AME Chain Whitepaper

Next
Table of Contents

Last modified 1yr ago

Table of Contents

Previous
AME Chain Whitepaper

Next
Disclaimer

Last modified 9mo ago

Disclaimer

Please read the “Disclaimer” section of this document scrupulously. This section of the AME Chain whitepaper was last updated on 20th January 2022.

It should be noted that this whitepaper serves only an informational purpose, and therefore, cannot be viewed as legal, financial, or investment advice. Additionally, this whitepaper is not meant as an invitation for investment, nor does it request for any form of contractual responsibility. If you have any reservations, we highly recommend that you seek the advice of a trusted licit or financial fiduciary.

All external references presented in the whitepaper are meant to be designated as representations and should not be regarded as AME Chain approving of their information or notional theorizations.

AME Chain has exercised a high degree of competence and diligence when drafting this document. However, there is still a liability of error. AME Chain does not explicitly ensure the precision of the information and facts presented in this document. Furthermore, by reading this whitepaper, you agree to exempt AME Chain from any damages emerging directly or indirectly from relying upon the information disclosed in this document.

The modification, duplication, or distribution of this whitepaper or any of its components, either in part or whole without prior written consent from AME Chain is discouraged. By utilizing this whitepaper, the reader accepts that AME Chain is the sole owner of any intellectual property mentioned in this document.

There are some estimations and notional theorizations presented in the whitepaper that can be termed as forward-looking statements. These include and are not limited to, evaluations made with regards to AME Chain’s projected revenue, growth rate, future products and services, and road map, among other statements similar in approach.

The reader of this whitepaper expresses explicit acknowledgement of the fact that these forward-looking proclamations are merely valuations and predictions that are subject to market risk.

The whitepaper published by AME Chain is not subject to the jurisdiction of any legal body. Furthermore, the information presented in this whitepaper has not been examined or approved by any regulatory body. Hence, no legal action will be accommodated under the laws and regulations of any jurisdiction.

Additionally, the AME coin is a utility cryptocurrency, and cannot be viewed as a form of investment, arbitrage, or any form of speculation that is projected for immediate sale and financial gains.

By agreeing to read this whitepaper, and by soliciting information about AME Chain or by purchasing AME coins, you, the reader has confirmed that you have read, understood, and accept the terms put forth in the section titled “DISCLAIMER.”

Previous
Table of Contents

Next
Introduction

Last modified 1yr ago

Introduction

> “Quantum technologies are difficult to understand, but that will not stop the disruption this set of emerging technologies will bring in the next few years!” — Kevin Coleman

Vision

AME Chain is an ambitious project dedicated to the establishment of an unconditionally secure blockchain that can withstand the threats arising out of Quantum computing.

Background on Blockchain technology

- In 1991, W. Scott Stornetta and Stuart Haber deliberated what the world has come to know as a "Blockchain". Their early work included shaping a cryptographically secured data where nobody could alter timestamps of records.
- In 1992, they updated their technique to consolidate Merkle trees that improved proficiency hence providing the assortment of more reports on a solitary block.
- Amid the financial crisis of 2007–08, a pseudonymous author called Satoshi Nakamoto released a white paper titled *Bitcoin: A Peer to Peer Electronic Cash System*. Nakamoto described Bitcoin as a "purely peer-to-peer version of electronic cash". The white paper caused a sensation—especially in the investing community, since it imagined the development of a currency with universal applicability, free from central banks’ monetary policies.
- In 2009, the first block of the Bitcoin blockchain was mined.
- In 2015, Ethereum blockchain was launched with support for Smart contracts.
- The period since 2015 has seen the proliferation of thousands of cryptocurrencies with minimal to no enhancements.

Blockchain technology promises a new dimension of conducting business transactions among untrusted entities; its features that support verification, identification, authentication, integrity, and immutability are guaranteed through cryptography, transparency, and decentralized smart contracts and smart ledgers.

Blockchain Security

The increasing adoption of blockchain in various sectors like finance, retail, insurance, logistics, supply chain, and public sectors raises a pertinent question of data safety, security and integrity of the blockchain itself.

The following is a summary of the security *claims* of a blockchain as read in various whitepapers and research papers.

> Blockchain creates a data structure with strong security derived from decentralization, cryptography and consensus, which ensure trust in transactions. The data is structured into blocks and each block contains a list of transactions. Each new block connects to all the blocks before it in a cryptographic chain in such a way that it's nearly impossible to tamper with. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is true and correct.
>
> Blockchain technology enables decentralization through the participation of members across a distributed network. There is no single point of failure and a single user cannot change the record of transactions.

The traditional view of blockchain is that it is decentralized, trustless, tamper-proof, resistant to cyberattacks and cryptanalysis, and secured by cryptography and digital signatures.

The threat from Quantum Computing

Quantum computing is a rapidly emerging technology that harnesses the laws of Quantum mechanics to solve problems too complex for classical computers.

Quantum computers promise exponential increases in computational analysis and brute force bandwidth. This has tremendous connotations for medicine, chemistry, AI, simulation and many other industries.

However, that same computational brute force can also be applied to the task of breaking encryption. With the power of a Quantum computer the big targets for security and privacy issues are more likely to initially centre around finance organisations including the cryptocurrency market with a $2 trillion aggregate market cap.

Purpose of AME Chain

AME Chain is a fast and secure decentralized digital asset ledger that is EVM compatible with high performance, scalability and security guaranteed by Quantum Physics.

This whitepaper is an attempt to explore some of the security challenges blockchains face due to the rise of emerging technologies like Quantum Computing and how AME Chain provides a solution in the form of a *Quantum secure blockchain*.

← Previous
Disclaimer

Next - Engineering in Deep Technology
The Era of Quantum Computing →

Last modified 1yr ago

The Era of Quantum Computing

> Quantum computing has established an unprecedentedly deep link between the foundations of Computer Science and the foundations of Physics
>
> — John Preskill

Quantum computing is a computational system that allows for an outcome to be predicted based on a summation of states, rather than be derived from a series of investigations into the physical binary states of all data required to define the outcome.

In this way, the algorithms involved can define the outcome before the physical measurement of an object and its state.

Think of a light switch in a cellar as an example. If you walk into the room and can see, you already know the light is on, the pre-existing factors determine it is on without needing to measure the factors that drive the outcome or review the physical state of the switch itself.

Engaging the quantum realm makes it clear that tools are needed to comprehend the two domains together, the micro-scale of the quantum and the macro-scale of lived reality. The issue concerns not only understanding more about quantum mechanics, but also linking the quantum and non-quantum domains such that the quantum realm can be activated in a useful way at the macroscale.

Moving from bits to qubits

Classical Computers

Classical computers are the laptops, desktops and mobile phones we use every day. A computer performs arithmetic operations like addition, subtraction, multiplication and division to perform any logical task.

In classical computing, the bit is the fundamental computational unit. The bit is an abstract mathematical entity that is either a 0 or a 1. Computations are constructed as a series of manipulations of 0s and 1s. In the physical world, a bit might be represented in terms of a voltage inside a computer, a magnetic domain on a hard disk, or light in an optical fiber.

Quantum computers

The qubit (quantum bit) is the equivalent system in quantum mechanics. The qubit is likewise an abstract mathematical entity (a logical qubit), existing in a superposition state of being both a 0 and a 1, until collapsed in the measurement at the end of the computation into being a classical 0 or 1. The qubit can be instantiated in different ways in the physical world. There are realizations of qubits in atoms, photons, electrons, and other kinds of physical systems. The quantum state of a qubit is a vector in a 2D space.

The interpretation is that whereas a classical bit is either on or off (in the state of 1 or 0), a qubit can be on and off (1 and 0) at the same time, a property called superposition. Superposition is the famous Schrodinger's cat type effect – the ability of particles to be in two places at once, or quantum bits (qubits) to be in a joint state of zero or one at the same time, with the outcome only being revealed upon measurement. One example of this is the spin of the electron in which the two levels can be understood as spin-up and spin-down.

A Brief History of Quantum Computing

Throughout a good part of the 19th century and the early part of the 20th century, scientists were trying to solve the puzzling behavior of particles, matter, light, and color. Scientists like Albert Einstein, Neils Bohr, Heisenberg, Paul Dirac, Erwin Schrodinger and Feynman got entangled (pun intended) in Quantum physics only to discover startling realizations.

> God does not play dice with the universe.
> — Albert Einstein, The Born-Einstein Letters 1916-55

Feynman suggested that a quantum computer could be an efficient universal simulator of quantum mechanics. Such a "universal quantum simulator" would be a different kind of computer that is not a traditional Turing machine. He posits two ways to simulate quantum mechanics with computers. One is reconceiving the notion of computers and building computers out of quantum mechanical elements that obey quantum mechanical laws. The other idea is trying to imitate quantum mechanical systems with classical systems.

Current status of Applied Quantum Computing

Quantum computers are in the early stages of development and would likely be complementary to existing computational infrastructure, interacting with classical devices, and being accessed either locally or as a cloud service.

There are several approaches to quantum computing. Those with the most near-term focus are superconducting circuits, ion trapping, topological matter, and quantum photonics. Irrespective of the method, the objective is to produce quantum computing chips that perform computations with qubits, using a series of quantum logic gates that are built into quantum circuits, whose operation is programmed with quantum algorithms.

Advances in recent decades have led to the practical realizability of quantum computers.

1. In the 1990s was the discovery of quantum error correction. Unlike classical bits that persistently stay in a 1 or 0 state, quantum bits are extremely sensitive to environmental noise and may decohere before they can be used to perform a computation.
2. Since 2012, there have been advances in room-temperature superconducting materials and a proliferation of ways of making qubits such that quantum systems have increased from 1–2 qubits to 50–100 qubits.
3. Currently, the top methods demonstrate 30–70 qubits of processing power and achieve fidelity rates above 99% (i.e. below a fault tolerance threshold of 1%).
4. In 2019, a breakthrough has been achieved with Sycamore, a Quantum processor created by Google. Sycamore completed a task in 200 seconds that Google claimed, in a *Nature* paper, would take a state-of-the-art supercomputer 10,000 years to finish. Thus, Google claimed to have achieved quantum supremacy. To estimate the time that would be taken by a classical supercomputer, Google ran portions of the quantum circuit simulation on the Summit, the most powerful classical computer in the world.

The following are some of the notable Quantum computers in the industry.

Organization	Qubit type	#qubits	Status
1. IBM	Superconducting (gate model)	19(50)	Available
2. D WAVE	Superconducting (quantum annealing)	2048	Available
3. Rigetti	Superconducting (gate Model)	19	Available
4. Google	Superconducting (gate Model)	72	Built, Unreleased
5. Intel/Delft	Superconducting	49	Built, Unreleased

Quantum Computing Hardware Platform

Quantum computing meets Blockchain

Since the quantum domain is conducive to the functionality needed by blockchains, and more importantly, because blockchains must articulate a quantum-secure upgrade path, a number of early-stage quantum solutions have been proposed. As in migration to the quantum domain more generally, the first step is to replace the blockchain features that are known to be at quantum risk, which are the cryptographic algorithms used by many blockchains.

The future of global network communications could include a quantum internet with various features such as quantum key distribution (QKD), secure end-to-end communication, quantum memories, quantum repeaters, and quantum-based applications such as quantum blockchains. Reactions toward the potential quantum information era are first, one of preparing to be quantum-resistant and quantum-secure, and second, being quantum-compatible and quantum-embracing by taking advantage of the new functionality offered by quantum systems.

Blockchain protocols would be translated into a framework of quantum circuits and processes.

- One quantum circuit could implement the consensus algorithm, replacing the classical Byzantine Agreement protocol with a quantum Byzantine Agreement protocol.
- Classical consensus (i.e. proof-of-work mining) is not the most scalable and efficient of systems, there are many ideas for implementing consensus in quantum formats. The mining process can be accelerated by using a modified Grover's algorithm (used in large data searches) (Sapaev et al., 2018).
- Another quantum circuit could encode quantum certificates and other quantum protection methods into the transaction syntax.
- A sophisticated idea for implementing blockchains with quantum-based logic relies upon entanglement. The project envisions a temporal Greenberger–Horne–Zeilinger (GHZ) blockchain in which the functionality of time-stamped blocks and the hash functions linking them is replaced with a temporal GHZ state which is entangled in time.
- Double-spending is envisioned to be prevented by using quantum teleportation technology for transactions (the transmission of an exact state of quantum information), which would prevent the owner from keeping coins once they are spent (after the quantum state is sent).

Quantum computing and security has the potential to revolutionize the entire Internet and its subsystems including Blockchain, giving rise Quantum Internet and Quantum Blockchain, which will allow devices to securely exchange information using the principles of quantum mechanics.

← Previous
Introduction

Next - Engineering in Deep Technology
The Threat to Blockchains →

The Threat to Blockchains

Blockchain and Quantum computing are two technologies on a collision course. Cryptography is an integral part of both quantum computing and Blockchain. There is a potential scenario where the blockchain solutions we have today will be obsolete as soon as quantum computers scale and become mainstream.

Most data on the internet that sits on servers and is locked down by today's security mechanisms is vulnerable to cyber-attacks. This threat becomes a ticking time bomb when we introduce quantum computers into the mix. Quantum computers could spell disaster for data stored on the internet. Information exchange on the internet as we know today uses the Rivest– Shamir–Adleman (RSA) algorithm and Elliptic-Curve Cryptography (ECC). These algorithms are used to encode and decode information transmitted on the internet. These algorithms are public-key cryptographic techniques where the encryption key used to encode data is public, and the encryption key used to decode data is private.

The advent of quantum computing constitutes a new paradigm in which digital technologies will endure both challenges and opportunities. Threats will come up in a variety of forms, especially when robust quantum computers will be able to break several important cryptographic algorithms currently used. Blockchain, as a technology that strongly relies on cryptography, is not safe from these threats.

The Weaknesses in Blockchain

Blockchain implements an open, distributed, cryptographically signed digital ledger that is secure against modification and verifiable by anyone. To prevent bulk rewriting of an entire sequence of blocks from some point in the past as well as attacks to deny service or grow the chain faster than legitimate sources can, a work requirement is added to make rewriting long chains prohibitive. For our purposes here, the relevant structure amounts to the following description: It is worth exploring the conjunction of blockchain technology and quantum computing in the following four areas.

- **The use of Pseudo Random Numbers (PRN)**
  The blockchain consists of a sequence of blocks that are stored on and copied between publicly accessible servers. Each block consists of four fundamental elements:

  a) the hash of the preceding block
  b) the data content of the block (i.e. the ledger entries)
  c) the nonce that is used to give a particular form to the hash
  d) the hash of the block

  All processes mentioned above require random numbers as inputs, which in the case of blockchains currently present, are obtained from pseudorandom number generator (PRNG). PRNG is not truly random, because it is completely determined by an initial value, called the PRNG's *seed* (which may include truly random values).
- **Digital signatures** are one of the most essential components of blockchain technology. Bitcoin and Ethereum use elliptic curve cryptography (ECC), particularly the ECDSA signature schemes on curve secp256k1. Others, such as EOSIO, use the NIST standard secp256r1 curve. NIST recommends that ECDSA and RSA signature schemes be replaced due to the impact of Shor's algorithm on these schemes.
- **Communication over the blockchain network** relies on protocols such as HTTP. The security of the communication happens in HTTPS within the SSL/TLS protocol stack. TLS supports one-time key generation (which is not quantum safe) with AES for symmetric encryption and several non-quantum-safe algorithms for exchange and authentication, such as RSA, DH, ECDH, ECDSA, and DSA. This means that all internet communications, including transactions and messages sent between applications and nodes in a blockchain, will not be quantum safe when robust quantum computers become fully operational.
- **Block mining**: Blockchain networks that use proof-of-work as the consensus mechanism rely on finding nonces. Quantum computers will be able to find these nonces quadratically faster using Grover's algorithm. However, this does not pose a major threat to the security of blockchain networks because the solution will be as easy as quadratically increasing the difficulty to compensate for the quantum advantage. In networks with consensus protocols that do not promote competition between nodes, such as the proof-of-authority used in the LACChain Blockchain, this threat will not exist.
- **Hash functions** take an element from a set of infinitely many elements and gives an output from a finite set of 2256 elements in the case of the SHA-256 function that is used by most of the blockchain networks today. Thus, from a hash value stored in the blockchain, it is statistically impossible to obtain the element that resulted in that value. This property, known as irreversibility or pre-image resistance, guarantees the security of these operations even in the presence of quantum computers.

  Additionally, hash functions are continually evolving for increased security. For example, if quantum computers evolve to the point of posing a threat to SHA-2, then SHA-3 is already standardized as an alternative that offers a higher level of security in NIST standard FIPS202.

The Quantum Threats to Blockchain

The computational data structure known as a blockchain provides an open, public, distributed ledger that has many interesting applications, including digital currencies. The security of this ledger depends on the difficulty of solving certain cryptographic problems which are undermined by the potential of quantum computation. Specifically, hashes as used in signing the blocks of the ledger can be compromised, as can any public/private key system which relies on the so called hidden subgroup problem.

Blockchains are at greater potential risk from quantum computing than other technologies because they are heavily dependent upon cryptography. The very premise of blockchain protocols is the computational infeasibility of inverting certain one-way hash functions, but these may be broken with quantum computers. On the other hand, block- chains also stand to potentially benefit the most from the innovations developed in quantum cryptography.

- **Grover's algorithm** can dramatically speed up function inversion. This allows the generation of a modified pre-image from a given hash (a hash collision) allowing a signed data block to be modified. This voids guarantees of authenticity of the ledger entries undermining the entire blockchain. The speed-up due to Grover's algorithm is a factor of the square root of the number of possible hashes, meaning that a hashsubjected to quantum attack would only be as secure as one with half as many bits subjected to classical attack.

  Grover's algorithm is specifically a solution to the problem of finding a pre-image of a value of a function that is difficult to invert. If we are given a signature that is the hash value of some data $s=H(d)$, and the function $H(d)$can be implemented on a quantum computer, then Grover's algorithm allows us to find d for a given sin time of order $O(\sqrt{n})$ where n is the size of the space of valid hashes. In other words, it allows us to generate hash collisions more efficiently than brute force search, which would be $O(n)$.

  For a hash of length k bits this means that we have a significant speedup by a factor of $2k/2$. This can be very large even for small values of k.
- **Shor's algorithm** applies to any aspect of blockchain that relies on asymmetric key cryptography. The most commonly referenced problem is that of breaking RSA encryption. RSA relies on the ease of multiplying prime numbers in contrast to the difficulty of factoring large numbers into prime factors. Shor's algorithm speeds-up this process exponentially, effectively breaking RSA encryption. Variants of Shor's algorithm do the same for other asymmetric key cryptosystems.

  It helps to find the two prime factors of a composite integer used as a public key in an algorithm like RSA. Being able to factor the integer, which is computationally challenging on classical computers, yields to the attacker the private key of the public/private pair. That makes it possible for the attacker to forge messages, signatures, etc.
- **Risk of quantum attack in mining**
  Mining is the consensus process that validates new transactions and keeps the blockchain secure. One way would be to attack the hashing algorithm by which the mining operation is conducted. In Bitcoin, the hash function, though, is quite strong, and possibly more quantum-resistant than other cryptographic algorithms used in blockchain operations. Bitcoin's Hashcash proof-of-work consensus algorithm uses a double SHA hash function, meaning two sequential applications of SHA-256; a SHA-256 of SHA-256 (a composite function of SHA-256(SHA-256(x))) (Kelly et al., 2018; Aggarwal et al., 2018).
- **Intercepting, decrypting and altering of data communications**
  Any encrypted communications used in the infrastructure upon which a blockchain is constructed are vulnerable to an attacker who can break the cryptographic security of the communications.

The general threat of quantum computation is that such algorithms become unviable because the premise of asymmetric effort of computation is invalidated. Quantum computing provides potential attacks on many cryptographic systems and algorithms.

The Urgency of the Threat

The operational consequence of the rise of Quantum computing is that whoever gets quantum computational capacity first has an advantage, but only until the defending parties develop the capacity themselves.

Estimates vary as to when quantum computing will be a threat to the current cryptographic infrastructure, blockchain-related and otherwise.

- An estimate from NIST, drawing from industry experts, suggests that quantum computers powerful enough to break the current 2048-bit RSA standard might be available by 2030 (Chen et al., 2016).
- Others predict that the elliptic curve signature scheme currently used by Bitcoin (ECDSA) is at even greater risk, and could be broken by quantum computing as early as 2027 (Aggarwal et al., 2018).

Current Threats

The popular cryptographic scheme used in blockchains or cryptocurrencies is the Elliptic Curve Digital Signature algorithm. Many attacks have been designed that try to recover a user's private key, since if an adversary finds a user's private key he can steal all the money from the user's account. Some of these attacks start by mapping the problem of finding the user's private key to a hidden number problem (HNP) and then, using a lattice reduction algorithm such as LLL or BKZ. These are polynomial time attacks and the private key can be recovered if there is a side-channel attack which leaks a portion of the nonces bits or if there is a known weakness in the pseudorandom number generator (PRNG) used to generate the nonces.

Previously, exploits such as Anyswap hack have happened because the random number required for signatures have been reused. The exploit used these signatures to reverse engineer the private key controlling AnySwap's cross-chain MPC account and steal the funds. In this case, the transaction was generated by a hardware bitcoin wallet using a pseudo-random number generator that was returning the same random number every time. The ECDSA signature algorithm requires the generation of a per-message secret nonce. If this nonce is not generated uniformly at random, an attacker can potentially exploit this bias to compute the long-term signing key.

Lattice attacks are used to solve for the hidden number problem to efficiently compute private ECDSA keys that were used with biased signature nonces. If a ECDSA private key is ever used to sign two messages with the same signature nonce, the private key is trivial to compute. The Hidden Number Problem (HNP) were formulated by Boneh and Venkatesan, who used it to prove the hardness of computing most significant bits of Diffie-Hellman protocols. Howgrave et.al, Nguyen et.al, applied the HNP to show that the DSA and ECDSA signature schemes are insecure if an attacker can learn some most significant bits(MSB) of the signature nonces. This technique has been applied in practice in the context of side-channel attacks.

The random numbers which are to be used as nonces, private keys, seeds to generate the private keys have to be random to prevent an adversary gaining any knowledge to derive the private keys. The seed are random numbers which are required by cryptography modules in a Linux kernel. These seeds are collected after system gaining sufficient entropy. But we can't be sure that every time these seeds are generated in a truly random fashion.

To summarize, many of the vulnerabilities arise because of deterministic seeding for generating random numbers that are in turn used to generate private keys. Apart from side-channel attacks, this weak seeding methodology also opens doors for decrypting harvested data.

Emerging Threats

Quantum computer rely on qubits to perform computation. These qubits take any value in the range of 0 and 1. The qubits are like transistors in the classical computer. What makes this type of architecture different is that state representation of the qubits. This architectural model helps process the algorithm simultaneously using the many state representative vectors.

We will take an analogous example. Suppose you are a commander in an army performing a scouting mission. You have 10 soldiers under your command. There are 10 roads before you. But at any point of time you could use only 2 soldiers for scouting even though you have 10 people. What if you could send 10 people to at once down the 10 roads! This process, although does not exactly represent a quantum computer, but helps us gain an intuitive understanding of what can be achieved using a quantum computer. This idea is called as Quantum Parallelism.

In the current ECDSA signatures used in blockchains, one-way functions are used. These rely on the mathematical hardness of discrete logarithm problem. But using a Quantum computer, and Quantum Fourier Transform, the discrete logarithm problem could be transformed into solvable period finding problem. The Shor's algorithm exploits interference in the qubits to measure periodicity of arithmetic objects. Though the Shor's algorithm does not allow a speed up on a classical computer, it drastically reduces the time required to solve the discrete logarithm problem when implemented on a Quantum Computer.

Quantum Computer Resistance

To summarize, there is a real threat of Quantum Computers, not only to the blockchains, but to every cryptographic standard we use in our everyday life like Banking, E-commerce, Password managers or TLS communication. There are particular cryptographic schemes that are being developed to resist the attacks of the Quantum computer, called lattice based schemes and are currently under review with NIST.

To be sustainable in the long term, it is important for blockchains to establish an implementation roadmap for quantum-resistant solutions. Given the complexity of blockchains, early applications in quantum computing would more likely focus on cryptographic problems that are easier to solve.

Engineering in Deep Technology - Previous
The Era of Quantum Computing

Next - Engineering in Deep Technology
Random Numbers in Blockchains

Random Numbers in Blockchains

What is randomness?

Randomness can be simply seen as the result of subjective ignorance, i.e., when an observer does not have a complete description of the particular physical system.

Random Numbers used in Blockchains are used to distribute the results of consensus in a fair manner. This is also related to distributing the authority to add a new block to the blockchain. This process which should be random is currently implemented using Verifiable Random Functions.

Use of Random numbers in Blockchain

Digital processing in blockchain is strictly deterministic. But sometimes randomness is required. The ability to generate random numbers is required for cryptographic protocols which are necessary to ensure digital security, privacy and integrity of a blockchain.

- Creating secure private keys and public keys
- TLS based peer-to-peer communications between the nodes
- Cryptocurrency transactions
- Block mining
- EVM State machine and Smart Contracts
- Hashing in Merkle trees and linked lists
- To compute a salt to produce passwords, nonce's
- Deriving random data sequences for securing cryptographic protocols.
- Blinding values: In cryptography, blinding is a technique by which an agent can provide a service to (i.e., compute a function for) a client in an encoded form without knowing either the real input or the real output. Blinding techniques also have applications to preventing side-channel attacks on encryption devices.
- OTP's. Random OTP's.
- To obtain unpredictable digital signatures to sign electronic documents
- Randomized algorithm
- Creation of non-deterministic session keys and thus to protect data in transit
- Blockchain Cloud
- Padding bytes
- Non-Fungible Tokens (NFTs) and Gaming

Current blockchains use Pseudo Random Numbers

A pseudorandom-number generator (PRNG) is a computer program or function that expands a short string into an arbitrarily long string that looks like random data. A PRNG can be used to efficiently convert a small amount of true randomness into a much larger amount of effectively random bits, meaning that it would be difficult for anyone to tell the difference between the output of the PRNG and a string of truly random bits.

A fair or completely random string gets deterministically expanded into a longer string that may present some properties typical of randomness, like a correct "typical" weight, but, roughly speaking, each output bit cannot be as random as the input bits. Randomness is being "diluted", as the output longer string can at most be as random (technically, be characterized at most by the same entropy) as the input string, given that a deterministic process cannot increase randomness.

Current blockchains use Verifiable Random Functions

A Verifiable Random Function (VRF) acts as a public key that is generated using a hashing mechanism (SHA-3, KECCAK-256 etc.,). The current blockchains in the market utilize the randomness of the VRF to support smart contracts in various ways depending upon their utility.

The users are charged in the native cryptocurrency to utilize these VRF's for extract random numbers.

Various mechanisms are employed to construct these VRF's in the current blockchains. Random numbers are generated by feeding data into these VRF's.

The Quality of Random numbers

The random numbers are only good if they are uniformly distributed in a very large range. The probability of picking a number at random number from a very large set of numbers. Typically, the mechanisms to generate these numbers need specific inputs to generate the large pool. Blockchains like Ethereum, Chainlink, Polkadot, Algorand make heavy use of these functions for use in game outcomes, integrity of the game, tamper proofing the random results.

Cryptographic random number generators typically use a transformation function to compute fresh random values from past random values. Different constructions such as pseudorandom number generators (PRNGs) or pseudorandom functions (PRFs) exist, all of which have their predictability properties tightly tied to computational intractability hypotheses.

Even perfect statistical properties, or seeming unconditional unpredictability that we hoped to get from chaos theory, which is, unlike much of cryptography, not based on computational intractability, may together fail to deliver good results for cryptography. It ends up being that, at least for pseudorandom number sequences, whose reproducibility is often the only reason to prefer them over true randomness, seem to require more complex constructions and computational intractability remains an unavoidable fundament up to today.

The Quality of initial seed

The first step in generating a random number is to determine a seed. It is extremely important to choose a seed that is difficult to influence or predict. If someone can influence or predict the seed, they could in theory try to collude with the oracle performing the request for randomness to give themselves a favorable. The primary role a Verifiable Random Function, as the name suggests, is for the parties to check and agree that indeed the process has been carried out in an unbiased and fair manner such that the results cannot be tweaked in anyone's favor. result.

The seed is then sent in a request to a oracle. The oracle then generates a pseudo-random number with the given seed, and returns the result back to the smart contract, along with the cryptographic proof that the random number was generated using the seed. This cryptographic proof is created via Public Key Cryptography, a widely accepted feature of blockchain technology. It is important that the result can be verified, because actors such as miners or oracles can try to influence the result of a random number to their own benefit.

This is a much deeper topic, where threats like side-channel attacks, timing-attacks pose a vulnerability. The gist is that you need a random number (seed) and function that generates a random number (public key). The function that generates the random should be a hard-to-invert function, i.e., pre-image resistant. For this procedure to be robust, the seed should be chosen in a totally random fashion.

Entropy Starvation

In cryptography, it is very important that the data be truly random, or at least unpredictable (even in part) to any attacker.

To supply this data, a system keeps pool of random data, called entropy, that it collects from various sources of randomness on the system: Precise timing of events that might be somewhat random (keys pressed by users, interrupts from external devices), noise on a microphone, or, on some processors, dedicated hardware for generating random values. The incoming somewhat-random data is mixed together to produce better quality entropy.

These sources of randomness can only supply data at certain rates. If a system is used to do a lot of work that needs random data, it can use up more random data than is available. Then software that wants random data has to wait for more to be generated or it has to accept lower quality data. This is called entropy starvation or entropy depletion.

Backdoors in RNG

Backdoors can be implemented in an RNG: assume that an RNG is sloppily specified of having a seed with some high entropy, then adding a bad seed like the above has devastating consequences:

- The specification is compliant to requirements like random generators need seeds with at least 128 Bit of entropy.
- But guessing the seed and reproducing the RNG's output is easy for the vendor of the RNG.

Even if the RNG is correctly initialized with seeds of high min-entropy, another attack could attempt to substitute the honest generator with a bad one.

For example, let two generators be given, both based on AES-encryption of counters, where G 1 has seeds and keys of high min-entropy, while G 2 has seeds and keys of high Shannon, but low min-entropy. Then, the output of G 1 is practically indistinguishable from the output of G 2 (since AES was empirically verified to provide this), so the unsuspecting user may unknowingly use random values that a third party can easily guess and reproduce. Any cryptographic keys or other parameters created in this way are intrinsically insecure, irrespectively of how good the rest of the cryptography is.

Use of RNG in Blockchain Cryptography

The public key encryption of current blockchain and cryptocurrencies use the Elliptic Curve Digital Signature Algorithm (ECDSA) based on the mathematical assumption that the discrete logarithm problem employed via ECDSA is computationally intractable i.e., there is no efficient classical algorithm for computing discrete logarithms in general. To be very precise, the mathematical odds of getting past the encryption is close to zero. This is called Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECDSA algorithm is also used to digitally sign the documents. Any transaction in the blockchain is digitally signed so that the intended parties can verify the validity of the signature.

A case study - Cryptography in Ethereum

To grasp a detailed understanding of the process we will now look at how ECDSA works in Ethereum Blockchain.

The Ethereum Blockchain uses KECCAK-256 algorithm which is a variant of SHA-3 algorithm. It uses secp25k1 curve. This is the elliptic curve. First a 'seed', which is a random number, is generated on the computer using the RNG native functionality of the hardware being used at the time of creation. The seed is generated by the computer using the entropy collected by various parameters like CPU jitter, mouse movements, user inputs, weather parameters etc., so that the seed value is truly random. The seed may be run through a hashing algorithm to generate a private key of certain length. This private key is input to the SECP256k1 to generate a public key.

Whenever a account is created on Ethereum, a private key is is generated at "random". A private key is made up of 64 hex characters. A public key is derived from the private key. The public address is then created by taking the last 20 bytes(160-bits) of the KECCAK-256 hash of the public key and adding 0x at the beginning. This public address is then used to receive funds as it is broadcasted to the concerned party. The public key, not necessarily the same one, is also used to sign contracts. Thus the private and public key pairs are heavily used in every step of the transaction.

Ethereum's weakness due to poor source of Entropy

Ethereum's entire cryptography suite uses PRNG. A non-cryptographic PRNG used within a cryptographic function renders the encryption or hash vulnerable to attacks. A pseudo-random number generator (PRNG) need not be designed for cryptography. Sometimes a poor source of entropy is deployed in algorithms that use random numbers. If the algorithm has known weaknesses or a possible method to reverse engineer the method for RNG, it makes the entropy pool source moot and allows easy methods to determine the primes.

The solution: Use of Quantum RNG in AME Chain

In contrast to deterministic random number generators that generate random values with entropy that is limited by the entropy of the initial seed, AME Chain uses non-deterministic random number generators that rely on the quantum state of matter for generation of truly random numbers.

Quantum Random Number Generators

> "Not only does God play dice but... he sometimes throws them where they cannot be seen."
> — Stephen Hawking

Background

Most random numbers in Classical Computer are generated through some mathematical formulas, therefore the generator is called Pseudo-Random Number Generator (PRNG). The resulting randomness is said to be predictable as it can be reproduced if the state of PRNG is known.

Quantum Random Number Generators

Quantum Computer can generate True Randomness, through nature behavior such as the randomness of electron movement in an atom. The devices that use quantum effects for generation of random numbers are called quantum random number generators (QRNGs).

QRNG represents the system that satisfies the single random quantum effect of resetting to the initial settings after system value measurements. Due to the laws of quantum physics, each measurement with identical initial conditions and the same measurement mode provides different values. Therefore, such a system has a broad application of random number generators where the randomness of measured values is highly desirable.

Such systems include the smallest units such as electrons (smallest quantity of charge) or qubits (smallest quantity of information). A single quantum of light (photon) can be used as qubit carrier which is favorable due to laws of quantum mechanics that prevents making a faithfully qubit's copy. In the early development of QRNGs, schemes based on measuring qubit states were widely adopted due to theoretical simplicity. A qubit cannot be split, copied or amplified without introducing detectable disturbances and it can be represented as a linear combination of two basic states (horizontal and vertical):

$$|\psi\rangle = \alpha \cdot |\updownarrow\rangle + \beta \cdot |\leftrightarrow\rangle \tag{1}$$

Parameters α and β are probability amplitudes: the probability that the outcome of the measurement will be a vertical or a horizontal base, respectively. Unlike the classical bit, which can only have two possible values, 0 or 1.

Random numbers - Causal determinism and Causal in-determinism

Probabilistic causation arises from Causal indeterminism. According to the Copenhagen interpretation of Quantum Mechanics, the most basic constituents of matter at times behave in-deterministically. This comes from the collapse of the wave function, in which the state of a system upon measurement cannot in general be predicted.

Randomness in statistics vs randomness in cryptography: In cryptography, we are primarily interested in independence, uniform distributions and unpredictability. Random numbers are essential for our modern information-based society.

The unbreakable security of the one-time pad (OTP) in cryptography is also based on the assumption of availability of uniformly random bits, unpredictable by any eavesdropper.

Defining randomness is by no means trivial. A random sequence should pass all possible statistical tests and should be in-compressible. In this context, incompressibility means that the random sequence cannot be generated by a program shorter than its length.

Min-Entropy is required whenever the quality of seeds for a random generator is taken into account. The random seeds, which are required to define the initial state of a PRNG, limit the amount of entropy. True random number generators require physical processes as inputs than applying algorithms on data.

Causal Determinism in current Blockchains

The ECDSA algorithm is one of the most widely deployed signature schemes today, and is part of many practical cryptographic protocols such as TLS and SSH. Its signing operation relies on an ephemeral random value called nonce, which is particularly sensitive: it is crucial to make sure that the nonces are kept in secret and sampled from the uniform distribution over a certain integer interval. It is easy to see that if the nonce is exposed or reused completely, then an attacker is able to extract the secret signing key by observing only a few signatures.

By extending this simple observation, cryptanalysts have discovered stronger attacks that make it possible to recover the secret key even if short bit substrings of the nonces are leaked or biased. These extended attate key recovery to the so-called hidden number problem (HNP) of Boneh and Venkatesane et.al, and are part of a line of research initiated by Howgrave-Graham and Smart et.al, who described a lattice-based attack to solve the corresponding problem, and Bleichenbacher, who proposed a Fourier analysis-based approach.

Disadvantages of PRNG's and the PRN's

Conventional computers are finite state machines. As a result, it is very hard to compute true randomness from running algorithms on it. A deterministic (finite) machinery can obviously not be expected to create the necessary lot of information to ultimately gain unpredictability.

We need new information in each output that cannot be obtained from past observations. Numbers based on pseudo random generator may have bad statistical properties that make them easy to predict from a record of past values.

Cryptographic random number generators typically use a transformation function f to compute fresh random values from past random values. Different constructions such as pseudo random number generators or pseudorandom functions exist, all of which have their predictability properties tightly tied to computational intractability hypothesis.

Backdoors can be implemented in an RNG. In order to generate a sequence of numbers, PRNGs use a so-called seed which is used as initial input for generating numbers but also pre-determines the output.

Although PRNGs can offer highly unbiased random numbers, they cannot be used for applications that require information-theoretic security for two reasons: Firstly, PRNG-generated sequences are unpredictable only under limitations of computational power, since PRNGs are inherently based on deterministic algorithms.

Advantages of QRNG's and QRN's

RNGs that rely on quantum processes (QRNGs), offer guaranteed in-determinism and entropy, since quantum processes are intrinsically random.

True-randomness are based on non-numeric techniques. Quality of randomness that quantum phenomena deliver is beyond question. One intriguing aspect of QM is that properties of a particle are not determined with arbitrary precision until one measure them, consequently the individual result of a measurement contains an inevitable intrinsic random component. This characteristic of the quantum theory provides fundamental randomness that can be used for generating true random numbers.

Quantum mechanical random numbers are random numbers that are derived from the fundamental principles of random processes from quantum mechanics.

Due to the laws of quantum physics, each measurement with identical initial conditions and the same measurement mode provides different values.

Unpredictability of QRNG's

In terms of unpredictability, a stream of Quantum random numbers exhibits two forms:

- **Forward unpredictability**
  If the seed is unknown, the next output bit in the sequence should be infeasible to predict, regardless of any knowledge of previous bits in the sequence.
- **Backward unpredictability**
  It should also not be feasible to determine the seed from knowledge of any generated values. No correlation between a seed and any value generated from that seed should be evident; each element of the sequence should appear to be the outcome of an independent random event whose probability is 50%.

Quality assessment of a Quantum RNG

Coherent states of light are used to produce random numbers. Coincidence is taken care of when proving the coherent state equations.

Hong-Ou-Mandel Experiment

The Hong–Ou–Mandel effect is a two-photon interference effect in quantum optics that was demonstrated in 1987. The effect provides one of the underlying physical mechanisms for logic gates in linear optical quantum computing. Indeed, two-photon interference has no classical analogue, giving it a distinct advantage for a range of applications.

The peculiarities of quantum physics may now be used to our advantage to outperform classical computations, securely communicate information, simulate highly complex physical systems and increase the sensitivity of precise measurements.

Bell Test

In experiments that are aimed at investigating fundamental physics, such as those of a Bell test, the choice of measurement settings has to be genuinely random for the collected data to be even considered as valid. The main goal of entropy evaluation of a secure QRNG is to quantify the amount of randomness available in the measurement outcome M, conditioned upon side-information E. This side information might be accessible by, controllable by, or correlated with an adversary (due to monitoring or direct manipulation).

Distinctness of values generated by otherwise independent generators, but also assure uniqueness of values over an exponentially long range in the sequence of random numbers emitted by the same generator (nonces). QRNG is suitable for even the most demanding applications, including the loophole-free Bell test.

PRNG vs QRNG - A comparison

Property	Traditional/Classical	Quantum
Entropy Source	Randomness based on complexity of process and partial ignorance.	Fundamental randomness.
Ease of certification	Limited ability to certify the underlying physical process, which is inherently a complex one. Certification of the quality of the output based on standard tests.	Can validate the underlying physical processes. Certification of the quality of the output based on standard tests.
Resistance to tampering	Some ability to run health check on entropy source.	Built-in check based on simplicity of process and more sensitive to tampering. Device-independent versions offer highest resistance against tampering of entropy source itself, even by the providers themselves.
Quality of entropy	Various degrees. The underlying process used as entropy source may work in a physical regime where there are large bias and relatively high correlations (that is, small entropy)	High entropy from the start based on the simple design of the source; a QRNG entropy source can be argued to be very close to i.i.d. from the start.
Speed	Can be very high, and several sources may be combined to obtain higher rates.	High, also because of the quality of the initial entropy, but device-independent implementations may be slow, for example.
Size	Can be very small and embedded on chip, e.g.: exploiting a randomness source like thermal noise.	Varies substantially, going from embeddable in smartphones to room-size dimensions for implementing device-independent randomness generation based on non-locality.

Engineering in Deep Technology - Previous
Random Numbers in Blockchains

Next - Engineering in Deep Technology
AME Chain as a Quantum blockchain

AME Chain as a Quantum blockchain

What is a Quantum blockchain?

Quantum blockchain refers to the idea of either an entire blockchain or certain elements of the blockchain functionality being instantiated and run in quantum computing environments. In fact, the quantum domain naturally lends itself to the implementation of blockchain features through,

- Quantum Random Number Generator (QRNG)
- Quantum key distribution (QKD)
- Quantum signatures
- Post-quantum cryptography
- Certifiable randomness
- Fast Byzantine Agreement (scalable consensus)
- Built-in zero-knowledge proof (through the QSZK (quantum statistical zero knowledge) computational complexity class)
- The No-cloning theorem (cannot copy (i.e. double-spend) assets)
- The No-measurement rule (cannot look at quantum information or eavesdropping is evident)

Use of Quantum RNG in AME Chain

In contrast to deterministic random number generators that generate random values with entropy that is limited by the entropy of the initial seed, AME Chain uses non-deterministic random number generators that rely on the quantum state of matter for generation of truly random numbers. By fact, quantum physics is fundamentally random in nature and is confirmed by theory and experimental research.

The process: Single Photon Splitting

AME Chain uses laser-based quantum source to generate the randomness for its cryptography, hashing and digital signatures. It is a highly-sophisticated engineering innovation which involves the power of complex deep-tech technologies such as semiconductors, optoelectronics, high precision electronics and quantum physics working together to create the highest level of randomness possible.

Photon Generation

A laser produces a stream of the elementary particle, photon. The photons generated from the laser are used to generate the random numbers.

Photons unlike classical objects are unpredictable under certain situations. When incident on a semi-transparent mirror, the photon has a 50/50 chance of being reflected or transmitted. The photon is then in a superposition of both the states (reflected and transmitted), i.e. the photon exists in both the states simultaneously. Upon measurement, it collapses to one of these states, which is intrinsically random and there is no way to predict which state the photon will collapse to. This gives the inherent randomness from the photons, which cannot be influenced by any external parameters.

Photons to high entropy random numbers

The process starts with the generation of light from a laser source, which is converted into single-photon level using attenuators. The photons are then sent onto a semi-transparent mirror for the superposition phenomenon and are detected using SPD (Single Photon Detector). They are then converted into bits of 1’s and 0’s, depending on the clicks generated on the SPD. Then there is post-processing in FPGAs to do the conditioning, statistical checks and then deliver the random numbers to the outside world.

The test suits check the randomness of the bits. Only if the conditions are met, they are forwarded to the AME Chain nodes, AME Chain wallet and D-Apps deployed in AME Chain.

How QRNG adds to AME Chain's security?

AME Chain's unparallelled Quantum Random Number Generators (QRNGs) leverage the random properties of quantum physics to generate a true source of entropy, improving the quality of seed content for key generation.

- The source of randomness is unpredictable and controlled by quantum process.
- The entropy source tends to produce true random output.
- Live/real-time monitoring of entropy source is possible and highly effective as well.
- All attacks on the entropy source are detectable.
- The above factors indicate that our QRNG is provably secure.
- AME Chain's QRNGs embed elementary components that can be easily monitored to detect any failure or attacks.
- Environmental perturbations can be ruled out by simple health checks, guaranteeing QRNG always produce high quality entropy.

← Engineering in Deep Technology - Previous
Quantum Random Number Generators

Next - ECONOMICS
AME Chain - The Fundamentals and ... →

Last modified 1mo ago

AME Chain - The Fundamentals and Utility

Fundamentals of AME Chain

AME Chain is a platform that facilitates peer-to-peer communication, Smart contracts and applications via its own native currency called AME. The primary purpose of AME is to facilitate and monetize the working of AME Chain to enable developers to build and run distributed applications (called Dapps).

AME Chain is a Turing complete blockchain framework, as it gives a foundation to programming languages using which you can write contracts that can solve any reasonable computational problem. AME Chain is compatilbe with Ethereum Virtual Machine (EVM), a consensus-based virtual machine that decodes the compiled contracts in bytecodes and executes them on the Ethereum network nodes. It also uses algorithms to prevent denial-of-service attacks that are widely observed in cryptocurrency markets.

AME Chain network is a group of nodes, connected to every other node in a peer-to-peer mechanism. Each node consists of a copy of the entire blockchain data store and competes with other nodes to mine the next block by validating transactions. If a new block is added, the blockchain gets updated and is propagated to the entire network so that every node is in sync.

Consensus Mechanism

AME Chain uses **Proof-Of-Authority (PoA)** as the consensus method that gives a small and designated number of blockchain actors the power to validate transactions or interactions with the network and to update its more or less distributed registry.

According to the chosen scheme, one or more validating machines are responsible for generating each new block of transactions that will be included in the Blockchain. The new block can be accepted directly without verification, or by unanimous vote of the block generators, or simply by a majority, depending on the configuration chosen for the Blockchain.

Unlike the Proof-of-Work mechanism, commonly referred to as “mining”, there is no technical competition between validators here. This consensus mechanism requires almost no computing power, and therefore almost no electricity for its operation.

Since the PoA requires only a limited number of actors, the network can afford to update the blockchain more frequently by reducing the time between each block (Blocktime) and process more transactions (Blocksize) for processing fees close to zero (Transaction fees).

Censorship resistance

The validating nodes of a PoA blockchain have full power to decide on new blocks. This means, for example, that they have the possibility to stop specific transactions, which can generate conflicts of interest and even compromise the security of the network. In the context where these nodes are controlled by actors who both do not trust each other and have sometimes conflicts of interests, the permanent control and monitoring of the validity of the operations ensures the stability of the system.

If, for example, one validator node wished to add one million AME to its balance without any particular justification, then the nodes under the control of other actors have the possibility to reject any block containing this transaction.

Each block validator is therefore encouraged to fulfil its role in an “honest” way because of the constant monitoring of the other actors. For similar reasons, each validator closely monitors the actions of the other validators.

The Proof-Of-Authority meets specific needs within this defined framework, and this solution is an evolution towards efficiency without requiring a revolution in usage or a paradigm shift.

Utility of AME Chain

AME Chain has the usual cryptocurrency use cases across industries such as finance, insurance, banking, healthcare, government, supply chains, IoT (Internet of Things), and media and entertainment to name a few. In addition, the following can be unique applications that can be served by AME Chain due to its quantum-secure properties.

Use case	Scenario	Rationale for using AME Chain
Decentralized Finance (DeFi)	Give users control by using AME Chain and open source coding to facilitate traditional financial services in ways that do not require a bank.	Adds a layer of automated trust and building market platforms.
Blockchain games and Casinos (GameFi)	The assurance that the randomness is genuine contributes to the trust the players put into the games. The business can use the easy verification to facilitate the smooth running of the activity. Smart contracts can be written in such a way that the game won't be rigged in favor of the house.	High-entropy random values.
IoT-enabled devices	Intelligent devices or machines which communicate to other devices, things, machines objects, or infrastructure.	Operational improvements in terms of efficiency, performance, and safety.
Property rights	Traditional top-down attempts have been costly to implement on large scale and have been unsuccessful at increasing global property rights. A bottom-up approach instead follows a process wherein claims are made by individuals verified by those affected aggregated by the community and then brought to the legal authority.	High value transactions require the utmost security guarantees.
Supply chains	Projects involving many different organizations can improve collaborations by creating a single database and source of truth.	Reduce fraud and corruption, automate a manual process, and control for issues of authentication.
Public Safety	Privacy is the major concern for all the devices and applications available online. Encrypting communications to and from these devices is essential.	Ensures the privacy of communications using encryption.
Decentralized Social Media	Participate directly without the intervention of third-party trust and we profit from the success of what we are posting. Incentive structure of social media with AME coin, and also the validation and authenticity of posts.	Advantage of earning AME Coin or other token, avoid censorship, immutability, transparency, creditability of AME Chain platform.

← Engineering in Deep Technology - Previous
AME Chain as a Quantum blockchain

Next - Operations
Roadmap →

Roadmap

2023

Quarter - 1

- Advertisement Campaigns
- Centralized Exchange Launch
- New Staking Portal
- Scaling Ecosystem

Quarter - 2

- Strategic Partnerships
- Release of DAO Platform
- Developer Grants for Dapps
- Tier 1 Exchange Listing

Quarter - 3

- Nodes & Validator Auctions
- Oracle Market Framework
- VPN UI Wireframe
- Blockchain Integration on Web 3.0 Oracle

Quarter - 4

- VPN Beta Launch
- Oracle Mainnet Launch
- VPN Mainnet Launch

ECONOMICS - Previous
AME Chain - The Fundamentals and ...

Next - Conclusion
Conclusion

Conclusion

AME Chain - A Future ready Quantum blockchain

Building resilience against future threats is key to ensure that vital parts of the Blockchain and cryptocurrency economy keep thriving. The issue is that investments for protection from medium to long-term risks are somewhat natural to overlook or dismiss, given more pressing present issues, and the costs may not seem immediately justified. It often takes some bad incidents to incentivize the necessary proactive steps.

While blockchain technology prides itself in providing a trustless system upon which the economy of digital currencies and assets operate, the underlying security mechanisms still rely on classical cryptographical processes, thus necessitating a certain level of trust in them. AME Chain has assimilated Quantum mechanical properties into its system, thus removing the trustful component of the security subsystem in blockchain, with ambitions of migrating towards of a truly trustless blockchain.

Operations - Previous
Roadmap

Last modified 1mo ago