THE BLOCKCHAIN FOR THE POST-QUANTUM ERA

Krzysztof Urbanowicz

SUMMARY

Current blockchain technologies rely on a decentralized network of block producers, such as miners in Proof-of-Work systems like Bitcoin or validators in Proof-of-Stake networks like Cardano and Ethereum 2.0. The security of these networks is based on conventional asymmetric encryption which are based on challenges and mathematical assurances that cannot be solved easily by conventional computers. However, these protections are known to be susceptible to quantum computing algorithms. This paper presents a blockchain framework that is immune to quantum computing and related attack methods that may threaten existing blockchains in the near future. We propose a dual blockchain structure that utilizes a cryptographic standard resistant to even the most advanced quantum computers, offering a future-proof network that is compatible with existing technologies. This includes a PQC blockchain network, decentralized price and verifiable random number oracles, as well as a quantum-resistant and EVM-compatible smart contract platform.

1. INTRODUCTION

In some number of years, quantum computing will pose a legitimate security threat to contemporary blockchains. Asymmetric cryptography, which is the most commonly used encryption standard in today's blockchains, will be susceptible to attack due to the superior computational power of quantum computing. It is commonly known that a quantum computer with a sufficient number of qubits could theoretically break public-key cryptography schemes using Shor's Algorithm. While there has previously been debate as to whether a quantum computer could be built that would be both powerful enough and stable enough to perform this task, a growing number of scientists and engineers now believe that this is no longer a question of if, but when. Some experts argue that within the next ten to fifteen years, quantum computers will be built that will be capable of breaking all public-key schemes currently in use. It has taken almost two decades to deploy and normalize modern public-key cryptography, and whether or not we can accurately estimate the exact date of the arrival of the quantum computing era — it is clear that we must act now to prepare our infrastructure and information security systems to be able to resist all kinds of upcoming technologies and future threats. In particular, the existential threats quantum computing poses to the cryptographic schemes we rely on in our digital and financial infrastructure today.

2. DEFINITIONS & PREVIOUS WORK

These threats to the blockchain and cryptocurrency ecosystem have inspired us to develop the PQC Blockchain, which leverages a cryptographic standard that will be resistant to even the most powerful quantum computers. In the process, we have solved the issues that have plagued early pioneers of quantum-resistant blockchain technology. One of the main characteristics of PQC (Post-Quantum Cryptography) cryptosystems is the need for large public keys and signatures. This can affect the ability to scale within the context of a blockchain due to the significant data storage overhead. This Blockchain removes that overhead on a single chain: a public key is carried inside a transaction only once, on an account's first transaction, which registers it on-chain. Every subsequent transaction from that account omits the key and carries only a signature. The chain therefore stays PQC compliant while sustaining transaction throughput comparable to contemporary blockchains. The Blockchain also leverages a proprietary consensus model called Proof-of-Synergy which combines the best features of Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-Authority (PoA). This means that in addition to being resistant to attacks from quantum

computers, the Blockchain will be environmentally friendly, resistant to DDoS attacks, and decentralized with a high transaction throughput rate. The Blockchain is primarily driven by the native payments and governance token, Native Coin, which is used as gas for network transactions, and as a financial incentive to participate in block validation.

2.1. The Network Components & Characteristics

- PQC (**Post-Quantum Cryptography**) is achieved on the Blockchain with the at least claimed as NIST-1 cryptographic standard, to ensure resistance to attack by quantum computers.
- **Future-Proof Security:** Dual-Layer Encryption with Dynamic Voting Mechanism, enabling swift pause and seamless upgrade of compromised cryptographic protocols.
- Proprietary consensus model **Proof-of-Synergy**, which is decentralized and energy-efficient, while preventing malicious actors from harming and destabilizing the Blockchain.
- The Blockchain is **EVM-compatible**, Turing-complete smart contract platform. Existing smart contracts can be migrated from other chains to leverage security benefits.
- **Escrow account** with delayed transactions, so manager of account has possibility to validate outgoing transactions and, in the case of fraud, cancel it.
- **Multi-signature account**, when more owners are possible, which can manage the account in the way defined when the account was created.
- Swapping tokens inbuild into the protocol. The **token swap** inbuild in protocol instead of being created on the level of EVM-engine.
- **Deflationary total supply** of asset and gas token, the Native Coin, with the number of new coins minted as validator rewards diminishing over time on a fixed schedule.
- **Decentralized oracles** for the coin price and verifiable random numbers, helping DeFi and GameFi applications reduce costs, add new features, improve security, and increase service reliability.

2.2. Existing Blockchain Networks

- **QRL**: Fully integrated PQC blockchain based on XMSS cryptography. Proof-of-Work consensus model. Average block interval of 1 minute. Problems with scaling and low transaction throughput (~10-12.5 TPS). Standardization of XMSS by NIST is due to happen in the near future. [2]
- **IOTA**: Hashgraph/tangle type of blockchain. Not a full PQC blockchain, quantum computers pose a moderate threat. In January 2018, the IOTA blockchain was hacked, resulting in losses of 11 Million USD. [3]
- **Monero**: Hidden public keys. Moderate threat from quantum computers.
- **Beam**: Hash-based cryptography used. Moderate threat from quantum computers.
- **Bitcoin**: The most popular cryptocurrency based on market capitalization. Proof-of-Work. Average block interval of 10 minutes. High threat from quantum computers.
- **Ethereum**: Second largest cryptocurrency based on market capitalization. Distributed virtual machine for smart contracts. PoW - layer 1, PoS - layer 2. Block interval is 14 seconds on average. 14-16 TPS. High threat from quantum computers.
- **Solana**: The blockchain with the largest throughput among blockchains. Proof-of-Authority. Smart contract functionality. Sensitive to DDOS attacks. In January 2022, Solana was halted for 4 hours due to network issues. [4] In June 2022, Solana was halted again to correct a bug that threatened consensus on the network. [5] High threat from quantum computers.

Below, we evaluate the architecture and consensus models of existing chains in comparison to an extended version of the well-known blockchain trilemma, and explore the trade-offs in features and functionality each carries to the underlying protocol.

Decentralization:

1. Private nodes
2. Proof of Authority
3. Public, but limited number of nodes
4. Public, but practically limited to large servers
5. Public, no limitations of nodes

Stability:

1. Proof of Authority
2. Delegated Proof of Stake with limited nodes
3. Proof of Stake with unlimited nodes
4. Proof of Stake with DDOS protection
5. Proof of Work, unlimited nodes

Security:

1. Standard encryption
2. Hidden public keys
3. Hash-based cryptography
4. PQC approved by NIST
5. PQC + changeable PQC encryption layer

Throughput:

1. TPS > 1
2. TPS > 10
3. TPS > 100
4. TPS > 1k
5. TPS > 10k

Utility features:

1. Only currency function
2. Possible to create new tokens
3. Smart contracts
4. Smart contract + feeless oracles
5. Smart contract + inbuild bridging to other blockchains

Env. friendly:

1. High energy consumption
2. Hardware intensive
3. Proof of Stake
4. Proof of Stake with limited nodes
5. Proof of Authority

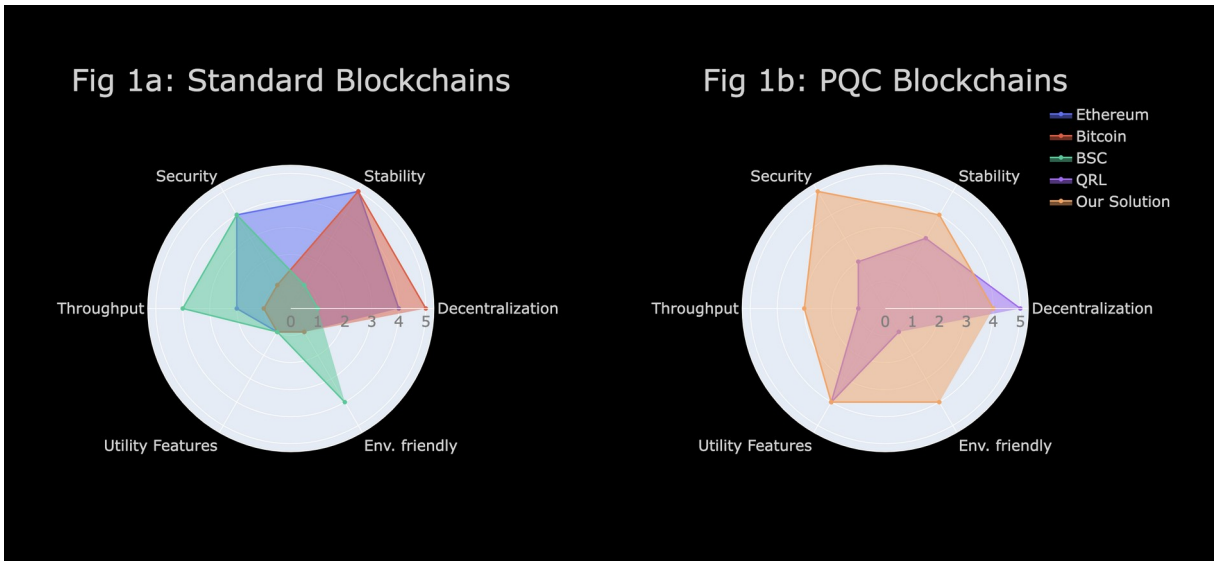

Figure 1. The most important properties of contemporary blockchains, and how their respective consensus models and architecture affect performance and functionality.

Attribute	Ethereum (PoW)	Ethereum (PoS)**	Solana	Cosmos	Avalanche	Cardano	Our Solution
Highly Decentralized	Yes	Yes	No	No	No	Yes	No
Robust against DDoS attacks	Yes	No	No	No	No	No	Yes
Low transaction fees	No	No	Yes	Yes	Yes	No	No
High throughput (TPS)	No	No	Yes	Yes	Yes	No	No
Low latency (time to confirmation)	No	Yes	Yes	Yes	Yes	Yes	Yes
Environmentally friendly	No	Yes	Yes	Yes	Yes	Yes	Yes
Trustless	Yes	No	No	No	No	No	Yes
Post-Quantum Cryptography (PQC)	No	No	No	No	No	No	Yes
Feeless RAND and PRICE oracles	No	No	No	No	No	No	Yes
Permissionless and public	Yes	Yes	No	Yes	Yes	Yes	Yes
No slashing	Yes	No	No	No	Yes	Yes	Yes

Figure 2. Comparison of the Blockchain against other blockchain solutions currently on the market.

- Trustless - there is no need to trust any user, independent authority, or validator in order for the protocol to work. A trustless blockchain is self-regulating and requires validation by other network participants.
- Slashing - stakers can lose all or part of the money they have staked with a node if that node behaves in a malicious manner. There is no slashing on the Blockchain to ensure individuals staking with a malicious node are not unfairly penalized.
- All networks listed support some variant of smart contracts

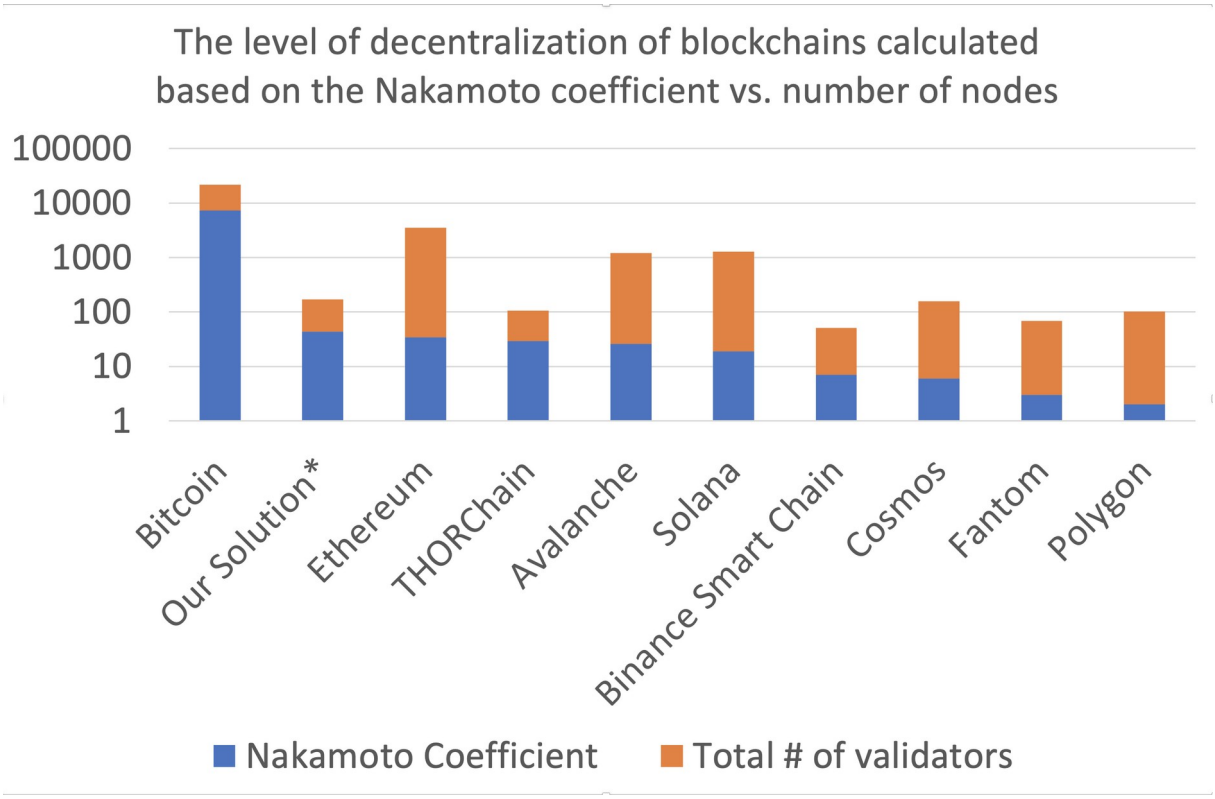

Fig 3. The level of decentralization of Our Solution vs. contemporary blockchains

- The Nakamoto Coefficient represents the number of validators (nodes) that would have to collude together to successfully block a blockchain from functioning properly.
- The source: https://crosstower.com/resources/education/nakamoto-coefficient/ https://twitter.com/vitalikbuterin/status/1333738057162362880?lang=en

3. THE BLOCKCHAIN OVERVIEW

3.1. The Coin

To incentivize participation in Blockchain's validation process and to facilitate the exchange of value between parties on the network, blockchain issues the Native Coin.

- Total supply of 2.3 BLN
- The number of mineable coins will be 2.07 BLN. As with conventional blockchains, the Native Coin asset is required to make transactions on the network, where they are used to pay transfer (gas) fees. As part of blockchain's consensus model, these fees, along with a diminishing block reward, are awarded to whichever participating validator authored the latest block.

Block rewards are diminishing. It can be calculated as follows:

IBR = MC * RR = 2,070,000,000.00 * 2e-8 = 41.4

where:
IBR - Initial block reward

RR – Reward Ratio (const: 2e-8)
MC – Mineable Coins
IMC – Initial Mineable Coins (const: 2,07 BLN)
NB – Number of Block (equivalent of Height)

NB is the height of the single chain.

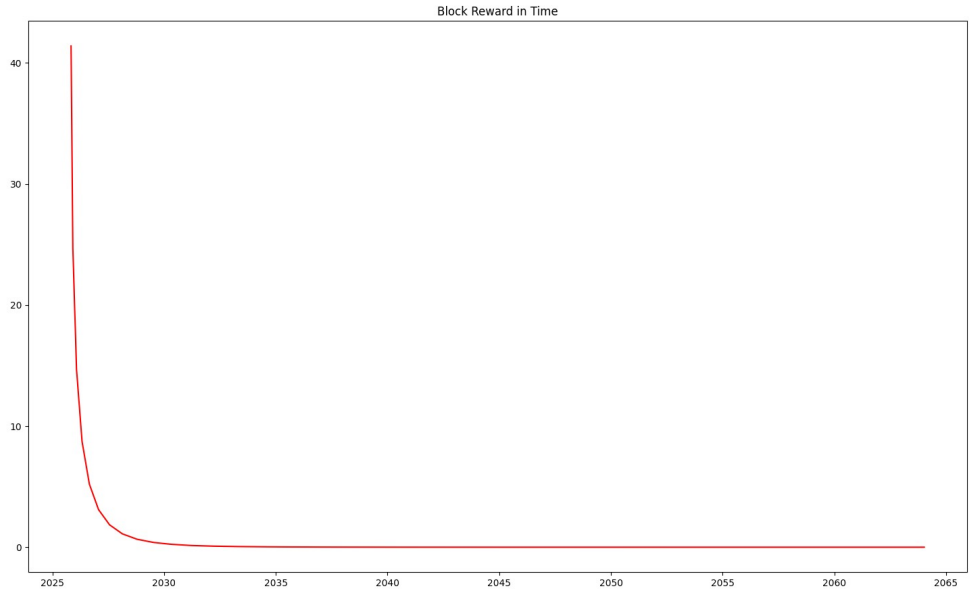

Figure 3. Hyperbolically diminishing block reward.

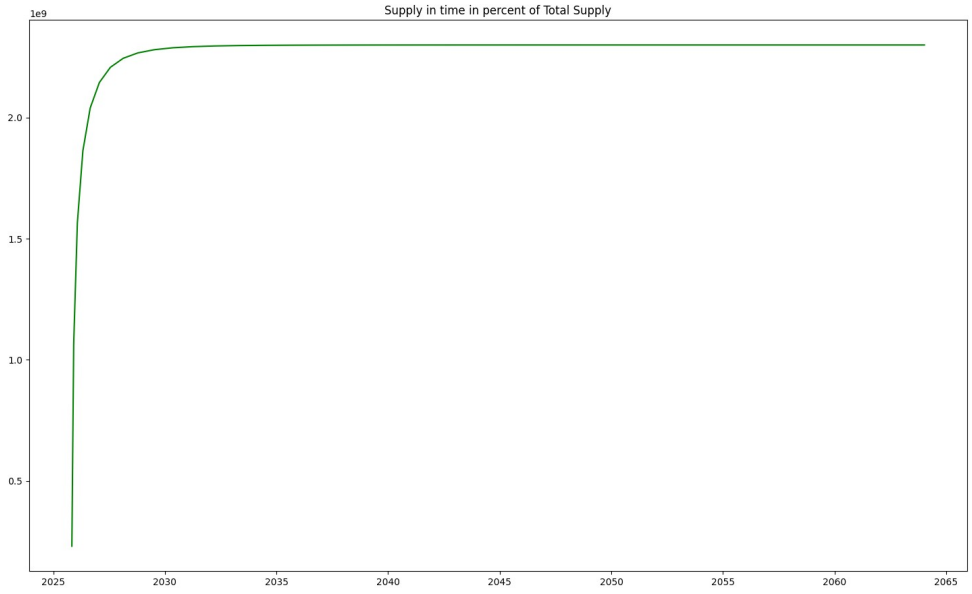

Figure 4. Total supply saturates to 2.3 BLN.

3.2. Chain Architecture

One of the most problematic characteristics of a PQC cryptosystem is the large size of the public keys, which are needed to verify new transactions. When one assumes that there will be circa 100,000,000 addresses (which is comparable to the Ethereum blockchain), we end up with 26 TB in data which needs to be made available to verify the signatures in every transaction. If implemented into popular networks today like Ethereum, the large public keys utilized by PQC models could reduce the rate at which blocks could be validated by a factor of 14. This is in a theory.

To solve this issue, the Blockchain keeps a single chain and makes the public key an optional field of the transaction itself. An earlier design split the data across two chains, one for transactions and one for public keys; the single-chain solution described here proved simpler and is the one that was implemented. Each transaction carries optional fields that may be filled with bytes or left empty. In the case of first transaction from specific account, the public key must be included in order to register in blockchain. After public key is registered, meaning stored in accepted block, in the following transactions this field can be empty. This reduce amount of bytes sending and processing. Creating smaller transaction make the Blockchain faster and cost effective.

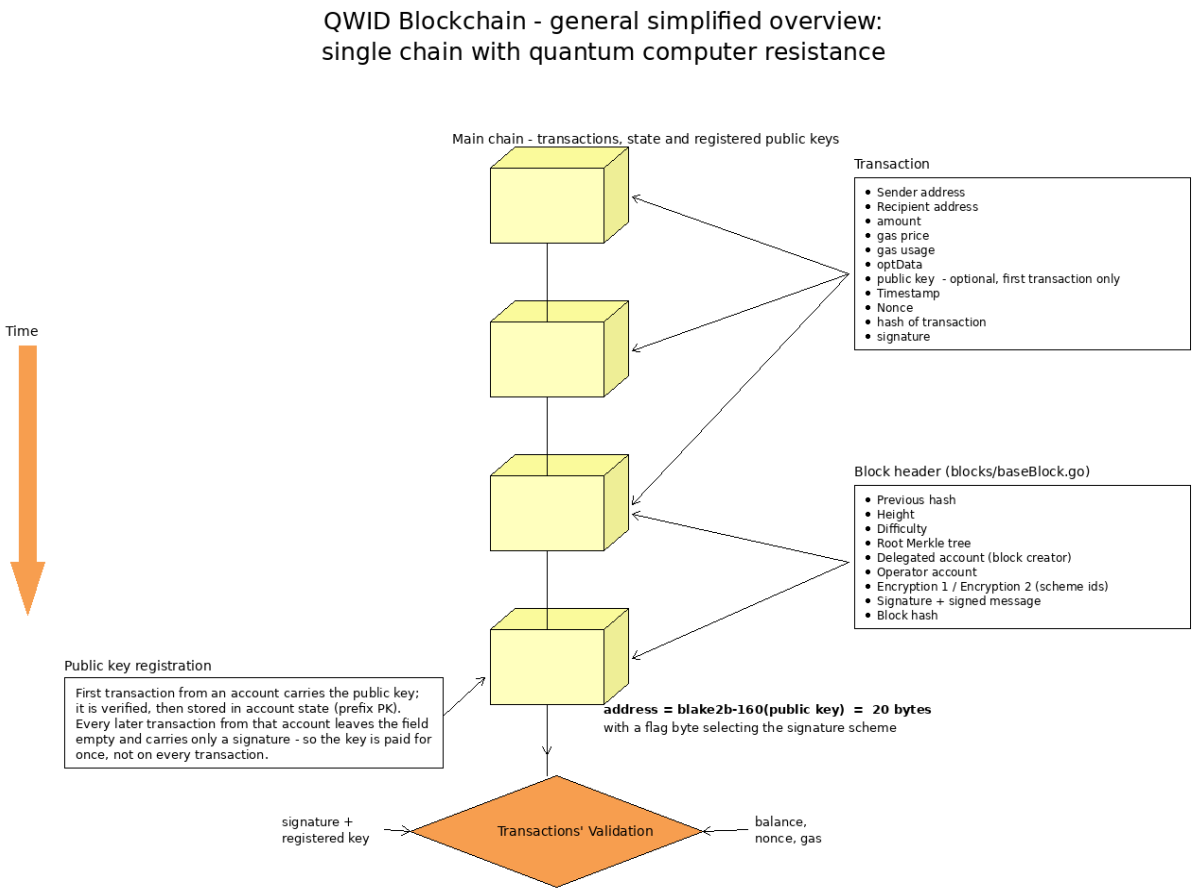

Figure 5. Overview of the blockchain's single-chain architecture with optional in-transaction public key registration.

Registered public keys are held in the node's key-value store, and reading them back during validation is bounded by I/O: current SSDs read at most about 7 GB per second. For example: the Badger key-value database is capable of loading around 12k values per second (714k per minute) 16kB each (see Fig. 6). This results in a theoretical limit for the Blockchain of around 10,000 TPS (Transactions per Second). Nevertheless a node is not only loading public keys but also is doing several other task simultaneously, so one have to keep it in mind and for the single node blockchain seems is accessible 2k TPS. In the case of mature blockchain no measurement has been assessment.

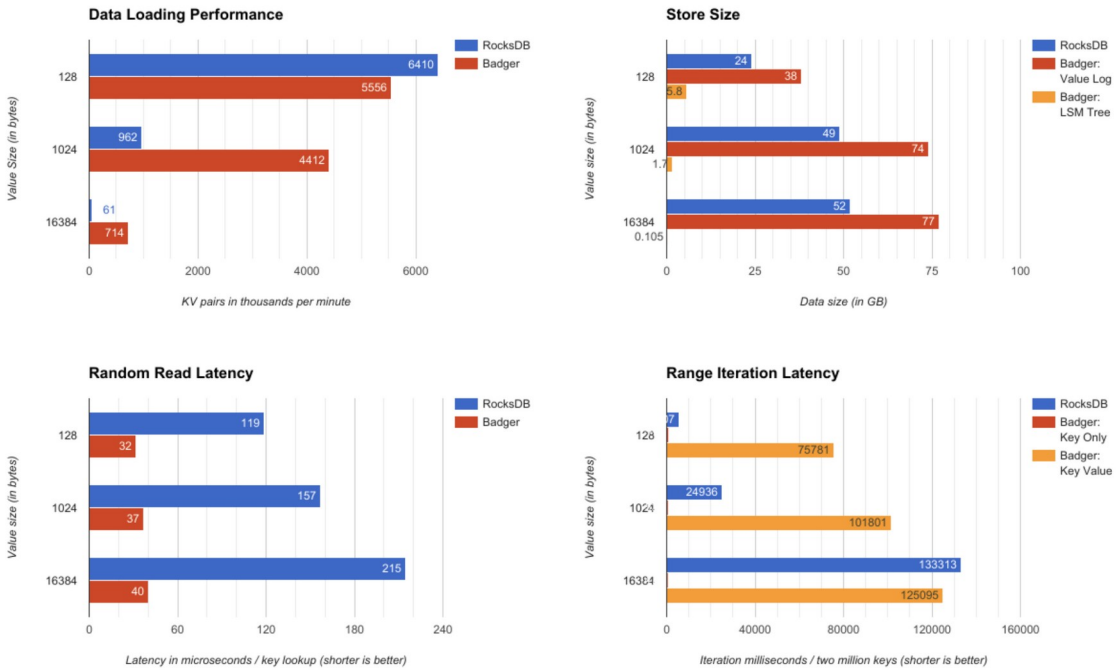

Fig 6. Performance of Rocksdb and Badger https://hypermode.com/blog/badger

3.3. Proof-of-Synergy Consensus Algorithm

Blockchain's proprietary Proof-of-Synergy model combines characteristics of three commonly used consensus algorithms:

- Proof-of-Work: To introduce complexity to block creation which ensures protection against DDOS attacks. We will use a modified POW model that is environmentally friendly. The first node to solve the POW calculation correctly will create the new block.
- Delegated Proof-of-Stake: This allows staking and DeFi-style yields.
- Proof-of-Authority: To limit the number of nodes while retaining high scalability and transactional throughput. The Blockchain will have a restricted number of nodes (128).

There will be a level of difficulty in creating new blocks (similar to the Bitcoin blockchain), which would be adjusted in order to keep the interval between blocks at the target of 10 seconds.

3.3.1. Staking and Delegated Accounts

- 256 delegate accounts will be created when the blockchain is first initiated. Anyone interested in staking (mining) needs to send coins to one of these accounts.
- The top 128 delegate accounts in terms of coins holding will act as nodes and validators. Out of the 256 delegate accounts in the blockchain's optional number, only 128 will act as nodes, and the remainder will remain sidelined until they have a large enough coins deposit and can join the top 128 delegators.
- Withdrawing coins from one of these accounts (unstaking) can be done at any time, and there is no fixed deposit period.
- Nodes can create blocks, as well as validate blocks created by other nodes.
- There are no special hardware requirements for a computer to remain as a node/validator. In a situation where a computer has insufficient resources (CPU/RAM), the node won't be able to create or validate blocks quickly enough.
- If the delegated account is below the threshold of 1 MLN coins, then it cannot create or validate blocks. Only delegated accounts that hold >= 1 MLN coins can act as nodes.
- Users can deposit coins in any of the 256 delegated accounts, as long as they deposit a minimum of 1000 coins.
- After the block is validated, rewards are sent to users' accounts according to the value of their stake.
- Delegated accounts cannot withdraw staked coins. Only the person that deposits coins to a delegated account can withdraw those coins.

3.3.2. Operational Accounts

- Each delegated account will have an operator. The operator will be responsible for the administration of the physical server on which the node is running.
- The operator of the node defines the percentage of the reward from block creations that they will claim. The percentage can be anywhere up to 50%.
- There will be competition within nodes to attract staked accounts. If the operator of a delegated account claims too much of the reward, then users will choose to deposit their funds in another account.
- Any participant is eligible to be an operator on any given delegated account. Participants need to signal their intent to become operators. The participant with the largest stake will be declared the operator for any given delegated account. If 2 participants have an equal stake, then the participant that is fastest to signal their intent will be awarded operator status.
- Every delegated account must have an operator in order to become a node.

3.3.3. Block Creation

- Each node on the network will try to solve the Proof-of-Work algorithm. When a node successfully solves this algorithm, then this node will create a new block.

- As part of this block creation process, a unique string value is generated that is derived from a combination of the node's UNIX timestamp, the address (32 bytes homomorphic hash of account public key), the hash of the last block, and the index of the last block in the chain (height). This string value is signed using the account's private key and is inserted into the header of the new block. This string value will change every second (due to the UNIX timestamp incrementing every second). For the purposes of this whitepaper, we will refer to this unique string value as the nonce.
- This block is then broadcast to all nodes on the network who will verify that the block is correct by validating the nonce and the hash value in the header of the block. The longest main chain will be considered the correct one.
- When the timestamp of the block is larger than the timestamp of the node plus 60 seconds, the block will not be accepted. This ensures clock synchronization across the network.
- The private keys for delegated accounts will be the keys of the node operators. These private keys will be used for generating the nonce and signing oracle broadcasts.

3.3.4. Difficulty

- The difficulty of the POW algorithm will be automatically adjusted to help maintain the rate of block creation to blockchain’s target of 10 seconds.
- Difficulty will be adjusted after every block creation in order to prevent any malicious nodes from creating a large number of blocks in a short period of time and overloading the network (DDoS).
- No slashing or punitive action is required against malicious nodes because the blockchain’s protocol is self-managing and will prevent situations where nodes behave maliciously. As a result, the network will be a trustless network much like the bitcoin network.

The chain uses a single consensus model (Proof-of-Synergy) with a block time interval of on average 10 seconds.

3.4. Post-Quantum Cryptography (PQC): A Dual-Layer Cryptographic Framework

The inaugural iteration of the Blockchain uses a dual-scheme cryptographic framework with exactly one scheme active at a time: Falcon-512 is the active signing scheme, and MAYO-2 stands by as an independent spare that takes over by on-chain vote whenever the active scheme is paused. The two were selected not only for their security margins and performance, but because they rest on unrelated mathematical assumptions: Falcon-512 is lattice-based (NTRU), while MAYO-2 is a multivariate Oil-and-Vinegar scheme. A cryptanalytic advance against one family therefore leaves the other standing. Falcon-512 has been selected by NIST for standardisation as FN-DSA (FIPS 206, still in draft); MAYO is a third-round candidate in the NIST Additional Signatures process, which NIST opened in 2022 specifically to reduce reliance on lattice assumptions.

Falcon-512 Key Attributes:

- High security level, comparable to 128-bit symmetric encryption models
- Compact signature size, facilitating efficient transaction processing

- Rapid signature verification, ensuring swift block validation
- Claims NIST-1 cryptographic level of security

MAYO-2 Complementary Features:

- Security comparable to 128-bit symmetric encryption, from an independent mathematical family, providing protection that does not share assumptions with the active scheme
- Optimized key sizes, balancing security with storage efficiency
- Alignment with anticipated post-quantum cryptographic standards (NIST-1)
- Capability to generate Mnemonic words for enhanced usability

3.4.1 Decentralized Cryptographic Governance

To ensure the perpetual security and adaptability of the Blockchain, a decentralized Voting Mechanism is integrated, empowering the community to:

- **Pause Protocol**: Suspend the use of either cryptographic protocol if a potential vulnerability is identified.
- **Protocol Upgrade**: Replace either protocol with a newly vetted, post-quantum secure alternative, subject to community approval.

Summary of Dual Cryptographic Framework:

Attribute	Falcon-512	MAYO-2
Security Level	Equivalent to 128-bit AES	Equivalent to 128-bit AES
Public Key Size	897 B	4912 B
Signature Size	<752 B	186 B
Private Key Size	1281 B	24 B
Security Classification	NIST Level 1	NIST Level 1

3.4.2 Private Key Management

Private keys are held only in the user's wallet, encrypted at rest; only public keys and signatures are ever stored on the blockchain. Wallets generated by the command-line tool are derived from a 24-word BIP-39 recovery phrase, selected from a list of 2048 words. The phrase is a seed from which the key pairs are regenerated, not a transcription of the keys themselves: a post-quantum secret key is far too large to be written out as words. Wallets created through the web interface use random keys and have no recovery phrase, so that a phrase never crosses an HTTP connection; for those the encrypted wallet file together with its password is the backup.

3.4.3 License and Security Assurance

Both Falcon-512 and MAYO-2 are published under permissive licenses, allowing for unrestricted use, modification, and distribution, even for commercial purposes. The Blockchain's dual cryptographic approach ensures a security posture comparable to, or exceeding, that of contemporary cryptographic standards, such as those used in Bitcoin, while maintaining future-proof resilience against quantum computing threats.

3.5. Oracles

The Blockchain was designed to help shape the future of decentralized finance. To this end, implements two decentralized protocol-level oracles that are free to use by developers in their smart contracts and applications.

3.5.1. PRICE Oracle

The Blockchain incentivizes nodes to provide data about the Native Coin/USD exchange rate to the PRICE Oracle. The blockchain establishes the current price of Coin by calculating the median price submitted by nodes. This is called the oracle price, which is used to determine the exchange rate of Coin to USD. To begin submitting data to the PRICE Oracle, a node operator must stake coins. An operational account's staking requirement may be raised by the protocol if individually submitted data points are significantly divergent from the median of all submitted prices.

The price, as determined by the PRICE Oracle, is included in the body of new blocks on the main chain, on a per-block basis. When a node solves the POW algorithm and creates a new block, it must solicit prices from other nodes representing at least two-thirds of the total amount of staked coins. Other nodes will broadcast the Coin price as a number with up to 8 digits after the decimal place. All of these prices will be added to the new block, and the median of all of these prices will be the official Coin oracle price.

3.5.2. RAND Oracle

The second oracle, called RAND, will provide a source of verifiably random numbers for use by developers. No special reward or punishment will be associated with RAND. In this model, each node proposes a random number. In the same manner as the price oracle, RAND needs to be proposed by nodes representing at least 2/3 staked coins. Submitted numbers will be distributed along with oracle prices, signed by the operational account. The overall RAND number of the block will be a 256-bit hash of oracle prices and proposed random numbers, making the result unpredictable. Random numbers need to be submitted as a 64-bit integer. In order to calculate the random hash, the submitted oracle price and random integers are converted to strings, and then consequently to bytes. The final random number would be the sum of homomorphic hashes of separated byte arrays of each number. In this way, will allow network participants to easily check the correctness of the resulting hash and RAND value by validator nodes. This model is resistant to manipulation of outcome by malicious nodes,

allowing developers to build secure and reliable GameFi or DeFi applications whose logic requires a tamper-proof random number.

3.6. Escrow account

Escrow account is a new idea of helping people to build dApps based on our solution. In any case one would like to protect Coins from hackers and does not care much about speed. In Escrow account each transaction is delayed by some specified time in order for manager to review each transaction in his working hours and cancel any suspicious ones.

3.7. Multi-signature account

Multi-signature account is inbuild in the Blockchain protocol itself. Similar like with token swapper, the solution is very similar to Ethereum multi-signature solution known as Gnosis. The Gnosis Multi-Signature solution is based on EVM-machine, so smart contract level. In our solution we have it inbuild in the protocol, so easier to use, and less cost full and trustless.

3.8. Token Swapper

In protocol there is inbuild possibility of token swapping. Tokens must be within the Blockchain EVM-machine, so this blockchain’s tokens. The math and calculations is done using similar to Uniswap (Ethereum swapper) formula. The difference is that Uniswap is built in the level of EVM-machine and in our solution is based on the blockchain’s protocol. Seems this makes swapping cheaper and trustless.

4. SUMMARY & DISCUSSION

We have outlined a practical implementation of a secure and performant blockchain that is resistant to quantum computers and their ongoing development. The proposed architecture for the Blockchain allows users and developers to securely store and transfer value within a permissionless, decentralized network, and to build and interact with decentralized applications that are resistant to future technological development, as outlined in Appendix A.

Blockchain's core mission is to provide a blockchain network that is able to thrive for many decades to come, and the design decisions illustrated here reflect this goal. The end result is a feature-rich and quantum-computer resistant blockchain whose upgrades can be directed by the community, without causing disruption of service or loss of value to users. The blockchain provides a complete toolkit to aid in the development of decentralized applications and DeFi primitives.

The Blockchain's EVM-compatible smart-contract platform allows developers to create native dApps within a secure post-quantum computing blockchain environment, and provides a means for existing dApps to be ported from other networks for increased speed and security — without any changes to the underlying smart contract code. In addition, the Price and RAND oracles help to ease the process of developing DeFi applications and to lower their operational costs — particularly those that rely on provably random numbers or live currency exchange rates, like gaming dApps and financial services like borrowing, lending, or decentralized exchanges.

REFERENCES

[1] IBM Quantum Composer user guide — Shor's algorithm
https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm

[2] Standardization of XMSS by NIST is due to occur in the near future
https://csrc.nist.gov/CSRC/media/Projects/Stateful-Hash-Based-Signatures/documents/stateful-HBS-public-comments-June2018-rfi.pdf

[3] Europol arrests UK man for stealing €10 million worth of IOTA cryptocurrency
https://www.zdnet.com/article/europol-arrests-uk-man-for-stealing-eur10-million-worth-of-iota-cryptocurrency

[4] Solana's Latest DDoS Attack Leads to Poor Network Performance
https://finance.yahoo.com/news/solana-latest-ddos-attack-leads-120022342.html

[5] Solana Halted by Bug Linked to Certain Cold Storage Transactions
https://www.coindesk.com/tech/2022/06/02/solana-halted-by-bug-linked-to-certain-cold-storage-transactions/

[6] Terra Blockchain Halted To 'Prevent Attacks' After Luna Token Crashes Nearly 100% Overnight
https://www.forbes.com/sites/jonathanponciano/2022/05/12/terra-blockchain-halted-to-prevent-attacks-after-luna-token-crashes-nearly-100-overnight

[7] When using Falcon-512 cryptographic standard, which has optimal size of sum Public key and signature for single chain blockchain
https://falcon-sign.info/

[8] Badger: A fast key-value store written purely in Go
https://dgraph.io/blog/post/badger/

[9] Open-sourcing homomorphic hashing to secure update propagation
https://engineering.fb.com/2019/03/01/security/homomorphic-hashing

[10] MAYO: Practical Post-Quantum Signatures from Oil-and-Vinegar Maps
https://pqmayo.org

[11] NIST Post-Quantum Cryptography: Additional Digital Signature Schemes
https://csrc.nist.gov/projects/pqc-dig-sig

[12] MAYO, The Open Quantum Safe Project
https://openquantumsafe.org/liboqs/algorithms/sig/mayo.html

[13] Bitcoin Improvement Proposal BIP-0039
https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt

[14] CC0 1.0 Universal (CC0 1.0) Public Domain Dedication

https://creativecommons.org/publicdomain/zero/1.0/

[15] Ubic, Eric Tobias, 128 or 256 bit Encryption: Which Should I Use?
https://www.ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/

[16] NIST Computer Security Resource Center - PQC security evaluation criteria
https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)

[17] Circuit for Shor's algorithm using 2n+3 qubits
https://arxiv.org/abs/quant-ph/0205095

[18] First quantum computer to pack 100 qubits enters crowded race
https://www.nature.com/articles/d41586-021-03476-5

APPENDIX A: CALCULATING THE TIME AT WHICH QUANTUM COMPUTING WILL THREATEN BITCOIN

Introduction:

Bitcoin uses a version of Elliptic Curve Cryptography (ECC) known as Secp256k1. 256-bit ECC is equivalent to 3072-bit DSA/RSA encryption (see Figure 1).

Minimum size (bits) of Public Keys

	Minimum size (bits) of Public Keys		Key Size Ratio	
Security (bits)	DSA / RSA	ECC	ECC to RSA / DSA	Valid
80	1024	160-223	1:6	Until 2010
112	2048	224-255	1:9	Until 2030
128	3072	256-383	1:12	Beyond 2031
192	7680	384-511	1:20	
256	15360	512+	1:30	

Figure 1: Security properties of RSA and ECC cryptography (https://www.ssl2buy.com/wiki/rsa-vs-ecc-which-is-better-algorithm-for-security)

To implement Shor's methodology on a quantum computer, one needs at least $2n + 3$ qubits. Where n is the number of bits in the public key of the RSA encryption model, [17] $2n + 3 = 2 \cdot 3072 + 3 = 6147$ ideal qubits are required to perform a successful attack on a 3072-bit RSA model. From this, we can infer that Bitcoin would be vulnerable to attack by quantum computers with 6147 or more ideal qubits.

The current state of quantum computing:

- Quantum chip with 433 qubits was built in December 2022 by IBM.
- IBM is planning a 1121 qubit quantum chip by 2023.
- "The 'Eagle' chip is a step towards IBM's goal of creating a 433-qubit quantum processor next year, followed by one with 1,121 qubits, named Condor, by 2023" [18]

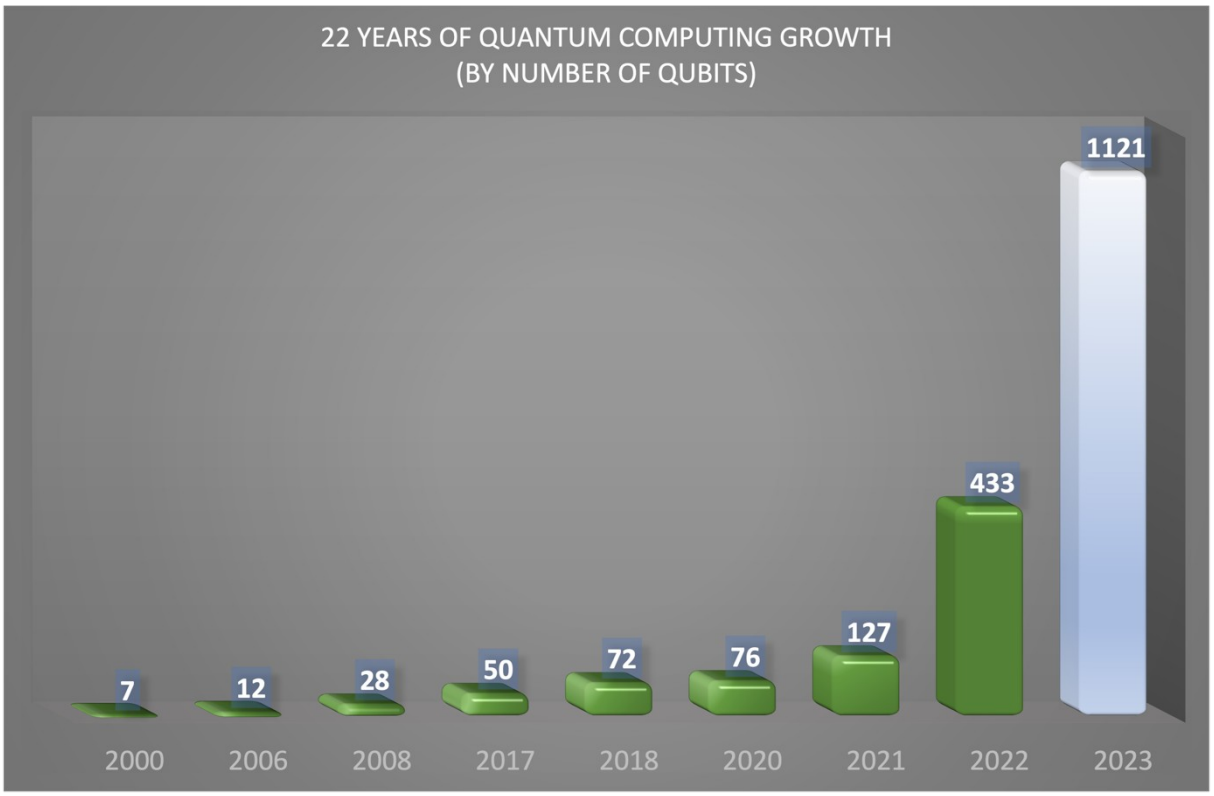

Figure 2: Quantum computing growth by number of qubits, between 2000 to 2023.

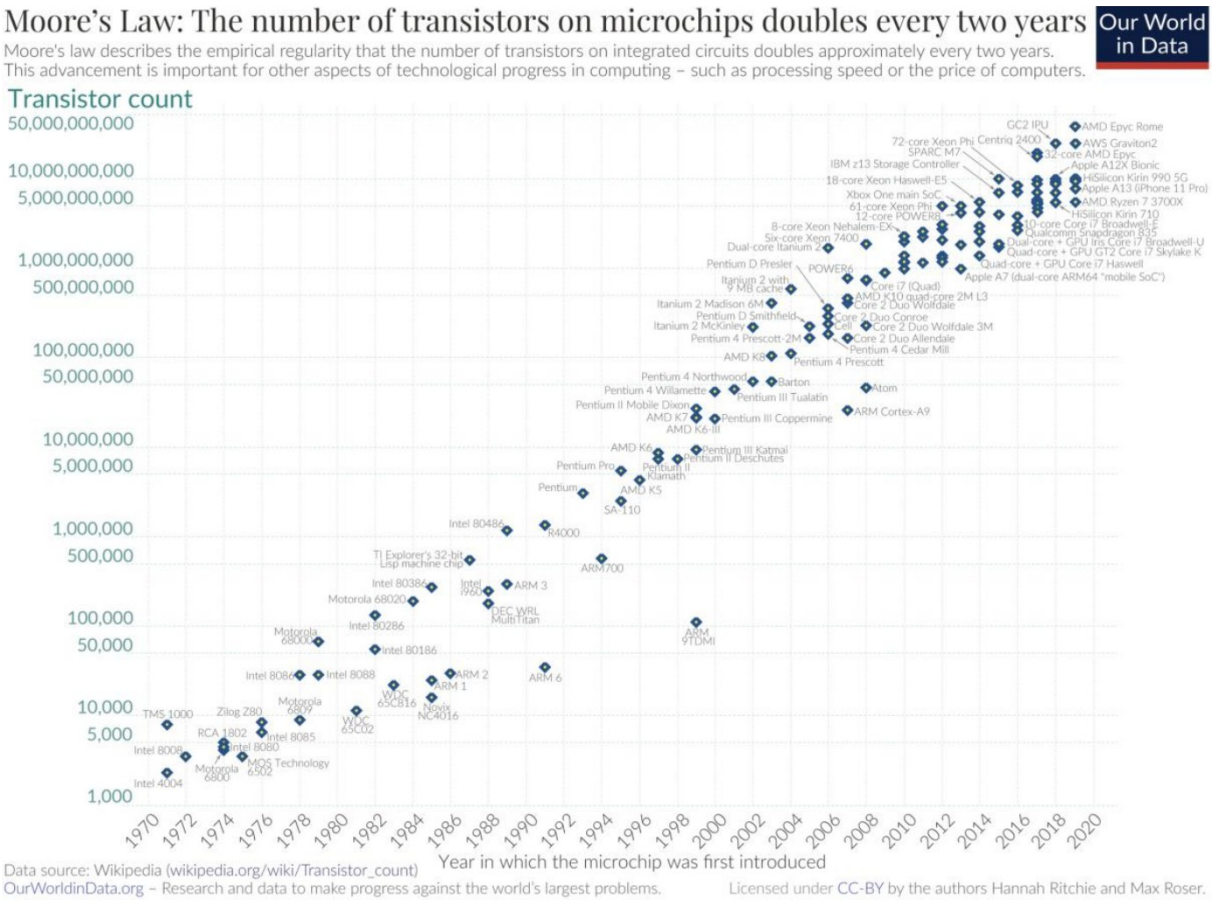

Figure 3: Moore's Law: The number of transistors on microchips doubles every two years. OurWorldinData.org

In Figure 4, we show the projected development of quantum computing if Moore's law is applied. The dotted straight line shows the trend of the number of qubits (see Fig. 2). The threshold (6147 qubits) shows the critical point at which the cryptographic schemes securing Bitcoin will be vulnerable to attack by quantum computers. The intersection of lines at 2029 and 2039 represent the range of time at which we could expect quantum computers to break Bitcoin's consensus model and underlying cryptographic standard.

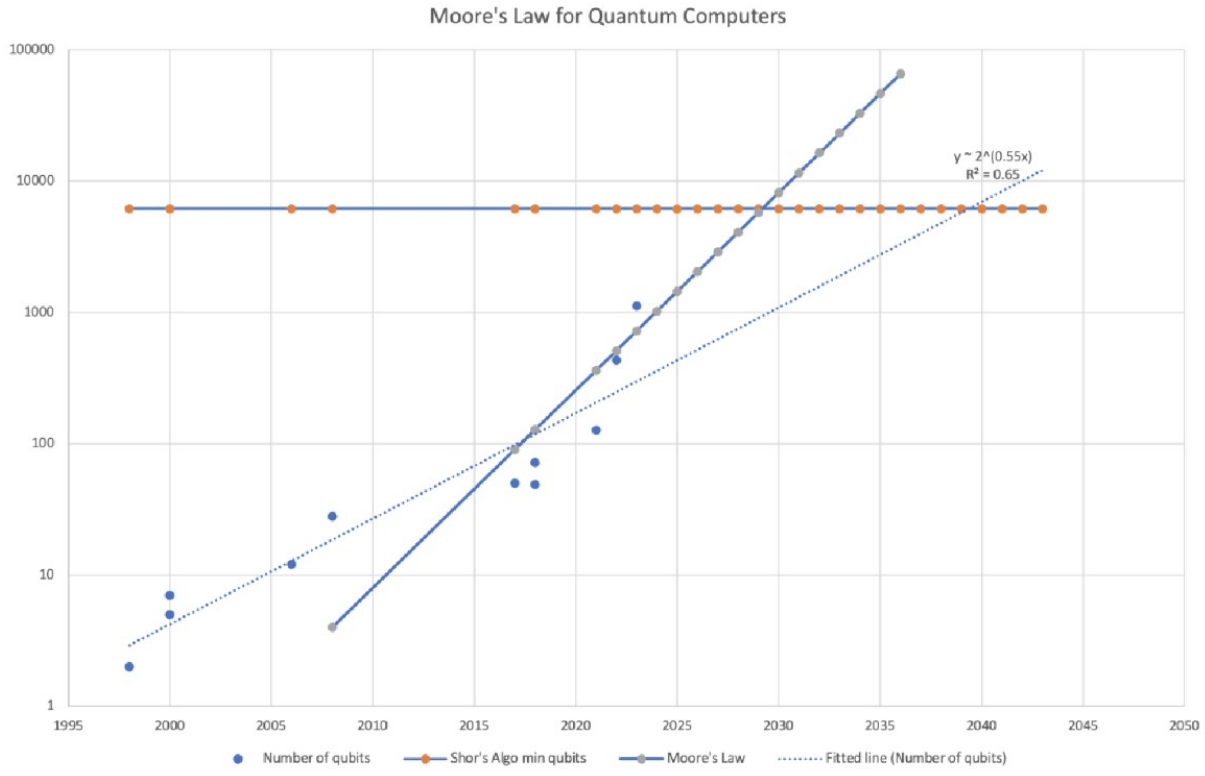

Figure 4: Moore's Law applied to quantum computers.

Conclusion:

The expected time at which quantum computers will be able to break Bitcoin's encryption is in the year 2039. We note three important factors:

1. The number of qubits forecasted to be achieved in 2022 and 2023 are very rapidly approaching the minimum attack threshold using Shor's algorithm.
2. The trend line does not precisely preserve Moore's Law, as the relative growth in performance is roughly half that of standard computers. If we were to precisely attribute Moore's Law to the progression of quantum computers – i.e., a doubling of the number of qubits every 2 years – then one can see that the trend line crosses the threshold needed to break Bitcoin by the year 2029.
3. The effects of the threat will appear faster than quantum computers are able to achieve it. Traders who are familiar with the threat may exit their Bitcoin positions as quantum computers are normalized, anticipating an attack to become reality.