Quantum-Enabled Cybercrime: A Portfolio Analysis of Cryptocurrency Theft and Double-Spending

Zhen Li
Department of Economics and Management
Albion College, USA
Email: zli@albion.edu

Qi Liao
Department of Computer Science
Central Michigan University, USA
Email: liao1q@cmich.edu

***Abstract*—Research suggests that practical quantum computers capable of breaking current cryptographic systems may emerge within the next decade, posing a significant threat to cryptocurrencies. Quantum-capable adversaries could exploit this advantage to perform theft (by breaking digital signatures) and double-spending (by breaking hashing functions) attacks. This study examines the economically optimized strategies of such adversaries by modeling a portfolio of Bitcoin theft and double-spending attacks. We propose a novel quantum threat model and conduct simulations to evaluate the financial motivations of attackers and the resulting equilibrium prices under various threat scenarios. Our findings indicate that while early-stage quantum attackers may have short-term incentives, these incentives decline as their actions erode market confidence and cryptocurrency value, ultimately reducing future profitability. This self-defeating dynamic creates a natural economic threshold that helps stabilize the network in a post-quantum era.**

***Index Terms*—Cybercrime, Quantum Attacks, Cybersecurity Economics, Cryptocurrency and Blockchain, Cheating (Stealing and double-spending)**

I. Introduction

Cryptocurrencies such as Bitcoin rely on cryptographic primitives to secure transactions and maintain consensus across a global network of participants. Specifically, Bitcoin utilizes secure hashing algorithms such as SHA-256 within its Proof-of-Work (PoW) protocol for mining, and public/private key cryptography, i.e., digital signature schemes such as RSA (used primarily in SSL/TLS) and the Elliptic Curve Digital Signature Algorithm (ECDSA), for transaction authentication. Together, these cryptographic tools function as technical defense mechanisms, protecting the security and resilience of the blockchain network.

As we rapidly approach the quantum computing era [1], [2], IBM has announced plans to build the world's first large-scale, fault-tolerant quantum computer capable of running quantum circuits comprising 100 million quantum gates on 200 logical qubits by 2029 [3]. The impact of quantum computing technologies on cryptocurrencies and their underlying blockchain security is twofold.

First, while hashing is generally considered quantum-resistant, quantum computers can accelerate brute-force attacks on hash functions using Grover's algorithm [4], reducing complexity from $O(2^n)$ to $O(2^{n/2})$, or a quadratic speedup. Since Bitcoin's PoW relies on secure hashing (e.g., SHA-256), miners with quantum supremacy may gain unfair advantages. A quantum supremacy miner or a post-quantum miner (hereafter referred to simply as a quantum miner) could potentially reverse their own transactions after receiving goods or services, effectively duplicating value. Cybercriminals with sufficient quantum power to dominate block creation could cheat by double-spending their coins, having acquired majority computational power, i.e., executing a 51% attack.

Second, both RSA signatures (based on the integer factorization problem) and ECDSA (based on the discrete logarithm problem) are solvable in polynomial time using Shor's algorithm [5]. Since digital signatures are fundamental for proving ownership, quantum-powered cybercriminals could steal cryptocurrencies by forging valid transaction signatures.

While Bitcoin is widely regarded as cryptographically secure under classical computing assumptions, its PoW protocol inherently favors miners with greater computational power, thus increasing their ability to exploit critical vulnerabilities such as cryptocurrency double-spending [6]–[8] and cryptocurrency theft [9], [10]. This quantum advantage could enable attacks involving double-spending, private key recovery, and unauthorized control over users' funds, thereby threatening not only Bitcoin's integrity but also the broader credibility of cryptocurrencies [11].

Although these cryptographic vulnerabilities have raised growing concerns within the cryptocurrency and cybersecurity communities, technical feasibility alone does not fully determine real-world risk. The motivations of quantum-enabled cybercriminals, whether financially driven, state-sponsored, or ideologically malicious, play a pivotal role in assessing the actual threat landscape. Therefore, evaluating cryptocurrencies' resilience to quantum computing must go beyond cryptographic robustness to include economic and strategic dimensions. Understanding the incentive structures behind potential attacks is essential for accurately assessing the long-term viability of cryptocurrencies in the post-quantum era.

In this research, we take a unique approach and investigate the financial incentives of quantum attackers in the post-quantum era, focusing on two types of attacks: cryptocurrency theft and double-spending. We center our analysis on one cryptocurrency, namely Bitcoin. Although both attack types increase the amount of Bitcoins available to the attacker, they differ in their effects on the attacker's net holdings and on

979-8-3315-8969-1/25/$31.00 © 2025 IEEE

the broader asset distribution within the network. Double-spending is a form of transaction fraud that allows the same coin to be spent multiple times without altering the attacker's actual holdings. It does not reduce the assets of classical miners directly but instead undermines trust in the transaction history. In contrast, coin theft involves a direct transfer of Bitcoins from classical miners to the quantum attacker, thereby reducing the classical mining community's asset base while increasing that of the attacker.

We pose several key research questions: When a quantum-advantaged attacker can profit from both double-spending and stealing, what is the optimal mixture of the both strategies? How profitable are these attacks, especially as they scale? How do repeated attacks affect Bitcoin's market value, and what are the long-term implications for the distribution of Bitcoin between classical and quantum entities? To answer these questions, we first develop a pricing model to evaluate Bitcoin's value, incorporating the potential impacts of quantum attacks. We then extend this model to assess the financial consequences of double-spending and theft, allowing us to calculate the attacker's net gains by weighing benefits against the resulting loss in Bitcoin value. Building on this economic analysis, we simulate a dynamic environment in which the quantum attacker makes strategic decisions over time, optimizing the scale of double-spending and theft each period to maximize short-term profits.

Our findings suggest that while these attacks can yield immediate economic gains, they simultaneously undermine the long-term value of Bitcoin by damaging trust and market stability. Our simulation results show that quantum attackers can initially profit from their computational advantage. In the early stages of quantum attacks, the damage to Bitcoin's value and reputation is limited, incentivizing aggressive strategies such as large-scale double-spending and theft. However, as the attacker accumulates a larger share of the Bitcoin supply, the adverse market effects of the attacks become more pronounced. Over time, the declining market value of Bitcoin erodes the profitability of continued attacks. Eventually, the marginal cost of attack outweighs its benefit, and the attacker is incentivized to stop. In the long run, the system reaches a new steady state, one in which quantum-enabled attackers no longer find it economically rational to attack the network.

To the best of the authors' knowledge, this research is the first to consider both cryptocurrency theft and double-spending attacks in a post-quantum era from an economic perspective. The main contributions include a simulation of the evolving cryptocurrency ecosystem under the influence of profit-driven quantum miners. The findings shed light on the complex interplay between quantum capabilities, miner incentives, and cryptocurrency security. Notably, theft and double-spending create a self-defeating incentive structure: quantum attackers are motivated to preserve the value of the cryptocurrency in order to maintain their own wealth. This suggests that large-scale quantum attacks could eventually self-extinguish as their profitability diminishes. Our analysis implies that, paradoxically, the expansion of quantum attacks may lead to their own decline and a restoration of the structural integrity of the cryptocurrency ecosystem. These insights underline the importance of understanding the economic limits of quantum threats.

The remainder of the paper is organized as follows. Section II reviews the background and relevant literature. Section III presents our pricing model, which incorporates the effects of double-spending and theft, and outlines the decision-making process of a quantum attacker. Section IV provides simulation results and discusses the main findings. Finally, Section V concludes the paper and suggests directions for future research.

II. Background and Related Work

Public/private-key cryptography forms the backbone of modern digital security systems, including cryptocurrencies and blockchain networks. The advent of quantum computing [1]–[3] poses a proven threat to many public-key systems. Shor's algorithm demonstrates that a sufficiently powerful quantum computer can factor large integers in polynomial time, effectively rendering RSA insecure [5]. Building on this, it has been estimated that a fault-tolerant quantum computer with approximately 20 million physical qubits could factor a 2048-bit RSA key within hours [12]. Similarly, Shor's algorithm can also solve the discrete logarithm problem in polynomial time, suggesting that quantum computers could completely break modern public/private-key digital signatures such as RSA and ECDSA [11], which serve critical roles in securing ownership and authorizing transactions in cryptocurrencies including Bitcoin. Furthermore, quantum computing may significantly accelerate brute-force attacks against cryptographic hash functions such as the Secure Hash Algorithm (SHA), using Grover's algorithm [4], by reducing the complexity from 2^n to $\sqrt{2^n}$ or a quadratic speedup.

While practical quantum computers remain largely theoretical today, the concept of "store now, decrypt later" raises immediate concerns. Attackers could archive blockchain data and target previously used addresses once quantum hardware matures. It is imperative to address this risk, particularly given the immutability of the blockchain, which permanently records public key exposures in its ledger [13]. Estimates suggest that practical quantum attacks on Bitcoin's ECDSA could become feasible within the next decade, assuming optimistic advances in fault-tolerant quantum hardware [14].

Quantum computers could empower early adopters with overwhelming capabilities. Most cryptocurrencies are designed to be decentralized. Drawing from Byzantine Fault Tolerance (BFT) theory, a distributed system remains secure only if faults or malicious actors affect fewer than a specific threshold [15]. Once a miner or coalition surpasses half of the network's hash power, it becomes capable of executing a 51% attack, reversing transactions and compromising ledger integrity [16]. Under certain conditions, even less than 51% of the hash rate may suffice to launch such attacks [17].

Double-spending [18] is the most direct way to monetize control over a majority hash rate [6], and such attacks can be profitable even at lower levels of hash power under specific

economic assumptions [19]. The rise of quantum computing could enable attackers to generate fraudulent transactions and steal coins directly from exposed addresses before the network confirms the original transaction [11]. Since quantum computing effectively breaks current digital signatures, cryptocurrency theft may become trivial [9], [10].

Quantum computers are expected to offer exponential speedups over classical machines [2], posing significant risks to core components of blockchain protocols and cryptocurrencies [9], [20], [21]. While quantum advantage may not make mining trivial, it could lead to network centralization, particularly during the transitional period when classical and quantum miners coexist [22]. The most immediate quantum threat lies in the vulnerability of ECDSA signatures [23]. While Bitcoin's security already suffers from malware, such as keyloggers, phishing schemes, and clipboard hijacking used to extract private keys [24], quantum computing introduces additional vulnerabilities that facilitate theft and double-spending attacks.

The technical vulnerabilities introduced by quantum computers have been widely studied. A parallel line of research investigates mitigation techniques against quantum-enabled miners, for example by slowing down or phasing in post-quantum-resistant mechanisms [25]. Beyond technical defenses, the economic incentives of quantum attackers are also crucial for evaluating the likelihood and persistence of quantum attacks. Recent research on the economics of cybercrime has emphasized how attackers make rational decisions by weighing potential gains against associated costs and risks [26]. Within the cryptocurrency domain, studies have focused on financial motivations behind specific attacks such as double-spending, theft, and market manipulation, demonstrating that attackers behave as profit-maximizing agents [27]. These analyses reveal that the prevalence and success of cybercrimes are tightly linked to the incentive structures embedded in digital ecosystems. For example, economically motivated cybercrimes like cryptocurrency pump-and-dump schemes can severely destabilize markets, with long-lasting effects on asset stability [28]. Additionally, the efficiency of cryptoasset investigations can be improved by linking related cases, underscoring the importance of robust and coordinated investigative techniques in addressing financially driven cybercrimes within the cryptocurrency ecosystem [29].

Specifically regarding quantum computing, several studies model quantum miners as rational, profit-seeking agents interacting within the Bitcoin network. These analyses suggest that despite the asymmetric computational advantage offered by quantum technologies, the economic impact of attacks may be self-limiting. For instance, executing a 51% attack can depress Bitcoin's market value, ultimately diminishing the attacker's own wealth [16]. Similarly, persistent quantum-enabled attacks are found to erode market confidence and reduce Bitcoin's capitalization over time, thereby diminishing the incentives for continued exploitation [7], [8].

In particular, the existing literature on the economics of quantum attacks focuses solely on double-spending, investigating the optimal scale of such attacks and analyzing competition or collusion among quantum miners through game-theoretic models. This research advances that literature by (i) integrating both theft and double-spending within a unified framework, and (ii) situating the analysis in the quantum-mining context, introducing the novelty of theft integration and a more detailed equilibrium taxonomy. It proposes a comprehensive simulation framework for post-quantum cryptocurrency attacks. By synthesizing existing research across quantum computing, cryptocurrency and blockchain, and cybersecurity economics, our work offers a holistic understanding of quantum threats.

TABLE I: Variables and Definitions

Symbol	Definition
B	Bitcoin supply
B_q	Bitcoin asset of the quantum miner
m	Newly mined Bitcoin
m_q	Bitcoin newly mined by the quantum miner
D	Scale of double-spending
S	Scale of stealing
P_B	Equilibrium Bitcoin price without double-spending or stealing
P_D	Equilibrium Bitcoin price with only double-spending
P_S	Equilibrium Bitcoin price with only stealing
P_{DS}	Equilibrium Bitcoin price with both double-spending and stealing
P_{ds}	Risky Equilibrium Bitcoin price with double-spending and stealing
w_d	Success rate of double-spending
w_s	Success rate of stealing
P	Overall price level of goods and services traded in Bitcoin
Y	Quantity of items traded using Bitcoin as medium of exchange
V	Velocity of Bitcoin, frequency at which Bitcoin is used to pay
T	Units of Bitcoin used as medium of exchange
n	Total miner population

III. Model of Cryptocurrency Cheating by Quantum Miner

In this section, we develop an economic framework to analyze the financial incentives that may drive quantum-capable adversaries to initiate cryptocurrency (i.e., Bitcoin) theft and double-spending attacks. Central to this analysis is the role of Bitcoin's market price, which fundamentally shapes the economic behavior of all participants, including rational attackers. The primary theoretical challenge lies in the pricing of Bitcoin itself, which remains a complex and evolving topic in the literature.

To address this, we construct a pricing model grounded in the classical quantity theory of money, supplemented by a market-based supply-and-demand framework specific to cryptocurrency dynamics. This hybrid model captures the interplay between Bitcoin's fixed issuance schedule and fluctuating market demand, providing a baseline for understanding its valuation under normal conditions.

We then extend the model to quantify the economic impact of adversarial actions, specifically, how Bitcoin theft and double-spending affect Bitcoin's effective circulating supply, alter perceived market stability, and ultimately influence price formation. These attack vectors introduce exogenous shocks to both supply and demand dynamics, thereby creating feed-

back effects that may either amplify or mitigate the financial incentives for further exploitation.

For clarity and ease of reference, Table I presents a list of the key variables/symbols employed throughout the models and their definitions.

A. Financial Incentives and Role of Market Value

Participation in the Bitcoin network is driven by a variety of incentives, which vary depending on the participant's role, such as miner, node operator, developer, investor, or service provider. Each class of participant contributes to the functionality and security of the decentralized system, and in return, receives different forms of value: financial, technological, or ideological. Among these, financial incentives are among the most significant, particularly for those involved in the validation and security of the blockchain, such as miners.

The economic appeal of Bitcoin stems in large part from its fixed and algorithmically enforced supply cap of 21 million coins. This programmed scarcity stands in contrast to fiat currencies, which are subject to discretionary monetary expansion by central banks. Bitcoin's deflationary design supports its position as a store of value and inflation hedge. Preserving Bitcoin's scarcity, decentralization and security is critical to maintaining market confidence and network participation. If these foundational attributes were to be compromised, the financial incentives for network participants would diminish, potentially undermining the system's stability. This necessity for preservation explains the network's strong social and technical resistance to inflationary changes and unvetted protocol upgrades.

Miners, as the primary security providers in the Bitcoin ecosystem, are incentivized through two main revenue streams: block rewards and transaction fees. The block reward, currently set at 3.125 Bitcoins following the 2024 halving, compensates miners for successfully appending new blocks to the blockchain. In addition, miners earn transaction fees from users whose transactions are included in these blocks. This is especially true after diminishing mining rewards designed in the protocol. Together, these income sources justify the significant capital expenditures miners incur for specialized hardware and electricity consumption.

Beyond immediate revenues, miners may also be financially motivated to retain the Bitcoin they earn, anticipating long-term price appreciation. This speculative holding strategy, if realized, can significantly increase their cumulative profits. More importantly, it aligns miner behavior with the long-term value proposition of the network: the stronger the market price of Bitcoin, the greater the incentive to continue mining and supporting the protocol. This alignment reinforces network security by encouraging sustained and honest participation.

Accordingly, the dominant financial incentive across roles in the Bitcoin network, whether through mining, investing, or infrastructure provisioning, ultimately depends on Bitcoin's market valuation. Regardless of whether miners liquidate their earned coins or hold them for speculative gain, their profitability is directly linked to the prevailing price of Bitcoin. This interdependence is particularly important in the context of emerging threats, such as quantum attacks, which could compromise the security of the blockchain if economically justified.

In the subsequent economic analysis of a quantum miner's strategic decision-making, we focus on the critical role of Bitcoin's market price. To isolate the effect of price, we adopt a simplified model that excludes transaction fees and mining/attack cost. Under these assumptions, both the potential benefits of successful attacks and the opportunity costs associated with attacks as functions of Bitcoin's market value. As such, fluctuations in the price of Bitcoin become the primary determinant of the economic feasibility and scale of attacks by financially motivated adversaries.

B. Quantity Theory of Bitcoin

The Quantity Theory of Money (QTM) is an economic theory that explains the relationship between the money supply and the price level in an economy. It is most commonly expressed using the equation of exchange:

$$MV_m = P_m Y_m \tag{1}$$

where M is the money supply, V_m is the velocity of money (how frequent a unit of currency is spent), P_m is the price level of goods and services, and Y_m is the quantity of goods and services exchanged. The theory posits that the total amount of money spent in an economy (MV_m) is equal to the total value of goods and services sold ($P_m Y_m$). Under the classical assumption that V_m and Y_m are relatively stable, any increase in the money supply will lead to a proportional increase in the price level.

In the context of Bitcoin or other cryptocurrencies, the QTM can be adapted as follows:

$$TV = P_{BTC} Y \tag{2}$$

where T is the quantity of Bitcoin used for transactional purposes, V is the velocity of Bitcoin (how often Bitcoin is transacted), P_{BTC} is the price of goods and services in Bitcoin, and Y is the volume of real economic transactions using Bitcoin. In this formulation, Bitcoin serves as the monetary unit used to price goods and services.

When expressed in fiat terms, and treating Bitcoin as a medium of exchange for digital payments, its monetary dynamics can be captured by the following quantity equation::

$$P_B TV = PY \tag{3}$$

Here, P_B denotes the fiat-denominated market price of Bitcoin. On the right-hand side, P stands for the general price level of goods and services traded in Bitcoin (also in fiat terms), hence both sides are equal to the market value of transactions conducted using Bitcoin in fiat terms.

It is important to emphasize that both P_B and P are measured in fiat currency units (e.g., USD), reflecting Bitcoin's exchange value and its purchasing power relative to conventional goods and services.

C. Quantum Attack-free Bitcoin Price

In equation (3), T is accurately interpreted as the "Bitcoin in use" rather than the "desire to use Bitcoin." That is, T reflects the effective circulating quantity of Bitcoin employed for transactional purposes, but does not directly capture transactional demand. It captures actual usage rather than latent or unexpressed demand. Nevertheless, for analytical tractability, we assume that the observed use of Bitcoin adequately reflects the underlying demand for it as a medium of exchange. Under this simplification, the volume of Bitcoin needed for transactional purposes is treated as equivalent to the real transactional demand, which can be expressed as follows:

$$T = \frac{PY}{P_B V} \tag{4}$$

Let B denote the total quantity of Bitcoin in circulation (i.e., the real supply of Bitcoin). The equilibrium in the Bitcoin market is characterized by the condition that:

$$B = T = \frac{PY}{P_B V} \tag{5}$$

Solving (5), the equilibrium Bitcoin price is

$$P_B = \frac{PY}{BV} \tag{6}$$

As indicated by the pricing formula, the price of Bitcoin rises with increasing demand and falls with an expanding supply.

For analytical simplicity, we hold Bitcoin demand constant (i.e., P, Y, and V are all exogenous) and allow only the supply to vary. Bitcoin supply grows through the mining process, where new coins are created as rewards for miners who validate transactions and secure the network. This issuance is governed by Bitcoin's underlying protocol, which ensures a predictable and gradually declining rate of coin creation. Ultimately, the total supply of Bitcoin is capped at 21 million BTC, a limit expected to be reached around the year 2140 [30], [31]. Consequently, the Bitcoin supply curve is asymptotic in nature, with the majority of coins mined early in the network's life and the rate of issuance slowing over time.

In a dynamic setting, the evolution of Bitcoin's supply can be expressed as:

$$B = B_{-1} + m \tag{7}$$

where B denotes the total Bitcoin in circulation in the current period, B_{-1} represents the total Bitcoin from the previous period, and m is the amount of newly mined Bitcoin added in the current period. The value of m decreases over time due to the halving mechanism embedded in the Bitcoin protocol.

D. Effects of Theft and Double-spending on Bitcoin price

Let D be the scale of double-spending, which increases Bitcoin supply from B to $B + D$, similar to counterfeit currency that injects unauthorized money into circulation. The market price of Bitcoin with double-spending is

$$P_D = \frac{PY}{(B + D)V} \tag{8}$$

Apparently, double-spending decreases the market value of Bitcoin, i.e., $P_D < P_B$.

Unlike double-spending, there is no straightforward or natural method to incorporate coin theft into the Bitcoin pricing model. Theoretically, large-scale Bitcoin theft, especially through the compromise of digital signatures by quantum attacks, can significantly erode the cryptocurrency's perceived value, even if the protocol itself remains technically intact. Bitcoin derives much of its value from trust in its security, including its resistance to unauthorized access and fake ownership. If theft becomes frequent or is associated with systemic vulnerabilities, such as those posed by quantum computing, market participants may lose confidence in Bitcoin, or cryptocurrency in general, as a store of value and shift their capital to alternative, more secure assets, thereby exerting downward pressure on its price.

For instance, if a quantum adversary successfully compromises high-value, dormant wallets (e.g., those belonging to early miners) and rapidly liquidates the stolen coins, the resulting sell pressure could cause a substantial price drop. In such a scenario, market dynamics may become self-fulfilling: the more market participants believe Bitcoin is no longer secure, the more they sell, accelerating the price decline. A successful quantum-based theft could thus trigger a broader crisis of confidence in the ecosystem.

Importantly, Bitcoin's value is not solely embedded in its code or scarcity. It also depends on the belief that it is secure, predictable, and resistant to future threats. Undermining this belief compromises Bitcoin's economic utility and market valuation.

The following formula captures how the negative impact of coin theft can be modeled in terms of its effect on Bitcoin price:

$$P_S = \frac{(1 - \frac{S}{B})PY}{BV} \tag{9}$$

where S denotes the scale of stealing and $\frac{S}{B}$ represents the reduction in effective Bitcoin demand, measured as the proportion of total stolen Bitcoin relative to the total Bitcoin in circulation. As the expression indicates, an increase in theft leads to a decrease in Bitcoin's price by undermining market confidence and perceived security.

In summary, both double-spending and theft exert downward pressure on the price of Bitcoin, albeit through different mechanisms. In a nutshell, double-spending reduces Bitcoin's price by effectively increasing the circulating money supply, while stealing lowers the price by diminishing market demand, as it erodes user confidence in Bitcoin's security. By combining Equations (8) and (9), we incorporate the effects of both double-spending and coin theft into an extended Bitcoin pricing model as follows:

$$P_{DS} = \frac{(1 - \frac{S}{B})PY}{(B + D)V} \tag{10}$$

E. Uncertainty in Quantum Attacks

The outcomes of cyberattacks are inherently uncertain. Their success depends on a complex interplay of factors

involving both the attacker's capabilities and the target's defenses, specifically, how effectively the attacker exploits vulnerabilities versus how robustly the system detects, mitigates, or prevents such exploits. In the context of quantum attacks, its advantages in cryptocurrency-related attacks manifest differently in double-spending and coin theft, both in nature and in feasibility.

Double-spending refers to the act of spending the same digital coins more than once by exploiting weaknesses in the network's consensus mechanism, e.g., the disproportionate hashing power enabled by quantum computing, and potentially enabling an attacker to outpace honest miners and execute a 51% attack to rewrite blockchain history. However, due to the quantum-resistant nature of cryptographic hashing functions, even with Grover's algorithm, the practical realization of such an attack is significantly more challenging than coin theft.

Coin theft, by contrast, involves directly compromising users' private keys used for digital signatures. Most cryptocurrencies, including Bitcoin, rely on elliptic curve cryptography (ECC) or similar asymmetric schemes, which are vulnerable to Shor's algorithm. Once a public key is revealed, typically after a transaction, an attacker equipped with a sufficiently powerful quantum computer could efficiently derive the corresponding private key. This would allow the attacker to sign fraudulent transactions and transfer funds out of compromised wallets. Unlike double-spending, this form of attack does not require controlling the network or mining infrastructure and is therefore considered a more immediate and tangible threat in a quantum context.

In summary, while double-spending requires significant quantum resources and coordination to manipulate consensus, coin theft more directly leverages quantum computational advantages. The capacity to break cryptographic keys presents a more immediate and focused threat. To more accurately reflect the probabilistic nature of quantum-enabled attacks, we incorporate uncertainty into the quantum attack game model. Considering the differing feasibility and likelihood of quantum-enabled double-spending and coin theft attacks, we model their impacts on Bitcoin price as stochastic processes. Let the success rates of double-spending and stealing attacks be random variables denoted by w_d and w_s, respectively, where $w_d, w_s \in [0, 1]$. These probabilities capture the uncertainty in attackers' capabilities and defenses' effectiveness.

We modify the Bitcoin pricing formula to incorporate these probabilistic effects:

$$P_{ds} = \frac{(1 - \frac{w_s S}{B})PY}{(B + w_d D)V} \tag{11}$$

where $w_d < w_s$, given the asymmetry in quantum advantage between double-spending and coin theft.

F. Welfare Impact of Theft and Double-spending

Financially, double-spending refers to the act of using the same Bitcoin for two separate transactions within a short time frame. A quantum attacker, with the ability to reverse transactions, could exploit this by making an on-chain payment and then using their superior computational power to reorganize the blockchain, effectively canceling the original transaction. This would be akin to receiving a refund while retaining the purchased item. The benefit of double-spending, therefore, corresponds to the market value of the transaction amount successfully duplicated. In contrast, coin theft directly increases the attacker's Bitcoin holdings, with the benefit equating to the market value of the stolen coins. While double-spending does not change the total Bitcoin balance of the attacker, theft results in a net increase in their assets.

Considering both the benefits and costs associated with double-spending and stealing, the net welfare gain to the quantum miner can be expressed as:

$$P_B(w_d D + w_s S) - (P_B - P_{ds})B_q \tag{12}$$

where B_q represents the Bitcoin holdings of the quantum attacker, and $w_s S$ denotes the amount of Bitcoin successfully stolen from other miners. Over time, the Bitcoin capital of a quantum miner evolves dynamically as

$$B_q = B_{q,-1} + m_{q,-1} + w_s S_{-1} \tag{13}$$

where B_q denotes the Bitcoin held by the quantum miner in the current period, $B_{q,-1}$ is the Bitcoin held in the previous period, $m_{q,-1}$ represents the Bitcoin newly mined by the quantum miner in the previous period, and $w_s S_{-1}$ is the amount of Bitcoin successfully stolen during that same period.

G. Optimal Portfolio of Quantum Attacks

When a quantum miner cheats through both stealing and double-spending attacks on the Bitcoin network, the attacker must determine the optimal scale of each attack. A profit-driven quantum miner selects an optimal attack portfolio by solving the following maximization problem, which incorporates equations (6), (11), and (12):

$$max_{D,S} = \frac{PY}{BV}(w_d D + w_s S) - (\frac{PY}{BV} - \frac{(1 - \frac{w_s S}{B})PY}{(B + w_d D)V})B_q \tag{14}$$

The first order condition with respect to D solves

$$\frac{1}{B} = \frac{(1 - \frac{w_s S}{B})B_q}{(B + w_d D)^2} \tag{15}$$

Isolating D, we get

$$D^* = \frac{\sqrt{(B - w_s S)B_q} - B}{w_d} \tag{16}$$

The first order condition with respect to S satisfies

$$\frac{w_s PY}{BV}(1 - \frac{B_q}{B + w_d D}) = 0 \tag{17}$$

This implies $B_q = B + w_d D$, or equivalently $D = \frac{B_q - B}{w_d}$. Substituting into (16), we derive the final expressions as $S^* = \frac{B - B_q}{w_s}$ and $D^* = \frac{B_q - B}{w_d}$.

However, since $B_q < B$, the optimization problem has no real solution with respect to double-spending. This is due

TABLE II: Assigned Values of Key Parameters in Simulations

Symbol/Variable	Value
B	$110 + 5 \times (1 - 10\%)^{t-1}$
w_d	$0.2 \pm 15\%$
w_s	$0.8 \pm 15\%$
P	1
Y	1,000
V	1
n	11

to the objective function being unbounded - it can increase or decrease indefinitely without reaching a finite maximum or minimum. On one hand, there is no upper bound on the domain of double-spending. On the other hand, the cost of double-spending is neglected. Together, these factors allow for the possibility of infinite growth in double-spending, thereby rendering the problem unsolvable in any practical sense. Additionally, since $S < (B - B_q)$ and $0 \leq w_s \leq 1$, the expression for S^* yields only one feasible boundary solution: $S^* = B - B_q$ when $w_s = 1$. Otherwise, the optimization problem has no real solutions for stealing either.

Given that the theoretical analysis of the quantum miner's attack portfolio yields no closed-form solution, we proceed with a simulation-based analysis to gain insight into the quantum miner's optimal strategies for exploiting the Bitcoin network through theft and double-spending.

IV. Simulation Results

In this section, we parameterize the proposed model and simulate dynamic quantum attacks on the Bitcoin network, incorporating both theft and double-spending. Using the Bitcoin pricing formula derived from the theoretical analysis, along with specified parameter values and simulation settings, we examine the dynamics of Bitcoin price, the quantum miner's decisions regarding stealing and double-spending, the distribution of Bitcoin among miners, and the evolution of the quantum miner's profits. The assigned values of key parameters used in simulations are summarized in Table II.

In the theoretical model, the nominal price level of goods and services traded in Bitcoin, the real demand for Bitcoin (i.e., the quantity of goods and services exchanged using Bitcoin), and the velocity of Bitcoin are all treated as exogenous variables. Without loss of generality, we set these parameters as $P = 1$, $Y = 1,000$, and $V = 1$. With these assigned values, equation (11) simplifies to

$$P_{ds} = \frac{1,000(1 - \frac{w_s S}{B})}{B + w_d D} \tag{18}$$

Let n denote the total number of miners participating in the Bitcoin network, with $n - 1$ being classical miners and one being a quantum miner. We set $n = 11$ and run the simulation over 100 stages. Initially, each miner, quantum and classical, holds 10 Bitcoin, resulting in a total Bitcoin supply of 110. At $D = S = 0$, the initial Bitcoin price prior to any quantum attacks is $P_B = 9.09$.

TABLE III: Strategy space at each stage by quantum attacker.

(a) Both stealing and double-spending

Steal	Double Spend
same	same
increase	increase
decrease	decrease
increase	decrease
decrease	increase
same	increase
same	decrease
increase	same
decrease	same

(b) Steal only

Steal	Double Spend
same	N/A
increase	N/A
decrease	N/A

(c) Double spend only

Steal	Double Spend
N/A	same
N/A	increase
N/A	decrease

In the first stage of the simulation, 5 new Bitcoins are mined. The rate of new coin issuance decreases by 10% in each subsequent stage. The probability that a new coin is mined by the quantum miner is $\frac{1}{\sqrt{n}}$, while the probability that it is mined by a classical miner is $\frac{1-\frac{1}{\sqrt{n}}}{n-1}$. For $n = 11$, in each round of the mining competition within the simulation, the quantum miner possesses a 30% probability of successfully mining a coin, whereas each classical miner has a 7% success probability.

A. Best Strategy of Quantum Attacks

The quantum miner decides on the scale of stealing and double-spending in each simulation round/stage. We exhaustively evaluate all possible moves to identify the best action in every stage. In total, there are nine possible combinations of actions the quantum attacker can choose from Table IIIa. The quantum attacker may either increase, decrease or make no change of the amount of cryptocurrency to steal and/or double spend.

It is important to note that random factors influence the success rates of stealing and double-spending at each stage. Additionally, newly mined coins are introduced into circulation. Therefore, choosing the same scale of stealing and double-spending as the previous stage does not necessarily yield the same net gain.

Considering the costs and benefits of both attack types, the quantum miner compares the expected net gains of the nine options, as represented by equation (12), and selects the action with the highest expected net gain. When adjusting the levels of double-spending and stealing from the previous stage, the scale of adjustment is fixed at 10%.

The uncertainty in the success of cyberattacks is reflected in the risky success rates of double-spending and stealing. Specifically, we set the success rate of double-spending to fluctuate within $\pm 15\%$ around a mean of 20%, while the success rate of stealing fluctuates within $\pm 15\%$ around a mean of 80%. The higher average success rate for stealing reflects the greater advantage quantum computing offers in executing theft compared to double-spending.

Simulation studies provide practical guidance on how a quantum miner might optimally decide on attack strategies over time. Figure 1 illustrates the scale of Bitcoins double spent and stolen successfully by the quantum miner in each

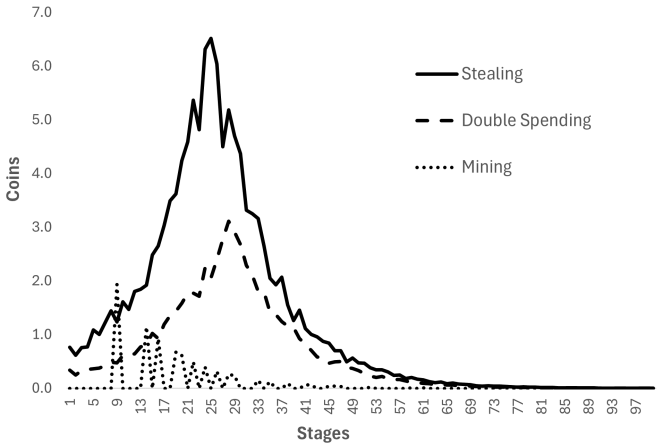


Fig. 1: Dynamics of cryptocurrency earned from stealing and double-spending by the quantum miner.

round of the simulation. It is unsurprising that successful stealing consistently exceeds double-spending due to its significantly higher success rate.

Both types of quantum-enabled cyberattacks intensify during the initial rounds, peaking around Stage 25 for stealing and Stage 28 for double-spending, before gradually declining and stabilizing at low levels toward the end of the simulation. The results highlight a strategic trade-off where aggressive attacks are favored in the early stages of quantum computing development, but the negative consequences of quantum-powered cyberattacks eventually suppress such behavior. In other words, quantum attacks on the Bitcoin network are not sustainable in the long term.

Note that Figure 1 also includes a curve showing the quantity of newly mined coins by the quantum miner. Mining is incorporated to enhance the realism and practical relevance of the simulations. Together with stolen Bitcoin, these mined coins contribute to expanding the quantum miner's Bitcoin holdings, as shown later in Figure 4.

B. Profitability of Quantum Attacks

The quantum attacker launches stealing and double-spending attacks on the Bitcoin network to generate profit. When the quantum attacker follows the best-response strategy described above, the net gain (profit) in each stage is maximized. Figure 2a displays the actual net gain earned by the quantum attacker in each simulation stage.

Interestingly, the quantum miner is only able to earn consistent profits during the early stages of quantum computing. As shown, quantum attacks are profitable at the outset, with profitability rising initially. However, after reaching a peak, profits begin to decline. Eventually, quantum attacks become unprofitable, and the quantum miner loses the financial incentive to continue launching such attacks. In the simulation, net gains drop to zero and remain at zero from Stage 75 onward, reflecting the erosion of financial incentives to continue attacking the network.

Figure 2b illustrates the cumulative net gain accumulated over the course of the simulation. The curve initially increases at an accelerating rate, driven by profitable attacks in early stages. As the profitability of attacks diminishes (as shown in Figure 2a), the growth in cumulative profits slows and eventually levels off. This plateau indicates that quantum attacks yield diminishing returns over time, making them unsustainable as a long-term profit strategy.

The results from Figure 2 highlights an important economic implication of quantum-powered cyberattacks: their profitability is inherently time-limited. In the early stages, the quantum miner benefits from the relatively low opportunity costs of quantum attacks, making quantum attacks financially attractive. However, as attack intensity distorts the Bitcoin network by lowering price, depleting available targets, and increasing systemic risk, the profitability diminishes rapidly.

C. Dynamics of Cryptocurrency Price

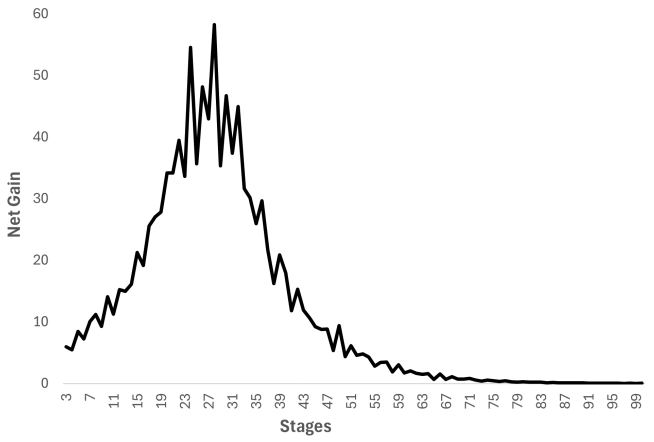
When the quantum miner conducts cyberattacks through both cryptocurrency stealing and double-spending, the market price of cryptocurrency fluctuates in response to the scale of these activities, as defined by equation (11). Theoretically, the Bitcoin price is inversely related to both types of attacks. An increase in double-spending or stealing reduces the market value of Bitcoin.

The quantum miner's chosen attack strategy in each stage directly influences the market price, which is computed using equation (18) and the assigned parameter values. Figure 3 presents the simulated equilibrium price of Bitcoin over time as the quantum miner engages in both double-spending and theft. Because the scale of cyberattacks is incrementally adjusted in each stage based on the previous stage, an increase in Bitcoin price signals a reduction in attack intensity, while a price decrease indicates an escalation in quantum attacks. Consistent with this, Bitcoin price declines in the early rounds, coinciding with the rising scale of attacks shown in Figure 1. Bitcoin price begins to recover slightly once attack intensity peaks and then recedes.

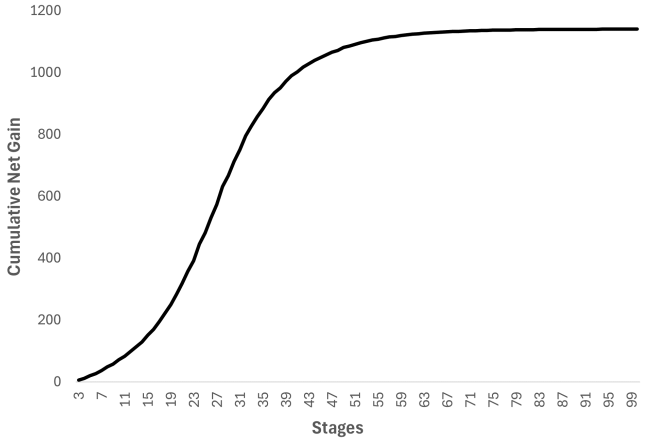
The price eventually stabilizes around Stage 70, reaching a long-run steady-state level of approximately 6.45. This timing aligns with the near cessation of both double-spending and theft attacks, as shown in Figure 1. The shape of the price trajectory suggests that the quantum miner intensifies attacks in the early stages, driving down the Bitcoin price. As the attacks are gradually abandoned and the supply of newly mined Bitcoin diminishes, the market stabilizes and the price converges to a new equilibrium.

D. Distribution of Cryptocurrency

As the quantum miner launches both stealing and double-spending attacks on the Bitcoin network, the distribution of Bitcoin across participants shifts significantly. Initially, all miners, both quantum and classical, begin with 10 Bitcoins each. Over time, the quantum miner accumulates additional Bitcoin by winning mining competitions and, more substantially, by stealing from classical miners. Meanwhile, classical



(a) Net gain from quantum attacks per stage



(b) Cumulative net gain from quantum attacks

Fig. 2: Net gains and cumulative net gains by quantum-enabled attacker over the course of the simulation.

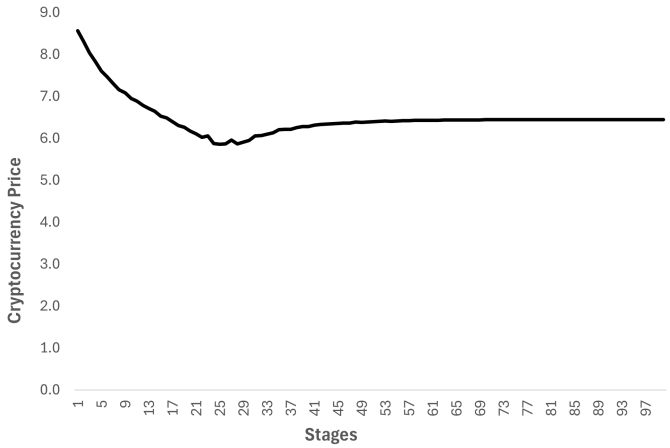


Fig. 3: Dynamics of cryptocurrency (Bitcoin) price in the presence of quantum attacks through theft and double-spending.

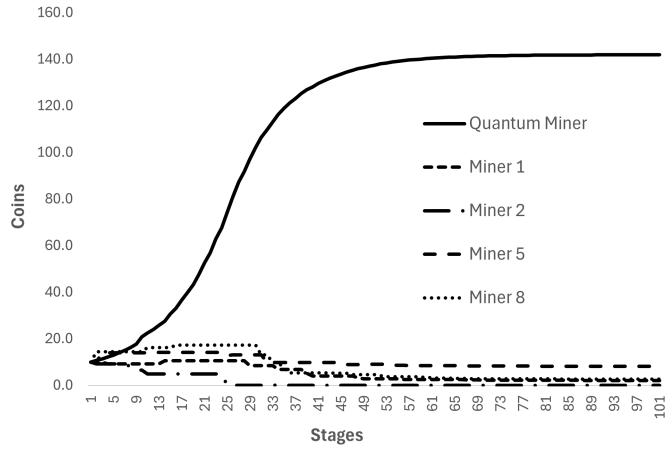


Fig. 4: Distribution of cryptocurrency holdings among quantum and classical miners over time.

miners can still earn Bitcoin through successful mining but also risk losing their holdings to theft by the quantum attacker.

In each simulation stage, the quantum miner selects an amount of Bitcoin to steal and randomly targets classical miners until this target is met. By the end of Stage 100, the quantum miner holds 142 Bitcoins out of a total supply of approximately 155. Among the 10 classical miners, one (Miner 5) retains over 8 Bitcoins, while a few others (such as Miner 1 and Miner 8) hold between 2 and 3 Bitcoins. The remaining classical miners are left with none.

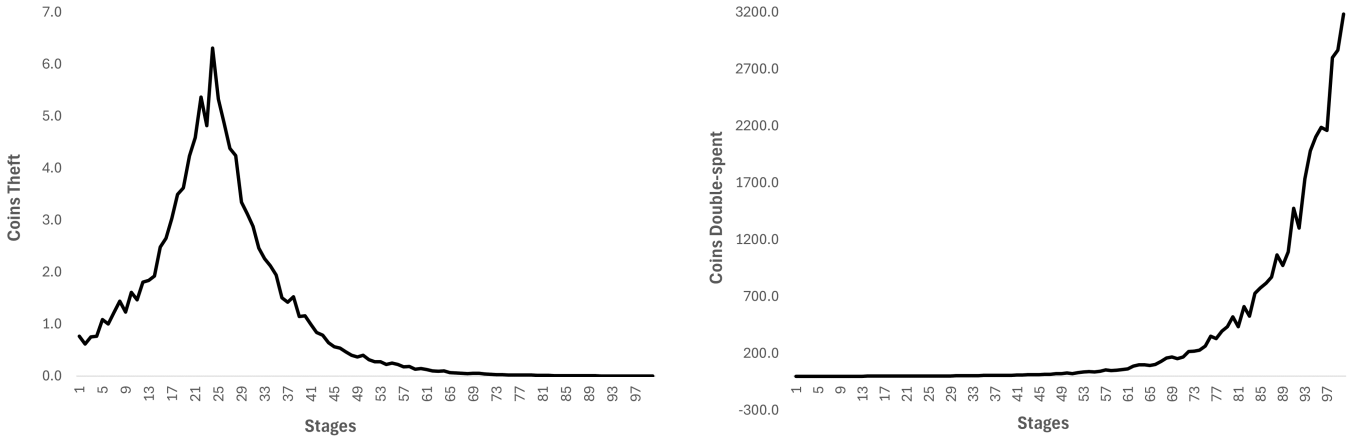
Figure 4 illustrates the evolution of Bitcoin holdings for the quantum miner and the classical miners throughout the simulation. For clarity, only the changing balance of Miner 2 is shown to represent the group of classical miners who end up with zero Bitcoin. As shown in Figure 1, the quantum miner acquires significantly more Bitcoin through theft than through mining. As the simulation progresses and the network comes under sustained quantum attacks, theft activity diminishes, and the total Bitcoin supply approaches its protocol-imposed cap. At this point, the distribution of Bitcoin stabilizes. In Figure 4, the quantum miner's holdings initially rise rapidly, then grow more slowly, and eventually plateau.

E. Stealing vs. Double-spending

For completeness, we also present simulation results in scenarios where the quantum attacker engages exclusively in either double-spending or coin theft attacks on the Bitcoin network. If the quantum attacker's objective is limited to either stealing coins from other participants or executing a double-spending attack, it selects one of the actions outlined in Table IIIb and Table IIIc, respectively.

Figure 5 illustrates the optimal strategy adopted by the quantum attacker regarding the intensity of coin theft (Figure 5a) and double-spending (Figure 5b) at each stage of the simulation. Notably, the trend in Figure 5a mirrors the shape of the solid line in Figure 1.

In scenarios where the attacker engages exclusively in coin theft, expansion of attacks proves profitable primarily



(a) Cryptocurrency earned through coin theft only

(b) Cryptocurrency earned through double-spending only

Fig. 5: Dynamics of cryptocurrency accumulation through coin theft only or double-spending only by the quantum attackers.

in the early stages of quantum computing. As the attacker accumulates Bitcoin holdings from prior thefts, the opportunity cost of further attacks, i.e., the adverse impact on Bitcoin's market value, gradually outweighs the marginal benefits. This dynamic ultimately deters the attacker from continuing to scale up theft. The overall magnitude of theft in this case is also lower: in the simulation, the peak theft level is 6.3, compared to 6.5 in the mixed-strategy case (both theft and double-spending).

In contrast, when double-spending is the sole form of exploitation, the attacker continually escalates the scale of such activity to ensure that profits from double-spending surpass the capital loss from Bitcoin's declining price. As shown in Figure 5b, the scale of double-spending starts at 0.3 and steadily increases. In later stages when Bitcoin's price has nearly collapsed (as shown later in Figure 7), the incentive to double-spend accelerates sharply. This surge reflects the attacker's need to offset asset depreciation through more aggressive exploitation. The explosive growth in double-spending is also attributable to a simplifying assumption in the simulation: double-spending incurs no direct cost for the attacker.

Figure 6 presents the profitability of quantum attacks under two exclusive strategies: theft-only and double-spending-only. Specifically, Figures 6a and 6b illustrate the net gains associated with each strategy, respectively. The trajectory in Figure 6a closely resembles that of Figure 2a, and it can be interpreted in a similar manner.

However, when the attacker is limited to double-spending, with no upper bound on attack frequency and no counterbalancing theft to incentivize price preservation, the net gain from double-spending increases substantially and becomes both volatile and persistent in the later stages of the simulation. As Bitcoin's price approaches negligible levels, the ability of double-spending to further elevate net gains diminishes.

It is also worth noting that if theft is the sole mode of attack, as opposed to a combination of theft and double-spending, the overall profitability of quantum-enabled attacks is reduced.

Figure 7 compares the evolution of Bitcoin's market price under two distinct quantum attack strategies: theft-only and double-spending-only. The dashed curve depicts the price dynamics in the theft-only scenario, which closely mirrors the pattern observed in Figure 3. Given that the intensity of theft is lower when it is the sole attack method, the steady-state Bitcoin price in Figure 7 is slightly higher than in the mixed-attack scenario shown in Figure 3 (6.4515 vs. 6.4513).

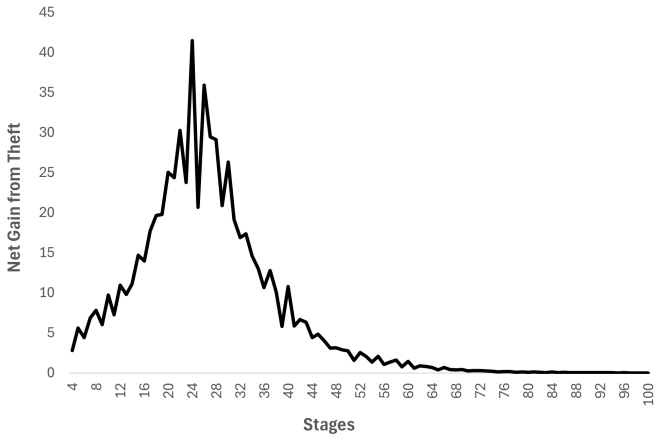
In contrast, when the quantum attacker engages exclusively in double-spending, the price of Bitcoin declines continuously as the scale of the attack expands, ultimately resulting in a dramatic loss of value.

The simulation results for these single-attack scenarios suggest that quantum miners are unlikely to sustain indefinite profits from quantum advantages alone. While double-spending yields higher short-term financial returns than theft, and despite quantum computing being inherently more effective for executing theft, the long-term consequence is a severe devaluation of cryptocurrency. By the end of the simulation, Bitcoin's price has dropped to an extremely low level.

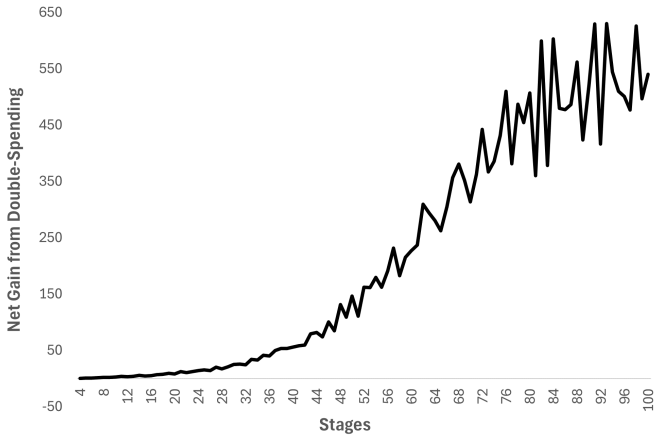
F. Discussion and Strategic Insights

The results reveal several important patterns. Quantum attacks are most profitable shortly after quantum computing capabilities emerge—a period when defensive measures are likely to be weak or nonexistent. Both theft and double-spending attacks intensify in the early stages and peak during roughly the first third of the simulation period before declining. However, these attacks inherently erode the network's economic value by driving down the market price of cryptocurrency, which reduces profitability and ultimately disincentivizes continued attacks. This suggests that quantum-enabled exploitation is not sustainable over the long term.

The profitability of these attacks is closely linked to Bitcoin's market value: when prices rise, attacks become more lucrative and intensify, but the increased attack activity depresses Bitcoin's price, reducing the rewards and making further



(a) Net gain from coin-theft-only attacks



(b) Net gain from double-spending-only attacks

Fig. 6: Net gains from quantum-enabled attacks

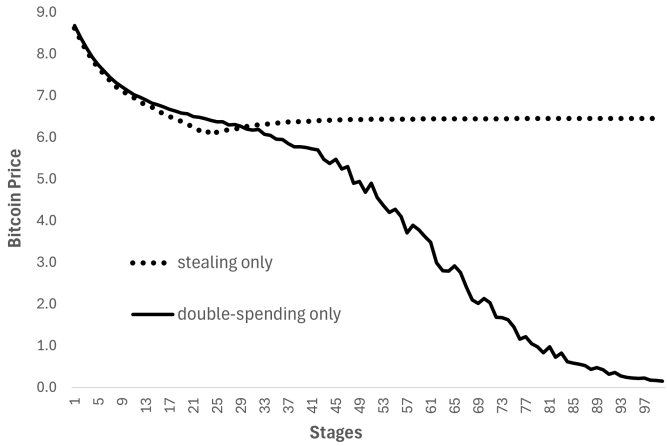


Fig. 7: Dynamics of Bitcoin price under stealing-only and double-spending-only quantum attack scenarios.

attacks less attractive. As the quantum miner accumulates Bitcoin through theft, preserving the asset's value becomes a priority, leading to a gradual cessation of attacks. From an economic perspective, the cryptocurrency network is governed by incentives that inherently constrain attackers motivated by profit. Similar to Gresham's law, where "bad money drives out good," excessive double-spending and theft undermine trust in the cryptocurrency system, causing participants to reject the currency altogether. To avoid destroying the value of their own holdings, quantum attackers cannot afford to "overattack." Even in the absence of active defenses, quantum attacks eventually become self-defeating.

The natural erosion of quantum attack profitability, evidenced by the plateau in cumulative net gains observed in the simulation, suggests that such attacks pose the greatest threat during the early transitional phase of quantum computing. Defensive efforts should therefore be concentrated during this period. From a policy standpoint, early adoption of quantum-resistant cryptographic standards and vigilant monitoring of network anomalies can substantially mitigate short-term risks. From a technical perspective, accelerating the migration to post-quantum cryptographic protocols will reduce the window of vulnerability.

It is worth noting that among the attack scenarios analyzed, theft-only yields the lowest peak net gain, making it the least damaging. A portfolio combining both theft and double-spending achieves a higher peak gain but remains self-limiting. The worst-case scenario is double-spending alone, as it allows unlimited attacker gains and results in the complete destruction of the cryptocurrency system. Therefore, while transitioning cryptocurrency networks to quantum-resistant cryptographic algorithms is essential, defensive strategies must prioritize strengthening cryptographic hashing to resist quantum attacks and minimize double-spending. Digital signatures for preventing theft can be a lower priority compared to securing hashing mechanisms against double-spending. Additionally, enhancing surveillance to detect suspicious activity, such as coordinated double-spending or abrupt shifts in Bitcoin holdings, and designing incentive mechanisms that render cybercrime economically irrational or prohibitively expensive are necessary to limit the feasibility of quantum attacks. One limitation of the current modeling and simulation is the exclusion of mining and attack costs, effectively representing the best-case scenario for quantum attackers in terms of potential financial gain. Incorporating attack costs into the framework would further discourage attackers from initiating additional attacks.

V. Conclusion

Quantum-based cybercrime poses a significant threat to current cybersecurity infrastructures, particularly cryptocurrency networks. This research investigates two types of quantum attacks, i.e., cryptocurrency (Bitcoin) theft and double-spending, from an economic perspective involving quantum-capable adversaries. A key observation is that double-spending effectively undermines Bitcoin's capped supply by introducing inflation, while coin theft erodes trust in the cryptocurrency.

We developed a novel modeling framework to quantify the costs, benefits, and net gains of quantum attacks under various scenarios. Through simulation studies, we analyzed the dynamic behavior of Bitcoin under sustained quantum attacks, with a focus on how a profit-driven quantum miner would adapt the intensity of theft and double-spending based on expected returns.

Our findings reveal that quantum attackers face an inherent paradox: their success in exploiting the system diminishes the very value they seek to extract. As attacks intensify, the loss of credibility and market value reduces the profitability of continued exploitation, introducing a natural economic constraint. This self-limiting dynamic suggests that quantum-enabled attacks may not be sustainable in the long term. These results carry important policy and technical implications. The window of vulnerability to quantum attacks appears to be temporally constrained, with the highest risk occurring during the early phase of quantum computing adoption. Accordingly, defensive strategies should be prioritized during this critical period. In particular, transitioning to post-quantum cryptographic protocols is essential. Among these, strengthening post-quantum-resistant cryptographic hashing algorithms (to prevent double-spending) should take precedence over post-quantum digital signatures (used to prevent theft). Additionally, enhancing network surveillance, anomaly detection, and coordinating international efforts to deter quantum cybercrime are vital components of an effective response.

Beyond cryptocurrency domain, future research should explore the broader landscape of quantum-based cybercrime. Deeper understanding of the economic incentives, behavioral adaptation, and long-term viability of quantum attacks will support the development of more resilient systems and enable the design of focused, timely, and economically-informed mitigation strategies.

REFERENCES

[1] Y. Kim, A. Eddins, S. Anand, K. X. Wei, E. van den Berg, S. Rosenblatt, H. Nayfeh, Y. Wu, M. Zaletel, K. Temme, and A. Kandala, "Evidence for the utility of quantum computing before fault tolerance," *Nature*, vol. 618, pp. 500–505, 2023.

[2] F. Arute, K. Arya, R. Babbush, and et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, October 23 2019.

[3] S. Bravyi, A. W. Cross, J. M. Gambetta, D. Maslov, P. Rall, and T. J. Yoder, "High-threshold and low-overhead fault-tolerant quantum memory," *Nature*, no. 627, pp. 778–782, March 27 2024.

[4] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC)*, Philadelphia, PA, May 22-24 1996, pp. 212–219.

[5] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124–134.

[6] C. Pinzón and C. Rocha, "Double-spend attack models with time advantange for bitcoin," *Electronic Notes in Theoretical Computer Science*, vol. 329, pp. 79–103, 2016.

[7] Z. Li and Q. Liao, "How much should i double spend my bitcoin? game theory of quantum mining." in *Proceedings of the 15th Conference on Game Theory and AI for Security (GameSec)*, New York, USA, October 16-18 2024, pp. 87–106.

[8] ——, "Is quantum computing the bitcoin terminator?" in *the 30th Americas Conference on Information Systems (AMCIS)*, Salt Lake City, Utah, August 15-17 2024, pp. 1–10.

[9] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, and W. J. Knottenbelt, "Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack," *Royal Society Open Science*, vol. 5:180410, 2018.

[10] S. Alghamdi and S. Almuhammadi, "The future of cryptocurrency blockchains in the quantum era," in *IEEE International Conference on Blockchain (Blockchain)*, December 6-8 2021, pp. 544–551.

[11] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum attacks on Bitcoin, and how to protect against them," *Ledger*, vol. 3, 2018.

[12] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *arXiv*, no. 1905.09749, May 2019.

[13] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Proceedings of 2015 IEEE Symposium on Security and Privacy*, San Jose, CA, 2015, pp. 104–121.

[14] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[15] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, July 1982.

[16] E. Budish, "The economic limits of bitcoin and the blockchain," National Bureau of Economic Research, Working Paper 24717, June 2018.

[17] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the instability of Bitcoin without the block reward," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 2016, pp. 154–167.

[18] N. Poluyanenko, N. A. Pisarenko, V. Safonenko, T. Makushenko, O. Pushko, Y. Zaburmekha, and K. Kuznetsova, "Simulation of a double spending attack on the "proof of work" consensus protocol," *Radiotekhnika*, vol. 3, no. 198, pp. 146–161, 2019.

[19] J. Jang and H.-N. Lee, "Profitable double-spending attacks," *Applied Sciences*, vol. 10, no. 23, 2020.

[20] S. Holmes and L. Chen, "Assessment of quantum threat to bitcoin and derived cryptocurrencies," *IACR Cryptol. ePrint Arch.*, vol. 2021, p. 967, 2021.

[21] D. A. Bard, J. J. Kearney, and C. A. Perez-Delgado, "Quantum advantage on proof of work," *Array*, vol. 15, p. 100225, 2022.

[22] O. Sattath, "On the insecurity of quantum bitcoin mining," *International Journal of Information Security*, vol. 19, pp. 291–302, March 2020.

[23] J. J. Pont, J. J. Kearney, J. Moyler, and C. A. Perez-Delgado, "Downtime required for Bitcoin quantum-safety," *arXiv*, no. 2410.16965, october 2024.

[24] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[25] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, and W. J. Knottenbelt, "Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack," *Royal Society Open Science*, vol. 5, no. 180410, pp. 1–12, June 20 2018.

[26] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610–613, 2006.

[27] M. Vasek and T. Moore, "There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams," in *Proceedings of the 19th International Conference on Financial Cryptography and Data Security (FC 2015)*, San Juan, Puerto Rico, 2015, pp. 44–61.

[28] J. Clough and M. Edwards, "Pump, dump, and then what? the long-term impact of cryptocurrency pump-and-dump schemes," in *Proceedings of 2023 APWG Symposium on Electronic Crime Research (eCrime)*, Barcelona, Spain, 2023, pp. 1–17.

[29] B. Haslhofer, C. Hanslbauer, M. Fröwis, and T. Goger, "Increasing the efficiency of cryptoasset investigations by connecting the cases," in *Proceedings of 2023 APWG Symposium on Electronic Crime Research (eCrime)*, Barcelona, Spain, 2023, pp. 1–10.

[30] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[31] M. A. Rudd and D. Porter, "A supply and demand framework for Bitcoin price forecasting," *Journal of Risk and Financial Management*, vol. 18, no. 2, p. 66, 2025.