Random Chain

August 30th

Executive Summary

1) Random Numbers & Security

Alphabetic and Numerical Security - Is it really security?

Random Number Security/Hash Functions – Is it the Most Secure?

Cold Security Versus Hot Security

Pseudo Random Numbers

Gaming and Pseudorandom numbers

Timestamps

Uport

Identities created using uPort

2) Blockchain Basics

Proof of Work & Delegated Proof of Stake

Main Chain and Auxiliary Chain (Merged Mining)

The Benefits of a Decentralized Two Factor Authentication Chain

3) How will Random Chain be realized?

GDAO – Global Distributed Autonomous Organization

Consensus Mechanism

Reward Transaction vs. Ordinary Transaction vs. Burning Transaction
Voting

Structural Design

Delegated Node

Encryption

4) Development Roadmap & Token Information

Project Roadmap

Token Distribution

Technical Specs

Application Summary (Random numbers for casino games)

Detailed Project Breakdown

Random Chain Analytics

Scalability

Potential Partnerships

Future Planning

Incentives

Conclusion

References

Executive Summary

The broad usages of computing and telecommunications systems have produced a relentless need for information security. Protection against unauthorized use of information––especially electronic data––or unspecified measures developed to achieve the collection of personal data have induced an evolution of methods to protect private data.

Conventional methods of information security are losing ground to more sophisticated means of protection. In the beginning, just a series of alphabetic and numerical were common practice and are still widely used today. As the need for protecting sensitive personal information has grown, a slightly more complex method called “two factor authentication” is becoming normalized amongst the mainstream technology brands. Today, more sophisticated information security techniques such as random number security (or hash functions) are not only finding uses within its traditional cryptographic community, but potential implications in virtually all matters involving information security.

This paper will highlight the common methods of traditional information security and elaborate on more sophisticated methods and implications. We will also explore growing techniques for information security through decentralized information security networks that is commonly referred to as “blockchains.”

The relationship between casino owners and players has always been insecure. Establishing true trust has been difficult to achieve due to kinks in the current system like owners who don’t endorse fair play or players who try to cheat the system. Random Chain looks to create this trust by implementing a blockchain based random number generation platform.

Random numbers are commonplace in the casino industry, specifically electronic based games like slot machines, black jack, roulette, poker, and many others. By using blockchain technology Random Chain can guarantee better fair-play to both, the player and the casino owners, this increases the security of the numbers generated by using smart contracts to maintain or change simple variables like the amount of numbers generated, the form of the number or speed of generation. The random numbers will be generated based on Random Chain's block hashes, which are linked together by our blockchain design with a specific timestamp, making them immutable.

By guaranteeing fair play it will increase Random Chain's player retention rate which for casinos, means more profit in the long run. With fair-play validation, Random Chain can prove to players it's not rigged based on factors like the size of the pot, player VIP status, previous interactions or money spent, and to owners it provides high quality analytic data which provides more potential opportunities in each specific player to exploit such as, which games they play, cross-selling and up-selling players to other games, or which type of player is more likely to respond to marketing emails.

Random Chain intends to establish trust between casino owners and game players!

Random Numbers & Security

Alphabetic and Numerical Security - Is It Really Secure?

At this point we are all familiar with the concept of an alphabets and numbers as a common attempt to protect private information. From gambling slot machine to online banking to email, we are heavily reliant on the use of an alphabetic and numerical number. An alphabetic and numerical number remain popular because it is a tried-and-true technique for a large population to intuitively understand how to use.

Although popular and easily implemented, an alphabetic and numerical sequence is the most susceptible to compromise. When a hacker wishes to obtain a alphabetic and numerical sequence, they have several techniques at their disposal: A brute force attack, a dictionary attack, or a downloadable tool that discerns between normal traffic and hashes within a network––to name a few (nFront Security, 2008).

Some ways to combat hackers from easily obtaining involve using special characters, longer values of more than eight characters, and avoiding using a variation used before. However, when given enough time and resources, a traditional alphabetic and numerical number can always be compromised.

Random Number Security/Hash Functions - Is it the Most Secure?

Random number generation is the generation (RNG) of a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance. A hash function is any function that can be used to map data of arbitrary size to data of fixed size, with slight differences in

input data producing very big differences in output data (Rune Skovbo Johansen, January 7, 2015). It is possible to combine random number generation with hash functions. A RNG is typically passed through a hash function using different seeds (or whole number i.e. 0, 1, 2...). An example of how a RNG can be incorporated into a hash function is seen below.

Picture

Using RNG or hash functions is proving essential in the information security environment of today as the level of sophistication of intrusive programs have elevated in recent years. Current mainstream applications of RNG and hash functions are found within the cryptographic community in the form of "pseudorandom number generation." Pseudorandom number generation (PRNG), although not wholly random, relies on the generation of a determined initial value (a seed). Cryptographic uses require the random sequence to not be predictable from previous generated sequences. In statistical terms, RNG versus PRNG are essentially indistinguishable and therefore PRNG is a highly secure method of securing digital information.

Cold Security Versus Hot Security

Cold security and a hot security are information security methods that are capable of containing the same data, but often used for different purposes. Cold security is the concept of protecting information that is stored offline whereas hot security is connected to the Internet. Although cold security and hot security are capable of storing the same information, they are usually used for different purposes.

An everyday example of hot security is email. We all generally have thousands of emails currently stored online in any number of email providing services. These services provide security usually by traditional security methods i.e. an alphabetic and numerical sequence. Some advanced examples of hot security are online banking and government related websites. These typically require more layers of security because they contain more sensitive information.

An everyday example of cold security is an external hard drive. Any number of documents or applications can be stored on this device and both online or offline. If the computer of the user is not connected to the Internet, the security of the information contained on the device is typically inaccessible to an outside source. Security of cold storage is limited only by the diligence of the user.

Pseudo Random Numbers

Pseudo random numbers are a set of numbers, which prove to be unpredictable in nature and are highly integrated with the information age we live in today because they provide high security in computer applications. The actual application type is referred to as a pseudorandom number generator (PRNG) or deterministic random bit generator (DRBG). PRNG's are highly regarded for their speed in number generation; pseudorandom number generation is meant to mimic that of sequences of true random numbers. They are called pseudorandom because they are not truly random due to them being determined by an initial value also known as the seed.

In the case of cryptography, the output cannot be predictable from earlier outputs and using the time of the block creation can generate the seed. To this day the only way to have a truly random number generated is by natural events like flipping a coin or throwing darts etc.

The seed of pseudorandom numbers is the initial state of the algorithm which acts as the key, it is very important for this initial state to be well chosen and hard to guess, when an encryption key is pseudo randomly generated, having the key allows one to unlock and obtain the generated key, in Random Chain's case the two-factor authentication code.

Gaming and Pseudorandom numbers

Random numbers and gaming have always inexplicably been linked even though in the early days of say, Atari they were more of an illusion to make the player think it was a random event. Today this is still kind of the case albeit a little more sophisticated as the technologies have developed 1000 fold, random numbers make the player feel like their experience is their own in the sense of any event happening is truly random but the reality is this is still not the case because it's just the way computers are made, what's changed is the intensity of the algorithms developing these pseudorandom numbers which make games feel less "determined" and more unique.

The benefit to the developer and the player is replay ability, which makes the game more valuable. Some common use cases today for pseudorandom numbers in games are procedural map generation like in Minecraft, the artificial intelligence in games like Halo or sprite generation in a game like Elder Scrolls V Skyrim. In Random Chain's case, casino games like slot machines or games of chance such as online blackjack or poker, the pseudorandom number generator is the most essential element. A popular game today which main component is using a random number generator is Hearthstone, developed by Blizzard. An improper random number could be the difference between a player being paid out correctly or incorrectly or allowing the player to guess the algorithm being used so they can easily predict when to bet high or low.

The pseudorandom numbers will be generated based on Random Chain's block hashes which are linked together by blockchain design with a specific timestamp which makes them immutable, this creates high security and also the ability to generate as many numbers as needed in a fast amount of time due to the Random Chains dual blockchain architecture using both PoW and DPoS consensus mechanisms.

Timestamps

A timestamp is a record in printed or digital form that shows the time at which something happened or was done. We are familiar with timestamps in digital format in the form of sending and receiving emails or conducting any sort of online transaction i.e. online banking, ticket booking services, etc. A timestamp ensures that at the time of the stamp, any information recorded at that point was present at the time of the stamp.

In matters involving information security, this can have a range of implications. Anything involving a digital signature will require a timestamp to ensure authenticity of the user to access or store information. Presently, timestamps are a reasonably secure method of ensuring data accuracy. It is possible to modify timestamps although it is difficult to change a timestamp without someone noticing the modification. Timestamps are generally ordered in the times they are received and assigned a corresponding sequencing value i.e. 1, 2, 3… in the order that they are received. To change a timestamp, the sequence as a whole would also need to be modified without anyone noticing. On timestamp servers this would be virtually impossible to achieve because storage is often copied and stored in many locations. Someone trying to modify a timestamp would have to modify all of the copies––at this

point it is impractical, especially on large timestamp servers, to attempt to modify a timestamp.
Timestamps are an integral aspect of blockchain technology. Blockchain technology is fast becoming a revolutionary application of the traditional timestamp method by storing information publicly in the format of a “digital ledger.” The ledger is distributed across a decentralized network of nodes (computers) that independently confirm the transfer of information (Judd Bagley, 2016). All transactions are checked separately for accuracy/authenticity against all previous records.

uPort

uPort is a service that will report a timestamp based on a few different details; who, what, when, where. This process is important to keep the chain transparent. An identity in uPort is really just someone or something that can sign data or transactions and also receive signed data about itself.

An identity has:

- An Identifier in the form of an MNID
- A signing key
- A public key stored on the uPort Registry

An identity can:

- Sign JWTs (JSON Web Tokens)
- Authenticate himself or herself to a third party
- Disclose private information about them
- Receive requests for disclosure about themselves
- Receive and store signed third party verifications about them
- Sign Ethereum transactions
-

Picture

Identities created using uPort

Currently most uPort users manage their identities through our mobile app. Identities created today consist of an instance of the Proxy smart contract deployed on a supported Ethereum-compatible blockchain.

Requests always consist of URLs that are handled by the mobile app. There are different built in ways of sending the URL to the mobile app.

The 3 basic ways of sending a request to the phone are:

- Open uPort URL on the phone
- Scan QR Code
- Send Push Notification

For all of these cases the request consists of a URL

Open URL

On the device any URL whose scheme is me.uport: or hostname is id.uport.me will be opened directly in uPort.
The benefit of using https://id.uport.me URLs is that they will open a web site with an App Store link if the uPort app is not installed. On a desktop browser, the browser will display a QR code containing the request and will ask the user to scan the code with their mobile app. The basic purpose of these URLs is to create links in a mobile web app containing requests to the uPort App.

iOS developers can work with the "URL" directly.
Android developers can use the "ACTION_VIEW intent" to open the URL as well. In addition to this basic interaction pattern, URLs starting

with https://id.uport.me can be sent as tweets, in messages, emails or any other way that you interact with your users.

QR Code

By encoding the request in a QR code it is very easy for users. You can also scan these using the system camera and the app will open.

While this is often used for interacting with an application in a desktop browser, they're other applications: QR codes can be printed or displayed at conferences, on posters, or in other real-world use cases.

Push Notifications

As part of a regular Selective Disclosure Flow you can request permissions from your user to send requests directly to their uPort app using push notifications.

Push notifications makes the interaction flow much simpler for users if they have to interact with multiple requests on their phone.

They can also be used to send Verifications or Ethereum Transaction Requests directly to the user outside of a regular logged in session based on some external event.

Blockchain Basics

Proof of Work & Delegated Proof of Stake

The consistent need for validation and consensus of authenticity of recorded information has challenged computer scientists to create new methods for solving these issues that will be valuable in the future of information security. Two proven solutions can be found within the cryptocurrency (digital money) community: Proof of work (POW) and delegated proof of stake (DPOS).

POW was the first solution developed and involves nodes (computers) of "miners." Miners are essentially computers dedicated to solving algorithms that receive a digital currency as a reward. Every time these miners solve an algorithm, they also verify all of the information of previous transactions of their blockchain (online ledger of recorder transactions).

DPOS is a newer solution that involves electing a group of "block producers" (computers used to solve algorithms and validate transactions) and scheduling their precise production times. The need to schedule their production times is essential so the chain can expect each subsequent block to arrive at an exact time from each specific block producer.

Below is a more detailed description of the concept of POW and DPOS from a white paper from John Greenfield IV of A Medium Corporation.

Proof of Work: A Proof-of-Work system requires its users to perform some form of work to participate. The work must be difficult for the client but easy for the server/network to verify. In Bitcoin and Ethereum, PoW exists in the form of Miner nodes competing to "solve a Block," or group transactions together in (potential) chronological order and have that block accepted onto the global Blockchain of that system.

Proof of Stake: Proof of stake is a different way to validate transactions based and achieves the distributed consensus. It is still an algorithm, and the purpose is the same of the proof of work, but the process to reach the goal is quite different. Unlike the proof-of-Work, where the algorithm rewards miners who solve mathematical problems with the goal of validating transactions and creating new blocks, with the proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake. This means that in the PoS system there is no block reward, so, the miners take the transaction fees. (Robert Greenfield IV, 2017)

The POW and DPOS methods have wider applications beyond cryptocurrency blockchain production. As blockchain technology strives to solve the issues of information security through decentralized encryption through a public ledger, a need for producers of blocks to authenticate transactions and validate information shared historically and real time will be essential.

Main Chain and Auxiliary Chain (Merged Mining)

In the cryptocurrency community there are hundreds of different crypto currencies, also known as coins or digital tokens. All cryptocurrency uses blockchain technology as a method of securing the information needed to make transactions. Because the bigger cryptocurrencies have more support and are in general more powerful than a newer cryptocurrency, a need for enabling smaller coins to become powerful enough to also become a useable coin.

Merged mining refers to the process of reusing proof of work (POW) solutions from an established cryptocurrency as valid proofs-of-work for one or more child cryptocurrencies (Auxiliary chains). It was introduced as a solution to the fragmentation of mining power among competing cryptocurrencies and as a connecting mechanism for small networks (SBA Research). Smaller coins tend to have less hash power to conduct their own POW, therefor by using the algorithms of an established blockchain they can increase their hash power and become viable.

A main chain is the original blockchain. It has an extensive POW that includes every transaction ever conducted on the chain within each subsequent block. Each block is organized chronologically because of their hash numbers. A block will have the hash number of the previous block thereby connecting each block to create the “blockchain.” An auxiliary chain will use the algorithm of the existing main chain and also create its own separate chain.

The Benefits of a Decentralized Two Factor Authentication Chain

Two-factor authentication is a reliable information security method that adds an additional layer of security over traditional information security techniques. Two Factor Authentication is a two-step verification that requires a alphabetic and numerical sequence and something that only the unique user possesses or can readily access. Although effective, there are some shortcomings, namely the user needs to have a dedicated device in order to receive and SMS or use a specified application on their phone to verify their identity. A growing need for a decentralized method of verification can be solved with blockchain technology.

A decentralized solution using a blockchain framework would issue a digital token using a designated blockchain containing the personal information of the consumer. Upon providing this token to digitally sign the login process the user is then authenticated to access the platform. Because every token would only be deemed valid through its private key, which is owned by the user, no one else can access the platform through their credentials (Jean-Pierre Buntinx, Bitcoin.com).

The benefits of decentralized two-factor authentication are simple, it would involve only one step for the user to access all personal information contained on the blockchain. This method would be as simple as traditional security methods involving an alphabetic and numerical sequence, which takes the same amount of time to access their information. The blockchain ensures complete decentralized encryption of all data from intrusive schemes unlike the modern networks of today.

How will Random Chain be realized?

GDAO – Global Distributed Autonomous Organization

Global Distributed Autonomous Organizations or GDAO's can be described as organizations, which are arranged and controlled by smart contracts using blockchain technology to provide digital security via a public ledger, or record, which is used to track interactions across the Internet.

These "smart contracts" are electronic agreements which facilitate themselves without a third party, they are written to do certain tasks upon a particular timeline or transaction happening which are completely self-executing, for example: when your food is delivered, your cryptocurrency wallet automatically deducts the money owed without you having to even interact with another human being. The idea is simple: to reduce time and money associated with traditional contracts, like hiring a lawyer to verify both parties agree on the terms or store your secure information on a company's servers.

Blockchain ledgers are secure because every transaction has a trusted timestamp, which is permanent and can be viewed by the public at any time via a distributed database (blockchain). These transactions can be verified due to the very nature of a distributed database. A distributed database is the idea that the information is stored and replicated across multiple devices or storage mediums which are not central to one computer, network or area which means in order to change a transaction you would have to change multiple copies of the ledger, not just one.

GDAO's remove the middle man such as Google or Apple which just about anyone who uses technology naturally trusts with very sensitive

information, which you may use for multiple other accounts or your banking information. By removing the middle man or third party it speeds up the process of just about any type of transaction whether its financial matters or property ownership because it's peer to peer (p2p).

In the case of Random Chain this is essential for security because it puts you in control of your sensitive data, eg: two factor authentication codes and not a third parties' servers.
Random Chain is a simple yet revolutionary concept which as stated above puts you in total control of your security, all users participate in the GDAO by default and it's maintained by you, the community. We are seeking to decentralize two factor authentication codes (2FA) by using blockchain and simplified smart contracts. Random Chain will be easy to understand and use, users will have full access to the community through the Random Chain website and clients, including a light client for quicker synchronization of nodes.

GDAO's main objective is to make a website like a blockchain browser, user can get information's about blocks, trades and smart contracts. Special users like casino's owners can get API of their random numbers produced by the smart contracts. Blockchain address balance will limit different users from different functions on the GDAO website.

The Random Chain GDAO website will include the following features:

Blockchain browser – An Etherscan.io like interface that contains block information like transaction hashes which include transaction history, amounts and more, smart contracts as well as token trades and balances.

API section - Users have different levels of access, eg: a casino owner would be able to view things like the speed of random number generation, the form of the numbers generated or view their API key based on their Random Chain address.

Full Client – A full client requires the user or node to download all of the current blocks on the chain, which requires a good network connection and high-quality hardware, where as a light client, is much easier to connect and simply use the network.

Light Client – Having a light client allows our users and casino owners to sync with the nodes faster and more efficiently because it only fetches the necessary information and fetches it on demand. These clients only download the block headers as they appear on the network (proofed by full nodes) they also do not use local storage, instead they use distributed hash tables.

Voting Section – Using DPoS requires a form of voting in the delegated nodes, which means the community who is using the Random Chain has the right to vote these trusted, delegated nodes into power, this also means they are responsible for making sure these nodes aren't doing any malicious activity within the network and if they do, they should revoke their vote immediately. Standard users who do not wish to part take in voting may hand off their vote or votes to someone else to do so for them.

Consensus Mechanisms

A central aspect of the Random Chain is the distributed ledger, meaning it's stored across many nodes throughout the world, a key operation of a distributed ledger is ensuring that the entire network of nodes collectively agrees on the content of the ledger, eg: a consensus mechanism.

There will be two blockchains involved with the Random Chain, using two different consensus mechanisms. The main chain which uses proof of work (POW) and generates seeds at slower speeds but higher

security and a secondary auxiliary chain, which uses delegated proof of stake (DPOS), which integrates information at a faster, speed but lower secutity and is responsible for the pseudorandom number generation.

Proof of Work – POW

POW consensus requires miners to solve a cryptographic puzzle and by completing the puzzle it proves that all transactions in the block are valid and the block is added to the blockchain and the miner is rewarded in a small amount of cryptocurrency.

The Random Chain keeps the two chains linked, you can think of this relationship like the memory (RAM) in a computer and the hard disk (HDD) of a computer. Hard drive chain is the main chain and most secure part of Random Chain and the ram is the auxiliary chain which provides the speed for pseudorandom number generation. The purpose of the main chain is to generate a random seed so that the information sent and received from the blockchain is very small which is a great way of guaranteeing the speed of delivery for the next block, the auxiliary chain supports the main chain in ways such as completing tasks like full pseudorandom number generation, the accounting, smart contract delivery, and other tasks which do not necessarily require as much security, the auxiliary chain will also store data and translate the random seeds for human interpretation. The GDAO will maintain the consensus mechanisms and the operation of how the two chains communicate and exchange their information. The biggest part of the consensus mechanism to remember is that it allows all users across the network to agree on the state of the data in the distributed database, but you need to note that the auxiliary chain can only read data from the main chain NOT write data so the seeds are truly safe and secure, our chain will also be based on burning transactions which will be touched on below.

Delegated Proof of Stake - DPOS

The difference between the two is that DPOS is more efficient and less energy dependent in relativity to POW. DPOS uses a reputation-based system and real-time voting to accomplish consensus and is highly scalable. The community gets to vote on “Super Representatives” or delegates to secure the Random Chain network whom are rewarded by validating transactions for the next incoming block.

Although we won’t be using Proof of Stake (POS) the advantage over POS is community control with DPOS of who is validating and producing blocks. If a voted in Super Representative/Delegate doesn’t perform to the community’s standard, the community can remove their votes, which is the equivalent to firing them.

DPOS consists of two types of nodes, block producers (delegates or super representatives) and block validators, block producers are those responsible for maintain the important part of the network, are limited in number and must be voted in by the community, where as anyone can be a block validator. Block validators verify the blocks created by the block producers.

Reward Transaction vs. Ordinary Transaction vs. Burning Transaction

How do they relate to Random Chain?

The idea behind Random Chain and using decentralization to store your own seed makes it quite secure because your seed is actually stored on your own device or Blockchain and generated by you, which puts the security in your hands. How it works is once the information is written

to a block the entire network can see this and therefore cannot be mutated, these “hashes” are extremely difficult to predict, and are built off of one after the other which only increases the difficulty of being able to regenerate the random number. Random Chain will link the generated numbers to these hashes and every block written corresponds to a new random number, which also increases the security of the seed.

The main point to keep in mind is that the security of the random numbers depends on the security of the random seed, and if the random seed is in the hands of corporations (eg: Google) like all two factor authentication methods today than they are susceptible to internal or external attacks which could put your security at risk.

The key to the Random Chain is using highly complex pseudorandom number algorithms, which are linked to the blockchains design by using timestamps plus high-level seed generation which means that the user is in total control of their security. If you think about Google’s two factor authentication for example you can see how the security is completely in Google’s hands because you don’t know the type of algorithms they are using or who has access to their servers and as stated above could be susceptible to outside attacks or vulnerabilities.

What exactly is a burning transaction?

A burning transaction means every time a transaction occurs a fraction of that transaction is “burned”, in blockchain terms this means a small part of the transaction is sent to an address that is verified as unusable, these addresses are unusable because they do not exist and can be compared to sending Bitcoin or Ethereum to an incorrect address string, there is no way to recover those coins because they are lost in cyberspace, forever. By burning part of the transaction, it creates scarcity and drives up the value of the overall coin. POB is often called

POW without the energy waste because the nodes are still rewarded in coins for their contribution to keeping the network agile.

There are two advantages to the proof of burn type of transaction 1) less energy waste, burning the coin is considered similar to the power and energy required to mine a coin in the reward type of transaction because its considered “hard” to do, can you imagine burning a $100.00 bill to prove your loyalty to the government? And 2) It promotes “miners” to stay more active on the network because they have already contributed by “burning” their coins. Similar to a one-time investment like the upfront cost of buying mining equipment for the POW consensus.

What is exactly is a reward transaction?

A reward transaction is a transaction in which the nodes or “miners” offer their hashing power on a grid as a single node and have to solve a cryptographic puzzle which earns them the right to mine the next block and they are rewarded in a small amount of whichever currency they are helping mine eg: Bitcoin, one big issue with this type of consensus mechanism is the energy consumption and the pace at which technology moves makes your mining equipment quickly outdated and therefore costs a lot to maintain.

POW/ Reward transactions are currently the most common type of consensus mechanisms across blockchain technology because they are technically still more secure and more decentralized than other types. Like in DPOS

How does this relate to Random Chain?

Random Chain will primarily use burning transactions, which is related to the GDAO but will also implement a reward transaction for each generated block. Every time a user uses the Random Chain there is a

reward transaction and each following transaction is a burning transaction, which means that the generation of the random value is extremely fast. The GDAO will check the timestamp of the last transaction, if the time has exceeded a certain amount of time, the burning transaction happens before the Random Chain generates a number, when the burning transaction happens the node only needs to listen up until the last burning transaction to verify the timestamp which keeps the number of transactions on the main chain quite small and the Random Chain generates a random number based on the hash value of the block.

Voting

Voting is related to the DPOS consensus mechanism, which means that the community is in control of who is running the nodes, these nodes are known as super representatives or delegates. These super representatives are responsible for validating the block transactions and are voted in by the community; at any time if a super representative doesn't perform to the community's standard they can revoke their votes and vote a new node in.

DPOS is a more democratic system and is much more efficient than the traditional POW, it allows blocks to be validated in a matter of seconds versus minutes and the voted in delegates are incentivized to maintain their nodes for monthly rewards as well as transaction fees. Generally speaking there can only a set number of delegates, who causes competitiveness, and therefore you are encouraged to maintain your node so the community does not vote you out.

DPOS consists of two types of nodes, block producers (delegates or super representatives) and block validators, block producers are those responsible for maintain the important part of the network, are limited

in number and must be voted in by the community, where as anyone can be a block validator. Block validators verify the blocks created by the block producers.

Voters on the network can also choose to delegate their stake in the network to another voter who can vote in the block producer election in their place.

Voting also isn't all equal, if you have more stake on the network, eg Proof of Stake, your vote counts for more.

Structural Design

The Random Chain is based on a double-stranded architecture, the main chain and the auxiliary chain; these two chains will work together to provide fast, efficient & secure randomly generated numbers. The main chain will use POW consensus to generate the contract seeds because the seed generation doesn't need to be fast. While the auxiliary chain will use the DPOS consensus mechanism to generate the actual pseudorandom numbers themselves at a much higher rate (up to 1 per second, per contract). The auxiliary chain will use a system similar to DPOS which asks nodes to sign all numbers and ultimately generates the final pseudorandom number result. This will make Random Chain more efficient by dividing the seed and the pseudorandom number generation tasks amongst the two chains, and creates an extra layer of security from a block producer being able to pre-calculate the potential outcome.

Concept

The idea is this node (N) uses their private key (SK) to sign the random number (RN) which generates Signed_RN, after Signed_RN is generated, RN is open to be generated by any of the nodes, once the random number (RMN) has been chosen it can be verified by using the nodes

(N) public key (PK), since the generation of the random number (RMN) is signed by the one and only nodes (N) private key (SK) only the chosen node can predict the random number (RMN).

Security Concerns with DPOS

Delegated Proof of Stake is much faster but is less secure because the producer of the block is aware that they have been selected to produce such block and has the potential to pre-calculate the most beneficial result to their situation which would remove the fair-play element of Random Chain.

EG: There are 100 transactions between block A and block B which means there are 100 different sets of numbers that would be generated, if the block producer knows they are selected to produce a particular block, then they can pre-calculate which one of the 100 transactions is most beneficial to their situation without anyone ever knowing the wiser.

With the double stranded architecture we can potentially avoid this problem by splitting the seed and the pseudorandom number generations between the two chains and using the below algorithm to select the node (block producer) and to generate the actual numbers themselves.

Node Selection and Pseudorandom Number Generation

Using the DPOS consensus mechanism, there will be 2 sets of 3 smart contracts working bilaterally that generate the initial psudorandom numbers which then concatenate parts of each of three into one random number (aRMN) eg: RMN1==123, RMN2==654, RMN3==789, so aRMN == 23 65 89, this process is happening bilaterally to create the fRMN which consists of aRMN + aRMN so in practice it should be. ((RMN1a + RMN2a + RMN3a) == aRMN) + ((RMN1b + RMN2b + RMB3b) == bRMN) which is equal to fRMN.

Although it is possible to predict the pseudorandom numbers which will be generated, the amount of computational power required would be enormous. The only other possible outcome of corruption would be if all of the delegated nodes (block producers) cheat together when they are selected to produce a specific block.

Main Chain

The main chain will record transaction information, and conduct the random seed generation. The role of the main chain is to generate secure, seed numbers with high security; the speed is not important because the basis of the pseudonumber generation happens on the auxiliary chain using DPOS. Before each block is generated, the main chain communicates with the auxiliary chain and the delegation node's candidate list is searched using the DPOS consensus mechanism, the candidate list is obtained by working alongside the GDAO by reading information such as who the Super Representatives are from the auxiliary chain. The very first transaction, which occurs, is a reward transaction and each following transaction is a burning transaction.

Auxiliary Chain

The auxiliary chain is capable of generating one block every second using the DPOS consensus mechanism; this means the generation of the actual pseduonumbers themselves will be very fast. This auxiliary chain is responsible for verifying transactions in real time and integrating them with the main chain like verifying the seed number along with recording both the reward transactions and burning transactions. The auxiliary chain is also responsible for sorting and recording the pseudorandom numbers generated and passed on to the end user. A key factor of the auxiliary chain is the simple smart contract function, which only use certain functions to generate pseudorandom numbers and its ability to only read data from the main chain.

How they can work together

To summarize the overall structure of the Random Chain, the two chains will work in unison with each other but have very different functionalities. The mainchain records little information but is much slower and is responsible for generating the initial seed numbers as well as the burning transaction and security, it accesses the burn time via the auxiliary chain. The auxiliary chain generates the pseudorandom numbers and records all of the main information like transactions and finishing the pseudorandom number generation but is much faster at 1 second per block. The POW consensus mechanism, which is used by the main chain, ensures security after accessing the list of delegated nodes through the auxiliary chain using DPOS, which combine the auxiliary and voting nodes, by using two chains and two consensus mechanisms it provides more reliability, security and decentralization to the Random Chain.

Main chain blocks recorded as = M0, M1, M2, etc.
Auxiliary chain recorded as = A0, A1, A2, etc.
AUXILIARY blocks generated between each of the MAIN blocks = 300

The main chain and auxiliary blocks are generated at the same time, eg: M0, A0, after A0 is generated, the GDAO integrates the node generating A0 and the mainchain communicates with the auxiliary chain which then uses it's DPOS consensus mechanism to vote on a list (L0) of 300 nodes, the auxiliary chain then selects a single node from (L0) by using the DPOS consensus again and the entrusted node then listens for the burning transaction which is then rewarded by completing the block. After A0 is written, A1 is generated and the process repeats in a loop.

If the main chain can produce 1 block in 100 seconds with it's POW consensus, at the start of the block production (0seconds), the main pseudorandom seed is generated which is in-fact unique to each contract, the GDAO then specifies which delegated node will be the

block producer. At 1 second the auxiliary chain generates the requested pseudorandom number and the delegated node signs for the random seed (generated by the main chain) using its verifyable private key.

Alternatives

An ideal public pseudorandom number should be fair in the first place, that is, all interested parties are absolutely equal in the process of generating pseudorandom numbers, and no one has a comparative advantage; Second, it should be public, including that the generated steps are public, the methods used are public, and the results are public; Then make sure that the process and results are auditable and that the resulting pseudorandom numbers are not tampered with and stand up to ex post checks. It is not impossible to introduce a third chain for security purposes, but to see if it is necessary, the random chain is designed to produce random numbers efficiently, safely, and fairly using blockchain technology, But there is no blockchain technology that can satisfy this requirement. The first edition of the White Paper, which focuses on blockchain protection schemes for random seed numbers, is acceptable, Choose a double - chain structure based on pow and dpos to ensure the above conditions, from an engineering point of view, The simpler the architecture, the better. Introducing one more link means increasing the complexity and difficulty of the system. The first solution of the double-chain I think basically meets this requirement.

If we master both the random number generation algorithm and the random seed, it is equivalent to controlling the random number, breaking the irreducibility and unpredictability of the random number. in other words, we can know the random number that will be generated in advance. Generally speaking, in order to guarantee the fairness of random number, the generating algorithm is open source, so the security of random seed is very important. The blockchain solution is to hook random numbers to the hash digests of these blocks, each of which

corresponds to a new random number, so such a random sequence of numbers will also inherit the extremely difficult predictability and very difficult reproducibility. Random seed is related to the generator of the block, transaction information and additional information in the block, and the information in the chain, which makes it very difficult to predict and reproduce, which guarantees the safety of the seed. The generation of random numbers is no longer dependent on the security of the random seeds held by the service side, but is generated by the entire network user of the block chain, The security of the algorithm and the seed can not be controlled or attacked, so the security of the random number can be improved greatly.

Of course, the degree of decentralization of DPOS is not high, people also have different views in order to use representative system more efficiently, but this is the view of the people who have different opinions, It is not true that a dpos supernode, if it dpos evil, should end up paying more than it should (in which case there is economic game theory), so in theory the DPOS approach to generating random numbers is not necessarily safe either, So we will be proposing to anchor DPOS behavior in the second chain via pow, but back to our initial discussion that the use of DPOS may lead to the prediction of random number generation, but the cost is considerable. There is no one blockchain that solves all the problems, and even the introduction of multiple chains may not solve the problem.

Delegated Node

Delegated nodes are related to the DPOS consensus mechanism that Random Chain will be using. These are nodes on the network that are voted in to verify transactions. If a delegated node doesn't hold up to the community standard it's votes will be revoked, and a new node will replace it, which is voted in by the community in real time.

For Random Chains case the delegated nodes are voted in by DPOS and then used to complete the burning transactions, which then completes the writing of the specific block.
Delegates are incentivized to maintain their equipment because they are rewarded with transaction fees and monthly rewards for network uptime and there are only a set number of delegates at any one time, so it can be highly competitive. If you are not up to the community standard you can be removed as a delegate (Super Representative) potentially losing your burned coins.

Delegation provides a high level of scalability with the cost being a limited number of validators on the network, which is why Random Chain will have two chains, the main chain and the auxiliary chain. The amount of delegated nodes is completely up to the specific consensus rules of the blockchain

A lot of people in the blockchain community believe that DPOS and using delegated nodes are decentralized but the reality is there is a tradeoff between speed and security and in certain use cases speed in more important. Random Chain believes that using two types of consensus fixes this problem for integrating speed with security.

Encryption

Encryption plays a key factor in any secure application and blockchain is no exception. Encryption is the process of encoding information so that only authorized people can access it. In simplest terms you can take a plain text file “encrypt” it with an alphabetic and numerical sequence and only those with the random number can “decrypt” it, generally this encryption key is generated using a pseudorandom number generator

and the key is passed along to the receiver so that they can decrypt the data within the text file.

Now let's talk about blockchain encryption, the ledger records everything that happens in reference to the particular blockchain the "transactions" get produced by a delegate and then verified by a producer, which is then uploaded to the blockchain and secured by anyone that is using the blockchain (Random Chains community). The way the encryption works is of course based on math and "blocks" of the blockchain being linked together to the block written and verified before it, which is completely immutable due to the public nature of the ledger. What makes it immutable is the fact that all of these blocks are broadcast across the network to every single node and at least 51% of the nodes need to agree on the integrity of the data for it to be verified, so in order to mutate information on the blockchain you would need to control 51% of the network to come to a consensus that malicious or edited data is in-fact "real"

In blockchain you usually generate a public key and a private key, the public key is for public use, consider it your user name, whereas the private key is for your own personal use and access to your account, think of it as a password. If you want to send someone a message, you find their public key (username) and you send them a message, which only they can access (by accessing their account with their private key.

Development Roadmap & Token Information

Project Roadmap

All the timelines are broken down in more detail in **Section ??** **(Detailed Project Breakdown** but here is a brief description of the blockchain/API/apps required for initial phases along with testing for function in real-world environments. Random Chain will aim to work in a test environment to help our team to create the proper procedures for this token structure system. Access to the system and how the token will gain its usage will be determined by the guidance from the application

Q3 2018:

Written Whitepaper with project roadmap and technical design of the Random Chain

- White paper completion
- Use case identified and proven
- Technology implementation laid out

Q4 2018:

Proof of Concept & Alpha Development

- Proof of Random Chain concept
- Start development of the Random Chain architecture
- Rollout of internal alpha

Q1 2019:

Beta Development & Testing

- Controlled testing of Main Chain (Blockchain 1)
- Start development of Auxiliary Chain (Blockchain 2)
- Announcement of partnerships
- Announcement of token distribution details

Q2 2019:

Integration & More Testing

- Integration testing of Auxiliary Chain (Blockchain 2) with Main Chain (Blockchain 1)
- Testing of DPoS & PoW consensus mechanisms working bilaterally

Q3 2019:

Functional Random Chain Blockchain using DPoS and PoW consensus mechanisms

- Scalability testing
- Token distribution
- Creation of the genesis block

Token Distribution

Token distribution is critical to the success of a proper blockchain implementation, it mitigates risks and illustrates trust and transparency which means Random Chain will need to be as clear and concise as possible regarding our token utility, cryptocurrency economics, and the terms of the initial investment by our users (ICO buyers).

Random Chain wants to avoid confusion and mistrust by getting it right the first time, which means establishing all of the small details, before Random Chain is launched.

First, we should establish our key demographic, which is casino computer generated games, eg: slot machines, electronic poker, blackjack and other algorithm-based games. To drive interest in the Random Chain platform we will use an initial hard cap of "Random Chain" (RDMC) tokens which means there is a limited number of tokens set and a specific time period for investing. The sale stops when the number is reached, or the time period ends.

Key information Random Chain needs to inform investors of are:

- The start date of the token sale
    - TBD

- How long the sale will go for?
    - TBD, Usually 4 weeks, plus presale

- The specific type of cap to the amount of tokens
    - TBD, Hard Cap, Soft Cap, Uncapped, Hidden Cap, Dynamic Cap

- Supply of tokens
    - How many tokens distributed in the initial sale?
        - TBD

    - How many tokens does Random Chain keep?
        - TBD

    - How many tokens go to the community, advisors, sponsors or other parties?
        - TBD

- How are tokens going to be mined?
    - Delegated Proof of Stake & Proof of Work

- Exchange rate (eg: how many RDMC tokens per 1 ETH)?
    - TBD

- Allocation of money (ETH) raised
    - How will the raised money be used?
        - Marketing
        - Chain Development
        - Community
        - Legal
        - Business Development

    - Percentage, which goes to: development, marketing, legal, business development etc.
        - TBD

- What are the criteria to be able to access purchased RDMC tokens post sale?
    - Good use case could be using the tokens as a currency more like a casino platform for certain games

The key take-away from token distribution is there are many questions to be answered before Random Chain can be fully launched and invested in by outside parties.

The token system organization will distribute tokens as follows:

- 10% – legal, accounting, financial audit, development of interfaces, website, marketing, promotion, staffing.

- 9% – utilized for programs

- 1% - Issued to our organization/team

- 50% – development of current Random Chain initiative and future improvements. We would also utilize funds as needed to enhance the token, develop other blockchain to improve security and compliance issues, and to maintain the ecosystem

- 20% – continued development of token sale, maintenance of server architecture, nodes, mining pool creation, and code algorithm.

- 10% – held in reserve for unforeseen issues related to development

It is to be noted that no founder will be receiving tokens during the Token sale.

Technical Specs

Random Chain's technical specifications will be broken down as follows:

Consensus Mechanisms:
Main Chain: Proof of Work (PoW) – more secure, but slower block time.

Auxiliary Chain: Delegated Proof of Stake (DPoS) – faster block generation, less secure – better for gaming related tasks like pseudorandom number generation.

The main chain will be developed first and later integrated with the auxiliary chain. The auxiliary chain will use DPoS for its faster block generation which means that it can generate pseudo numbers at a much higher rate versus a typical PoW consensus mechanism like the main chain which will generate more secure seeds but at a slower speed, we will then integrate the two together for a higher security and more efficient outcome.

Dual strand chain, one for fast blocks, one for secure blocks, we will develop the main chain first and later integrate the auxiliary chain to create the dual strand technology.

The speed of generating and verifying new random numbers must be very fast; this can be achieved by quickly generating new blocks or some structure tricks.

The seemingly simple act of generating a 4 digit code possibility; verifying against the database and back catalogue, hashing the original encryption, sending to the users display, decrypting and verifying again. Can only be done with the automation and processing power of DPoS and PoW technology. This is mostly for functionality towards encryption, not only the users benefit.

To increase speed we can look towards a structure or framework, that quickly generate a new block of data. In doing so the process is automated once the genesis block is activated. If we look towards the future, each encryption could branch a new structure. The chain must support simple smart contract automation. Users can write simple scripts but the whole system depends on automatic processes between generations of encryption. To generate random numbers, of count or form, at any given speed. Other functions are not necessary when depending on automation. The usability must be easily implemented and end user friendly. There must be a balance of security and ease. The

more secure the system is, in general the harder it is to use. The easier to use, most likely it is less secure.

The reason Random Chain's generation of pseudo numbers must be quick is due to the security of making the casino games algorithm as unpredictable as possible. This can be achieved by using the Delegated Proof of Stake consensus mechanism because it comes to full consensus before the block is generated; the initial speed is 1 block per second. Before each block gets generated the delegated node searches the candidate list using the DPoS mechanism, this list is obtained in conjunction with the GDAO according to information on the Auxiliary chain. The commissioning node uses a reward transaction style consensus but every transaction on that block thereafter is a burning transaction, which means it's only necessary to verify the last time stamp via uPort and because the transaction is a burning transaction the ejection speed is extremely fast.

By using both Delegated Proof of Stake (DPoS) and Proof of Work (PoW) we are able to ensure fast block production and high security, therefore fast pseudo number generation for casino games, which prevents players from deciphering the algorithm.

The idea is that the POW chain can generate higher security seeds at a slower rate (the main chain) and the auxiliary chain will use DPOS to actually generate the pseudorandom numbers at a much higher speed, as well as conduct all the day to day tasks like smart contract management.

By developing a Layer 2 solution we can guarantee fast throughput of our randomly generated numbers and top-notch security. Some examples of companies doing Layer 2 blockchains are Lightning Labs, Blockstream, Ripple and Parity, Ethereum also introduced Layer 2 scaling solutions in early 2018 known as Plasma and Truebit.

The chain must support simple smart contracts. Users can write simple scripts to generate random numbers of given count, form, at given speed. Other functions are not necessary.

Simple smart contracts are those, which only contain a few functions or sometimes only one function.

Random Chain's smart contracts will contain 3 variables:

Length of randomly generated numbers (100, 1000, 10000. 100000, etc.)
The form of the number (00.12, 1.2, 1.20 etc)
Speed they should be generated (250, 1000, 2500 times per second etc).

Random Chain will provide a template for smart contract generation on the blockchain, which gives the casino owner the ability to change the above variables but also create their own particular set of functions as well. (Limited to Random Chain's discretion).

By allowing the casino owner to modify these variables it makes the pseudorandom number generation even more secure because you could change the speed at which the numbers are generated or the number of decimals on a daily basis so even if someone brute forced the algorithm, it changes the next day, hour, etc.

Application Summary (Random numbers for casino games)

It's been widely accepted by now that casinos use pseudo number generation to control their virtual slot machines, poker, blackjack, and

just about any electronic game without a physical dealer, this of course includes online casinos as well.

Let's look a basic use case, a virtual slot machine:

There are 5 reels (columns),
There are 12 symbols per reel.

Each symbol on a reel gets assigned a value, 1 through 12.
The random number generator comes up with a value between 1 and 12 for each of the 5 reels, if each reel lines up with the same number, eg: 6-6-6-6-6 (eg: the matching symbols, generated by the random number generator) you are paid out according to the machines current payout.

In the case of Random Chain, it is of course a lot more complicated and secure than this simplified example because it's based on timestamps generated and recorded by uPort plus block transaction hashes which can be longer than 40 digits.

By using random number generators, the Random Chain can guarantee fair-play on behalf of the casinos and the player base, our random number generators will be vigorously tested and evaluated to ensure there is no game rigging or malicious activity happening. By guaranteeing fair-play it means that the games being played are not influenced by things like the amount of credits at play, VIP status, size of payout, number of players, previous payout and other variables.

Detailed Project Breakdown

Our initial stages for deployment are as follows:

Stage 1 – *MVP Development v 1.0*

Smart contracts are written on the blockchain to provide access to including demographic info, and data. The members with the right privileges can directly access the data without the tokens. The platform will be a permission-based system.

Blockchain environment testnet, Platform environment

Stage 2 – *MVP Development v 2.0*

Smart contracts are updated to handle additional tasks. The integration of components are completed and tested. Test environments are certified before going to Beta.

Blockchain environment testnet, Platform environment, Secure Datastore

Step 3 - *Beta version*

Further transactional components will be added based on our ongoing user engagement.

Blockchain environment testnet, Platform environment, Production environment, Secure Datastore.

Stage 4 – *Release 1.0*

A stable, secure and functioning platform ensures the most stable release of our technology is used. Complete security testing with a test environment. Complete token integration with the chain so that the token can be utilized on the platform.

Blockchain environment testnet, Platform environment, Production environment, Secure Datastore, Token functionality.

Stage 5 - *Release 2.0*

A stable, secure and functioning platform fixes any defects observed in previous releases. Add integration to the platform to incentivize the Random Chain tokens and other reward types based on reward programs offered by Random Chain partners.

Blockchain environment testnet, Platform environment, Production environment, Secure Datastore, Token functionality, Reward programs.

Stage 6 - *Release 3.0*

A stable, secure and functioning platform fixes any defects observed in previous releases. Integrate the blockchain platform to the Random Chain analytics platform.

Blockchain environment testnet, Platform environment, Production environment, Secure Datastore, Token functionality, Reward programs, Analytics platform beta edition.

Random Chain Analytics

Analytics technology and gathering user data are essential to being competitive in the casino and gambling market of 2018, the better your analytics, the better you know your player base and therefore the more profits you generate and better player retention you carry.

A lot of Casinos don't pay close enough attention to their player bases, which in the long run loses them millions of dollars. Basic casino games can quickly become boring, and players end up switching to other

competitors, which offer better incentives such as welcome bonuses, daily bonus cash and more. In order to avoid this problem with Random Chain a vast amount of attention to detail will be put into the player experience, which means gathering analytics about our player base, in 2018 it's not as easy as just sending an email out to less active users trying to convince them to return to Random Chain.

Random Chain's goal is to drive value by showing the player base why they should stay with our particular platform instead of using up their welcome bonus and leaving for different platform, this is touched on more in the incentive section.

Random Chain's automated analytics system will measure everything the player does and make calculated decisions based upon their actions, these promotions can be targeted based on each particular type of player so that the incentive makes the most sense for them.

Random Chain automated player analytics will measure:

- Previous activities
- Behavior patterns
- Game choices
- Specific bets
- Time of play
- Duration of play
- Marketing History
- Spending Patterns

Predictive Analysis

Based on the above measurements Random Chain can automatically predict which specific incentives and promotions will be best suited for each player and potentially win back or continue their loyalty to

Random Chain which means more revenue and profits plus a more satisfied player base.

Customer data is very important; it's a well-known fact that harnessing this power properly can help understand direction.

Predictive analysis can be used in various areas across Random Chain, but the main ones include:

Customer Acquisition – Based on the above measurements we can better predict which customers will respond better to a sales offer or marketing email. This is most important in casino games because customer acquisition can be quite high by offering a welcome bonus of x dollars.

Up Selling & Cross Selling – Better understand which games are played together which helps identify cross selling opportunities to higher profit games.

Next Product Offering – Based on historical data, it has been proven that online gamers prefer to play games in a certain sequence; this will allow us to identify and target these sequences.

Attrition and Churn – Important because it can allow us to retain our player base based on incentives and loyalty programs. There are two main types of churn, 1) product churn, which means Random Chain would lose revenue from the customer via a particular product but not the customer themselves and 2) customer churn, where Random Chain would actually no longer retain the player or worse, lose them to the competition.

Loyalty and Incentives – By offering players loyalty programs or incentives we can better predict where our players will spend more money based on what we are providing them through our deep dive

analytics and marketing campaigns, these programs could be redeemable bonus cash, bets etc. in game.

Lifetime Values – By predicting lifetime value of a customer Random Chain can offer more accurate bonuses to customers who have the potential to use Random Chain longer, lifetime values include estimated revenue from that customer or expected games they will play.

Scalability

Random Chain will be highly scalable and secure because of the overall design of the two blockchains; one uses DPOS, which is known to be super-fast and scalable whereas POW is known for its security due to the time it takes to solve the cryptographic puzzles. This means that our network can be both fast for generating pseudorandom numbers and secure for keeping prying eyes from figuring out your seed and stealing your information.

Potential Partnerships

With online casino games there is potential for all kinds of partnerships such as, energy drinks like Red Bull or Monster, car brands like Ferrari or Maserati, professional sports leagues or e-gaming leagues like the NBA or MLG. The potential is endless, but when you add in the idea of blockchain and casino games the potential becomes exponentially greater given the current craze of the blockchain space.

Other options could tie into our loyalty rewards or player incentive options by partnering with a loyalty points program like Points Loyalty which allows customers to get the most from their Chinese rewards points.

Another exploitable area could be the first wave of truly decentralized applications (DApps), these applications include:

File Storage

- Storj
- Siacoin
- Filecoin
- IPFS

Video Calling

- Experty.io

Messaging

- Status

Operating Systems

- Essnetia.one
- EOS

Social Media

- Steemit
- Akasha

Web Browsers

- Brave browser

All of the above DAPPs are good targets because they want to get their name out into the wild as much as Random Chain wants to.

Future Planning

Being that Random Chain will be focusing on the gaming industry. Since the data will be vital for future models, Random Chain plans to utilize the generated number in various roles, these will include:

- As Random Chain progresses data will be utilized for machine learning/AI purposes. We believe as the dataset grows it will create the ability to speed the processes in return decreasing the chances for missed opportunities.

- As part of the Random Chain initiatives, we will be increasing partnerships, providers, and loyalty programs. Some of the areas we can monitor as part of an initiative could include: decreased loss of time, improving scores, increased activity levels, etc. Random Chain will create a list of metrics, such as those listed above to track and data mine to determine effectiveness.

Incentives

Random Chain will require incentives for multiple reasons, but the main reason is player retention, it's all too easy in the online casino gaming world to find an alternative. If Random Chain can have good player retention it means higher revenue and therefore higher profits and most importantly, higher satisfaction of our player base.

Random Chain intends to introduce many incentives, some of these may include:

Welcome Bonus – Includes bonus RDMC tokens for signing up, as a thank you for investing in the Random Chain ICO or signing up after the fact to the Random Chain casino platform.

Loyalty Rewards – Extra tokens or in game currency to use for continuously using the Random Chain platform.

Instant Tokens Back – Receive RDMC tokens instantly for using a Random Chain game like an online slot machine, these tokens can be used on any of Random Chain's online games.

Bonus Rounds/Bets – Provide users with extra black jack rounds or bets in poker, pulls on a slot machine for using our service every 24 hours.

Friend Referral System – Friend referrals, eg word of mouth speaks volumes in relativity to marketing, these players should be rewarded handsomely for referring other players with all of the above, loyalty rewards, instant tokens, and bonus rounds/bets.

Tasks, Achievements, and User Level – These will be simple at first but get more complicated and difficult as the user progresses. They will also include rewards for leveling up their user level.

As user involvement and usage improves, we will initiate token incentive programs for members as well. Areas where token initiation will occur in future releases includes:

- Organizations who help Random Chain to create standards for programs and track progress indirectly will be awarded tokens.

Institutions can create incentives for their own staff to create better processes for integration, and even reward their teams for gains made through internal incentive programs.

Conclusion

The main goal of this white paper is to design a block chain (GDAO (Global Distributed Autonomous Organization)) that can generate high frequency and stable blocks. It is to design a product that can generate pseudorandom numbers at a high frequency and stability. Decentralized secure random numbers. For product design goals, we will use a consensus mechanism that combines POW and DPOS while maintaining two links that are interrelated. The random chain contains two interrelated chains: the main chain and the auxiliary chain. The main chain uses the POW consensus mechanism and the auxiliary chain uses the DPOS consensus mechanism. The information recorded on the main chain includes transactional information and random seed generation and translation that is information for human understanding. The role of the auxiliary chain is to generate blocks at high speed to generate random numbers, which generate blocks at a very high frequency.

References

"Everything Administrators Need to Know about Security." NFront Security, 2008, nfrontsecurity.com/downloads/security-whitepaper.pdf.

Bagley, Judd. "What Is Blockchain Technology? A Step-by-Step Guide For Beginners." BlockGeeks, 2016, blockgeeks.com/guides/what-is-blockchain-technology/.

Buntinx, Jean-Pierre. "Is Blockchain Technology The Future of Two-Factor Authentication?" Bitcoin News, 12 Oct. 2015,

news.bitcoin.com/blockchain-technology-future-two-factor-authentication/.

Dieckow, Andreas. "Using Two-Factor Authentication." Intersystems, 2015,

www.intersystems.com/wp-content/uploads/assets/Using_Two-Factor_Authentication_WP.pdf.

Greenfield, Robert. "Explaining How Proof of Stake, Proof of Work, Hashing and Blockchain Work Together." A Medium Corporation, 20 July 2017,

medium.com/@robertgreenfieldiv/explaining-proof-of-stake-f1eae6feb26f.

Johansen, Rune Skovbo. "A Primer on Repeatable Random Numbers." Unity Blog, 7 Jan. 2015, blogs.unity3d.com/2015/01/07/a-primer-on-repeatable-random-numbers/.

Judmayer, Aljosha, et al. "Merged Mining: Curse or Cure?" SBA Research,

eprint.iacr.org/2017/791.pdf.

https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

https://medium.com/tron-foundation/an-easy-to-understand-guide-to-pow-pos-dpos-consensus-mechanism-and-super-representative-eb1f5504a8e

https://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10

https://en.wikipedia.org/wiki/Pseudorandom_number_generator

http://mathworld.wolfram.com/PseudorandomNumber.html

https://www.quora.com/What-is-the-difference-between-a-pseudo-random-number-and-a-truly-random-number