryptocurrencies are thought to be decentralized, in every case these systems tend towards centralization as they become more popular and the size of their network grows in complexity. Now this centralization is rarely overt but is most certainly covert. First of course there are the software development foundations who control the code and own the trademark names to the tokens. One could always fork open source code if unhappy by the direction such a team can take, but the practical truth is that the majority of users will near always follow the trademark name, and p2p networks live on the majority. Hence if an ill intended organization takes control of the development activity of a cryptocurrency and gains control of its marketable name, it is covertly centralizing it and can steer its evolution despite users thinking that development is established by public consensus. This is in itself one of the most powerful form of covert centralization. Also, as the resource usage required to operate a cryptocurrency increases over time, it becomes easier to control for a few powerful ones. For example, proof of work (POW) uses the cost of electricity and computing power as a limitation factor. Proof of Stake (POS) uses the difficulty to acquire funds and prove long periods of ownership and Delegated Proof of Stake (DPOS) the difficulty to acquire popularity among an informed group. The irony of these limiting factors is that as the bar to entry increases, they become the very wall that prevents the common people from maintaining democratic and thus decentralized control, and ergo only powerful entities get to wield its power. For example, for POS, it is much easier for a large hedge fund to achieve a strong and aged position in stake than for a (relatively) poor user with no previous exposure to cryptocurrencies.

In many cases, POW for example, this centralization comes through the use of mining pools who end up controlling a majority portion of the mining network, effectively gaining the ability to become the mint. A single owner could give the appearances of decentralization by splitting its computing power into different seemingly independent pools, but if the pools are still owned by the same powerful entity in the background, then it is effectively covert centralization. Also, as the blockchain size on disk increases constantly over time, it further becomes less and less accessible to the common user, and only usable through large datacenters that can accommodate the ever-increasing computational load. This very same limit makes it constantly harder for users to verify the truth on a chain, as the entire data is required for full and thorough validation. Multiple cryptocurrencies have tried to address this problem but with no success at this point. In fact, some recent proposed solutions amount to what is essentially centralization.

Covert centralization is much worse than overt centralization as it provides the illusion

of freedom to users who believe to be free from influence while a hidden hand is pulling the strings of the ecosystem in the shadows. Such a system comes with none of the benefits of an intentionally and well managed ecosystem and at the very least has as much or more negatives.

Having realized the truth about cryptocurrencies, Neuralium decided to avoid the hypocrisy of decentralization and instead has embraced a role of benevolent custodian of the ecosystem. In this vein, the Neuralium is semi-centralized in that the network is a fully decentralized peer-to-peer network and transaction selection is fully democratic and mostly performed by the miners, but the block emission in itself is relegated to trusted nodes only. This gives it multiple advantages not available to covertly centralized systems, while giving it the ability to perform new and innovative things that will improve the overall experience of the users. For example, it can ensure a certain level of security of third parties by employing certifications of quality. This would in itself remove one of the worst type of scams on cryptocurrency networks from key stealing third party websites. It can also offer special security features such as 2 factor authorizations, stolen fund returns, and wallet reset services. All these features benefit the users directly by improving their experience and would be impossible in traditional crypto systems.

5.1 Fully Decentralized and Independent Account Ownership

The Neuralium custodian has no super key that can override private user account keys and has no ability to operate on behalf of anyones account. Every account is fully owned and protected by their own local highly secure cryptographic keys, and the custodian has no ability whatsoever to control a users account. The ownership of accounts is thus fully decentralized. What the custodian can do is use its reputation as a trusted voice on the p2p to recommend change operations. By trusting the custodian, nodes can decide to accept certain recommendations from the custodian which will then make them effective. This is the manner in which accounts can be reset, by trusting the voice of the custodian saying that an account can effectively be considered as reset. In order to do so and for public nodes to accept the change as valid, the custodian still requires the account protection key, which only the account owner can provide. If such a recovery key was ever lost, then the account is lost forever.

5.2 Variable Block Rates

The Neuralium uses a variable rate block emission system which will adjust the block emission speed in order to optimize various factors such as network load, size on disk and transaction backlogs. The rate of block emission can be adjusted as required in real time. For example, under high demand, the block rate may be accelerated to help transactions be confirmed faster. In lower transactional load periods, the rate can be slowed down to adjust to the demand. It can reach a theoretical speed limit of 1 block per second on a very fast network.

5.3 51% Attack Resistant

With the fact that block emission is always performed by a trusted node, it becomes impossible for a powerful ill intended external entity to gain control of the majority of the network hashing power to emit ill intended transactions and double spends. The infamous 51% attack that is essentially the dreaded death stroke for most cryptocurrencies is impossible in the Neuralium network. This gives the users very strong assurances as to the ongoing quality and security of the transactions included into blocks no matter the network topography. The Neuralium blockchain ensures a 100% certainty of truth on the blockchain with no ambiguity.

5.4 Verifiable Blockchain and Trustworthiness

As previously mention, the truth about all successful decentralized cryptocurrencies is that they are all at the very least covertly centralized. This can give the less sophisticated users the very perverse illusion that the network is free from Machiavellian influence and can cause them to lower their guards. But this could not be further from the truth and is a very dangerous situation.

Neuralium, by overtly taking the role of custodian to the block emission process, is fully honest about its position from the start and does not apologize for it. In this manner, the users are well aware right from the beginning and there is no ambiguity as to who is managing the ecosystem. This results in a clear and honest understanding of the offering for the users, who are then free to operate in a well-informed manner. On the flip side, the trusted block emission can potentially create an irrational sense of insecurity in regard to the intentions of the trusted custodian, but in truth, this very thing exposes the custodian to much more explicit scrutiny and will result in constantly increasing standards of security and quality as more and more independent eyes monitor the public ledger.

In truth, this extra scrutiny will make the Neuralium crytpo token much safer than other similar technologies. Since the Neuralium is clear and overt about its management of the crypto ecosystem, it makes it right away much more trustworthy and honest. But even then, the people do not need to trust the custodian blindly, they can at any time analyze the ledger history for tangible proof. This is thanks to the amazing property of the blockchain where every operation is public, immutable and verifiable to all. Neuralium has no choice but to operate the crypto token to the highest level of quality and honesty at all times and forever, because anybody can see the public blockchain and analyze it. If the emission was ever in any way dishonest, it would be immediately clear and provable to all and for ever, immediately destroying the most important asset of the custodian: its reputation and hard-earned trust. The Neuralium custodian is thus forever bound to the utmost levels of honesty because a single bad move would destroy it forever and be provable as a symbol of ill intention. Trust is very hardly won and very easily lost; and mostly is never fully recoverable once lost.

As an analogy, our structure is somewhat similar to a government, which we know is desirable to organize a large population to ensure order in an otherwise undesirable chaos, where every action and expenses of the said government would be immediately and permanently publicly available to all for review. A government which is fully accountable to the public is a dream that we may never see in real life politics, but it is here the permanent model for Neuralium.

6 Proof of Election and Green Mining

Neuralium has invented a completely new mining algorithm which makes different assumptions about the nodes on the network and allows it to perform with a minimal amount of computational resources. This means that the mining is absolutely green and will never result in abuse of resources and thus destruction of the Earth.

6.1 Fair and Democratic

At the moment of writing, the most popular mining methodologies are POW, POS and DPOS. While these algorithms really do work, they all have serious shortcomings that make them either dangerous or near destructive to use. And one of their greatest weakness for the miners is that these methodologies are inherently unfair to the so called decentralized network of peers. This is because these algorithms are designed to be based on limiting factors which are by their very own design exclusive to a certain subset of the peer population. This is intended to isolate

a small portion of leaders in an otherwise infinitely large group of nodes. For example, POW requires a very high amount of computational power and electricity usage to find a block. This means that people located in countries where electricity is very expensive are at a disadvantage in mining compared to those where cheap electricity is available. Since it also requires very powerful computers, it also rewards large datacenters, completely excluding the small players that can only afford regular home computers. Effectively, the end game in a POW network is that only a few well-funded and very large datacenters will be able to mine, resulting in complete centralization of block emission. So, in short, POW rewards the large datacenters in cheap electricity countries, POS rewards the rich and early players and DPOS rewards the marketable and popular (and most often rich) which effectively creates de facto monarchies that govern these cryptocurrencies. A regular user just starting out cannot simply begin using a POS token and have the same ability to mine a block as a whale that has been there from day one. Instead, the rich players that were early gain more power every day, effectively becoming a perpetual and irreplaceable monarchy. The regular user stands no chance of ever having a voice on these networks and are effectively shut out from mining. These cryptocurrencies are inherently unfair and exclusive to only a small group of elites that get locked into power into perpetuity.

In order to address these flagrant issues and inequalities, Neuralium created an entirely new patent pending mining technology called the Proof of Election (POE). The POE is designed in such a way that make it equally fair to everyone. The way this algorithm works is by declaring an election in a block, and those that are elected by the rules of the system have mined a block and are then given a chance to select the transactions that will go into the block as a reward. In this system, a single block can elect multiple miners giving a much better variance factor to participants. The limiting factor in the POE is the IP address of the node, and since everyone has an IP address and each address is perfectly equal to another, everyone is free to use it and mine blocks on an equal footing. One could have access to more IP addresses than others, but the design requires them to share a node that is live on the network at all times on this specific address. This increased presence on the network makes the peer-to-peer network faster and more stable to everyone and thus offers increased value which is of course rewardable. There are no other limiting factor to mining with POE, and thus somebody on a old under-powered cell phone and somebody on a large data center have the exact same ability to find a block. Same for the rich and poor, it has no impact on the ability to mine. Anyone can do it on any computer from day one and have the same ability to mine a block as a rich user on a supercomputer who has been there for years; the only requirement is to have a running node, and that's it. It is the first time that mining, with all its benefits is available to all, in a completely fair manner, whomever you are, wherever you are, and whatever means you have. It is completely universal.

6.2 The Proof-of-Election Methodology

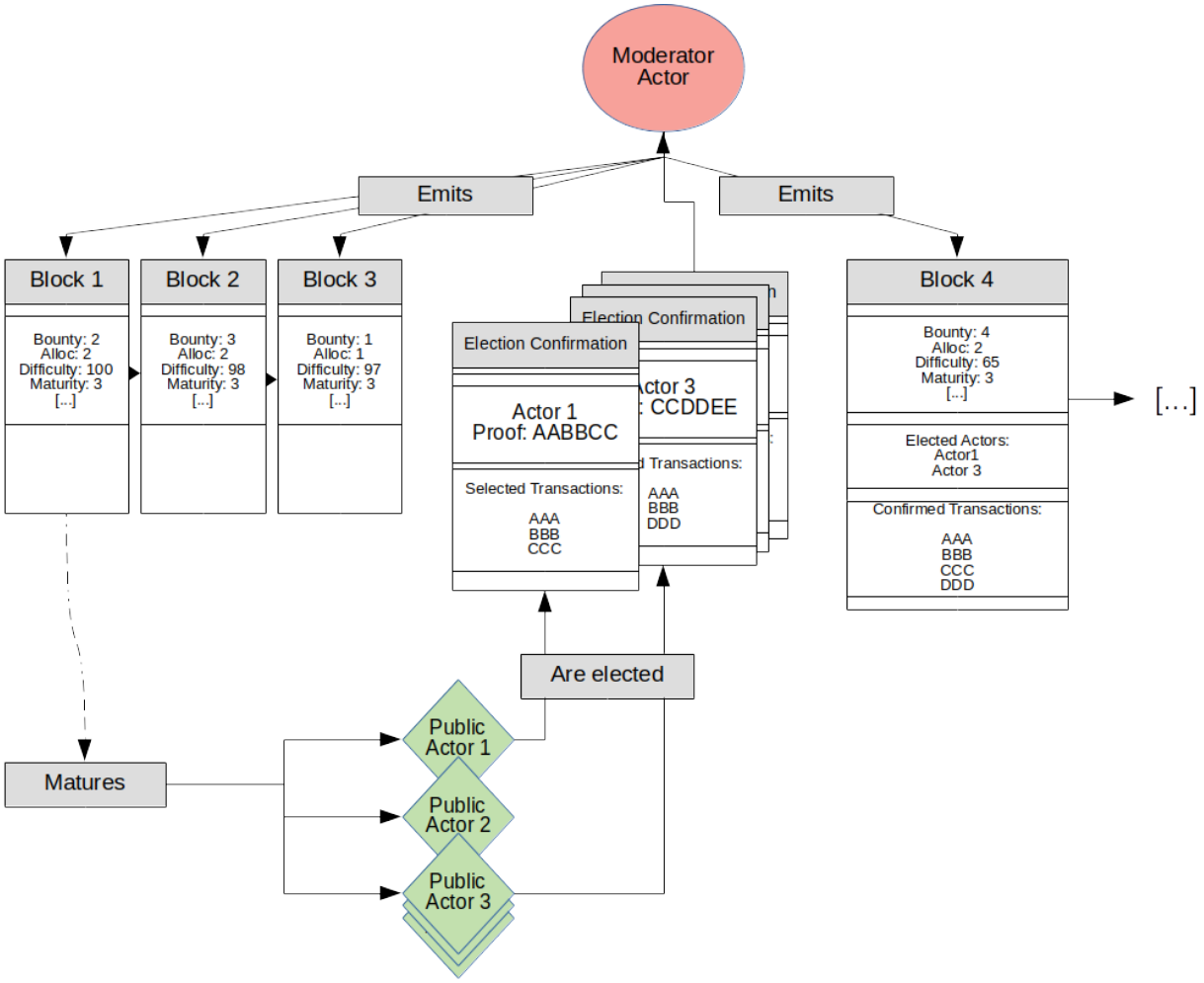

Figure 3: The Proof Of Election workflow

In order to mine, a block must be created with the instructions to perform an election. An election is a reasonably complex process that will span across multiple blocks through a form of workflow and will culminate with a mined block once the election has been completed. Each time a block is created with the intention to mine, an election context section is inserted that will be used to provide the immutable rules and instructions required for the nodes to know how to elect a certain number of actors on the network. Once the election context is created, the parameters of that election are permanently set and cannot be modified anymore. This prevents malicious manipulation from being possible. At the bare essential, a difficulty controlling factor is included to control the elected count. This difficulty indicator is any filtering condition that will narrow down the ability to get elected. It may consist of any condition or mathematical formula with an adaptive parameter provided by the difficulty factor of the block. Statistical methodologies may be employed to determine the ideal difficulty factor based on the election feedback of previous blocks to ensure a relatively constant percentage of representatives for the number of actors on the blockchain. Another example filter could be the same hash minimum algorithm that Bitcoin uses.

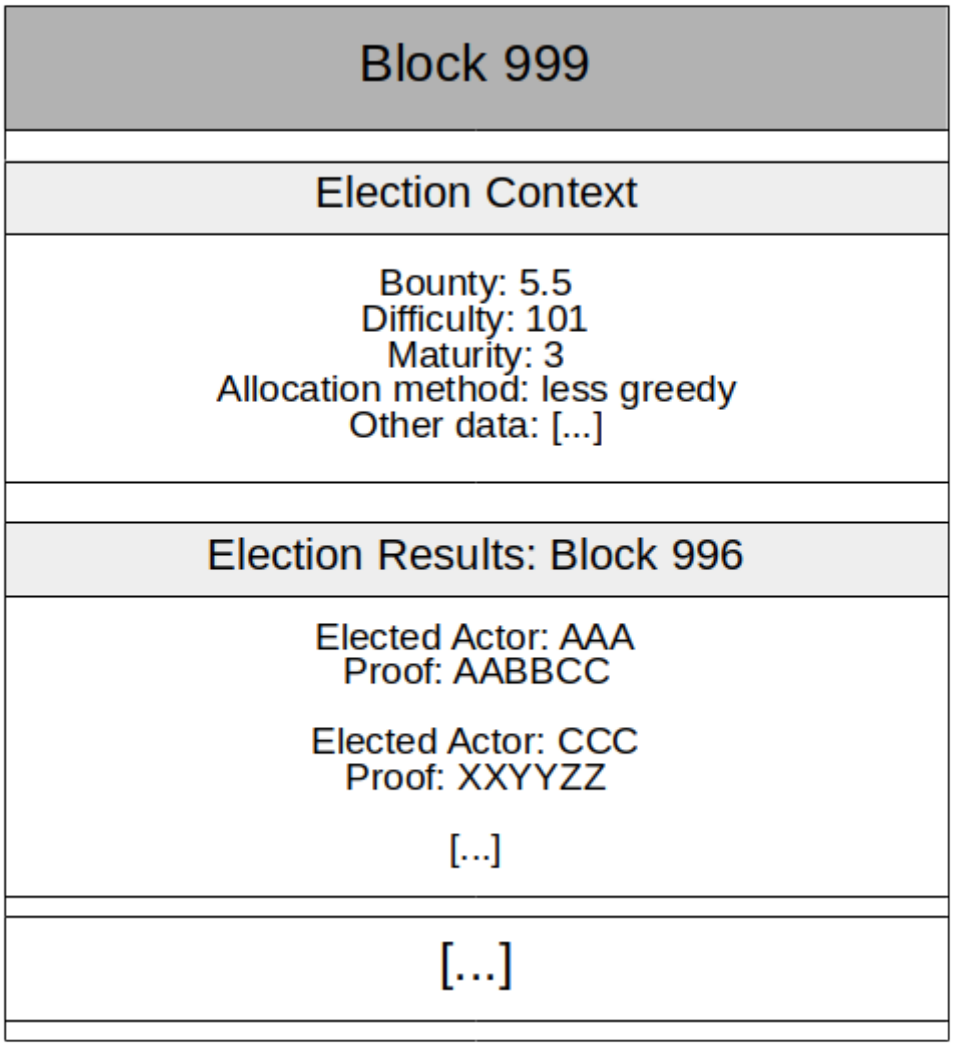

Figure 4: Election context in a block

The nodes who receive the blocks during blockchain synchronization will see the election context and begin the election process. The first thing it will do is take the maturity factor which will instruct it how much time (in block time) it must wait for the context to mature. This maturity time is to provide enough entropy to ensure inability to predict who will be elected on that future turn. In this manner, there is no way for the custodian to game the elections or steer it towards an intended direction. The entropy ensures that elections are absolutely unpredictable and fair to all.

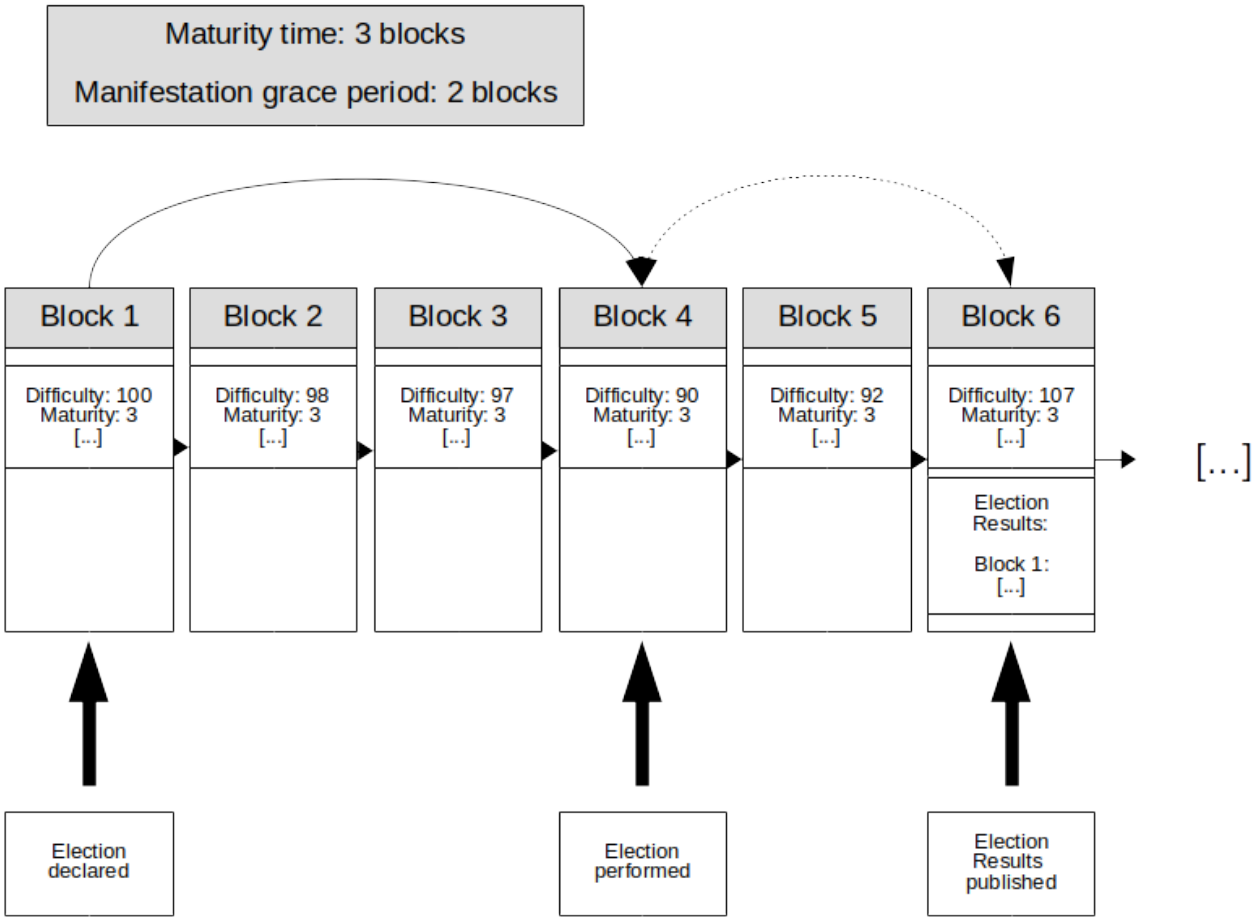

Figure 5: Maturity delays on an election in block time

Once the election context reaches maturity, the election will begin and the actors on the network will have to perform the following action they will combine and hash together the unique hash of the previous block (before maturity) on the blockchain with their own unique published account id. The combination of their own account id with the previous block hash is sufficient to give them a unique entry on the blockchain for the given block number. They will then factor the difficulty level provided in the context for this block and determine if they fall within the range determined by the given filtering formula. This process is very simple and performed only once per election. The energy requirement to perform this is minimal and the computations are very fast, and thus makes this mining process use no more computation power than any other regular non-looping computing activity.

If the miner does not fit within the required election range, then they are not elected, and no further action is taken and their turn is over. They must then wait for the next election to begin so they can get another turn at mining. If they do fall within the required filtering range, they are considered as elected and get to participate in the decision of what will be the contents of the blockchain during this particular block. They will then combine their election proof into a special election confirmation message, sign it with their account numbers private key and publish it on the network for all to see with any other data their elected status gives them the privilege to select such as transactions that should be included into the block.

The trusted nodes will receive and gather these election confirmation messages and validate the account numbers, signatures and election proofs. They will then combine all the valid elected account numbers and apply the rules that were set in the election context to determine if all their selected transactions will be merged together in the next block, or if one will be given

prime elected actor status and get to decide the contents of the next block by themselves. In this next block, the trusted node will again adjust the difficulty based on the number of elected nodes received in the previous block(s) to ensure a constant elected representative percentage of the whole network and the cycle continues with the following blocks.

6.3 IP Address Verification

In the POE algorithm, the limitation factor for mining is the combination of the unique account ID and the previous (to maturity) block hash with the IP address of the node on the network. In order to ensure that this combination remains unique for each account, a registry of those combinations must be maintained and kept up to date and this is where the role of the custodian comes into play as a sort of mining pool. Thus, in order to begin mining, the first step is for the node to register for mining. What it will do is create a special blockchain message where it will encrypt to a trusted node encryption key its IP, its account ID and a password. When the message is sent on the gossip protocol, the trusted nodes will capture this message and insert the miner into its registry. In order to enable mining, it will employ a special verification service that will confirm that the node truly is at this claimed IP address and available. It will do so by establishing a quick TCP connection and sending the shared password. If the node responds with the proper account ID, the IP is confirmed, and the node is now in the process of mining.

6.4 Optional Transaction Fees

In the Neuralium, transaction fees (appropriately called Tips) are entirely optional and at the discretion of the user. The Tips can be offered if desired when creating a transaction for the purpose of speeding up the confirmation of the transaction or to help support the network. Since elected miners will receive the Tips of the transactions that they select to insert into the block, they will usually pick the highest tipping transactions first, giving them priority. But if a transaction offers no Tip, it will still be confirmed into a block no matter what, albeit possibly at a later time. This is because contrary to POW systems where transactions with low or no fees can remain stuck in the limbo and never make it into a block, in the Neuralium, the trusted nodes can always add their own transactions into a block for the purpose of clearing the pool. This means that transactions that are never picked by miners will still eventually make it into a block and will never remain stuck, since the trusted nodes do not have the tipping incentive to pick transactions and can empty the transaction pool as required to improve performances and operation flow.

7 Secured Accounts and Funds

The Neuralium supports various security features that are made possible thanks to its managed ecosystem. Features like these are difficult or impossible to implement in other crypto tokens but are features that are very important to the user experience of participants.

7.1 Theft Freeze and Unwinding

The main security feature that the Neuralium supports is the ability to report theft, freeze the tree of stolen funds, investigate and then either unfreeze or unwind a fraudulent transactional tree. For example, if a certain user or group of users have their funds stolen, they can report this theft to the custodian, and it will be possible to freeze the tree of transactions moving the stolen funds to other accounts. Once this is performed, a thorough investigation can be

performed to determine which funds should and can be returned to their original owner and which ones must be let go. Once the investigation is completed, the funds can be returned to their rightful owners and the tree of fraudulent transaction effectively unwound. This in itself will serve as a strong deterrent to theft, since any dishonest activity will not be much worth it since stolen funds can be restored and the theft undone. Thieves will have a strong incentive to skip the Neuralium blockchain and operate their ill intended activities on other much less safe crypto tokens instead. This will further help secure the users of the Neuralium.

7.2 Integrated SAFU

The Neuralium also supports an integrated and opt-in SAFU (Secure Asset Fund for Users). The Neuralium will emit a daily figure that will determine how much a user must contribute into the SAFU daily to protect 1 Neuralium token for one day. The user can then contribute to the SAFU account and become an active member. Then, if the user is victim of theft, it becomes possible to request a compensation. An investigation will be performed and when it is completed and the request is determined to be truthful, the user may be given back the lost tokens from the SAFU account.

7.3 Account Resets

It is possible for users to opt-in the ability to reset their account keys in the event that the wallet was ever stolen or lost. To opt in, they need to register on the blockchain certain combination of factors that will become their reset key. If they ever lose their wallet, then they can use this special reset key to request a reset of the account. The custodian will alert the account reset 3 times on the blockchain over a period of many days . If anybody manifests with the wallet keys that can prove account ownership, then the reset will be stopped. Otherwise, the account will be reset with new keys and the user will regain control of the account.

7.3.1 Custodian Powers

As previously mentioned, the custodian does not have any control on user accounts. Only their private keys can directly control an account and its contents. In order to enable features like account resets, the Custodian uses its position as a trusted voice on the p2p to recommend a change, which is performed with acceptable conditions can be accepted by the decentralized public nodes. In order for the public nodes to accept a recommendation, the custodian must provide the secret recovery keys which can only be provided by the account holder. Without these keys, the custodian is powerless, and the account is permanently lost.

8 Digests: Reduce The Blockchain Size

One of the greatest strength and weakness of the blockchain is that it is an ever appending log of activity. Every new block is appended to the chain of blocks and grows the size of the blockchain on disk over time. It is not really possible to remove blocks from the disk, because then they would not be available anymore to verify the entire history of transactions, they must thus remain available. This means that the blockchain grows endlessly and may, over time become unusable for the average users, who will require an infinite amount of disk space and synchronization time.

The Neuralium supports the concept of Digests, which is essentially a form of super block that can be emitted at any time and will compress the state of the blockchain at the given block time. This way, once a digest has been emitted, the user computer is free to physically

remove from disk the blocks covered by the influence of the digest if they want to, or not. The old blocks remain available for those who wish to download them at any time, but for users wishing to keep the size of their blockchain to a minimal, digest can be used to give a starting point and save the disk space of blocks coming before it. Over time, new digests can be emitted to replace previous ones , and thus allow for more blocks to be deleted. When a new node begins syncing from scratch, the first thing it will do is sync the latest digest and then continue with the following blocks. This will also result in dramatically faster synchronization times.

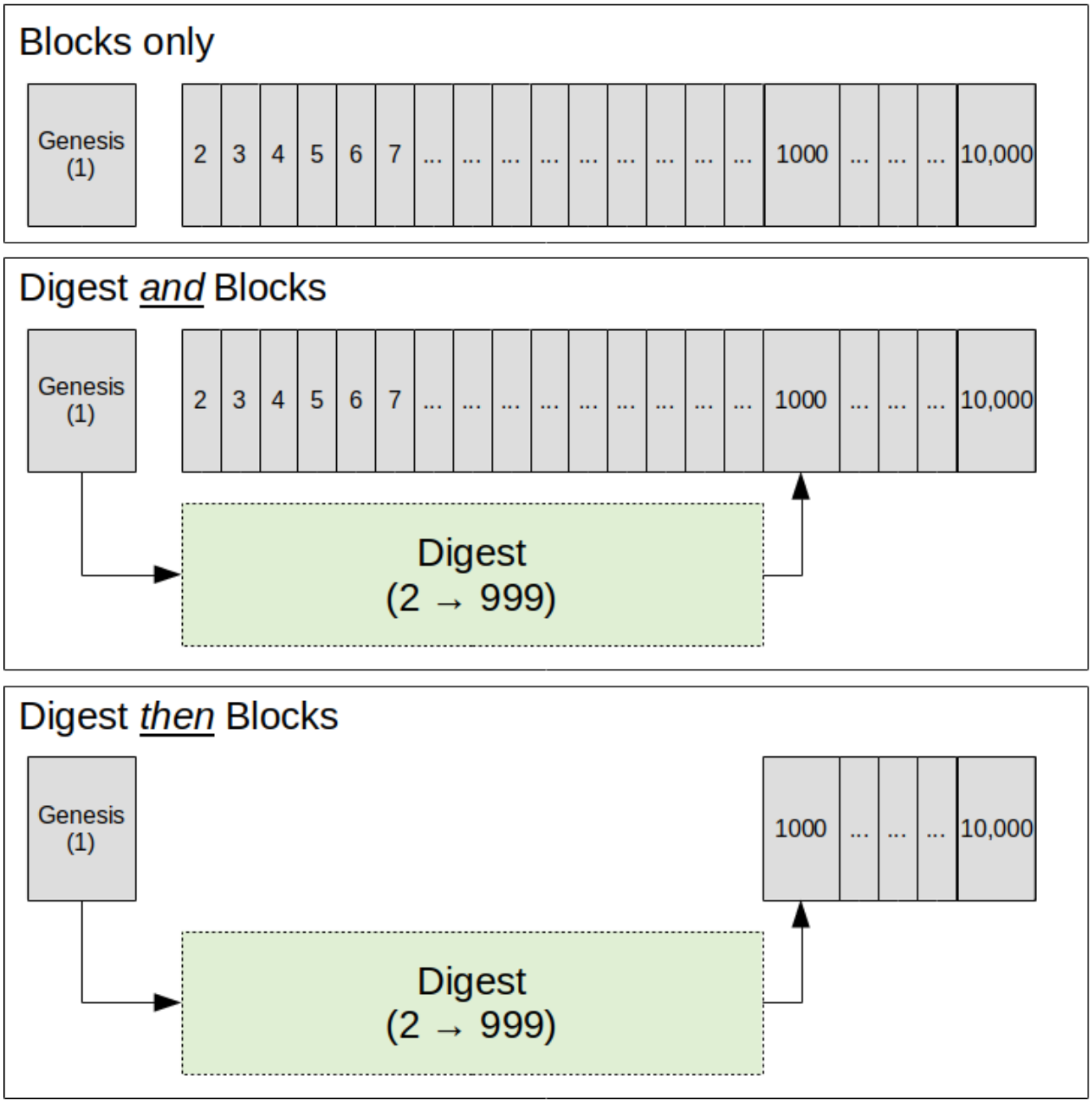

Figure 6: The different blockchain saving options

9 Accreditation Certificates

One of the greatest weaknesses of existing cryptocurrencies relative to the average users is their inability to control the quality of their own ecosystem. Because nobody has the ability to police the quality of the players in play, they quickly become the target for hackers and ill intended

players who develop faulty services on the ecosystem. The average unsophisticated user does not have any ability to discern a quality player in the field compared to a less reputable one. This results in very high amount of key theft and hacks by less than reputable third-party websites and operators.

The Neuralium has the ability to accredit certain players to operate on the blockchain by validating their infrastructures and making them accountable to ensure certain quality and security standards. It is only when such a third party meets or exceeds these expectations that they will be certified on the blockchain to operate. When this happens, a special accreditation certificate is emitted on the blockchain publicly for all to see. The player can then operate by providing its certificate to prove its accreditation. The third-party player is responsible to maintain quality, and its certificate can be revoked at any time if it ever lowers the quality of its service guarantees. The end result of this system is that the average user can be sure that the third-party ecosystem is of much higher quality than would be otherwise, and cryptographically certified players are acting with a valid license and thus abide by certain standards of quality. In this manner, the ecosystem of the Neuralium will be of higher quality than other cryptocurrencies where the ecosystem are completely unregulated and amount to a far west style bandit paradise.

10 Parallel Blockchains

The Neuralium is built in such a way that it is capable of handling multiple blockchains in parallel, either independently or interdependently. At launch, the Neuralium will have a single token, but it may very well support more in the future as further enhancements are made to the ecosystem. Each blockchain can be custom programmed and perform any type of operations independently of the others in the same runtime core. Users are free to enable certain blockchains, all or none as they desire as it is entirely configurable.