# FUTURE OF CRYPTOCURRENCY BASED ON QUANTUM COMPUTING: ECONOMICAL VIEW-POINT

**Kervalishvili P.,**
**Tavkhelidze M.**
*Grigol Robakidze University, Tbilisi, Georgia*

https://doi.org/10.5281/zenodo.16539239

**Abstract**

The rapid advancement of quantum computing presents both transformative opportunities and existential threats to the future of cryptocurrency. Quantum computing's ability to solve complex problems exponentially faster than classical systems could revolutionize cryptographic security, mining efficiency, and monetary systems. However, it also poses significant risks to existing cryptocurrencies, such as Bitcoin and Ethereum, which rely on classical cryptographic algorithms vulnerable to quantum attacks like Shor's and Grover's algorithms. The paper examines quantum-resistant cryptocurrencies (e.g., QRL, IOTA) and theoretical qubit-based systems that leverage quantum properties such as superposition, entanglement, and the no-cloning theorem for secure transactions and unforgeable "quantum money." It highlights the challenges of quantum decoherence, scalability, and the need for hybrid quantum-classical systems as transitional solutions. Additionally, the economic implications of quantum mining—including energy efficiency and hardware requirements—are analyzed, contrasting classical and quantum approaches. A novel concept of "quantum money" is introduced, offering tamper-proof currency based on quantum mechanics, with potential applications in decentralized finance and central bank digital currencies (CBDCs). The paper also discusses hypothetical threats, such as quantum-enabled money laundering, and the dual-edged nature of quantum technologies in fostering both hyper-transparency and unbreakable anonymity. The integration of quantum computing into cryptocurrency systems will likely occur in phases, beginning with quantum-resistant defenses and evolving into fully quantum-native economies. Proactive adaptation by policymakers and industry stakeholders is critical to harnessing the benefits while mitigating risks in this emerging quantum-cryptocurrency era.

**Keywords**: Quantum computing, cryptocurrency, quantum-resistant cryptography, quantum money, blockchain, economic paradigm.

## Quantum computing: Approach to Economy. Brief introduction

Quantum computing is the use of quantum systems to perform computation by the manipulation of quantum particles via different configuration of logical gates. The general expectation in quantum computing is a quadratic speedup in the computation of certain kinds of equations. Accordingly algorithms of quantum computing could take advantages of the quantum objects processing of tasks of linear algebra, Fourier transformations, matrix operations, etc. [1-3].

At the same time progress in many areas of foundational physics is enabling new technologies that translate to practical use in quantum computing. Superposition and entanglement are two counterintuitive features that are harnessed in quantum computation. Superposition is the quantum property of an unobserved particle existing in all possible states simultaneously, until collapsing to only one when measured. Entanglement is the quantum property of physical attributes being correlated between particles (position, momentum, polarization, and spin), even when separated by distance. [4-6].

One of the most immediate high-profile applications of quantum computing is cryptography. The postquantum cryptographic algorithms that are resistant to quantum computer based attacks need to be implemented in a worldwide roll-out effort. The development of quantum resistant public-key cryptographic standards is underway, with the algorithm selection process announced by the U.S. National Institute of Standards and Technology (NIST) that their postquantum cryptography standardization process had entered the final phase. [7-10].

Quantum-secure algorithms mainly involve a shift to mathematics based on lattices (group theory) as opposed to factoring (number theory). Some of the first quantum algorithms developed to take advantage of nonclassical properties were Shor’s quantum factoring algorithm and Grover’s quantum search algorithm. Shor’s algorithm is a period-finding function with a quantum Fourier transform (a classical discrete Fourier transform applied to the vector amplitudes of a quantum state), which is exponentially faster than classical algorithms. [11-13]. More recently proposed quantum-secure cryptographic methods include access based on location instead of authorization, with quantum secret sharing localized to space-time, and time entanglement (entanglement in time instead of space) is also possible for cryptographic key exchange within a short time window.

Quantum approach to economy and finance is the application of physics methods to problems of option pricing, trading strategies, risk management and optimization. Markets have long been modelled as complex physical phenomena per the principles of wavefunctions, thermality, dissipation, and Brownian motion, and now these models are being implemented with real-life quantum hardware instead of simulation. Quantum economy and finance could be one of the first mainstream fields to develop in quantum computing as the industry is typically an early adopter of new technologies, and currently finds itself in a potential progression from classical to digital (blockchains) to quantum methods. Other quantum economical projects use quantum amplitude estimation likewise for bond portfolio value-at-risk assessment per interest rate movement, anharmonic oscillators to define a price–energy relationship in Schroedinger wavefunctions for asset pricing and market dynamics. [14-17].

**Quantum Bit-Based Crypto Currency Overview**

Developing a qubit-based cryptocurrency is a highly theoretical and experimental concept that merges quantum computing with blockchain or distributed ledger technology. Below is an in-depth exploration of the key components, challenges, and potential architectures for such a system.

1. Quantum-Resistant Cryptocurrencies

Most "quantum-related" cryptocurrencies today focus on quantum resistance—meaning they use cryptographic algorithms that are secure against attacks from quantum computers. Examples include: a) QRL (Quantum Resistant Ledger) – Uses XMSS (Extended Merkle Signature Scheme), a post-quantum secure signature algorithm. b) IOTA - decentralized blockchain infrastructure (with Quantum Resistance) – Implemented Winternitz one-time signatures (WOTS+) for quantum resistance. c) Algorand – Plans to integrate quantum-resistant cryptographic schemes in the future. [18].

2. True Quantum Bit (Qubit) Based Cryptocurrencies

A fully quantum-based cryptocurrency would theoretically use qubits (quantum bits) for transactions or consensus mechanisms. However, such projects are still largely theoretical or in early research phases due to the challenges of quantum stability and error correction. Some experimental concepts include: a) Quantum Blockchain-based Ledgers – Hypothetical systems where quantum states (like entangled qubits) secure transactions. b) Quantum Money – A concept proposed by researchers where quantum states (e.g., unclonable qubits) prevent counterfeiting. [19].

3. Quantum Computing Threats, Existing Cryptocurrencies and Challenges

a) Bitcoin and Ethereum (ECDSA & SHA-256) are vulnerable to Shor’s algorithm, which can break classical public-key cryptography. b) Grover’s algorithm could weaken symmetric encryption (e.g., hashing), but doubling key sizes (e.g., SHA-512) mitigates this. c) Quantum Decoherence – Qubits are fragile and require near-absolute-zero temperatures. d) Current quantum computers (like IBM’s or Google’s) lack enough stable qubits for real-world crypto applications.

A true qubit cryptocurrency would leverage quantum mechanical properties (superposition, entanglement, and no-cloning) to achieve: a) Quantum-secure transactions (unhackable via quantum or classical attacks). b) Quantum-native consensus mechanisms (e.g., using entanglement for validation). c) Quantum money (unclonable digital cash).

Key Quantum Properties could utilized: Quantum feature and application in cryptocurrency; Superpositioned qubits can represent 0 and 1 simultaneously, enabling ultra-fast parallel transaction processing; Entanglement of quantum-secure communication between nodes and tamper-proof transaction validation. No-Cloning Theorem prevents counterfeiting of quantum money (quantum states cannot be copied). [19].

Possible Architectures for Qubit Cryptocurrency could include Quantum Blockchain (Hybrid Classical-Quantum Ledger): a) Classical Layer – Handles traditional transactions when quantum nodes are unavailable; b) Quantum Layer – Uses qubits for Quantum signatures (e.g., BB84 QKD or quantum digital signatures), Entanglement-based consensus (nodes verify transactions via shared entangled states), Post-quantum hashing (e.g., lattice-based or hash-based PQ cryptography). Pure Quantum Money (Unclonable Digital Currency) is based on quantum states as currency (proposed by Wiesner in 1983 [20] ), Each "quantum coin" is a unique qubit state that cannot be copied (no-cloning theorem), Requires quantum memory (still experimental) to store qubits long-term.

There are explainable challenges in qubit cryptocurrency development (table 1).

Table 1:

**Qubit cryptocurrency development**

| Challenge | Description |
|---|---|
| Quantum Decoherence | Qubits lose state quickly (~microseconds); error correction needed |
| Quantum Networking | Requires quantum internet (entanglement distribution over long distances) |
| No Practical Qubit Storage | No reliable quantum RAM for long-term qubit storage. |
| Scalability | Current quantum computers (NISQ era) have <1000 noisy qubits—insufficient for global ledgers. |
| Classical Interface | Hybrid systems need secure classical-quantum communication. |

The hybrid approach stands to benefit hugely in that regard. Any further increase in critical sectors-financial, health care, defence, among others-situated atop digital infrastructure will demand the necessity for highly impenetrable communication systems. [21]. Hybrid quantum-classical networks then offer improved resistance to cyberattacks, both classical and quantum based, with high assurance of even greater data confidentiality, integrity, and availability Hybrid quantum-classical communication networks demonstrates the revolutionary possibility of integrating quantum technologies into cybersecurity frameworks. These networks also promise to increase data security with their enhancement, smooth communication, and strength against emerging cyber threats using the principles of quantum mechanics. Quantum cryptography and its applications in secure data storage and processing demonstrate the superior solutions put in place compared with classical methods, especially when dealing with vulnerabilities as a result of quantum computing advancement. Quantum key distribution (QKD) is the one aspect of quantum communication wherein encryption keys can potentially be distributed and exchanged in such a manner that they should be theoretically impossible to intercept. combines quantum and classical channels, allowing it to implement real-world communication networks for improving data security beyond what is achievable by traditional approaches. Hybrid networks bridge the gap between today's classical systems and the promise of fully quantum networks, enabling quantum security in a stepwise manner.

**Quantum Threats to Classical Cryptocurrencies**

Quantum computing could disrupt cryptocurrency economics by enabling energy-efficient mining, unhackable transactions, and novel monetary systems but only if scalability and cost barriers are overcome. For father explanations of this thesis as example we could analyze the paradigm of Internet of Things (IoT) where many of our daily objects will be interconnected and will interact with their environment in order to collect information and automate certain tasks. Such a vision requires, among other things, seamless authentication, data privacy, security, robustness against attacks, easy deployment and self-maintenance. Such features can be brought by blockchain, a technology born with a cryptocurrency called Bitcoin. [22]. Using the basics of blockchain, the most relevant BIoT applications are described with the objective of emphasizing how blockchain can impact traditional cloud-centered IoT applications. (Fig.1).

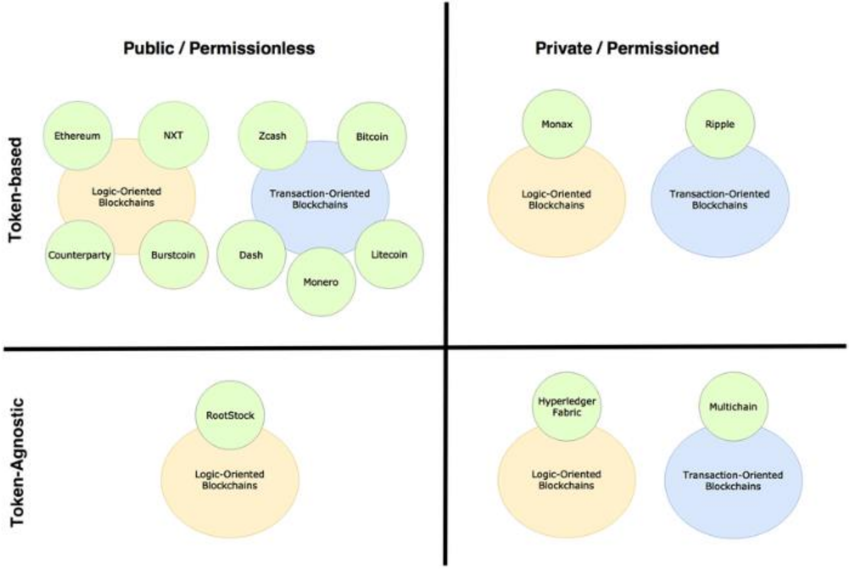
Public / Permissionless
Private / Permissioned
Token-based
Ethereum
NXT
Zcash
Bitcoin
Logic-Oriented Blockchains
Transaction-Oriented Blockchains
Counterparty
Burstcoin
Dash
Monero
Litecoin
Monax
Ripple
Logic-Oriented Blockchains
Transaction-Oriented Blockchains
Token-Agnostic
RootStock
Logic-Oriented Blockchains
Hyperledger Fabric
Multichain
Logic-Oriented Blockchains
Transaction-Oriented Blockchains

*Fig. 1. Blockchain taxonomy and practical examples.*
*[Fernández-Caramés, Tiago and Paula Fraga-Lamas, A Review on the Use of Blockchain for the Internet of Things, IEEE Access, volume 6, May 2018, 32979-33001 doi = 10.1109/ACCESS.2018.2842685].*

Crypto is still a young breed. It grows new limbs almost every day. No core list should prevent us from readiness to open new opportunities across the crypto stack. At the same time, it is essential to set a certain focus in the increasingly overwhelming crypto landscape. The following predictions represent verticals across the Infrastructure and Consumer stack to which we generally attribute large and disruptive market potential. However US national Institute of Standards has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms (Report on Post Quantum Cryptography). Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography. These algorithms are vulnerable to attacks from large-scale quantum computers [23,24]. It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

**Quantum Mining: Energy and Hardware Economics.**

Quantum computing has the potential to revolutionize cryptocurrency mining by offering significant energy savings and improved computational efficiency. While current quantum computers are not yet powerful enough to replace traditional mining hardware for most cryptocurrencies, research suggests that quantum-based mining could drastically reduce energy consumption and enhance the scalability of blockchain networks. Schematic representation of possible development pathways for qubit-based cryptocurrency mining is shown at the figure 2.

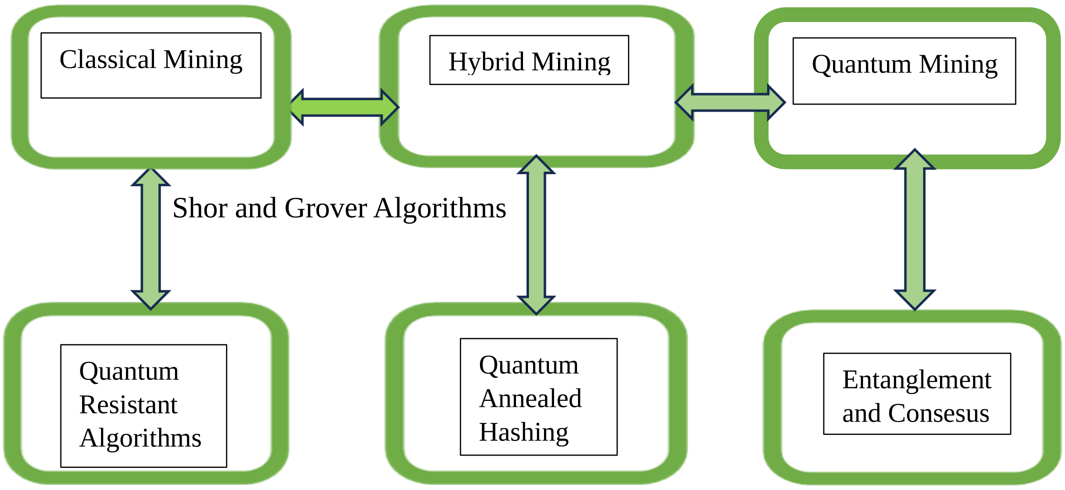
Classical Mining
Hybrid Mining
Quantum Mining
Shor and Grover Algorithms
Quantum Resistant Algorithms
Quantum Annealed Hashing
Entanglement and Consesus

*Fig. 2. Evolution from classical to hybrid and quantum. a) Classical Mining (Pre-Quantum Era); b) Transitional Hybrid Mining (Today); Fully Quantum Mining (Nearest Future)*

The electricity needs and hardware parameters of qubit-based cryptocurrency mining differ drastically from classical mining due to quantum computing's unique requirements.[25-27]. Below is a detailed analysis of power consumption, cooling, and hardware specifications for both near-term hybrid quantum-classical mining and long-term full quantum mining.

Table 2.

**Electricity Consumption Analysis**

| Classical Mining | Bitcoin, Ethereum | Power Consumption~100 TWh/year | Hardware ASICs (28nm–5nm) GPUs | Energy Efficiency ~30–50 J/TH ~0.1–1 J/MH |
|---|---|---|---|---|
| Hybrid Quantum-Classical Mining | Bitcoin,Ethereum, Qubit coin | Parameter ~0.01 TWh/year | Hardwar FPGAs/ASICs with PQ corese | Qubit Count 500–1,000 |
| Quantum-Annealer-Assisted Mining | Qubit coin | ~25 kW/system | Mostly cooling (cryogenic) | Qubit Count 5,000–7,000 |
| Post-Quantum Secure Mining | Qubit coin | Power Consumption~500 kW–1 MW (per h) | Cryogenic or optical traps | Hashing Acceleration10–100x |
| Energy Efficiency Comparison | Mining Type | Classical<br>Hybrid Quantum<br>Full Quantum<br>Quantum Money | ~1,000 kWh/t<br>~100–500 kWh/tx<br>~10–50 kWh/tx<br>~1–5 kWh/tx | Baseline Annealing +<br>PQ hashing<br>Boson Sampling<br>High efficiency |

Summary of table: Short-Term: Quantum mining is more energy-intensive due to cryogenics but may optimize PoW; Long-Term: If qubit stability improves, quantum mining could be greener than classical ASICs.

**Quantum Money: A New Economic Paradigm**

“Quantum Money” is a fascinating concept that merges quantum information science with monetary systems, offering a radically new economic paradigm based on principles of quantum physics rather than classical computation. Here's a concise overview tailored to your interest in new scientific-economic frontiers: First proposed by Stephen Wiesner in the 1970s (published later at 1983 [20]), quantum money uses the no-cloning theorem of quantum mechanics to create unforgeable currency. (Figure 3.). While classical data (and hence traditional money) can be copied, quantum states cannot be duplicated precisely, making counterfeiting theoretically impossible.

Table 3.

**Key Features of Quantum Money**

| Classical Money | Quantum Money |
|---|---|
| Easily copied (counterfeit risk) | Quantum no-cloning ensures security |
| Verified by signature, code, or bank | Verified via quantum state and quantum key |
| Based on classical computing | Based on quantum entanglement, superposition |
| Traceable with effort | Quantum traceability via entangled systems |
| Vulnerable to digital fraud | Inherently secure by physics laws |

Table 4.

**Types of Quantum Money**

| Private-Key Quantum Money | Public-Key Quantum Money |
|---|---|
| Requires the issuing authority (like a central bank) to verify authenticity. | Anyone can verify authenticity. |
| Based on secret quantum keys known only to the issuer. | Still a subject of active research |

Above mentioned data could merge with quantum blockchain or quantum-secure distributed ledgers.

Table 5.

**Economic Paradigm Shift**

| Traditional | Quantum Transition |
|---|---|
| Security | Fraud and duplication become physically impossible |
| Decentralization | Possibility for quantum money without a central bank. |
| Global Economy | Enables trustless, tamper-proof financial ecosystems |
| Inflation Resistance | Customizable issuance based on entangled resource limits |
| Automation | Could be integrated into quantum AI-driven economies |
| Future Directions and Implications | Quantum Central Bank Currencies (QCBCs): National-level rollout of quantum-backed digital.<br>Quantum Blockchain: Enhancing classical blockchain with quantum security and computation.<br>Post-Capitalist Economies: Fully quantum-native economic systems, possibly modeled on energy-information exchange rather than fiat. |

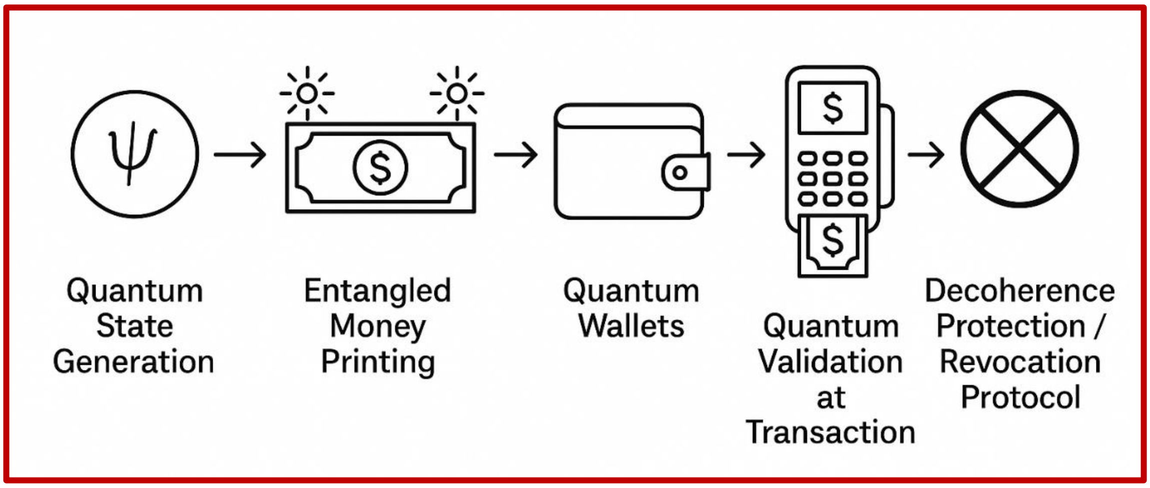
ψ
Quantum State Generation
$
Entangled Money Printing
Quantum Wallets
$
$
Quantum Validation at Transaction
Decoherence Protection / Revocation Protocol

*Fig. 3. Quantum Money Lifecycle.*

Our approach to methodology is focusing on economics: weigh energy savings against R&D costs. Interdisciplinary: It bridges quantum physics, computer science, and economics. (Figure 4.). This approach ensures your review is data-driven while addressing the "So what?" for economists and policymakers.

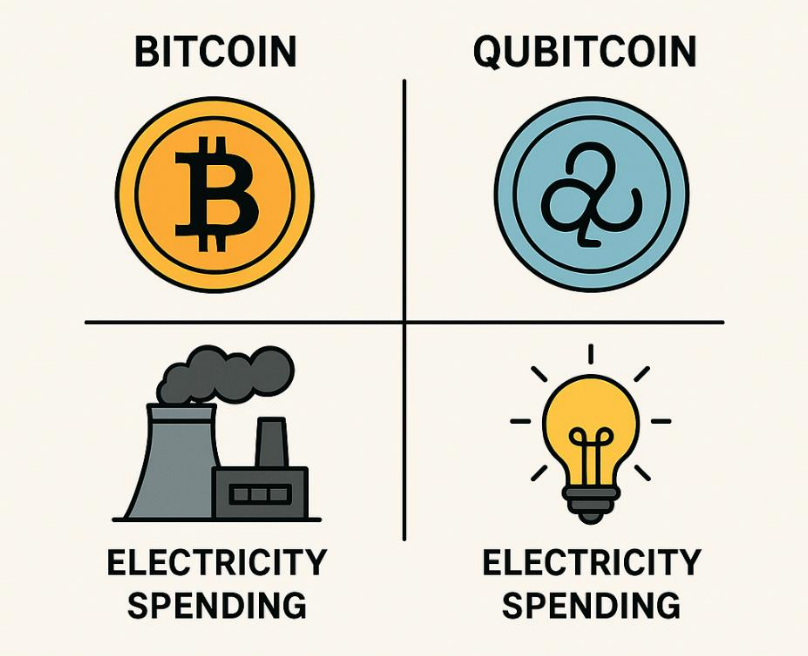

*Fig.4. Economic advantage of qubitcoins*

**Instead of conclusion:**

The integration of quantum computing into cryptocurrency systems presents a paradoxical future—simultaneously disruptive and evolutionary. The "quantum cryptocurrency era" will not arrive abruptly but through phased adoption—first as a defensive tool against quantum threats, later as a transformative monetary system. Economies that navigate this transition proactively will reap rewards; those that delay face existential risks. We should add to this summary some interesting remarks such as that: "Unclonable quantum states enable unforgeable money, but require quantum memory for storage"; Publicly verifiable quantum money avoids centralized banks but remains experimentally infeasible"; Large-scale quantum computers may demand 1–10 MW, comparable to small data centers", etc.

**Case Study: Hypothetical Quantum Laundering Scheme**

A Hypothetical Quantum Laundering Scheme of crypto money refers to a theoretical scenario where quantum technologies are used to obfuscate or anonymize illicit cryptocurrency funds beyond the capabilities of classical tracing tools. This idea blends principles from quantum computing, quantum communication, and cryptography, and should be seen as a specific academic exercise—not a practical guide or endorsement of illegal activity.

Quantum laundering would exploit quantum properties to evade traditional blockchain tracking: Superposition: A transaction could exist in multiple possible states; Entanglement: Funds or identities could be correlated across distant accounts or nodes; Quantum teleportation: Information (e.g., keys or transaction data) could be "moved" without traversing the network visibly.

Structure of hypothetical quantum laundering should be based on a network of quantum nodes capable of: Receiving crypto funds in classical form (e.g., Bitcoin or Ethereum); Converting these to quantum-encoded assets (like Qubitcoins or quantum tokens) and Splitting the funds across multiple entangled accounts in superposition. At final stages, the quantum asset is converted back to classical crypto at clean wallets where each wallet is generated and is unlinkable to the original. Imagine a laundering system that doesn't just hide your money — it makes it exist in multiple places, unlinkable identities, and can teleport through the network without ever showing its face. This quantum laundering scheme would be like a Heisenberg black market—you can't know where it is *and* where it came from at the same time If we will precisely look on a System Architecture and Protocol Flow we will see that quantum mixers are operating as a *Quantum Obfuscation Network (QON)* (Fig.5), where at the stage one the Classical-to-Quantum Conversion, and at the stage two Entanglement-Based Obfuscation were performed. The evasion techniques and Obfuscation Logic of this kind of performance include some steps: Qubits are measured in rotating bases — makes reverse tracing impossible, Wallets are cross-entangled, so no single path can be tracked, Funds don't "move" linearly in time; they're spread probabilistically, Each movement is a non-copy, non-local action – no record on the network, and A possible quantum zero-knowledge proof verifying only that laundering is *complete*, not how it happened.

At the same time evasion technology ensures the anti-traceability of the transaction based on Quantum Mixes (Q-Mix) Dynamic Entanglement Cascades Quantum Zeno Effect for Timing Jitter Teleportation Chains Quantum Proof-of-Anonymity.

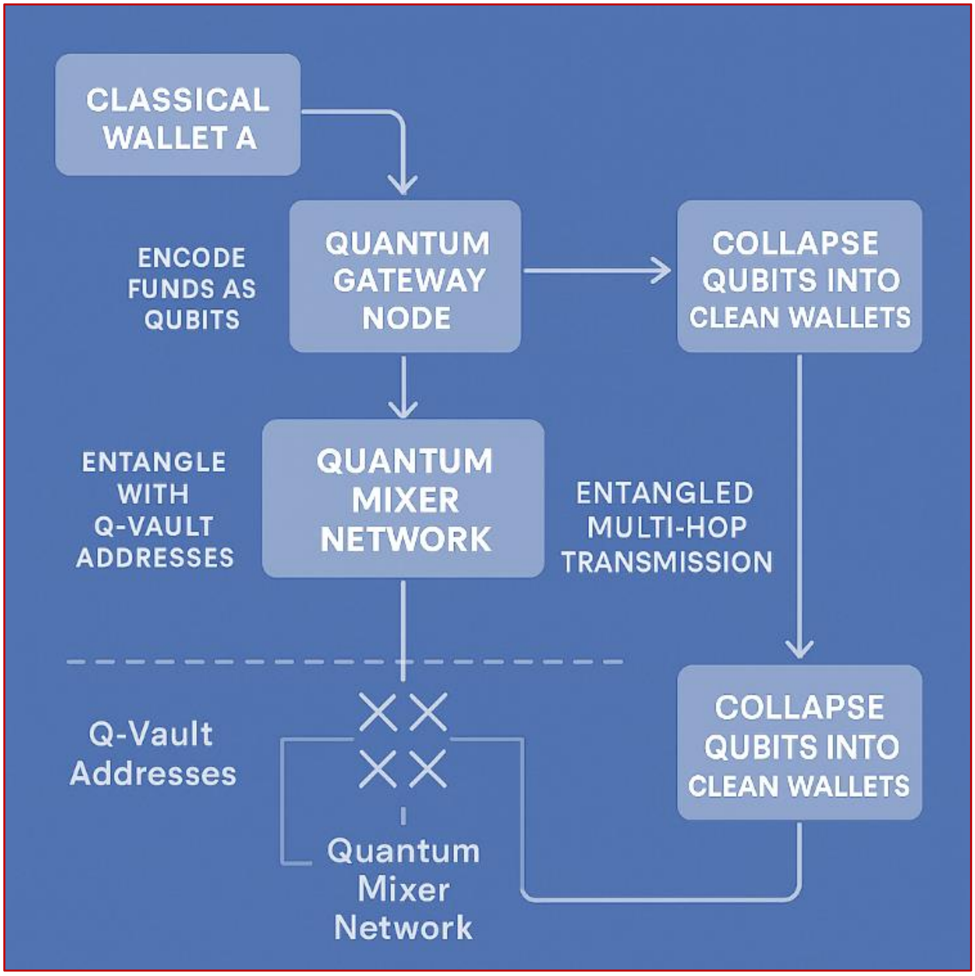
CLASSICAL WALLET A
QUANTUM GATEWAY NODE
ENCODE FUNDS AS QUBITS
COLLAPSE QUBITS INTO CLEAN WALLETS
ENTANGLE WITH Q-VAULT ADDRESSES
QUANTUM MIXER NETWORK
ENTANGLED MULTI-HOP TRANSMISSION
Q-Vault Addresses
Quantum Mixer Network
COLLAPSE QUBITS INTO CLEAN WALLETS

*Fig.5. Quantum Obfuscation Network (QON)*

**Conclusion for case study**

Quantum computing could supercharge money laundering through unbreakable anonymity but also enable hyper-transparent ledgers via quantum auditing. The outcome depends on who deploys the technology first—criminals or regulators.

## References:

1. Renato P. dos Santos, Quantum Information Science, IEEE Internet Computing 2022, 8 p
2. Kervalishvili P. J. Quantum information science: some novel views. In book Information and Computer Technologies. Nova Publishing, USA. 2012 pp 114-132
3. Paata Kervalishvili, Dimitris Tseles, Quantum information: philosophy and technology, September 2016, , International Scientific Conference eRA – 11, ISSN-1791-1133, 14p.
4. P. Kervalishvili, S. Michailidis. Philosophy and synergy of information. NATO Science series, IOS press, v.93, 2012. 285p.
5. Zurek, W. H. Decoherence, einselection, and the existential interpretation. Philosophy of Science, 2003. 70(5), 720-731.
6. Paata Kervalishvili, Quantum Information Technology and Quantum Sensory Systems

Development, Journal of Internet Technology and Secured Transactions (JITST), Volume 4, Issue 4, December 2015, 430-443.

7. Paata J. Kervalishvili, Quantum information technology: Theory and applications. Published in: 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS), IEEE Xplore: 04 February 2016, ISBN Information: INSPEC Accession Number: 15756870. DOI: 10.1109/IntelCIS.2015.7397187, Publisher: IEEE. 15p.
8. Paata J Kervalishvili. Leptons Based Quantum Computing. Acta Scientific, Computer Sciences. Published: June 23, 2023; Volume 5 Issue 7: 12-14.
9. Soni, L., Chandra, H., Gupta, D.S. et al. Quantum-resistant public-key encryption and signature schemes with smaller key sizes. Cluster Comput 27, 285–297 (2024). https://doi.org/10.1007/s10586-022-03955-y.
10. National Institute of Standards and Technology (NIST). Post-quantum cryptography standardization. 2022, Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography.
11. The quantum computer and its implications for public-key crypto systems, Security of the present-day public key primitive, Entrust datacard, White paper, 2019, 16p.
12. P. W Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In S. Goldwasser, ed., Proceedings of the 35th Symposium on Foundations of Computer Science, Santa Fe, NM, 20{22 November, Los Alamitos, CA: IEEE Computer Society Press 124{134, 1994.

13. L. K. Grover, “A Fast Quantummechanical Algorithm for Database Search”. in Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, (New York: ACM 1996) 212{219, 1996.

14. Micciancio, D., & Regev, O. Lattice-based cryptography. In Post-quantum cryptography,. Springer Berlin Heidelberg. 2009. (pp. 147-191).

15. Manjula Gandhi Selvaraj, Chaitrali Mulay, Karthiganesh Durai et al. (16 authors), Quantum blockchain: Trends, technologies, and future directions, IET Quantum Communication, December 2024, 5(4):516-542, Wiley, DOI:10.1049/qtc2.12119

16. Itan Barmes, Bram Bosch and Olaf Haalstra, Quantum computers and the Bitcoin blockchain, Delloite, 2025. For information, contact Deloitte Global.

17. Scott Aaronson, Quantum Computing Since Democritus, Publisher Cambridge University Press, April 29, 2013, 398p.

18. Benoit Morenne, "Machines That Shop for Themselves Promise to Save Time and Money". Wall Street Journal. 7 April 2021. ISSN 0099-9660. Archived from the original on 28 April 2021. Retrieved 24 April 2021.

19. Scott Aaronson, Paul Christiano. Quantum Money from Hidden Subspaces. Cryptology ePrint Archive, 2012, 46p.

20. S. Wiesner, Conjugate coding, Conjugate coding. SIGACT News, 15(1), 1983, 78-88. https://doi.org/10.1145/1008908.1008920.

21. B.T. Geetha, R. Viswanathan, Sulay N Patel, M.A. Mukunthan, Sushil Jindal, Communication Networks: New Directions In Cybersecurity Hybrid Quantum-Classical, Nanotechnology Perceptions 2024, 20 No. S12 632-645.

22. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, 9p. www.bitcoin.org.

23. Alagic G, et. al. Status Report on the Third Round of the NIST Post-Quantum Cryptography, Publication Date(s) July 2022 (includes updates as of 09-26-2022), URL/DOI https://doi.org/10.6028/NIST.IR.8413-up.

24. F Wu, B Zhou, J Jiang, T Lei. Blockchain Privacy Protection Based on Post Quantum Threshold Algorithm. CMC/ Vol.76, No.1, 2023/ 10.32604/cmc.2023.03877.

25. IBM United States What Is Quantum Computing? Jun 10, 2025. https://www.ibm.com › think › topics › quantum-computing.

26. McKinsey & Company. The energy challenge in quantum computing. 2023. Retrieved from https://www.mckinsey.com/industries/semiconductors/our-insights/the-energy-challenge-in-quantum-computing.

27. D-Wave Quantum. The first and only quantum computer built for business. 2024. https://www.dwavequantum.com › media › htjclcey.

28. FATF 2023/24 report: crypto compliance risks & gaps. Crypto Regulations | March 25, 2025.

29. Anne Broadbent; Raza Ali Kazmi; Cyrus Minwalla et al. A Quantum Vault Scheme for Digital Currency. 2024 IEEE International Conference on Quantum Computing and Engineering (QCE), Date Added to IEEE Xplore: 10 January 2025.