Enhancing Usable Security and Privacy of Cryptocurrencies in the Quantum Age

Samuel T. Oakes
Sacred Heart University
oakess2@mail.sacredheart.edu

1. Introduction: Where Decentralization, Usability, and Quantum Risks Collide

When Bitcoin was introduced in 2008, it launched more than just a digital currency—it introduced an entirely new financial philosophy. This vision revolved around decentralization: a system where people could transact freely, without relying on traditional banks or institutions. At the heart of this innovation is cryptography—a way to ensure trust and integrity through code rather than people [22].

Fast forward to today, and cryptocurrencies have grown into a global industry. Billions of dollars are stored on blockchains, and millions of users engage with these systems daily. But behind the innovation lies a set of challenges that are becoming harder to ignore.

First, decentralization, while empowering, shifts responsibility onto users in ways many aren't prepared for. In a bank, if you forget your password, you reset it. In crypto, if you lose your private key, your money is gone—forever [3, 21]. The promise of financial independence comes with a steep learning curve and a high risk of user error.

Second, there's a major misunderstanding around privacy. Many assume cryptocurrencies are anonymous. But in reality, most blockchains are transparent by design. Every transaction is public, and with enough analysis, it's often possible to link wallet addresses to real people [3, 5].

Now add quantum computing into the mix. Though it's still developing, quantum computers have the potential to break the cryptographic foundations that secure cryptocurrencies. Algorithms like Shor's can reverse-engineer private keys from public ones—something that would devastate current blockchain systems [13, 16, 18]. Worse yet, attackers can already start collecting public keys and encrypted data today, with plans to decrypt them once quantum technology matures. This "Harvest Now, Decrypt Later" threat turns quantum computing from a future problem into a present concern [17, 23].

This paper looks at how we can address these intertwined challenges—usability, privacy, and quantum security—while keeping crypto's core values intact. It explores what it would take to build a quantum-resistant cryptocurrency that is secure, private, and, most importantly, usable by regular people—not just experts.

2. The Building Blocks: Decentralization and Cryptography Explained

To understand the challenges cryptocurrencies face in a post-quantum world, we first need to understand how they work under the hood. At their core, blockchains are decentralized databases where no single entity has control. Instead, a network of participants collaborates to validate transactions, record them in blocks, and link those blocks together chronologically [2, 5, 22].

This system is powered by two main concepts: consensus and cryptography.

Consensus is how a decentralized group agrees on what's true. In Bitcoin, for example, the Proof of Work (PoW) algorithm forces miners to solve complex puzzles to add a block to the chain. This process makes it incredibly expensive to cheat. Newer blockchains like Ethereum 2.0 are switching to Proof of Stake (PoS), which uses financial incentives to reward good behavior and penalize bad actors [2, 5].

Cryptography, meanwhile, ensures that transactions are secure and verifiable. When you send someone cryptocurrency, you're not sending actual “coins”—you’re signing a digital message that says, “I authorize this transfer.” Your private key generates that signature, and anyone can verify it using your public key [4, 22].

The most common type of digital signature used in blockchains is based on ECDSA (Elliptic Curve Digital Signature Algorithm). It's fast, lightweight, and has served crypto well—so far.

But here’s the catch: quantum computers can break it.

Shor’s algorithm, once run on a powerful enough quantum computer, could derive private keys from public keys in a matter of minutes [13, 15]. This would make any exposed address a sitting duck. If you’ve ever made a transaction and exposed your public key—which is almost everyone—you’re at risk.

And while blockchains are designed to be immutable, their reliance on consensus makes change hard. You can't just "update the software" overnight. Every node has to agree. This means that migrating to quantum-resistant cryptography won’t be fast or simple—it will require coordinated efforts across the ecosystem, and users will play a key role in making that happen.

3. Usability Challenges: When Power Comes with Complexity

One of the biggest promises of cryptocurrency is putting users in full control of their money. But with that control comes complexity. Managing wallets, safeguarding private keys, navigating transaction fees—it’s all overwhelming for the average person.

Take private keys, for example. They’re essentially the passwords to your crypto wallet. But instead of a memorable string of characters, you get a 12- or 24-word recovery phrase. Lose it, and your funds are gone. No help desk. No recovery options. That level of responsibility is empowering, sure—but also unforgiving [3, 21].

Studies show that most people don’t store these recovery phrases securely. Some save them in phone notes, others take screenshots, and many forget to back them up at all. A single mistake can cost someone their entire savings [3].

Then there’s the issue of transaction complexity. On networks like Ethereum, you need to calculate gas fees—payments to miners that vary based on demand. Send too little, and your transaction fails. Send too much, and you overpay. That’s a tough balancing act for anyone unfamiliar with the system.

As we shift toward quantum-resistant cryptography, things will only get more complicated. The new algorithms often require larger keys and longer processing times. Wallets will need to be updated, funds migrated, and users educated on what these changes mean. Without thoughtful design, these updates could push people away from crypto rather than welcoming them in.

4. Privacy Risks in Post-Quantum and Traditional Cryptocurrencies

Many people think Bitcoin is anonymous. It's not. Every transaction is recorded on a public ledger, visible to anyone. While wallets are identified by random strings—not names—that pseudonymity is paper-thin. With enough effort, it's surprisingly easy to trace transactions back to real people [3, 5, 21].

This lack of privacy has real consequences. Imagine if all your financial transactions were visible to the world—every coffee you bought, every donation you made. That's the reality of using traditional cryptocurrencies. And with companies specializing in blockchain analysis, users are more exposed than they think [5].

Some cryptocurrencies, like Monero and Zcash, are built for privacy. They use clever math—like ring signatures and zero-knowledge proofs—to hide transaction details. But these tools aren't easy to use, and they face regulatory pressure in some countries [5, 21].

Quantum computing adds another wrinkle. If cryptographic protections are broken, even private transactions could be exposed retroactively. That means today's transactions may not be private tomorrow. It's a ticking clock.

In a post-quantum world, privacy tools must become the default—not the exception. Users shouldn't need a PhD in cryptography to protect their data. Wallets should guide them with simple language and default to privacy-preserving settings. That's the only way to ensure financial freedom remains safe and private.

5. The Quantum Threat: What Happens When the Rules Change?

Quantum computers don't work like the laptops or smartphones we use today. They rely on principles of quantum mechanics to solve certain types of math problems dramatically faster than classical machines. That sounds abstract—but it has very real consequences for cryptocurrencies.

The main threat comes from Shor's algorithm. It's a quantum algorithm that can quickly factor large prime numbers—a problem that underpins the security of widely-used cryptographic systems like RSA and ECDSA. If someone runs Shor's algorithm on a sufficiently powerful quantum computer, they can derive private keys from public keys. That would allow them to forge signatures and steal funds [13, 15, 17].

The second major algorithm is Grover's, which speeds up search problems. It reduces the security of hash functions like SHA-256 by half. So while it doesn't break hashing completely, it weakens the security guarantees that make blockchains immutable [16, 18].

The scariest part? Attackers can collect encrypted or public key data now and just wait until quantum computers catch up. This is the "Harvest Now, Decrypt Later" strategy—and it's already happening [17, 23].

All of this means that quantum computing isn't just a future threat. It's a present one. And the crypto community needs to start acting like it.

6. The Road to Post-Quantum Cryptography (PQC)

Thankfully, researchers have been working on quantum-resistant cryptography—algorithms that can stand up to quantum computers. These include lattice-based systems like Dilithium, hash-based systems like SPHINCS+, and others based on code theory or multivariate polynomials [10, 15, 18].

These algorithms are promising, but they come with trade-offs. They're often bulkier, requiring more storage and processing power. Signatures and keys can be 10x larger than what we use today. That affects everything from transaction size to network bandwidth.

NIST has already selected some PQC algorithms for standardization, and some projects are starting to integrate them. But the transition won't be simple. Blockchains can't just "flip a switch." They'll need to support both legacy and PQC systems during a transition period—using hybrid signatures or sidechains to test and roll out new methods [17, 23].

Most importantly, the user side of this migration must be frictionless. Wallets should provide automated upgrades, clear messaging, and secure ways to move funds. If we get this wrong, we risk mass confusion—or worse, mass loss of funds.

7. Designing for Humans: The Key to a Quantum-Resistant Future

All the cryptographic brilliance in the world means nothing if users can't understand or use the tools. Usability must be built into the foundation of crypto systems—not added as an afterthought.

7.1 Usable Security and Privacy

Wallets should make secure behavior the default. Use strong encryption. Rotate addresses. Back up seed phrases. But don't expect users to do it manually. Automate it. Hide the complexity. Let users benefit from best practices without needing to configure anything [21, 22].

7.2 Making Migration and Recovery Foolproof

When it's time to move to PQC wallets, the process needs to be seamless. Think onboarding wizards, visual indicators, and checklists. And for recovery, ditch the fragile 24-word seed phrase. Let users opt into social recovery or threshold wallets, where trusted friends or devices can help restore access [21].

7.3 Testing with Real People

Crypto has a habit of designing for developers, not end-users. That has to change. New tools should be tested with people from diverse backgrounds—people with different devices, internet speeds, languages, and technical skills. Build with empathy.

7.4 Inclusive by Default

If crypto is for everyone, it needs to work for everyone. That means screen-reader compatibility, multi-language support, and interfaces that function on low-bandwidth connections. Don't assume your users are experts with the latest tech. Build for the margins.

7.5 Educate in the Flow

Users shouldn't need to read a whitepaper to use a wallet. Embed short tooltips, gamify secure actions (like "backup completed!" badges), and guide people as they interact with the product. Learning should happen as part of using the system—not as a prerequisite.

8. Conclusion: Can Quantum-Resistant Cryptocurrencies Balance It All?

So where does that leave us? Can we really build a cryptocurrency that's quantum-safe, private by default, and easy enough for everyone to use?

Yes—but only if we're intentional about it. Quantum-resistant algorithms are already here. The building blocks for privacy exist. And we know how to design great user experiences. The missing piece is commitment.

Crypto's next chapter doesn't just depend on better math. It depends on better design, better defaults, and better communication. If we make the right choices now, we can build systems that empower users instead of intimidating them—and protect them in a world where quantum computers are no longer science fiction.

In the end, it's not just about securing blockchains. It's about securing trust, agency, and access for the people using them. That's the future worth building

References

1. 891500a132.pdf - Exchange of Preparatory Information for Secure and Usable Cryptocurrency Transactions
2. 165023T.pdf - Security and privacy policies of blockchain and cryptocurrency
3. TheOtherSideOfTheCoin.pdf - The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy
4. AReviewonCryptocurrenciesSecurity.pdf - A Review on Cryptocurrencies Security
5. Security_sensors-23-03155.pdf - Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments
6. the-challenge-of-cryptocurrency-in-the-era-of-the-digital-revolution-a-review-of-systematic-literature.docx-1.pdf - The Challenge of Cryptocurrency in the Era of the Digital Revolution: A Review of Systematic Literature
7. 08470240.pdf - Is Blockchain in Our Future?
8. ssrn-3132235.pdf - Quality Certification and Market Transparency with Decentralized Information Management
9. cryptography-02-00010.pdf - ReSOLV: Applying Cryptocurrency Blockchain Methods to Enable Global Cross-Platform Software License Validation
10. A_Secure_Cryptocurrency_Scheme_Based_on_Post-Quantum_Blockchain.pdf - A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain
11. bmss.pdf - A study on the use of quantum computers, risk assessment and security problems
12. Paper18902.pdf - Enhancing Cyber Security Using Quantum Computing and Artificial Intelligence: A Review
13. A_Review_of_Quantum_Cybersecurity__Threats__Risks_and_Opportunities.pdf - A Review of Quantum Cybersecurity: Threats, Risks and Opportunities
14. chapter_12_paper_9.pdf - Quantum Bitcoin: The Intersection of Bitcoin, Quantum Computing and Blockchain
15. 17-4039-blockchain-and-quantum-computing.pdf - Blockchain and Quantum Computing
16. Bachelor_Thesis.pdf - Impact of Quantum Computing on Cryptographic Systems and Blockchain Technology
17. Committing_to_quantum_resistance_A_slow_defence_fo.pdf - Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack
18. s41598-023-32701-6.pdf - Quantum-resistance in blockchain networks
19. TheImpactofQuantumComputingonCryptographicSystems.pdf - The Impact of Quantum Computing on Cryptographic Systems
20. 1604.01383v1.pdf - Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics
21. UsableCryptocurrencySystems.pdf - Usable Cryptocurrency Systems
22. bitcoin.pdf - Bitcoin: A Peer-to-Peer Electronic Cash System
23. A_Comprehensive_Tutorial_on_Cybersecurity_in_Quant.pdf - A Comprehensive Tutorial on Cybersecurity in Quantum Computing Paradigm