UNIFIED SOCIETY

QUANTUM

Table of Contents

Abstract

Bitcoin, which is based on blockchain technology, has transformed international currency exchanges and elevated the formerly tedious cash/credit payment processes to an innovative state that requires new investments, currencies, and technologies. Ripe for competition, numerous competitors entered the cryptocurrency market shortly after Bitcoin launched, such as Litecoin, Dogecoin, and USX (USDE). Due to the industry's dominance of traditional computing, both the blockchain and cryptocurrency markets are considered secure from cyberattacks. This will not always be the case as quantum computing becomes more prevalent and begins to pervade ordinary activities. Quantum computing will have a profound effect on many facets of life and technology. While Shor's and Grover's algorithms are essential for the security of quantum blockchain-enabled technologies, the power of quantum computers will expose their flaws. Quantum computing, which is based on quantum mechanics and a multitude of other quantum principles, will have a profound effect on blockchain, cryptocurrencies, and the international business community. USX will establish the next generation of blockchain technology by utilizing quantum mechanics. Quantum entanglement will be critical in the development of an unbreakable cryptographic hash. USX quantum will be the world's first blockchain with true quantum capabilities.

Introduction

Even after the April 2021 rise of Dogecoin, Bitcoin continues to be the most widely known and traded cryptocurrency. Thousands of similar cryptocurrency projects have since been launched, but few have been able to replicate Bitcoin's sustained success. The majority of cryptocurrencies use the same elliptic curve public-key cryptography (ECDSA) to generate digital signatures that enable secure transaction verification. Today's most widely used signature schemes, including ECDSA, DSA, and RSA, are theoretically vulnerable to a well-planned and executed quantum computing attack. As a result, developing and securing quantum-based blockchains would be beneficial. Not only will this technology transform the future of blockchains, but it will also secure previous generations of blockchains.

Asymmetric cryptography generates a private-public key pair in such a way that the two keys are mathematically related. The private key, as the name implies, is kept secret, whereas the public key is made publicly available. This enables individuals to generate a digital signature (using their private key) that can be verified by anyone who possesses the associated public key. This is a very common method of establishing the authenticity and integrity of transactions in the financial industry. Asymmetric cryptography's security is based on a mathematical concept known as the "one-way function." This principle implies that the public key can easily be derived from the private key, but not vice versa. All known classical algorithms for deriving the private key from the public key are impractical because they require an astronomical amount of time to perform the computation. This is excellent news for everyone involved in any modern cryptocurrency, but it could create significant problems in the future once quantum computing is incorporated.

In 1994, mathematician Peter Shor published an algorithm that could compromise the security of the most widely used asymmetric cryptography algorithms when applied to a quantum computer. This means that anyone with a sufficiently powerful quantum computer could use this algorithm to derive a private key from its associated public key, thereby enabling the falsification of any digital signature. These consequences are not limited to a single user, as they could delegitimize the entire blockchain. This would eventually result in the devaluation of the entire cryptocurrency industry, resulting in a mass exodus.

Another possible vulnerability is Grover's algorithm. Grover's algorithm can exponentially accelerate mining due to the computational power of a quantum computer. When it comes to the state of cryptocurrencies, single entities with exponential computational power pose a greater threat. The ability to mine quickly in a quantum environment could result in price destabilization and, more importantly, chain control. This would result in significant mining centralization and, potentially, 51 percent attacks, in which the majority of the blockchain is compromised. forcing the blockchain to use the attackers version

USX

With thousands of distinct projects offering a vast array of products, solutions, innovations, and other promising technologies, Unified Society Quantum will act as a gateway to the quantum world. Connecting, securing, and empowering all networks to continue innovating while retaining quantum supremacy. USX's mission is to unite the cryptocurrency community through education and collaboration with researchers and developers to secure and develop the future of quantum-based blockchains. We are living in the quantum era's infancy. USX will create blockchain quantum encryption by leveraging the power of quantum computers. This paves the way for transactions faster than the speed of light, which we will require in the future of space exploration, industry 4.0, and beyond. A unified society capable of laying the groundwork for the next generation of encryption. We will leverage existing projects to acquire and develop the necessary technology. With a strong community, committed team members, and contributors, we are well on our way to success. One of the primary goals is to create a free premium educational De-Fi platform where anyone on the planet can learn about a variety of subjects. Physics, chemistry, and computer science are just a few examples. We will provide an exceptional education to each user, thereby fostering future generations dedicated to the research and development of quantum-based blockchains. A platform that will enable students, developers, researchers, and ordinary citizens to escape poverty and pursue their dreams. Creating a more sociable and friendly ecosystem for the benefit of humanity.

The USX token will provide many use-cases such as:

- Being a digital currency of the future in which you will be able to transact on the most secured and advanced network,
- Providing incentives to the community (researchers, developers, creators, learners, and the entire USX community) to work together on the securing our precious blockchains.
- An online education platform
- Future discounts and incentives will continually be updated and added

To power the Quantum learning platform, a usx quantum contract will be created on the Binance smart chain.

This platform will be used to publish quantum-related research and news.

Additionally, this platform will support quantum-encrypted NFTs.
Our protocol will encrypt and sign your nft.

The characteristics of the Quantum platform Quantum physics, blockchain technology, and science are discussed.

A location on the quantum network where users can trade nfts and digitally sign transactions.

Assist smaller organizations in initiating their endeavors

We want to prevent too many tokens from being released into circulation all at once. Our tokenomics are built in a manner that will encourage long-term investors to hold. Strong vesting schedules are applied to all parties, enabling a more transparent and stable journey. We must provide new investors with prospectus and we do require acknowledgement that USX is a long-term, strategic investment.

TOKENOMICS & PARAMETERS

Max Supply: (2,600,000,000). 6 Decimals. The smallest denomination of USX will be 6 Decimals

- Initial distribution supply: ~1.3875% (36,075,000.00) of max Token supply. That is once vesting schedules for the first quarter of 2022 are released.
Initial market cap valued at $.025/token will be $901,875.00

DISTRIBUTION

❖IDO - Presale: 0.57% (15,000,000)

- Target: 800BNB ~ $364,800 USD. Percentage of max supply: 0.057% (15,000,000)
- Price per coin: $0.025 USD.
- Liquidity: 60% (BUSD & Token) Locked for 365 Days on PancakeSwap

❖Private sale: 0.175% (4,500,000)

- Target: $114,000 USD. Percentage of max supply: 0.175% (4,500,000)

- Stage 1 - Price per coin: $0.005 USD.

- Stage 2 - Price per coin: $0.0085 USD.

- Stage 3 - Price per coin: $0.0095 USD.

- Private Sale is for early investors. We only want investors who will contribute to the project for the long term and not for a short financial gain. Therefore, please acknowledge that any purchases on the private sale are subject to vesting schedules.

- 12 months vesting schedule released 8.33% monthly.

- Initial distribution for Q1 2022 will be 36,075,000.00 USX Token

Standard POS Rewards:

Standard Rate is 20% APR for the first year. No minimum requirements and no maturity periods for the standard rates.

Token Lockup Rewards:

- 3 Months: 5% APR
- 6 Months: 20% APR
- 12 Months: 35% APR
- 24 Months: 80% APR

Staking: 63% (1,638,000,000)
(excluding team holdings, reserves, & community)

- 0-12 months - 20% APR
- 12-24 months - 16% APR
- 24-36 months - 13% APR
- 36-48 months - 10% APR
- 48+ months - 7% APR

❖**Team holdings: 10% (260,000,000)**
❖Vesting schedule Released quarterly for a duration of 5 years. 5% (13,000,000).

• Initial distribution for Q1 2022 will be 13,000,000.

❖ **Long term hodlers 2% (52,000,000)**

Long term holders from 2013 onwards, will be eligible to swap their USX from the current block chain to new Binance Smart Chain USX Tokens by 6/15/21.

• There will be a 5:1 ratio (5 old coins for 1 new token).
• The locked tokens will be eligible for staking, incentivizing holders to hold their tokens for the longterm and thus decreasing the probabilities of holders selling.
The initial distribution will be (1,625,000) and available 90 days after the conclusion of the IDO. The vesting schedule releases are as follows:
• **90 Days after LP Launch:** 1,625,000 (3.125%) per month.
• **12 Months after LP Launch:** 2,080,000 (4%) per month.
• **18 Months after LP Launch:** 3,185,000 (6.125%) per month until exhausted

❖ **Community: 5% (130,000,000):**

• These funds are intended to reward the USX community for their dedication and contributions to the project, also known as bounties. Small amounts would be used for airdrops, contests, advertisements, influencers, bounties, etc. After all, this is a community-led initiative, and we want to look after our community. The tokens will be subjected to strict vesting schedules. We will maintain a consistent distribution for several years to come. Rather than selling them or incorporating them into the team's properties, we want to distribute them to the group, which would also increase decentralization.

• Vesting schedule (4%, 5,200,000) released quarterly for a duration of 6.25 years.
Initial distribution will be for Q1 2022 (5,200,000).

❖ **Reserves: 10% (260,000,000):**

• Tokens will be reserved for additional funding through investors who can give the project long-term benefits. The majority of cryptocurrency projects fail during bear markets, as we saw during and after the 2018 crash. We want to accumulate the resources necessary to withstand such adverse conditions and maintain the community's health.
• 4 years vesting schedule, 6.25 of the 10% (16,250,000).
• Initial distribution will be for Q1 2022 (16,250,000)

🔒**Token Security**

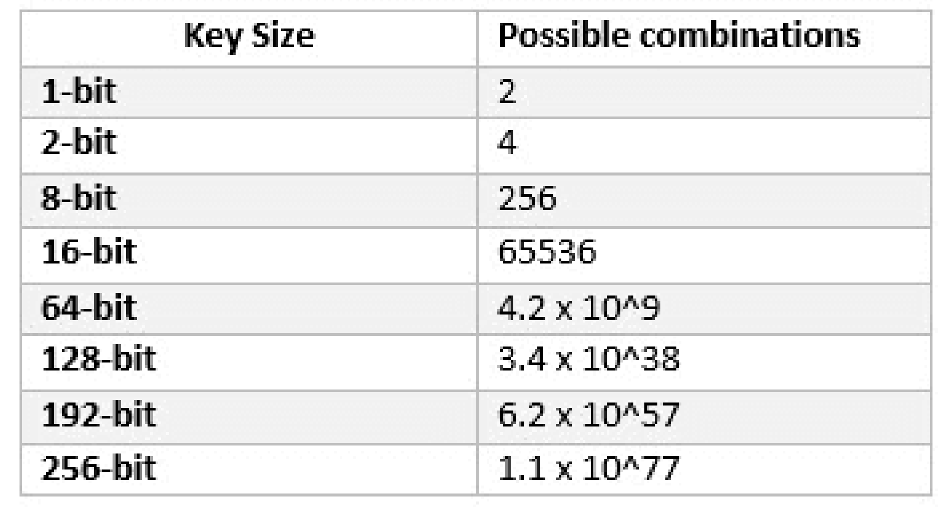
- Anti-Sniper Bot integrated within the Contract (Pinksale)
- Full Contract Auditing

Conceptual Awareness

To process the information contained in this whitepaper effectively, a foundational understanding of physics, cryptography, and mechanics in both the classical and quantum realms is required. Additionally, there is a blockchain and cryptocurrency framework that must be understood prior to proceeding. If you are already familiar with these concepts, feel free to proceed. This section will define and identify critical concepts necessary for a proper understanding of any applications derived from this quantum cryptocurrency whitepaper.

Throughout this paper, the terms "classical computing" and "quantum computing" will be used interchangeably. Computing in the modern era is referred to as classical computing. That is, the MAC or PC on which you are currently working. Quantum computing is a term that refers to quantum computers that are not yet commercially available and are being used by a small number of businesses and governments. Unless otherwise specified, all discussions will be in terms of classical computing, unless the section or principle in question is explicitly identified as a quantum principle.

Cryptography and many of the quantum computing principles that will be discussed require an understanding of bit size, combinations, and their differences from qubits.
The potential bit key size, as well as the correlated factoring combinations, are detailed in Figure 1.1. Due to the fact that the majority of cryptocurrencies, blockchains, and algorithms discussed in this cryptocurrency whitepaper use 256-bit encryption, that will be the standard going forward unless otherwise stated.



Key Size	Possible combinations
1-bit	2
2-bit	4
8-bit	256
16-bit	65536
64-bit	4.2 x 10^9
128-bit	3.4 x 10^38
192-bit	6.2 x 10^57
256-bit	1.1 x 10^77

FIGURE 1.1
Source: Pro Pirvacy

With 1.1 1077 possible combinations, it's obvious that 256-bit would be the most difficult bit key to attempt to decrypt. Due to the fact that 256-bit has 1.1 1077 possible numerical combinations, the time required to correctly decipher any key would be far too lengthy to provide actionable or timely results. As a result, 256-bit is the current industry standard for bit sizes in the blockchain, cryptocurrency, security, and business worlds. Later, we'll discuss why decryption takes so long at this bit size and how quantum computers render the 256-bit key size nearly obsolete.

Another critical concept on the bit spectrum to grasp is the distinction between bits and qubits, as both will be discussed in this paper. A bit is essentially the unit of measurement that a conventional computer uses to communicate digitally. A qubit is analogous to a bit, except that it is applicable only in the quantum realm. In a nutshell, a bit denotes classical computing, whereas a qubit denotes quantum computing.

The distinction between a bit and a qubit is illustrated in Figure 1.2. At any given time, a bit can only be in a single position, which can be represented by the values 1 or 0. Due to entanglement and superposition, qubits can exist in multiple states concurrently. Qubits are mathematically represented by the formula:

$$X \text{ or } Y = |0\rangle \text{ or } |1\rangle$$

As a vector, they are visually identified as:

$$|0\rangle = \binom{0}{1} \text{ and } |1\rangle = \binom{1}{0}$$

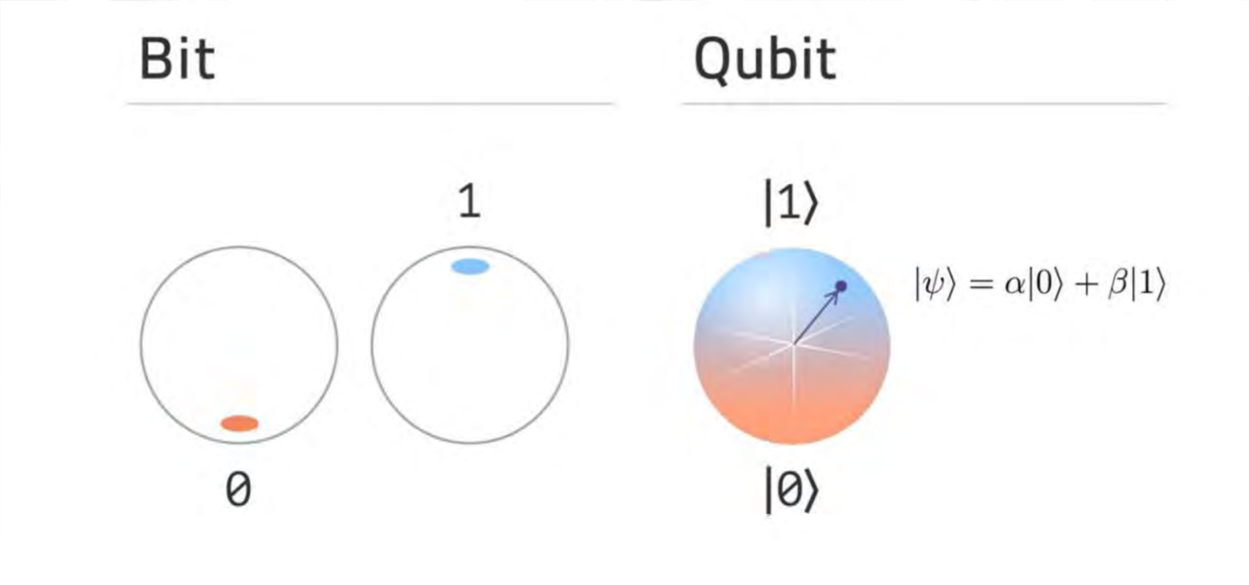


FIGURE 1.2
Source: Toward Data Science

Superposition is a principle of quantum physics that allows an object to exist in multiple states concurrently until it is measured. This is true only in quantum discussions, as superposition is impossible in the classical world.

Entanglement is a quantum mechanics principle that has no application in classical physics. This occurs as a result of the interaction of two particles. Rather than strictly splitting and acting as two distinct separate particles, two entangled particles will remain dependent on one another and will behave in accordance with one another regardless of their spatial separation. When qubits are entangled, computational power is significantly increased. As a result, this is a fundamental principle underlying quantum computing's advanced capabilities.

The majority of current blockchains or cryptocurrencies encrypt and protect messages and transactions using RSA or elliptic curve cryptography. Figure 1.3 illustrates how RSA encryption secures transactions. RSA encryption is named after the three individuals who invented the algorithm in 1977: Rivest-Shamir-Adleman. RSA is widely regarded as the first and most widely used cryptosystem for the secure transmission of messages and transactions. RSA is a type of asymmetric cryptography. Asymmetric cryptography is also known as public key cryptography, which RSA employs, as illustrated in Figure 1.3. The public and private keys in symmetric key cryptography may be identical. There are significant security and privacy concerns with symmetric cryptography when it comes to cryptocurrencies, as it is possible to learn someone's wallet address. As a result, blockchain technology and cryptocurrencies employ asymmetric cryptography to secure transactions. We've discussed RSA in detail, but other methods exist. Elliptic curve cryptography is more secure than RSA because it uses smaller key sizes. Elliptic curve cryptography, or ECC for short, encrypts and decrypts data using an ecliptic curve rather than prime factorization. Additionally, ECC serves as the foundation or equation for ECDSA, which stands for elliptic curve digital signature algorithm.
The majority of blockchains and cryptocurrencies encrypt their data using RSA or ECDSA.

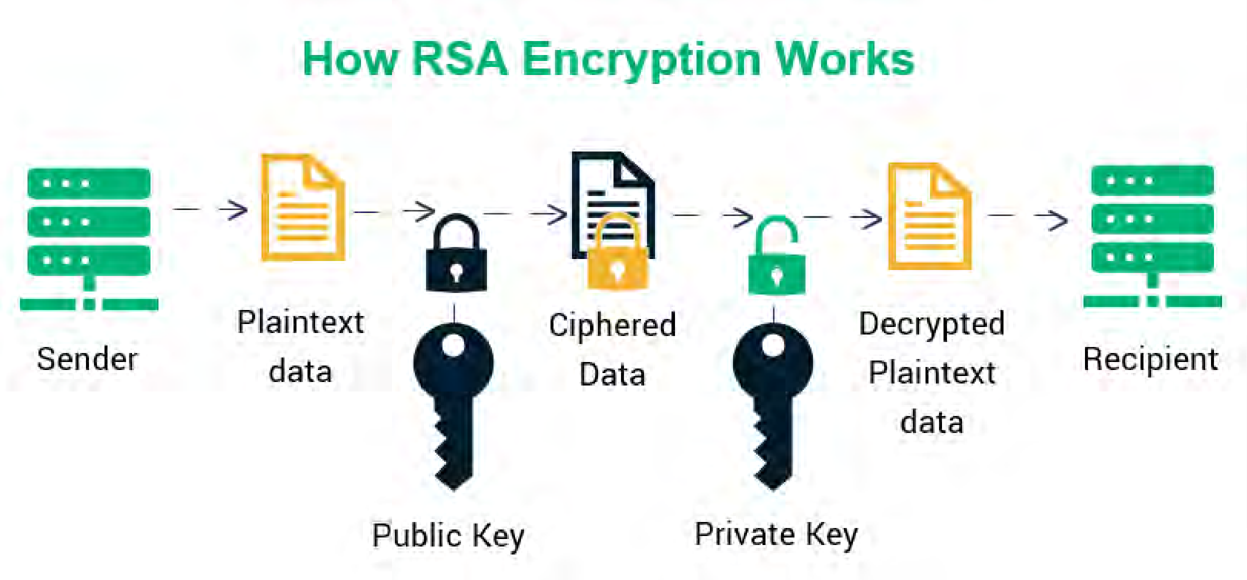


Figure 1.3
Source: Infosec Insights

The cryptographic hash function, colloquially referred to as "hash," is ultimately the process of converting the text input to a string of scrambled digits. A nonce is also referred to as a random number that can be used only once during a communication. The nonce adds value to authentication by identifying malicious actors and fortifying hash functions. For a visual representation, see Figure 1.4.

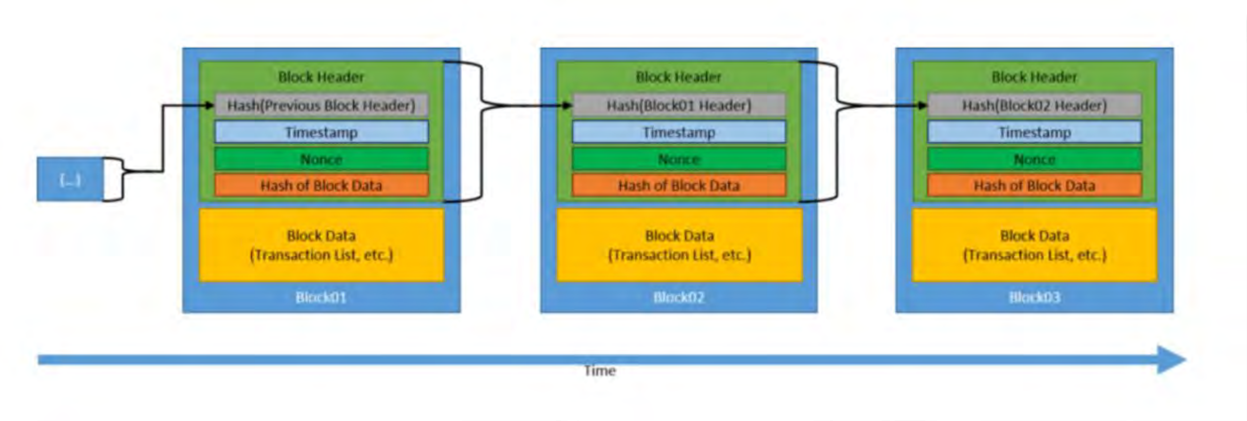


Figure 1.4
Source: NIST

How Bitcoin/Crypto works

To circumvent the need for banking or financial institutions to conduct payment transactions, Sitoshi Nakamoto created Bitcoin, igniting a cryptocurrency race that accelerated the adoption of blockchain technologies. In comparison to previous digital payment methods, Bitcoin was founded on the premise of cryptographic proof rather than trust. In essence, payments based on cryptographic proofs are impossible to reverse, which safeguards both buyers and sellers. Buyers could benefit from an enabled escrow account, while sellers would be safeguarded against fraud. This ensures that both buyers and sellers enter into a transaction with mutual consent.

Figure 1.5 depicts a high-level transaction. Due to the fact that these coins are created using digital signatures, they provide the purest form of ownership. Each transaction's public keys are hashed, ensuring that the same address is not used twice. Additionally, the private key is hidden for the transaction's digital signature. This security protocol minimizes the possibility of being a victim of an attack.

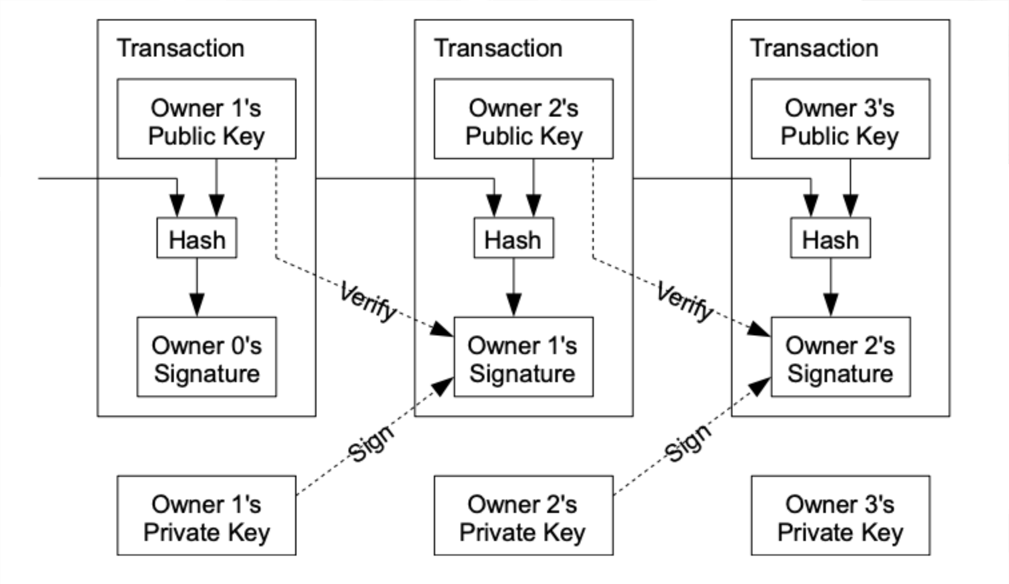


Figure 1.5
Source: https://bitcoin.org/bitcoin.pdf

Initially, one of the major concerns was regarding how to ensure individuals don't spend money they have already spent. This is also called the double spending possibility. The combination of a timestamp network and a proof-of-work system are the building blocks to preventing the double-spending possibility. Each transaction is stored essentially building upon one another. As the blockchain builds, the more honest nodes on the block, the more secure it will be come. Should an attacker modify a previous block, they would also have to modify all the sequential blocks to catch up to where the block currently is, and then take it over. The main reason this is impractical is because of the CPU power it would take to perform such actions. Attackers would also potentially be better off initiating their own coin rather than modifying an existing one. As creating your own digital coin is less expensive, time intensive, and creates more value, the likelihood of attacks are lowered. Modifying an existing blockchain, not only takes an exponential amount of effort, but also devalues the coin. Should the coin devalue enough, there wouldn’t be a strong rationale to possess the coin. Sitoshi Nakamoto’s original proof-of-work chain can be seen in figure 1.6.

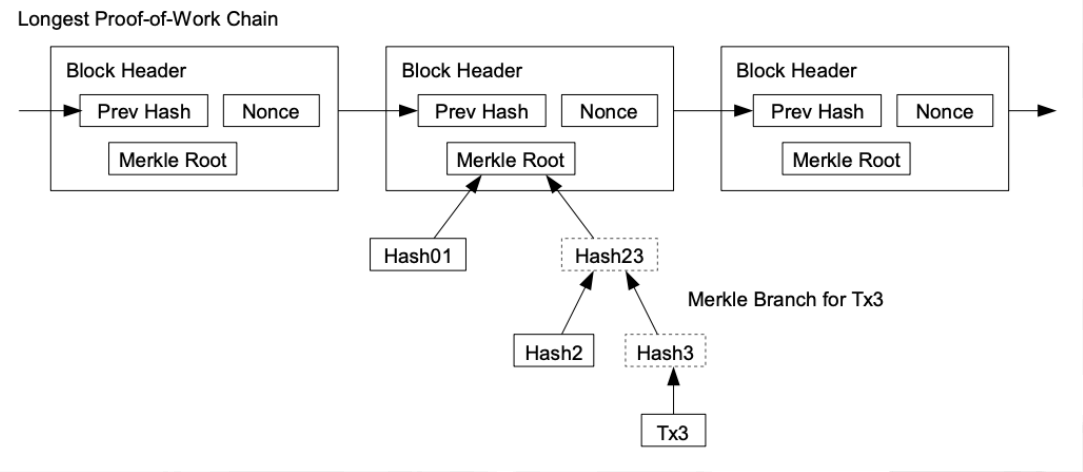


Figure 1.6
Source: https://bitcoin.org/bitcoin.pdf

Quantum Physics

Because the limitations of quantum physics are unknown, the application possibilities are vast. We previously discussed superposition and entanglement, but there are a plethora of other quantum physics concepts that are critical for quantum computing.

Rather than a coin being in a heads or tails state, consider the coin being in both states concurrently. This is the superposition principle.

A coin that is entangled is in both states (heads and tails) in sequence. However, in reality, only one of the pairs would be true. In layman's terms, this means that there are two systems, but only one truly exists.

Interference enables events to be predicted. Interference demonstrates how particles interact with one another based on the wave length and whether the waves are destructive or constructive. The double-slit experiment demonstrates the true and probabilistic nature of waves and particles quite effectively.

In quantum physics and mechanics, bosons and fermions continue to play a role. A photon is an example of a boson. Photons are critical to quantum computing and its potential application, as described in this quantum whitepaper. Electrons, protons, and neutrons are all examples of Fermions.

Spins will be critical for quantum technology advancement. One of the primary reasons for this is the expectation that spins will eventually result in the creation of qubits. This would enable qubits to be created without the use of moving electrons and on a fundamentally smaller scale.

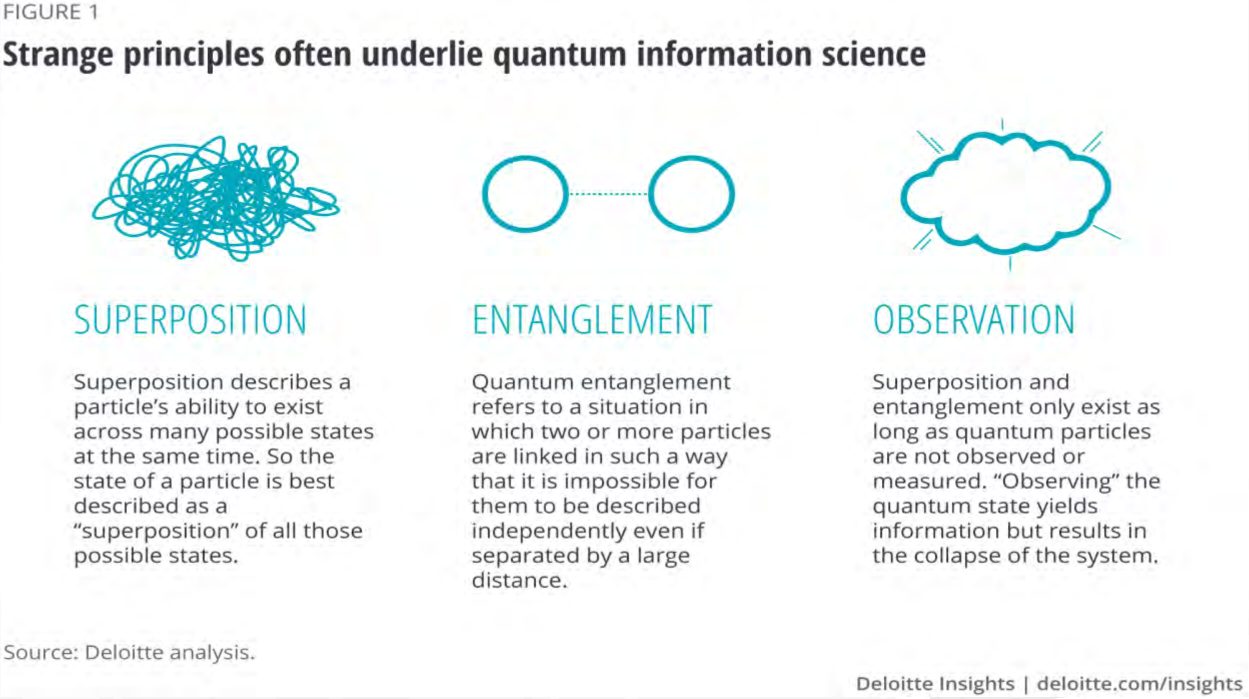


FIGURE 1

Strange principles often underlie quantum information science

SUPERPOSITION

Superposition describes a particle's ability to exist across many possible states at the same time. So the state of a particle is best described as a "superposition" of all those possible states.

ENTANGLEMENT

Quantum entanglement refers to a situation in which two or more particles are linked in such a way that it is impossible for them to be described independently even if separated by a large distance.

OBSERVATION

Superposition and entanglement only exist as long as quantum particles are not observed or measured. "Observing" the quantum state yields information but results in the collapse of the system.

Source: Deloitte analysis.

Deloitte Insights | deloitte.com/insights

Source: Deloitte

Quantum Computing

Quantum computers share some characteristics with classical computers. Both, for instance, are composed of three primary components:

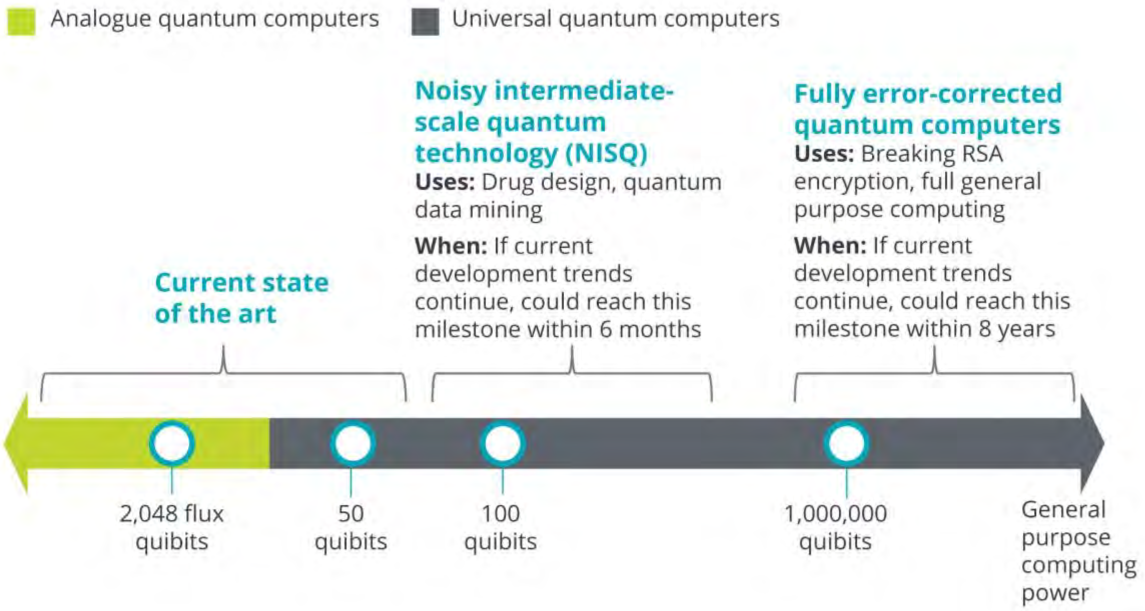
1. Processor
2. Memory
3. input/outputs

One of the current distinctions that jeopardizes quantum computer commercialization is the requirement for quantum computers to be housed in a facility with a temperature close to absolute zero. Additionally, quantum computers operate via photons. Additionally, fiber optic cables are required for quantum computing. This is a significant departure from current computing standards, one that will require considerable time for businesses, let alone individuals, to adapt to.

Quantum computers are also notorious for being prone to errors. Until constant errors are mitigated, quantum computers will serve little useful purpose. While quantum computers are currently being used in a variety of projects by companies such as Google, IBM, and Microsoft, there is a significant amount of validation that goes into any result produced by quantum computers. A concern about error correction is related to the fragility of qubits. Due to the extreme fragility and volatility of qubits, they are difficult to forecast, contain, and leverage.

FIGURE 2

Quantum computers vary in how they can be used



🟩 Analogue quantum computers ■ Universal quantum computers

Current state of the art

Noisy intermediate-scale quantum technology (NISQ)
Uses: Drug design, quantum data mining
When: If current development trends continue, could reach this milestone within 6 months

Fully error-corrected quantum computers
Uses: Breaking RSA encryption, full general purpose computing
When: If current development trends continue, could reach this milestone within 8 years

Source: Deloitte analysis.

Deloitte Insights | deloitte.com/insights

Source: Deloitte

It may be well into the 2030’s to see a truly operational quantum computing model that meets commercialization criteria. Even then, widespread commercialization may be years away due to hardware constraints and temperature cooling requirements. The image below depicts a quantum computer. As you can see, there would be little appeal for an individual to own an item of this nature in its current design in a household.

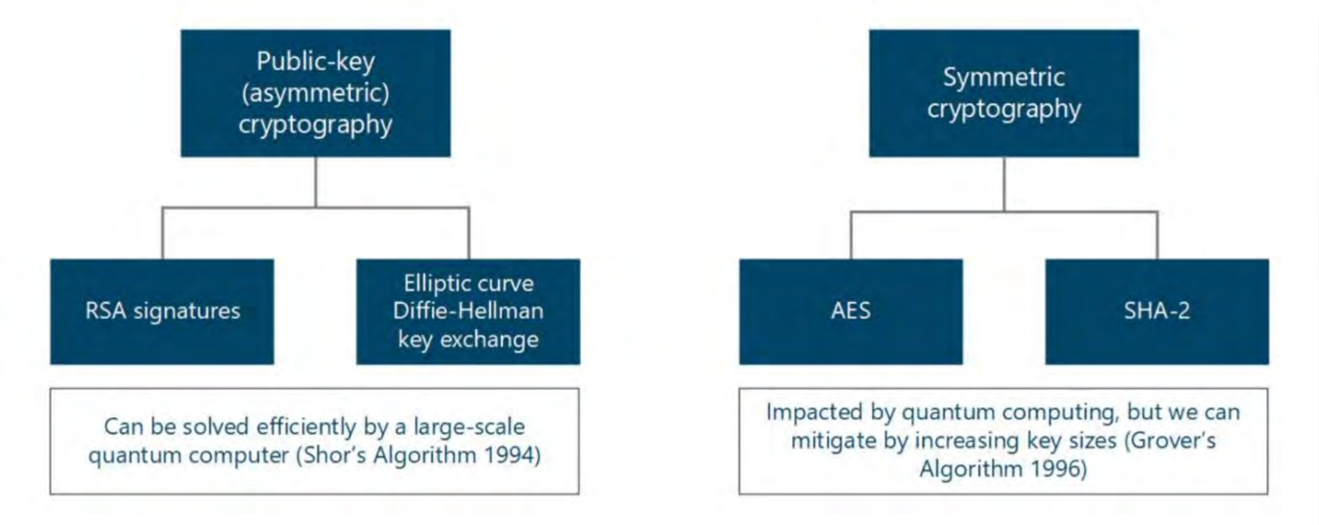
Quantum Cryptography

Quantum key distribution, also known as QKD, is perhaps the most vital aspect to quantum cryptography. Utilizing light particle properties, QKD encodes messages. This important component is critical to the security of quantum computing. Measuring the light particles would be required in order to hack or attack the key. However, due to quantum physics, any act of measuring the particles effectively changes the measure. This would immediately trigger alerts and any monitoring or alarm system would begin to show red flags.

Currently, there are two major cryptographic methods:

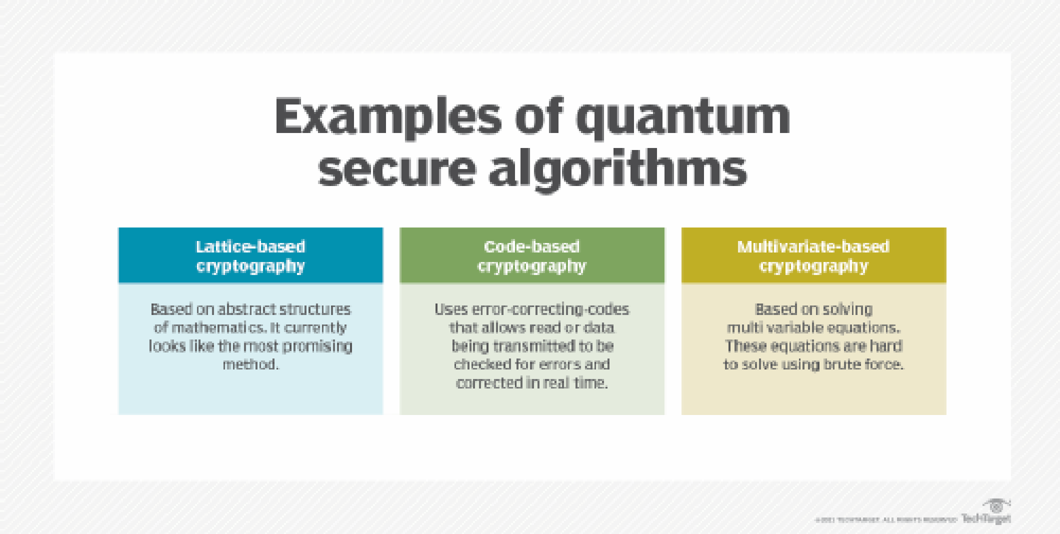
1. Asymmetric
2. Symmetric

Asymmetric cryptography shares the public key, but maintains the private key as confidential. Based on the infrastructure, purpose, and security method used, this could involve nonce, hashes, and other scrambling techniques. RSA is an example of an asymmetric cipher. Symmetric cryptography utilizes the same key to encrypt and decrypt messages. AES or Advanced Encryption Standard is a cipher in use by symmetric methods. RSA and ECC which are currently in use by blockchain are at a major risk due to the astronomical quantum computing computational power. AES and 3DES are considered safe from current predicted quantum computing abilities. NIST also recommends extending the bit key length size to a minimum of 2048 bits to ensure quantum resistant ciphers.


Public-key (asymmetric) cryptography
RSA signatures
Elliptic curve Diffie-Hellman key exchange
Can be solved efficiently by a large-scale quantum computer (Shor's Algorithm 1994)
Symmetric cryptography
AES
SHA-2
Impacted by quantum computing, but we can mitigate by increasing key sizes (Grover's Algorithm 1996)

Source: Microsoft

Besides asymmetric and symmetric cryptographic methods, there is also lattice-based, code-based, and multivariate-based cryptography. Out of all of the encryption methods mentioned here, lattice-based is currently the number one option to be utilized in a quantum environment. A large reason why is that, even though lattice-based encryption is still mathematically based in its framework, it has no reliance to prime numbers. It is instead, based on abstract mathematical structures.



Examples of quantum secure algorithms

Lattice-based cryptography	Code-based cryptography	Multivariate-based cryptography
Based on abstract structures of mathematics. It currently looks like the most promising method.	Uses error-correcting-codes that allows read or data being transmitted to be checked for errors and corrected in real time.	Based on solving multi variable equations. These equations are hard to solve using brute force.

Source: Tech Target

There are a number of key organizations that are working to ensure cryptography standards are up to par for the future of quantum computing. These organizations include:

- National Institutes of Standard & Technology
- IEC Technical Committee 65
- OSI/IEC/JTC1/Subcommittee 27

Shor’s Algorithm

Based on the premise of factoring prime numbers more efficiently and quicker than any other algorithm known to date, Shor’s algorithm will play a critical role in cryptography and cyber security once quantum computing becomes mainstream. While the algorithm has been known. There is no classical computer that carries the computational power to capitalize on the algorithm to make it a threat today. Below, figure 1.7 details the drastic difference between the classical computing efforts and the iterative operation efforts a quantum computer would need to leverage with Shor’s algorithm. The application of Shor’s algorithm to cryptographic problems breaks the asymmetric cipher leading to the ability to modify digital signatures, ledgers, and other related protocols. The implications of this would be devastating to blockchain and any cryptocurrency as, if ever completed, it would allow the manipulation and modification of ledgers and wallets. This would lead to a cascading effect of a loss of legitimacy in blockchain and subsequently impact a number of industries and currencies.

The portion of Shor's algorithm that becomes critically important once a quantum computer is introduced is when it comes to period finding. The factorization polynomial complexity formula utilized is

$$O(\log n)^2 (\log \log n)(\log \log \log n).$$

As shown below, Shor's algorithm, specifically, this formula, is only leverageable with a quantum computer.

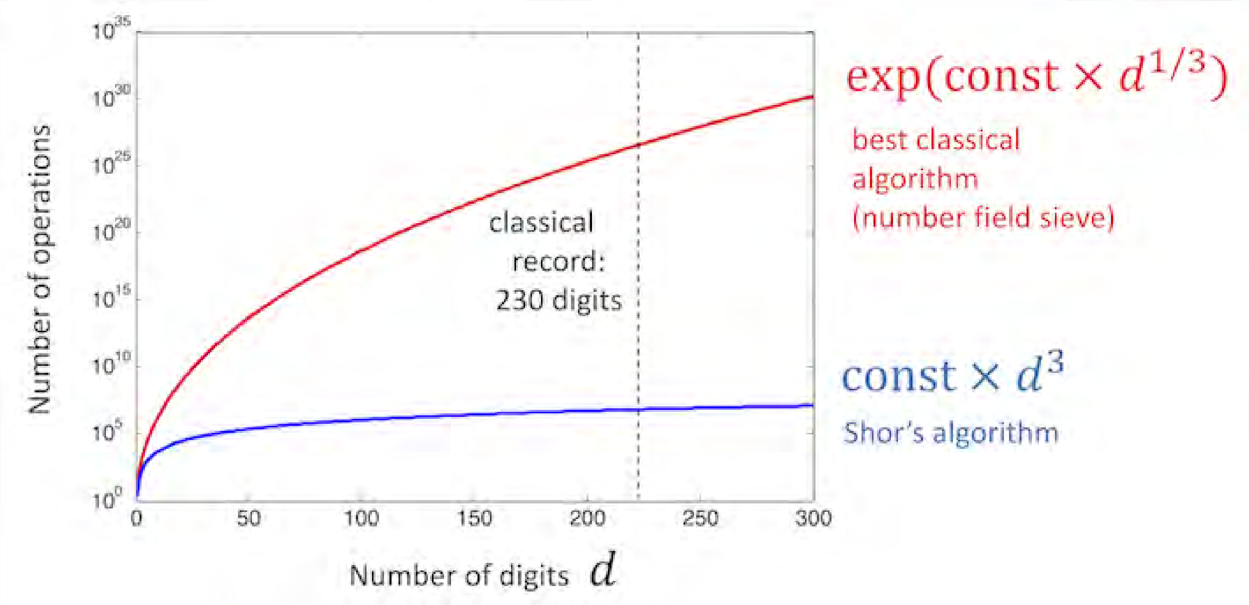


Figure 1.7
Source: IBM

QFT, or Quantum Fourier Transform, in a paper on the subject by Ian Tillman, is defined as:

$$A \equiv \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} |c\rangle \langle a| \, e^{2\pi i a c/q}, \quad q \equiv 2^l$$

QFT lowers the computational complexity to a degree where a quantum computer would be able to quickly identify polynomial factors. The below applications and outputs described are based on Tillman's research.

Application of a Hadamard gate must be done to put the structure into a state such as:

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle_i \, |0\rangle_o$$

The output will provide us with a solution to inequality:

$$\left|\frac{c}{q} - \frac{d}{r}\right| < \frac{1}{2q}$$

Once completed, the solution will provide the answer to *r* which enables the cipher to be broken.

Grover’s Algorithm

Where Shor’s algorithm focuses on asymmetric cryptography, Grover’s algorithm is responsible for ultimately halving any security by reducing the complexity of all symmetric ciphers and hash functions. Grover’s algorithm does this by taking ciphers and functions from *O(N)* to *O(√ N)*. Grover’s algorithm is extremely effective in reducing the amount of evaluations required even with a classical computer. The original calculation of finding *t* after $\frac{N}{2}$ iterations is very methodical and slow which would poise essentially zero threat to classical computers, let alone to quantum computers. This factor of 2 allows Grover’s algorithm to overcome symmetric ciphers and hash functions. There is a secondary component within Grover’s algorithm that can also identify collisions within the hash function. That formula is $O(\sqrt[3]{N})$. This is important as collisions can lead to increased vulnerability of the security of a target. The effect of this algorithm is essentially that digital signatures can be modified and thus renders the authenticity of the transaction, as well as the entire ledger of the blockchain as illegitimate.

The calculations below are presented from Daan Sprenkels paper on Grover’s algorithm. The paper, titled *“Grover’s Algorithm”* provides a comprehensive, granular description of the inner workings of the algorithm.

Noted as the coin flip operator or Hadamard operator, *H,* is applied to each qubit.

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The next step in the algorithm is to begin the iterative process. Here, we apply Z_t to begin the inversion of the amplitude of *t*

$$Z_t\left|x\right\rangle = (-1)^{f(x)}\left|x\right\rangle$$

For the second part of the iteration process, we must apply the diffusion transform. The below is applied to all separate state components of $|x\rangle$ and $|\psi\rangle$.

$$D\left|x\right\rangle = (2m-1)\left|x\right\rangle$$

Below is an example of a two-bit iteration on a quantum level that Sprenkels details. The below matrices are for a state with two qubits.

$$\mathbf{Z_t} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{D} = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

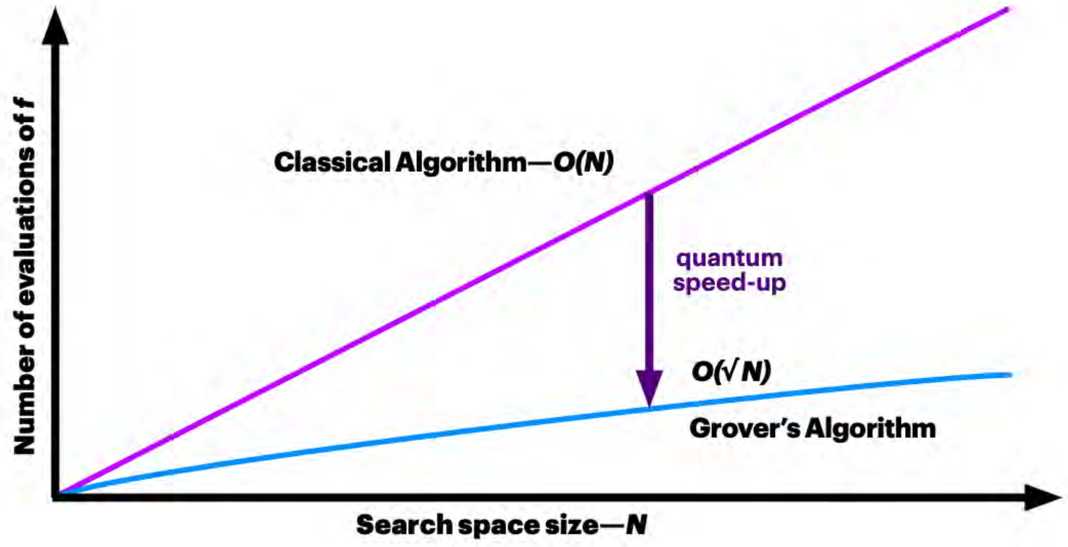
The first step is to apply Z_t:

$$\mathbf{Z_t} \cdot \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix}$$

Then apply the matric diffusion D:

$$\psi' = \mathbf{D} \cdot \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

The outcome is $|10\rangle$



Source: University of Tokyo CompSci

This example of Grover's algorithm showcases the efficiencies gained based on the computational abilities of a quantum computer running the formula.

Is Quantum A Threat to Blockchain?

Both blockchain and quantum computing becomes more mainstream by the day. Blockchain more so than quantum computing, but there will be a day where that may change. Blockchain has two critical potential threats proposed by quantum computing. The first is if quantum computers are able to dramatically increase the effectiveness of inversing hashes. The second would be the potential for quantum attacks to disrupt and essentially render useless the current public/private or asymmetric key cryptography methods used by blockchains. The development of quantum resistant cryptography is necessary not only to protect the future stability of blockchain and cryptocurrencies, but also to protect the viability of an advanced quantum world.

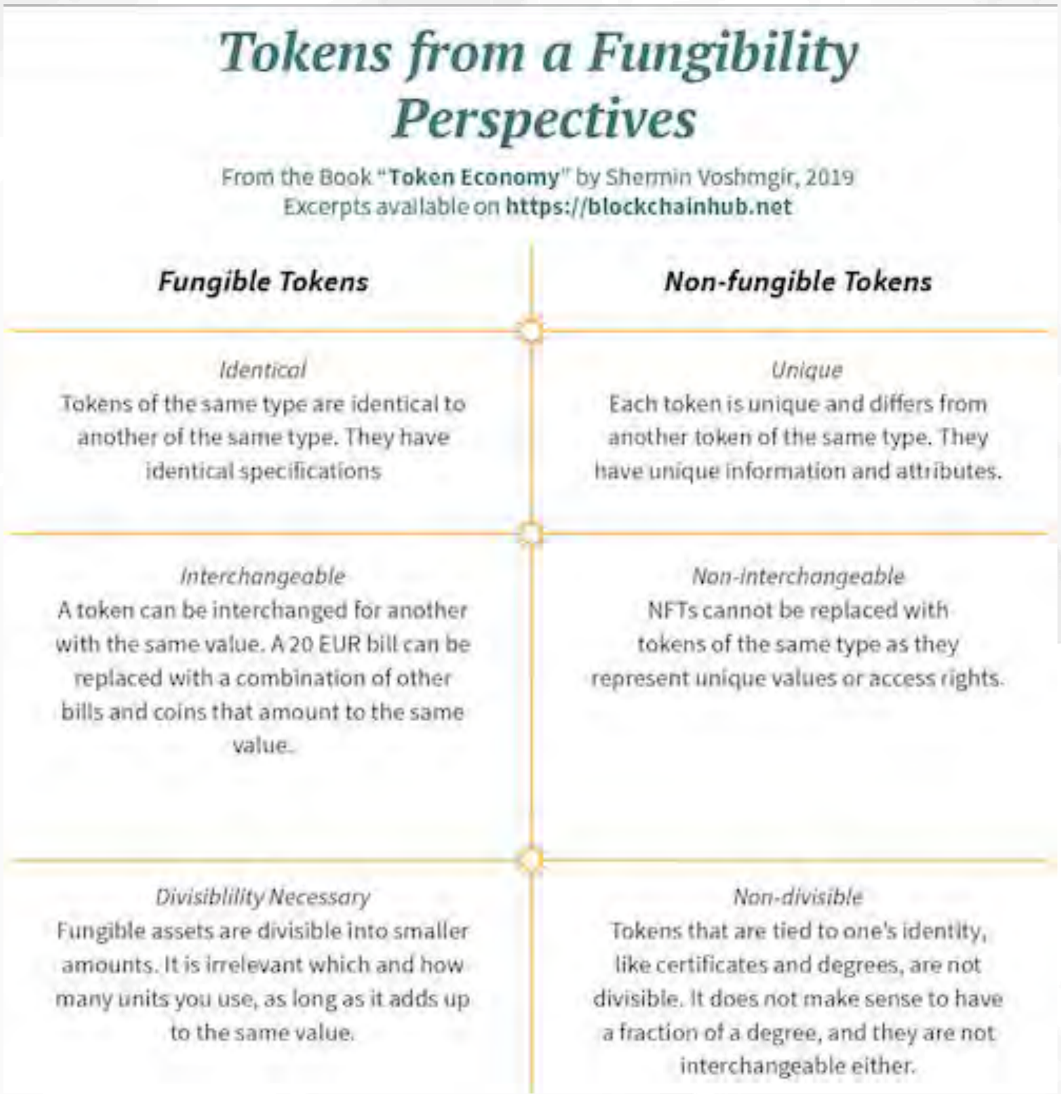
As mentioned in the section above, The National Institute for Standards and Technology, or NIST, is making numerous strides on this front including hosting competitions to ensure there is adequate competition in creating quantum algorithms and cybersecurity protocols. For this reason, it is normal to be skeptical of the threat quantum computing may pose, however, the threats may be overstated. As quantum computers cannot and will most likely not be ready for use by many enterprises outside of governments and large tech companies, the potential for a threat to destroy an entire industry with so much promise as blockchain has, is slim. NIST, along with the likes of IBM, Microsoft, and more, are focused on creating a quantum safe environment, which would do well to put concerns to rest that there is a major threat to blockchain posed by quantum computing.

Tokens & NFT's

Tokens are assets that can be transferred between two people or enterprises and reside on a blockchain. Coins and tokens are often discussed interchangeably but they are not the same. Coins represent the digital version equivalent of real-life money. Examples of coins include Bitcoin, Bitcoin Cash, Litecoin, Ethereum, NEO, Dogecoin, and many, many, more. Ethereum is the most common token on a blockchain platform, and its tokens are known as ERC-20. Tokens are to be used on decentralized applications rather than for peer-to-peer payments. That is the key difference between tokens and coins. NEP-5, WPR, and BNB are additional examples of tokens.

Tokens can be either fungible or non-fungible. Characteristics for fungible tokens include being identical, interchangeable, and divisible. Nonfungible tokens are the exact opposite of fungible and thus are unique, noninterchangeable, and indivisible. Figure 1.8 details a breakout of tokens from a fungibility perspective. Tracking balances and making payments are the major use cases for fungible tokens. Thus, in essence, fungible tokens represent normal day-to-day transactions.

Non-fungible tokens, often referred to as NFT's, represent ownership in its entirety. For example, a NFT could represent a real estate mortgage, a business, or video game.



Tokens from a Fungibility Perspectives

From the Book "**Token Economy**" by Shermin Voshmgir, 2019
Excerpts available on **https://blockchainhub.net**

Fungible Tokens	***Non-fungible Tokens***
Identical Tokens of the same type are identical to another of the same type. They have identical specifications	*Unique* Each token is unique and differs from another token of the same type. They have unique information and attributes.
Interchangeable A token can be interchanged for another with the same value. A 20 EUR bill can be replaced with a combination of other bills and coins that amount to the same value.	*Non-interchangeable* NFTs cannot be replaced with tokens of the same type as they represent unique values or access rights.
Divisiblility Necessary Fungible assets are divisible into smaller amounts. It is irrelevant which and how many units you use, as long as it adds up to the same value.	*Non-divisible* Tokens that are tied to one's identity, like certificates and degrees, are not divisible. It does not make sense to have a fraction of a degree, and they are not interchangeable either.

Figure 1.8
Source: Blockchain Hub

Additionally, there are utility and security tokens. A descriptive breakout appears in figure 1.9 regarding these two types of tokens. In short, utility tokens are tokens that help achieve an objective whereas a security token shows ownership of the digital assets. Utility tokens are typically provided via an ICO or initial coin offering. Security tokens are token that can be traded. In the modern world, security tokens are similar to securities. They can be traded, owned, etc. In order for a token to be a security token, it must pass the Howey test. The Howey test references the SEC v W.J. Howey Co supreme court case. The result of this case set the standards for what is deemed an investment contract and would require disclosure to the SEC and subject to any and all investing regulations.

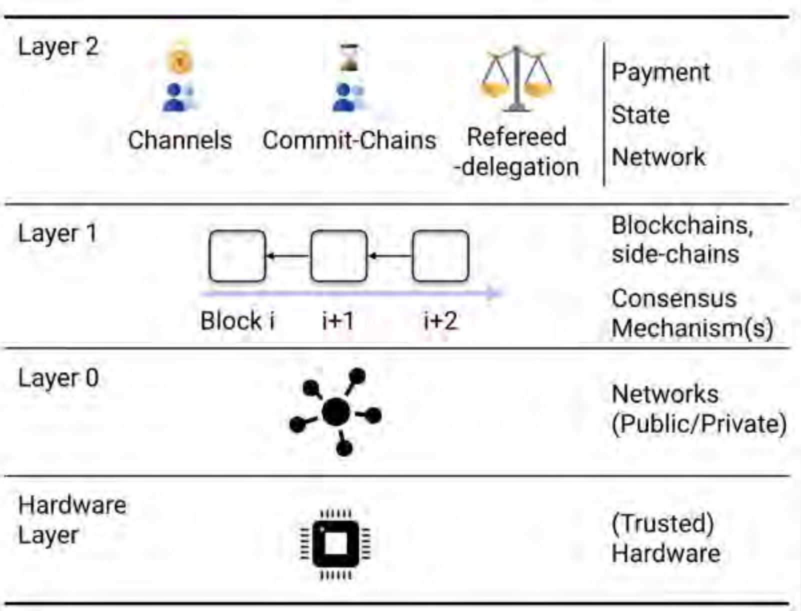
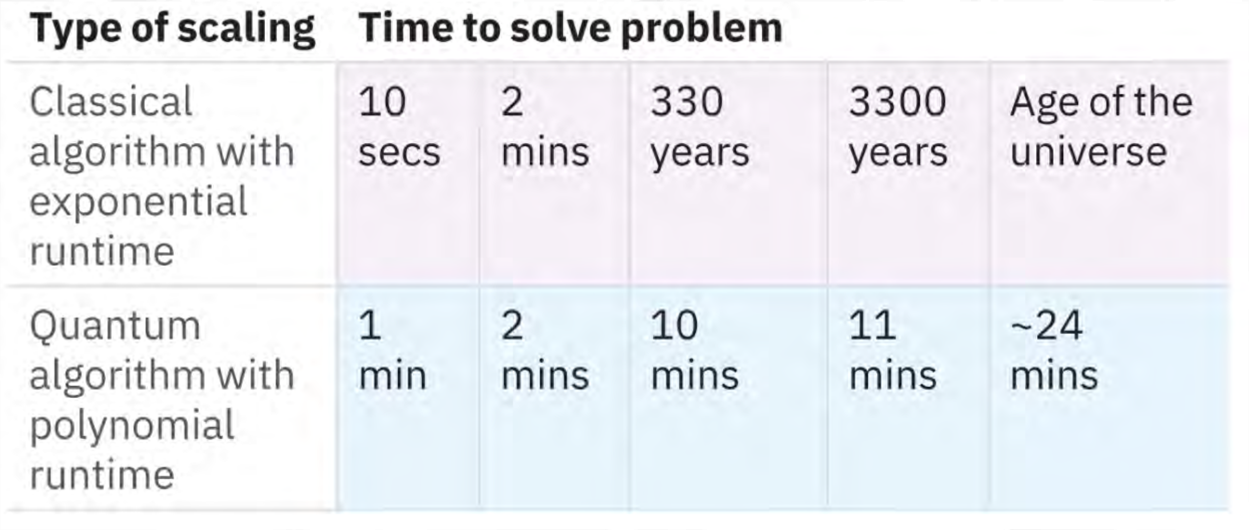


Figure: 2.0
Source: Springer

Possibilities with Quantum Blockchain

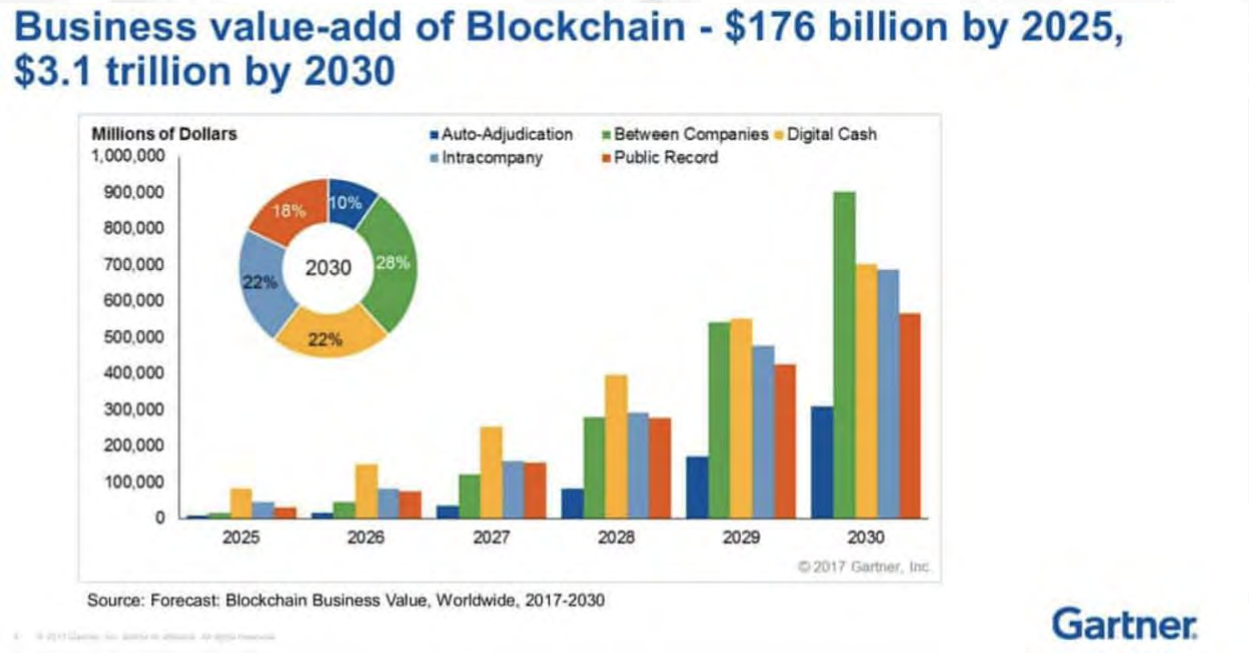
The quantum future offers enormous opportunities across multiple verticals, with billion- and trillion-dollar forecasts. As more businesses become aware of the potential impact of quantum technology, they are developing use cases that are critical for accurate application. Along with business use cases, there is also a design component. Quantum technology is opening more doors than any other technology has ever done, from user design to implementation. The effects can be felt in a variety of industries, including gaming, insurance, medical and pharmaceutical research, and even social policy and politics. Quantum technology combined with blockchain technology enables unprecedented levels of transparency and power.



Type of scaling	Time to solve problem				
Classical algorithm with exponential runtime	10 secs	2 mins	330 years	3300 years	Age of the universe
Quantum algorithm with polynomial runtime	1 min	2 mins	10 mins	11 mins	~24 mins

Figure 2.1
Source: IBM

According to a report by Gartner, blockchain alone will add $176 billion worth of value to enterprises and businesses alone by 2025. This doesn't factor in the potential impact to individual consumers on a peer-to-peer basis. The same report concludes that by 2030, that figure will grow to $3.1 trillion. Blockchain alone has tremendous value without factoring in any quantum component. Blockchain is largely thought of in combination with Bitcoin or other distributed ledger transactions. Blockchain has much more to offer than just a standalone DLT. Gartner identifies that as only 22% of blockchain will be leveraged for digital currency. That comes in tied for second along with intracompany utilization. The number one spot for utilization of blockchain is actually between companies. This could include procurement, financial transactions, managed services, contractual agreements and modifications, among many other processes.



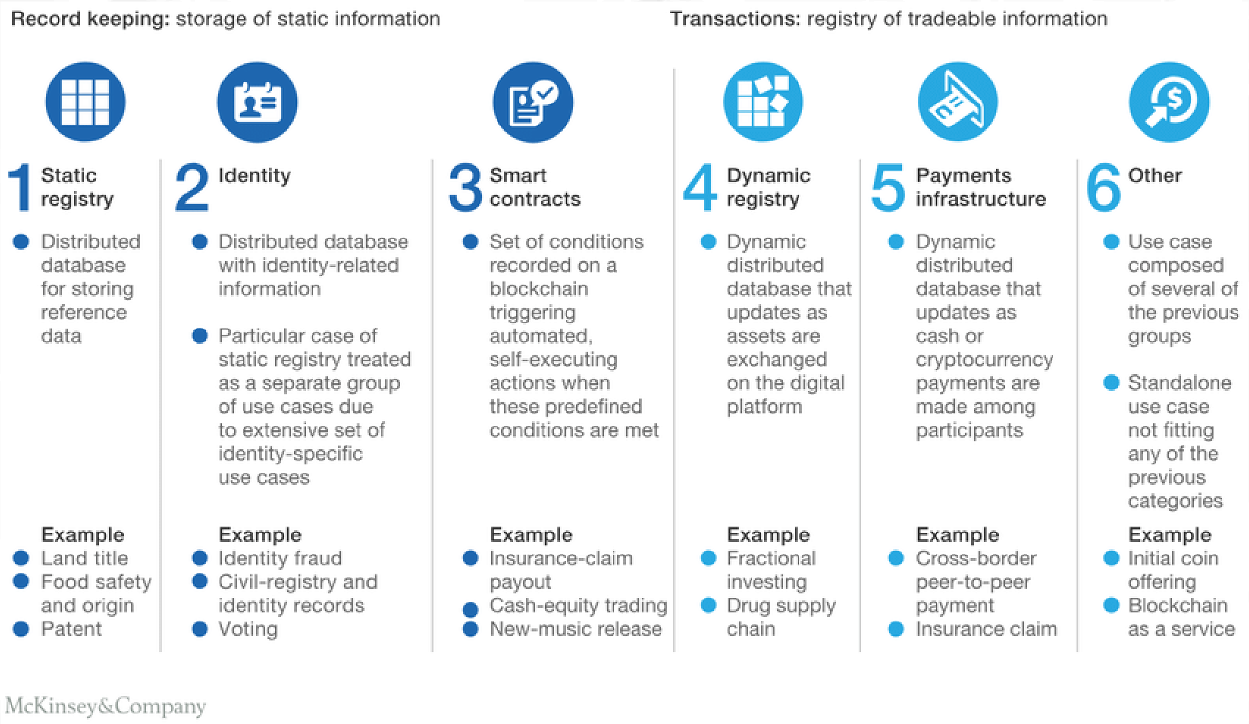
Business value-add of Blockchain - $176 billion by 2025, $3.1 trillion by 2030

Source: Forecast: Blockchain Business Value, Worldwide, 2017-2030

Figure 2.2
Source: Gartner

We’ve already begun to see the impact of quantum technology on the gaming industry. IBM for example create a limited Minecraft game. While this was limited in nature and the controlled variation was restricted to the terrain, the elements impacted appeared more natural and were ultimately more visually appealing. In the future, quantum computers will leverage the ability to create parts of games. Whereas critics are concerned this could lead to maps, games, and quests that are unsolvable; a quantum computer could actually browse and transverse a number of configurations selecting only the ones that are solvable and choosing from that subset to reveal to the player. As of early 2020, IBM has committed to partner with commercial game studios in an attempt to build out quantum games. All this comes with the caveat that ancillary quantum technology must be in place in order to supplement the games being made in order for a full quantum experience. This could potentially mean that we are at least a decade or so away of actually being able to play quantum games in full experience.

Blockchain is most effective in two scenarios: record keeping and transaction registration.



Record keeping: storage of static information

Transactions: registry of tradeable information

1 Static registry

- Distributed database for storing reference data

Example
- Land title
- Food safety and origin
- Patent

2 Identity

- Distributed database with identity-related information
- Particular case of static registry treated as a separate group of use cases due to extensive set of identity-specific use cases

Example
- Identity fraud
- Civil-registry and identity records
- Voting

3 Smart contracts

- Set of conditions recorded on a blockchain triggering automated, self-executing actions when these predefined conditions are met

Example
- Insurance-claim payout
- Cash-equity trading
- New-music release

4 Dynamic registry

- Dynamic distributed database that updates as assets are exchanged on the digital platform

Example
- Fractional investing
- Drug supply chain

5 Payments infrastructure

- Dynamic distributed database that updates as cash or cryptocurrency payments are made among participants

Example
- Cross-border peer-to-peer payment
- Insurance claim

6 Other

- Use case composed of several of the previous groups
- Standalone use case not fitting any of the previous categories

Example
- Initial coin offering
- Blockchain as a service

McKinsey&Company

Figure 2.3
Source: McKinsey & Company

With regard to record keeping, blockchain has many use cases. Whether it be for data validation, a static registry, or implementing executable actions based of preconditioned requirements, blockchains have numerous impacts across many industries. For example, patent disputes could be settled by who truly filed first based on the forced timestamped protocol within the blockchain technology rather than relying on a potentially biased patent approver which could side with an established enterprise rather than to a startup.

As the recent 2020 election was ripe with accusations of voter fraud, election interference, and other potential influences on the outcome, voting is a major opportunity for blockchain. No matter the side you’re on politically, the 2020 election had a number of accusations and potential influences. A simple solution to remove any and all theoretical fraud accusations would be to implement a blockchain voting record structure. A quantum blockchain voting structure would be even more secure and also lead to quicker results, processing, and transparency.

As health insurance becomes increasingly important and a topic that spans across ethical, political, and societal landscapes, quantum blockchain has an opportunity to change the outlook in a major way. Claim processing would be sped up dramatically as a result of implementing quantum technology. While there would be a large cost to implementing such technologies, the processing speed alone would offset those costs. This ultimately opens an opportunity to lower the total cost for healthcare and enhance operational efficiency.

Smart contracts are a component that potentially has the broadest application base. This could be applied across housing contracts, business-to-business contracts, financial contracts, and many others. This could include automated process transitioning, reporting, and payments. On the quantum level, this could lead to same day turnarounds rather than transactions taking days or weeks to accomplish.

Transparency has always been lacking when it comes the prescription drug industry. Quantum blockchain has a major disruption opportunity here where it can increase the speed of clinical reviews, FDA approvals, while at the same time, increasing the efficiency of the drug trials involved.

We've seen a number of "AAS" variations within the software industry. This could be platform as a service, software as a service, contact center as a service, and number of others. One of the next advancements in this evolution could be Blockchain as a service. Blockchain as a service could upend and disrupt a number of industries as its foundations are applicable to nearly every industry.

Post Quantum World

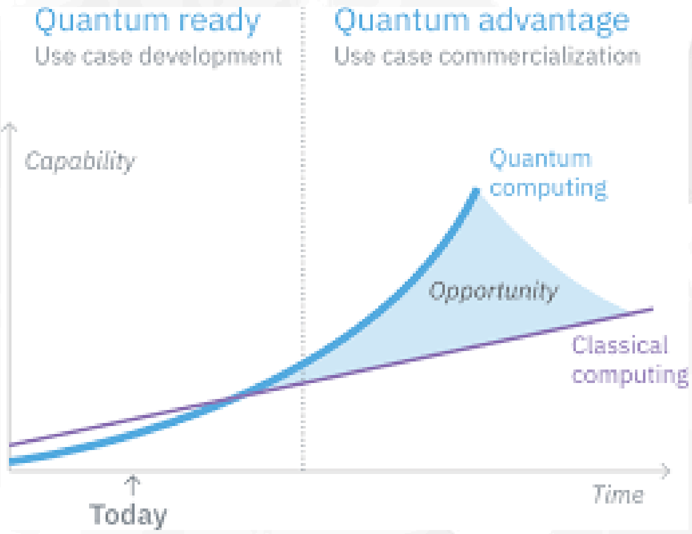
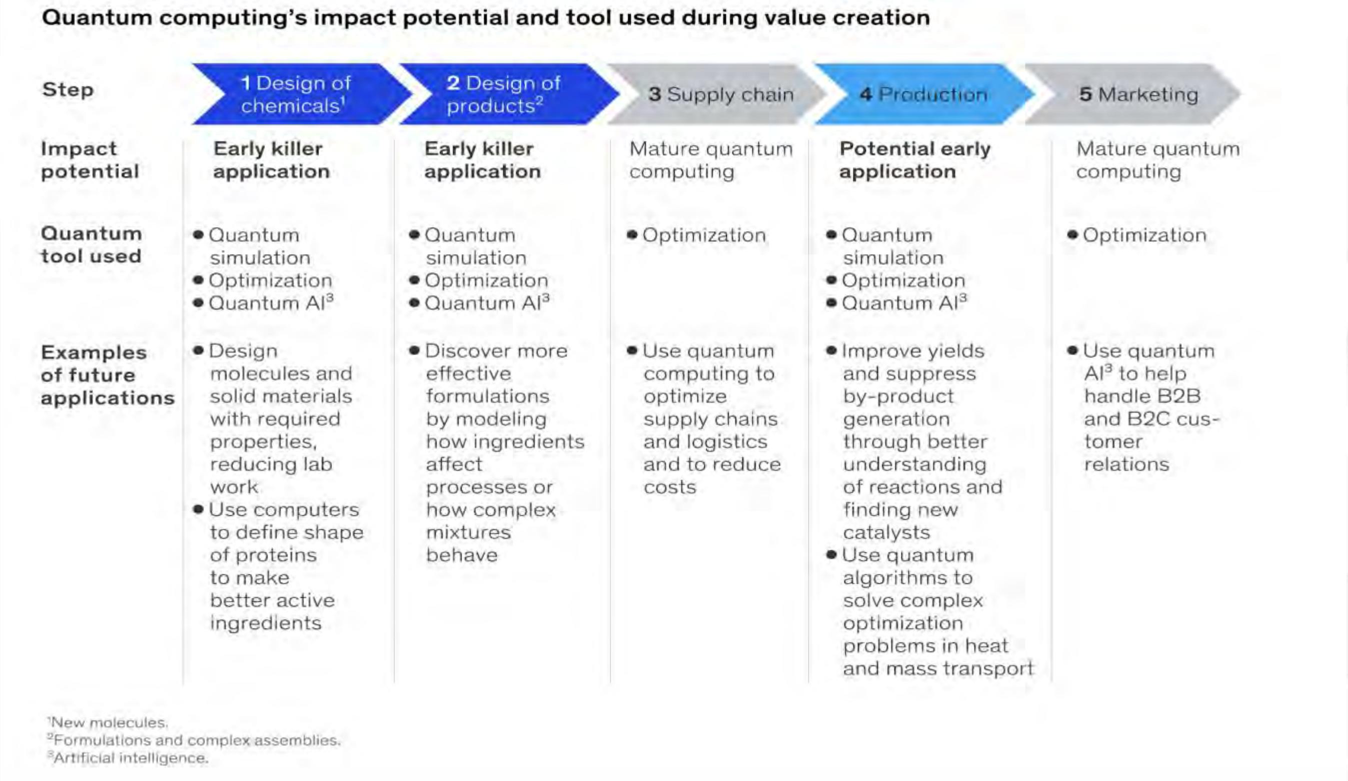


Figure 2.4
Source: IBM

As illustrated in figure 2.4, we've got a long way to go before quantum development takes off. However, when it comes to a post quantum technological advanced world, the number one concern is regarding security. Secondly, the vast business opportunities and technological enhancements are already being examined.

Privacy and security are constant topics at the forefront of societal issues. As most individuals don't understand the risk of their personal information with today's classical computers, most will be lost when it comes the risks quantum technologies pose. As a result, more than ever before, individuals and companies will be reliant on cyber security companies to ensure they are quantum compliant and protected from quantum hacking attempts.

Earlier in the whitepaper, we discussed the numerous use cases enabled by blockchain. In this section, we will examine the parallel opportunities presented by quantum advancements, with or without blockchain. Quantum computing will have an impact on both the B2B and B2C markets. The cumulative effect of design, prototyping, marketing, and customer experience or feedback will be felt. The time to market will be significantly accelerated, as will the ability to detect red flags in prescription drugs, medical treatments, and other highly regulated industries. Ultimately, this could result in increased surgical success rates, medical treatment success rates, and personnel selection success rates, among other outcomes. Once unlocked, quantum computational power has the potential to significantly advance science and enable the development of new innovations and technologies. These could include new medicines, novel chemical components, and other highly lucrative specialized fields that appear to have reached a stalemate and require the astronomical computing power provided by quantum computing to advance further.



Quantum computing's impact potential and tool used during value creation

Step	1 Design of chemicals[1]	2 Design of products[2]	3 Supply chain	4 Production	5 Marketing
Impact potential	Early killer application	Early killer application	Mature quantum computing	Potential early application	Mature quantum computing
Quantum tool used	• Quantum simulation • Optimization • Quantum AI[3]	• Quantum simulation • Optimization • Quantum AI[3]	• Optimization	• Quantum simulation • Optimization • Quantum AI[3]	• Optimization
Examples of future applications	• Design molecules and solid materials with required properties, reducing lab work • Use computers to define shape of proteins to make better active ingredients	• Discover more effective formulations by modeling how ingredients affect processes or how complex mixtures behave	• Use quantum computing to optimize supply chains and logistics and to reduce costs	• Improve yields and suppress by-product generation through better understanding of reactions and finding new catalysts • Use quantum algorithms to solve complex optimization problems in heat and mass transport	• Use quantum AI[3] to help handle B2B and B2C customer relations

[1] New molecules.
[2] Formulations and complex assemblies.
[3] Artificial intelligence.

Figure 2.5
Source: AI Multiple

We'll keep adding and improving roadmap events. Any suggestions made by the community will be considered. Almost certainly, the events listed below will not occur in the order listed. While certain events may occur sooner or later, it is our intention to expand and advance the project at a rapid pace while meeting key performance indicators.

Q2 2021
- Finalize website
- Finalize whitepaper
- Begin marketing campaign
- Devise legal strategy for launch
- Grow and Assign Specialized Team Roles
- Collect Data on Holdings of Previous USDex Holders
- Initiate Token Swap
- Expand Social Media Channels and Networking
- Initiate ICO private sale
- Binance smart chain integration

Q3 2021
- Initiate IFO/ICO sale
- Pancakeswap exchange, pools, and farming listings.
- Trust wallet listing.
- Tracking platform listings; CMC, Coingecko, blockfolio, etc.
- Partnerships with at least 5 content creators, influencers, and other crypto communities.
- Expand the team. Hire more developers, marketers, social media moderators, researchers, ambassadors, and legal support.
- Top 50 exchange listing.
- Team and holders vesting schedule releases.

Q4 2021
- AMA videos concluding Q3 & Q4 review, accomplishments, and what lies next for Q1 & Q2.
- Top 20 exchange listing.
- Establish partnerships with content creators, influencers, and other crypto communities.
- Continue expanding the team to at least 10.
- AMA videos with the team.
- Release new products, use cases.
- Vesting schedule releases for holders and team.
- End of year review and accomplishments.

Q1 2022
- Begin development on the premium de-fi learning platform.
- Mobile app development
- Establish quantum research facility
- Travel the world to attend conferences, meetings, crypto events. Attend quantum physics/computer events with scientists and policy makers.

Conclusion

The future of blockchain technology is extremely bright over the next decade. In today's business and cryptocurrency environments, there are virtually no threats to blockchain. Algorithms such as Grover's and Shor's have the potential to expose attacks if a quantum computer is commercially developed and used before quantum safe cryptography methods are implemented. While this may seem like a long way off, quantum computing is expected to achieve these capabilities by the mid-2020s. As a result, NIST, Google, Microsoft, IBM, and a variety of other organizations and companies are rapidly developing new encryption and decryption techniques to ensure security in the quantum and post-quantum worlds. Blockchain will continue to thrive in a post-quantum world. As computing power increases, the scale and scope of possible blockchain use cases expands. As a result, the advent of quantum computing does not pose a threat, but rather a massive opportunity. USX will seize these opportunities by leveraging its expertise, scale, and an infrastructure optimized for both classical and quantum environments.

References

Nakamoto, S., 2012. Bitcoin: A Peer-to-Peer Electronic Cash System. [online] Mitre.org. Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 4 May 2021].

Accenture, 2021. CRYPTOGRAPHY IN A POSTQUANTUM WORLD. [online] Available at: <https://www.accenture.com/_acnmedia/PDF-87/Accenture-809668-Quantum-Cryptography-Whitepaper-v05.pdf> [Accessed 4 May 2021].

Post-Quantum SSH. (2019, August 06). Retrieved from https://www.microsoft.com/en-us/research/project/post-quantum-ssh/

Shor's algorithm. (n.d.). Retrieved from https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm

Tillman, I., 2020. Shor's Algorithm. [online] Mitre.org. Available at: <https://wp.optics.arizona.edu/opti646/wp-content/uploads/sites/55/2020/12/OPTI_646_Final_Paper_Ian_Tillman.pdf> [Accessed 4 May 2021].

Sprenkels, D., 2021. Grover's Algortihm. [online] Available at: <https://dsprenkels.com/files/grover.pdf> [Accessed 4 May 2021].

Thakkar, J. (2020, August 31). ECDSA vs RSA: Everything You Need to Know. Retrieved from https://sectigostore.com/blog/ecdsa-vs-rsa-everything-you-need-to-know/

Pazima. (2020, June 24). Security vs. Utility Tokens: The Complete Guide. Retrieved from https://cryptopotato.com/security-vs-utility-tokens-the-complete-guide/

Evolution of Quantum Computing Based on Grover's Search Algorithm. (n.d.). Retrieved from https://ieeexplore.ieee.org/document/8944676

Gudgeon, L., 2020. SoK: Layer-Two Blockchain Protocols. [online] Available at: <https://link.springer.com/chapter/10.1007/978-3-030-51280-4_12> [Accessed 4 May 2021].

Clyde, R., & Gillis, A. S. (2021, January 06). What is Post-Quantum Cryptography? Retrieved from https://searchsecurity.techtarget.com/definition/post-quantum-cryptography

The realist's guide to quantum technology and national security. (n.d.). Retrieved from https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html

Rodenburg, B. and Pappas, S., 2017. Blockchain and Quantum Computing. [online] Mitre.org. Available at: <https://www.mitre.org/sites/default/files/publications/17-4039-blockchain-and-quantum-computing.pdf> [Accessed 4 May 2021].

Biswas, P. (2019, October 20). Grokking Quantum Computing - A Quirky Guide for Curious People. Retrieved from https://towardsdatascience.com/grokking-quantum-computing-a-quirky-guide-for-curious-people-8cea6eb67803

What is a Fungible Token? What is a Non-Fungible Token? (2020, December 10). Retrieved from https://blockchainhub.net/blog/blog/nfts-fungible-tokens-vs-non-fungible-tokens/

Borbely, E., 2021. Grover's Search Algorithm. [online] Arxiv.org. Available at: <https://arxiv.org/pdf/0705.4171.pdf> [Accessed 1 May 2021].

Blockchain. (n.d.). Retrieved from https://www.nist.gov/image/blockchain

Takeda, S., 2019. An Introduction To Quantum Computing. [ebook] Available at: <https://conf.compsci-alliance.jp/wp-content/uploads/recs2019/Takeda-Tutorial2019.pdf> [Accessed 4 May 2021].

Richard J. Lipton; Kenneth W. Regan, "Shor's Algorithm," in Quantum Algorithms via Linear Algebra: A Primer , MIT Press, 2014, pp.97-108.

Bobko, D. C. (2019, February 04). AES Encryption: Everything you need to know about AES. Retrieved from https://proprivacy.com/guides/aes-encryption

Quantum computing is coming to your business. (n.d.). Retrieved from https://www.ibm.com/thought-leadership/institute-business-value/report/quantumstrategy

Dilmegani, C. (2021, April 08). Top 20 Quantum Computing Applications / Use Cases in 2021. Retrieved from https://research.aimultiple.com/quantum-computing-applications/

FAQ

USX Quantum: PLANS & DEVELOPMENT FAQ

1. What is USX Quantum?

A: The USX quantum project is an evolution of the unified society platform, working towards creating the first quantum computer encrypted blockchains that will greatly benefit the entirety of existing and future blockchains. We aim towards creating our own quantum computers that will be used for the main-interest of the blockchain industry. We are a community driven project with our main priority being

2. What is the Purpose of an ICO and Creating the USX Quantum Token?

A: We are creating the USX Quantum token on the Binance-Smart-Chain to sell shares, to set up staking, be able to receive fundings for the project, and to create a liquidity pool. The ICO will raise funds for research and the creation of the quantum blockchain. Our project will require a substantial amount of capital, as it requires a large infrastructure and a dedicated team of researchers, developers, and community members working together. The USX Quantum token will evolve to be a virtual currency on a quantum-based network.

3. Who will Benefit from USX Quantum?

A: Our project is dedicated to the creation of a quantum block chain through the application of quantum physics. This will benefit all cryptocurrency projects and every community member. We are devoted to protecting the community from the potential threat that quantum computing poses to cryptocurrencies.

4. What Does USX Quantum Aim to Achieve/Develop?

A: Quantum computers. New quantum-based encryption and algorithms. A large community driven project in which everyone will be able to contribute towards the same goals. We aim to create partnerships with: researchers, developers, investors, cryptocurrencies projects, and just about anyone who has an interest in the project.

5. How does USX Quantum Plan to Achieve These Goals?

A: Lots of hard work and very complex research and development. Having wonderful humans proving great contributions to the project. Establishing partnerships with: researchers, developers, investors, other projects, companies, and just about anyone who will bring great contribution.

6. What is the Timeline for USX Quantum to Reach These Goals?

A: Our main goals at the moment are to create the company and accumulate investors, We will then hire researchers and engineers to design and create the quantum computer, enabling us to begin the creation of quantum blockchains. The roadmap on the whitepaper explains further in detail about the timeline.

7. What Are the Plans for Obtaining the Infrastructure Needed to Develop the Technology?

A: The start of the plan is to have a successful ICO that will enable us to receive fundings. We will work towards obtaining long-term investors that are primarily interested in the development and creation of the technology. We will focus heavily on marketing, allowing us to reach out to various audiences and potential investors throughout the entire world. We will aim towards creating partnerships with companies that have the existing infrastructure and technology and are in the process of developing the technology. While our main goal is to create our own quantum computer, we must cooperate and partner with others that will provide us with the opportunities.

8. Are Quantum Computers a Threat to Block-Chains?

A: Because quantum computers will have an astronomical amount of computational power in contrast to classical computers, they will have the capabilities and advantages to decode modern encryption. Quantum computers will pose a threat to blockchains in the future, USX Quantum will not only be quantum proof, it will be created and enhanced by a quantum computer.

9. How Will USX Quantum "protect and secure" existing block-chains from the potential threats of quantum computers?

A: We will introduce a new cryptographic hash function in which modern block-chains will be able to transition to a quantum blockchain, which will be quantum proof.

10. What Technology Will USX Quantum Develop to Reach Our Goals?

A: Quantum computers that will enable us to develop new encryption algorithms allowing us to secure and create the future of blockchains.

11. Who Will be Able to Contribute to the Project?

A: USX Quantum is a community driven endeavor. Everyone will be allowed to contribute. Our team will review submitted code changes and additions for approval.

12a. The technology of quantum computers will affect the entirety of modern encryption. Companies, governments, organizations will surely find new encryption methods to secure modern data. Should we really be worried knowing that these large entities will also be working on methods to secure modern encryption?

Aa: Not at all, There is nothing better than getting in a space early before everyone and getting a head start. Competition is what creates innovation. As for their intentions in regards to cryptocurrencies, we never know what they might be.

12b: These entities will most-likely be working on securing bitcoin and other block-chains. Should we really consider working/investing on USX knowing that other large entities will most-likely be working on the same area?

Ab: Our project isn't just dedicated to protecting against a quantum computer. Our blockchains will be designed to use quantum computers to enhance the speed and encryption of blockchains. You can consider it the next evolution. We have the interest to protect all existing blockchains, not just our own. We never know the intentions of large entities, whether they will aim to take over blockchains or just focus on securing specific ones. Therefore it's important to have a variety of options that are working for the best-interest of the entire cryptocurrencies communities and not just for their interest. We happen to be the ones that want to primarily do this for the entire community!

13: What is the Previous History of USX (Since 2013)?

USDE was created in 2013. The original creator got into an accident and allowed us to take over the project in 2017.

14: Why Was USX Unable to Previously Succeed?

After we took over USDE from the previous creator, we raised capital through an initial coin offering, allowing us to drastically improve the blockchain. Our ICO was small and sold out extremely fast. The capital was quickly exhausted to pay for marketing and exchange listings. Just months after the successful ICO, the entire cryptocurrency market entered a decline that would last for multiple quarters. The decline of the entire market led to hundreds of projects to die off, exit scam, and sell out. USX has remained loyal to the entire community throughout these years. Now we are venturing into the quantum era, with new team members, new capital, and a new passion for the future. We definitely see ourselves succeeding.

15: Why Did USX Decide to Work on Quantum Blockchains?

Quantum blockchains are the future of blockchain technology. Our team loves quantum physics and is excited about the potential of developing quantum enhanced blockchains. We believe that quantum computing and encryption will completely change the way we explore the virtual world. All modern encryption will require adjustments to be able to intertwine along quantum computing. Quantum computing will be a double-edge sword and we must be able to wield it properly.

16: What Are the Plans for Marketing?

Prior to the ICO launch, we have already been in contact with: communities, investors, developers, researchers, content creators, influencers, quantum physicists, and just about anyone that is interested in contributing to the project. Partnerships will soon be established. We have already secured a substantial amount of capital that will enable us to advance forward in our marketing and advertising investments.

17: Are There Plans To Expand the Community Internationally?

We have always been working on expanding the community internationally since day one. We will continue to expand the community, allowing us to reach investors, members, and anyone that wants to make a contribution. Communication is a priority for us. We will be having different ambassador roles for many languages that will provide support and growth to our international community.

18: Will USX Quantum be Working With Lawyers to Ensure Compliance?

We have audits planned for all coded projects and are working with legal teams to make sure everything is done correctly. We'll assure our community that there will be no legal obstacles on our journey.

19**: What Strategies Will USX Quantum be Implementing to Ensure the Investors are Secure in a Volatile Market?**

Strict vesting schedules have been implemented along with ICO funds being dedicated to running the project without interruptions. Our main priority is to focus heavily on building/maintaining a strong capital reserve that will allow us to operate freely in any market condition. We will focus on implementing different methods that will allow us to generate revenue. Creating long-term partnerships with researchers, developers, investors, and other communities will strengthen our community.