Is Quantum Computing the Bitcoin Terminator?

Completed Research Full Paper

Zhen Li
Albion College
zli@albion.edu

Qi Liao
Central Michigan University
liao1q@cmich.edu

Abstract

Cryptocurrencies such as bitcoin rely on proof-of-work mining to secure the underlying blockchain protocols. The appearance of quantum computing could mine blocks that classical computers cannot compete with, thus threatening the decentralization and trustfulness of blockchain technologies. We study the financial incentives of double spending for quantum miners. Double spending increases the money supply of total bitcoin, diluting the value of bitcoin. Our novel model of bitcoin price formation linked with double spending suggests that killing bitcoin is not optimal for money-driven quantum miners as the short-term gain from double spending comes at a long-term cost of deteriorating bitcoin value. We derive the optimal range of double spending that allows quantum miners to gain from double spending while providing sufficient incentives for regular miners to participate in the network. With emergent quantum computing, this research offers insights to better understand the economic underpinnings of blockchain and cryptocurrency security.

Keywords

Quantum computing, quantum miner, quantum supremacy, blockchain, cryptocurrency, bitcoin, double spending, economics, financial incentives.

Introduction

Bitcoin is a decentralized cryptocurrency for managing and transferring payments based on the concept of proof-of-work that allows users to execute payments by digitally signing their transactions. Users of bitcoin broadcast the transactions over a peer-to-peer network and the miners collect blocks of transactions, verify their integrity, and append them to the block chain. Miners are motivated by receiving rewards with newly mined bitcoin and transaction fees [Kroll et al.,2013; Nakamoto, 2008].

The security of bitcoin network is guaranteed by its decentralized nature [Pagnotta, 2022]. The mining difficulty of bitcoin is quantified by its hash rate that measures the computational power of the proof-of-work network. The bitcoin blockchain network adopts a secure hashing algorithm that randomly generates a hash code. Mining computers on the network compete to guess the hash value. Hash rates are measured by the number of guesses made per second by a single miner, a pool, or across the entire network. Hash rates are vital for overall security of the bitcoin blockchain network. They increase with the miners participating in the network. The more miners who are part of the network competing to mine blocks, the higher is the hash rate and thus the more secure is the network [Crosby et al., 2016].

The bitcoin protocol grants miners with superior computing power the advantageous position to win the computational competition. A malicious actor or a group of miners who control more than half of the network's mining hash rate can launch an attack on the blockchain network, known as a 51% attack [Budish, 2018]. Attackers could use their dominant computing power to alter the blockchain such as interrupting the recording of new blocks by preventing other miners from completing blocks. A 51% attacker could also reverse transactions to double spend tokens [Pinzon & Rocha, 2016].

The techniques used in cryptocurrency blockchains make them virtually unhackable if the networks are powerful enough to outpace hackers. The limitation of computing power of classical mining devices makes 51% attacks more of a theoretical possibility than realistic threat. Researchers found that the current state of security in bitcoin makes 51% attacks economically unfeasible [Hao, 2022; Nuzzi et al., 2024]. Although such attacks may not be viable in current status, it would be possible with quantum computing. Researchers have suggested that 51% attacks on bitcoin by quantum computers may not be possible until 2028, and recent evidence indicates it could happen sooner [Kim et al., 2023].

Any miner who is first equipped with quantum computing will be in a dominant position winning all mining competitions [Benkoczi, 2022]. The miner possessing quantum computing power, referred to as the "quantum miner" hereinafter, may threaten the decentralization of mining-based bitcoin blockchain protocol. The quantum miner has the potential to double spend, decrypt the private key from a public key, control, and ultimately steal others' bitcoin, thus posing a significant threat to the survival of bitcoin and cryptocurrencies in general [Aggarwal et al., 2018]. This leads to an interesting research question, i.e., will quantum computing kill bitcoin and blockchain technology?

In this paper we study the effects of quantum computing on bitcoin blockchain networks in terms of the financial incentives of double spending by the quantum miner. We model a money-driven quantum miner acting on profitable double spending following the benefit and cost comparison. The supply and demand analysis is applied to the bitcoin market to find the equilibrium price of bitcoin and key determining factors that cause bitcoin price to change. The quantum miner faces a dilemma of obtaining short-term gain from double spending at a long-term cost of deteriorating bitcoin value. Our model suggests that killing bitcoin is not necessarily in the best interest of the money-driven quantum miner and shows how the quantum miner can walk a fine line to balance the short-run benefit and the long-run benefit while in the meantime, providing sufficient incentives for regular miners to participate in the bitcoin network to make double spending profitable and sustainable.

The rest of the paper is organized as follows. We first discuss related work. We then conduct economic analysis of bitcoin price formation and fluctuation, and the welfare effects of double spending on the quantum miner and regular miners. We solve for the profitable range of double spending for the quantum miner while in the meantime, providing sufficient incentives for regular miners to remain in the bitcoin network. Further discussions and future research directions are also addressed before concluding the work.

Related Work

Bitcoin is found to be a unique asset possessing properties of both a standard financial asset and a speculative one [Kristoufek, 2015]. As a virtual currency, bitcoin operates collaboratively without the need of financial intermediaries [Bohme et al., 2015; Murtazashvili et al., 2022]. As an investment asset, bitcoin is found to have a role in portfolio diversification [Bakry et al., 2021; Kajtazi & Moro, 2018; Khaki et al., 2023]. Bitcoin's security model relies on miners' speculative investment in the network's future, including 51% attackers whose interests can be aligned with the network [Ebrahimi et al., 2019; Hao, 2022].

A proof-of-work protocol like bitcoin requires decentralized miners to be honest for its record-keeping function to work [Porat et al., 2017]. If a single miner or a set of colluding miners were to command much of the mining power in the network, the ledger could become controlled and result in a 51% attack, in which the group can alter the previously verified records [Budish, 2018]. Theoretically a 51% attack would be even made possible with much less than 51% of the hash power in some circumstances [Carlsten et al., 2016]. The possibility of such attacks creates systemic security risks [Aponte-Novoa et al., 2021].

One reason to argue the security of blockchains is Byzantine Fault-tolerance (BFT) concept [Lamport et al., 1982]. BFT states that a computing system is only resistant to a certain number of faulty or malicious participants to be reliable. Bitcoin addresses the BFT problem by increasing the cost of participation in the blockchain system. Participants are required to engage in resource-consuming mining activities before being able to make state changes to the system. In bitcoin blockchain networks, miners' probability of finding a block is a function of their own hash rate relative to the entire network, and the mining process follows a Poisson distribution [Nakamoto, 2008]. To break BFT, the attacker must own half of the network's hash rate at which the attacker's rate of success surpasses any other miners in the network. 50% is thus the threshold to break BFT in bitcoin system.

The theoretical threat of the majority 51% attack was made aware in a 2018 paper emphasizing the high threat in bitcoin [Budish, 2018]. Although the scenarios described or the pricing model used may not be realistic, it raised a very important question and laid the foundation to look deeper into bitcoin's security and pricing models. More research followed by expanding the framework, assumptions, dimensions, and scenarios of the analysis [Aponte-Novoa et al., 2021; Lovejoy, 2020].

To assess the risk of 51% attack, it is important to understand how concentrated the mining capacity is. Bitcoin mining capacity is found to be highly concentrated and there is significant geographic clustering of miners [Makarov and Schoar, 2021]. The concentration of hash rate power has been rising in a very small set of miners, generating a real risk for current blockchains [Aponte-Novoa et al., 2021]. Mining pools function like aggregators of hashing capacity and can therefore have substantial influence over the bitcoin protocol. They do not necessarily control their miners though. The power of a pool operator depends on the ease with which miners can shift capacity across pools, which in turn depends on the underlying size distribution of the miners [Cong et al., 2020].

Unlike pool mining that requires collaboration, the arrival of one single quantum miner would breach the 51% threshold of hash power [Benkoczi, 2022]. Quantum computing is fast approaching, and the security of bitcoin is at risk [Aggarwal et al., 2018; Kim et al., 2023]. Quantum computers are expected to have dramatic impacts on blockchain protocols due to their superior computing power [Bard et al., 2022]. Bitcoin's signature algorithm is vulnerable to quantum attacks [Stewart et al., 2018]. Possible solutions and preventive measures are studied considering the threats a quantum-capable attacker could impose on blockchain networks including bitcoin [Allende et al., 2023; Kappert et al., 2021; Stewart et al., 2018].

Double spending is the most straightforward way to monetize the ability of breaching the 50% threshold [Pinzon & Rocha, 2016]. Owning 51% of the nodes on the bitcoin network theoretically gives the controlling party the power to alter the blockchain. They would be able to reverse transactions that were completed while they were in control, allowing them to double spend tokens, one of the issues consensus networks like proof-of-work were created to prevent [Chohan, 2021; Karame et al., 2012; Poluyanenko et al., 2019]. It was even theoretically shown that a double spend attack at any proportion of computing power can be made profitable [Jang & Lee, 2020]. The advent of quantum computing threatens the financial security of cryptocurrencies with double spending vulnerability [Holmes & Chen, 2021].

It has been suggested that double spending can be prevented by costly mining and delaying settlement [Chiu & Koeppl, 2022; Kang, 2023]. Applying preventive mechanisms is costly, if ever possible. If the probability of detecting fraudulent activity is low, allowing for double spending may be optimal [Li & Wang, 2022].

The Economic Model of Double Spending

In this section, we develop a formal model to study the financial incentives for the quantum miner to double spend profitably. The supply and demand analysis of the bitcoin market, under some given assumptions, is used to solve for the equilibrium bitcoin price both with and without double spending. The modeling analysis specifies the optimal range of double spending for the money-driven quantum miner.

Suppose there are N + 1 miners in a bitcoin blockchain network including N regular miners and one quantum miner in possession of quantum computing. All the miners are money-driven. Armed with superb computing power, the quantum miner can do the following:

- Successfully mine all the coins left to be rewarded upon acquiring quantum computing power.
- Create duplicate bitcoin with double spending.

Key assumptions of the model are

- Bitcoin miners are also bitcoin users and speculators.
- There are no transaction fees. Miners' wealth is measured by the market value of possessed bitcoin.
- Upon acquisition of quantum computing, the quantum miner wins all mining competitions and receives all remaining bitcoin rewards.
- Only the quantum miner has the computing power to double spend.
- The quantum miner does not consider double spending until bitcoin rewards are exhausted.

- The quantity of goods and services traded in bitcoin is constant, but units of bitcoin needed to buy an item fluctuates with bitcoin price.

The unique abilities of the quantum miner imply that the quantum miner acts like the monetary authority controlling the supply of bitcoin. Once the quantum miner has won the competitions successfully mining all the remaining coins, the quantity of "true" bitcoin reaches the designed upper limit. Double spending increases the supply of bitcoin by the amount of double spending, equivalent to printing money. One of the chief characteristics of bitcoin is its limited coin supply that increases its scarcity over time (known as "halving"), which tends to increase demand and price. We make an interesting claim that double spending breaks the cap and essentially imposes an "inflation tax" on bitcoin holders by diluting the value of bitcoin.

When exercising the super ability of double spending, the quantum miner faces a tradeoff between current gain and future benefit. Double spending imposes the inflation tax not only on regular miners but on the quantum miner as well. To study the rational choice of the quantum miner, we model the quantum miner's decision-making on the level of double spending in a two-period setting, the present period and the future period. As for regular miners, the inferior computing power prevents them from winning the mining competition, but they reserve the freedom of leaving the bitcoin network.

We extend the classical Quantity Theory of Money to find the equilibrium price of bitcoin and extend the bitcoin pricing model in [Li & Liao, 2018] to consider the economic impact of double spending. Table 1 lists the symbols for variables used in the model and their definitions.

Symbol	Definition
B_M	Capped bitcoin designed supply
B_o	Bitcoin rewarded to regular miners before quantum computing occurring
D	Quantity of double spending by the quantum miner
P_B	Initial bitcoin price without double spending
EP_B	Expected bitcoin price without double spending
EP_D	Expected bitcoin price with double spending
P	General price level of goods and services
Y	Quantity of goods and services traded using bitcoin as medium of exchange
V	Velocity of bitcoin
S	Units of bitcoin currently demanded for speculative purpose
S^e	Expected units of bitcoin demanded for speculative purpose
R	Required risk-adjusted return on bitcoin investment
N	Regular miner population
C	Per-regular-miner operation cost of participating in bitcoin network

Table 1. Symbols and Definitions

Using the defined variables, we can derive that the units of bitcoin held by the quantum miner is $(B_M - B_0)$, and the maximum possible range of double spending is $0 \leq D \leq (B_M - B_0)$.

Supply and Demand Analysis of the Bitcoin Market

Bitcoin is not merely a computer protocol. It is more of a digital asset, medium of exchange, and unit of account. Initially, bitcoin was adopted by tech enthusiasts and libertarians. The first known bitcoin purchase for goods took place in May 2010 where bitcoin got its value working as medium of change. In more recent years, there has been substantial growth in the number of bitcoin transactions. The number

does not represent transactions for goods and services but rather any movement of bitcoin around the network. Bitcoin nowadays is largely perceived as a financial investment asset hence the demand for bitcoin comes from both transaction and speculative needs.

We use the supply and demand analysis of the bitcoin market to find the equilibrium bitcoin price. The supply of bitcoin comes from block mining. After the quantum miner has won the mining competition in obtaining all the remaining bitcoin rewards, the supply of bitcoin reaches the designed maximum of B_M. Demand for bitcoin includes transaction demand (for buying items) and speculative demand (for earning expected capital gains). The bitcoin market equilibrium without double spending is

$$B_M = \frac{PY}{P_B V} + S \tag{1}$$

where the right-hand-side is the combined demand for bitcoin consisting of transaction demand and speculative demand.

Solving (1), we find the equilibrium bitcoin price without double spending is

$$P_B = \frac{PY}{(B_M - S)V} \tag{2}$$

As can be seen, bitcoin price is increasing in speculative demand for bitcoin and decreasing in the supply of bitcoin.

Speculative demand for bitcoin depends on the market's expectation on future bitcoin price. Market participants (miners in the context of the model) desire a certain risk-adjusted rate of return on bitcoin investment, i.e., $R = {}^{(EP_B - P_B)}/_{P_B}$. Accordingly, we can write bitcoin price without double spending as

$$P_B = \frac{EP_B}{1 + R} \tag{3}$$

Combining Equations (1) and (3), we solve for the units of bitcoin demanded for speculative purpose as

$$S = B_M - \frac{PY(1 + R)}{EP_B V} \tag{4}$$

In Equation (4), B_M, P, Y, R and V are all predetermined. There is a one-to-one correspondence between the expected future price of bitcoin and speculative demand for bitcoin. As EP_B increases, S increases. As $EP_B \rightarrow 0$, $S \rightarrow 0$.

Welfare Impact of Double Spending

We consider two periods, the present and the future. Double spending in the present period adversely affects the bitcoin price in the future period, ceteris paribus, modeled as an increase in the supply of bitcoin in the future period by the quantity of double spending in the present period. With double spending, the expected bitcoin price changes to

$$EP_D = \frac{PY}{(B_M + D - S^e)V} \tag{5}$$

Apparently, $EP_D \leq P_B$. It is also reasonable to believe $EP_D \leq EP_B$ and $S^e \leq S$. No matter how bitcoin market fluctuates, the future bitcoin price will be lower in the case of double spending than otherwise. Facing the tradeoff between current gain and future benefit, the money-driven quantum miner must choose a profitable quantity of double spending. How does double spending affect the wealth of the quantum miner?

Double spending involves spending the same bitcoin twice in a short period of time. The quantum miner owns the power to revert transactions that occurred by replacing the initial transaction with a version where the transaction never took place, thus able to make an on-chain payment only to then use the superior power to reverse the chain to cancel it out, almost like receiving a refund while getting to keep the purchased item, hence the net gain the quantum miner receives from double spending in the present period is $P_B D$. Nevertheless, double spending decreases the value of all coins in the future period thus adversely affects the future welfare of all miners, including the quantum miner.

Table 2 compares the welfare effects of double spending on the quantum miner and regular miners with and without double spending in the two periods. The present wealth of regular miners is not listed because it is not affected by double spending. The column "Present Wealth" is the total bitcoin wealth in the current period. The column "Future Wealth" is the total bitcoin wealth in the future period. The row "change" shows the double spending tradeoff of the quantum miner as well as the negative impact of double spending on individual regular miners.

Scenario	Present Wealth (Quantum Miner)	Future Wealth (Quantum Miner)	Future Wealth (Regular Miner)
Without Double Spending	$P_B(B_M\text{-}B_o)$	$EP_B(B_M\text{-}B_o)$	$(1/N)(EP_BB_o)$
With Double Spending	$P_B(B_M\text{-}B_o)+P_BD$	$EP_D(B_M\text{-}B_o)$	$(1/N)(EP_DB_o)$
Change	P_BD	$-(EP_B\text{-}EP_D)(B_M\text{-}B_o)$	$-(B_o/N)(EP_B\text{-}EB_D)$

Table 2. Welfare Effect of Double Spending on Miners

Finding Profitable Double Spending

The present value of net gains the quantum miner expects to receive from double spending in both periods combined is

$$P_BD - \frac{(EP_B - EP_D)(B_M - B_0)}{1+r} \tag{6}$$

where the latter term is the present value of future wealth loss at the discount factor reflecting the time value of money, and $EP_B \geq EP_D$.

Double spending is profitable for the quantum miner if

$$D \geq \frac{(EP_B - EP_D)(B_M - B_0)}{P_B(1+r)} \tag{7}$$

Since the maximum possible range of double spending is $0 \leq D \leq (B_M - B_0)$, the profitable double spending must satisfy

$$\frac{(EP_B - EP_D)(B_M - B_0)}{P_B(1+r)} \leq D \leq (B_M - B_0) \tag{8}$$

Profitable double spending would be possible as long as $EP_D \geq EP_B - P_B(1+r)$ or $EP_D \geq P_B(R-r)$. Since R is the required return on bitcoin and r is the time value of money, R > r for investors to hold risky bitcoin, indicating that the post-double-spending price of bitcoin must be positive to make double spending profitable. Hence, the necessary condition for profitable double spending is that it does not wipe off the market value of bitcoin. In other words, the quantum miner has no motivation to terminate the bitcoin network so long as the quantum miner has financial interests in bitcoin.

In the meantime, regular miners must have incentives to remain in the network. Regular bitcoin miners are indifferent in the present period with and without double spending, but they lose in future with falling bitcoin value. Specifically, the per-miner loss is the bottom right entry of Table 2.

Regular miners have the financial incentives to support bitcoin network as long as the remaining value of bitcoin exceeds the cost of maintaining the network, i.e., $EP_DB_0/N \geq C$ where C is the per-regular-miner operation cost of the bitcoin network. That is,

$$EP_D \geq \frac{NC}{B_0} \tag{9}$$

Let $A \equiv \frac{B_M - B_0}{P_B(1+r)}$, Equation (8) becomes

$$A(EP_B - EP_D) \leq D \leq (B_M - B_0) \tag{10}$$

Combining the left-hand-side of the inequality with Equation (5), we get

$$D^2 + FD + G \geq 0 \tag{11}$$

where $F \equiv B_M - S^e - AEP_B$ and $G \equiv A(\frac{PY}{V} - EP_B(B_M - S^e))$.

Combining necessary conditions on all miners' financial incentives, profitable double spending must keep bitcoin price at

$$EP_D \geq \max\{P_B(R - r), \frac{NC}{B_0}\} \tag{12}$$

And the quantity of double spending is restrained by $D \in [\frac{-F+\sqrt{F^2-4G}}{2}, B_M]$ for all F, and the additional range of $D \in [0, \frac{-F-\sqrt{F^2-4G}}{2}]$ for F<0.

In summary, the financial impacts of double spending on bitcoin networks are as follows. Bitcoin supply increases by the amount of double spending. Expected future price of bitcoin decreases with double spending. Double spending decreases also speculative demand for bitcoin. Gaining in the short term with double spending costs the quantum miner in the longer term. Although the quantum miner may have the supreme computing power to shake the foundation of bitcoin blockchain networks, the quantum miner may not want to do so out of financial considerations.

Further Discussions

The cryptocurrency network is a complex system of economic incentives that govern its inner working. Thinking total bitcoin as the system's money supply, double spending increases the money supply by the amount of double spending, diluting the value of money. Unless the quantum miner's goal is to disrupt or even destroy the bitcoin network, the miner pursuing monetization of the quantum computing power must use the 51% power cautiously. We conduct the supply and demand analysis to study price formation in the bitcoin market and how it is affected by double spending. Optimal range of double spending is derived that allows the quantum miner to gain from double spending while providing sufficient incentives for regular miners to participate in the network.

It is uncertain when sufficient quantum capabilities will arrive to reach a performance that would suffice to meet the 51% attack threshold. It is also uncertain how much time can be expected to pass until more quantum computer participants are to join the bitcoin network. The arrival of one single quantum miner can be a realistic scenario for a certain period but certainly not long-lasting. Once quantum computing is available to one participant, it is only a matter of time until others with quantum computing will also join. We can imagine that if all miners were equipped with quantum computing power, none would have the absolute advantage on top of other miners. Indeed, as long as there are two competing quantum miners, neither would be able to have the 51% computing power. In that sense, the plausible manipulation of the bitcoin system by a quantum miner would be short-lived and is limited to the first quantum miner.

The first quantum miner has an incentive to maintain the monopoly manipulation power as long as possible. The first quantum miner hence may want to hide the quantum identity, both for the purpose of maintaining the credibility of the bitcoin network and not to provide momentum for others to push for quantum computing. The appearance of quantum mining in bitcoin network negatively affects the trustfulness of the system. Bitcoin would be killed if other users/miners totally give up on it. Although the quantum miner could generate sufficient financial incentives for others to remain in the system, psychological and risk factors may still make people quit on bitcoin. Therefore, it is to the benefit of the quantum miner not to make others be aware of the presence of quantum mining.

Given the resource requirements on quantum computing, it is highly likely that the first occupant of quantum computing power is an organization, an institution, or even a government. Our analysis suggests there can be circumstances for the firstcomer to keep it secret for a certain time period.

Like bitcoin, other cryptocurrencies largely use blockchain and other such mechanisms for determining authentic cryptocurrency. Some cryptocurrencies are competing with bitcoin (such as Ethereum). Some are

complementary to bitcoin (such as Litecoin). When quantum computing is found to be used in mining bitcoin, the plausible impact on other cryptocurrencies in terms of users and market value are at least twofold, one through market competition, the other through credibility.

If quantum mining made bitcoin users shift to other competing cryptocurrencies, the market value of those cryptocurrencies would increase, and the price of bitcoin and its complements would decrease. Nevertheless, if the occurrence of quantum computing in bitcoin startled cryptocurrency users, the usage of all cryptocurrencies could fall. The initial impact of quantum computing on cryptocurrencies is likely to be negative due to lost confidence in network security. As more quantum miners join the mining and verification process of bitcoin and other cryptocurrency networks, the impact on all cryptocurrencies might eventually disappear.

Limitations and Future Work

This research on the economic analysis of quantum computing's impact on bitcoin network is based on given assumptions. While they serve well the purpose of this research, relaxing some assumptions will allow us to delve into other aspects of the impacts of quantum computing. For example, the quantity of goods and services bitcoin users want to purchase with bitcoin is held constant. It is likely that this real demand for bitcoin may decrease as the trust level of bitcoin network decreases. To compensate for the lack of trust, traders must ask for more bitcoin, equivalent to a decrease in bitcoin price, as modeled in this paper. Another example is that miners, bitcoin users and speculators are modeled as an entirety. A three- or four-party model could be built including quantum miners, regular miners, bitcoin users and/or speculators to study the details of welfare effects of double spending and other forms of 51% attacks on various stakeholders.

All bitcoin users/miners, in particular the first quantum miner, are assumed to be money driven. If the sole quantum miner has other incentives, such as grabbing as much short-term gain without caring about the future (being myopic or being in urgent need of wealth in the present term), the quantum miner would double spend up to the limit and kill the bitcoin network. It would be interesting to study the breaking point of double spending that can effectively kill a cryptocurrency, for both bitcoin with limited supply and cryptocurrencies with unlimited supply.

In a bitcoin network, miners are motivated by receiving reward with newly mined bitcoin and transaction fees. Transaction fees are omitted in the paper. Serving as the money issuing authority with double spending, the quantum miner may establish a fee rewarding system to build a sustainable blockchain system. Incentive mechanisms motivating various stakeholders are of interest.

The study is oriented on bitcoin. It would be interesting to see in what way the findings are also applicable to other blockchains, especially cryptocurrencies. For further studies, we will have an in-depth analysis on the implications of quantum computing on various cryptocurrencies and the effects of individual versus general features in cryptocurrencies may have on minimizing the risk of malicious actions such as 51% attacks.

Quantum miners, empowered with super computing power, have the potential ability to crack encryption. Malicious attackers could do a lot more damage to bitcoin networks than merely double spending. The possession of much of the computational power allows the attacker to launch a range of attacks including network-word censorship attack, fee market manipulation, etc. Other scenarios for a consensus attack may include Denial-of-Service (DoS) attacks against bitcoin participants (addresses) by excluding specific transactions for the period they control the network. This keeps the honest miners from reacquiring control of the network before the dishonest chain becomes permanent.

This research focuses on the economic implications of double spending as an example to illustrate the importance of financial incentives preventing quantum-equipped miners from destroying the system. The qualitative analysis provides insights to guide the potential preventative measures factoring in economic parameters to build quantum-resilient blockchain networks. Future research can extend to other forms of manipulations and attacks using quantum computers.

As future extension of the work, we also plan to provide a run-through example for formulas and have simulation and case studies to delve into practical issues in different scenarios to strengthen the robustness of the results.

Conclusion

Cryptocurrencies such as bitcoin rely on proof-of-work mining to secure the underlying blockchain protocols. The imminent arrival of quantum computing, as the most disruptive technology in modern history, imposes a fundamental threat to the survival of bitcoin and similar cryptocurrencies that require decentralization. Early adopters of quantum computing will gain dramatic absolute advantage over traditional miners and the supreme computing power they own will deplete others' chance of successful mining hence decreasing others' incentives to participate in the bitcoin network.

Security concerns such as 51% attacks launched by quantum miners may lead to a phenomenon called double spending, which seriously threatens the trustfulness of distributed ledgers like blockchains. We made interesting observation that double spending essentially breaks the theoretical bitcoin cap limit by introducing inflation thus diluting the value of bitcoin. This novel work studied the effects of double spending by a money-driven quantum miner on the sustainability of bitcoin networks. The market supply and demand analysis of bitcoin price formation was conducted by taking into consideration both the transaction and speculative demand for bitcoin, and the supply of bitcoin. Our modeling analysis suggests that the quantum miner faces a tradeoff between the short-term gain and the long-term benefit. The risk of deteriorating bitcoin value in the future prevents the quantum miner from over-double-spending, i.e., the quantum miner is restraint to the derived profitable range of double spending that provides sufficient financial incentives to induce network participation of regular miners as well, thus keeping the quantum miner from destroying cryptocurrencies.

The research findings indicate that killing bitcoin is not necessarily in the best interest of the quantum miner. As an early study focusing on the interplay between quantum computing and cryptocurrency, it is our hope that this research sheds light on understanding the economic aspect and security implications of quantum supremacy on cryptocurrency networks.

REFERENCES

Aggarwal, D., Brennen, G., Lee, T., Santha, M., and Tomamichel, M. 2018. "Quantum Attacks on Bitcoin, and How to Protect Against Them," *Ledger* (3).

Allende, M., Leon, D. L., Ceron, S., Pareja, A., Pacheco, E., Leal, A., Silva, M. D., Pardo, A., Jones, D., Worrall, D. J., Merriman, B., Gilmore, J., Kitchener, N., and Venegas-Andraca, S. E. 2023. "Quantum-resistance in Blockchain Networks," *Scientif Reports* (13): 5664.

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., and Wightman, P. 2021. "The 51% Attack on Blockchains: A Mining Behavior Study," *IEEE Access* (9), pp. 140549–140564.

Bakry, W., Rashid, A., Al-Mohamad, S., and El-Kanj, M. 2021. "Bitcoin and Portfolio Diversification: A Portfolio Optimization Approach," *Journal of Risk Financial Management* (14:7), pp. 1–24.

Bard, D. A., Kearney, J. J., and Perez-Delgado, C. A. 2022. "Quantum Advantage on Proof of Work," *Array* (15), p. 100225.

Benkoczi, R., Gaur, D., Nagy, N., Nagy, M., and Hossain S. 2022. "Quantum Bitcoin Mining," *Entropy* (24:3), p.323.

Bohme, R., Christin, N., Edelman, B., and Moore, T. 2015. "Bitcoin: Economics, Technology, and Governance, " *Journal of Economic Perspectives* (29: 2), pp. 213–238.

Budish, E. 2018. "The Economic Limits of Bitcoin and the Blockchain," *National Bureau of Economic Research*, Working Paper 24717.

Carlsten, M., Kalodner, H., Weinberg, S.M., and Narayanan, A. 2016. "On the Instability of Bitcoin Without the Block Reward," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, pp. 154–167.

Chiu, J., and Koeppl, T. V. 2022. "The Economics of Cryptocurrency: Bitcoin and Beyond," *Canadian Journal of Economics* (55:4), pp. 1762–1798.

Chohan, U. W. 2021. "The Double Spending Problem and Cryptocurrencies," *SSRN*.

Cong, L. W., He, Z., and Li, J. 2020. "Decentralized Mining in Centralized Pools, " *The Review of Financial Studies* (34:3), pp. 1191–1235.

Crosby, M., Pattanayak, P., Verma, S., and Kalyanaraman, V. 2016. "Blockchain Technology: Beyond Bitcoin," *Applied Innovation* (2), pp. 6–10.

Ebrahimi, Z., Routledge, B. R., and Zetlin-Jones, A. 2019. "Getting Blockchain Incentives Right," *Technical Report*, Carnegie Mellon University.

Hao, Y. 2022. "Research of the 51% Attack Based on Blockchain," in *Proceedings of the 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA)*, Changchun, China, pp. 278–283.

Holmes, S., and Chen, L. 2021. "Assessment of Quantum Threat to Bitcoin and Derived Cryptocurrencies," IACR Cryptol. ePrint Arch., p. 967.

Jang, J., and Lee, H.-N. 2020. "Profitable Double-spending Attacks," *Applied Sciences* (10:23).

Kajtazi, A. and Moro, A. 2018. "Bitcoin and Portfolio Diversification: Evidence from Portfolios of U.S., European and Chinese Assets, " *SSRN Electronic Journal*.

Kang, K.-Y. 2023. "Cryptocurrency and Double Spending History: Transactions with Zero Confirmation," *Economic Theory* (75), pp. 453–491.

Kappert, N., Karger, E., and Kureljusic, M. 2021. "Quantum Computing - the Impeding End for the Blockchain?" in *Proceedings of Pacific Asia Conference on Information Systems (PACIS)*, Dubai, UAE.

Karame, G. O., Androulaki, E., and Capkun, S. 2012. "Two Bitcoins at the Price of One? Double-spending Attacks on Fast Payments in Bitcoin, " IACR Cryptol. ePrint Arch., p. 248.

Khaki, A., Prasad, M., Al-Mohamad, S., Bakry, W., and Vo, X. V. 2023. "Reevaluating Portfolio Diversification and Design Using Cryptocurrencies: Are Decentralized Cryptocurrencies Enough?" *Research in International Business and Finance* (64), p. 101823.

Kim, K., Eddins, A., Anand, S., Wei, K. X., Berg, E. van den, Rosenblatt, S., Nayfeh, H., Wu, Y., Zaletel, M., Temme, K., and Kandala, A. 2023. "Evidence for the Utility of Quantum Computing before Fault Tolerance, " *Nature* (618), pp. 500–505.

Kristoufek, L. 2015. "What are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis, " *PLOS ONE* (10:4).

Kroll, J.A., Davey, I.C., and Felten, E.W. 2013. "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," in *Proceedings of the 12th Workshop on the Economics of Information Security*, Washington DC.

Lamport, L., Shostak, R., and Pease, M. 1982. "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems* (4:3), pp. 382–401.

Li, Y., and Wang, C.-C. 2022. "A Search-theoretic Model of Double-spending Fraud," *Journal of Economic Dynamics and Control* (142), p. 104157.

Li, Z., and Liao, Q. 2018. "Toward Socially Optimal Bitcoin Mining," in *Proceedings of the 5th IEEE International Conference on Information Science and Control Engineering (ICISCE)*, Zhengzhou, China.

Lovejoy, J. P. T. 2020. "An Empirical Analysis of Chain Reorganizations and Double-spend Attacks on Proof-of-Work Cryptocurrencies," MIT, Ph.D. dissertation.

Makarov, I., and Schoar, A. 2021. "Blockchain Analysis of the Bitcoin Market, " *National Bureau of Economic Research*, Working Paper 29369.

Murtazashvili, I., Murtazashvili, J. B., Weiss, M. B. H., and Madison, M. J. 2022. "Blockchain Networks as Knowledge Commons, " *International Journal of the Commons* (16:1), pp. 108–119.

Pagnotta, E.S. 2022. "Decentralizing Money: Bitcoin Prices and Blockchain Security," *The Review of Financial Studies* (35:2), pp. 866–907.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-peer Electronic Cash System," [Online]. Available: https://bitcoin.org/bitcoin.pdf

Nuzzi, L., Waters, K., and Andrade, M. 2024. "Breaking BFT: Quantifying the Cost to Attack Bitcoin and Ethereum, " *SSRN*.

Pinzon, C., and Rocha, C. 2016. "Double-spend Attack Models with Time Advantange for Bitcoin," *Electronic Notes in Theoretical Computer Science* (329), pp. 79–103.

Poluyanenko, N., Pisarenko, N. A., Safonenko, V., Makushenko, T., Pushko, O., Zaburmekha, Y., and Kuznetsova, K. 2019. "Simulation of a Double Spending Attack on the "Proof of work" Consensus Protocol, " *Radiotekhnika* (3:198), pp. 146–161.

Porat, A., Pratap, A., Shah, P., and Adkar, V. 2017. "Blockchain Consensus: An Analysis of Proof-of-Work and Its Applications," [Online]. Available: https://api.semanticscholar.org/CorpusID:32100244

Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M. F., and Knottenbelt, W. J. 2018. "Committing to Quantum Resistance: A Slow Defence for Bitcoin against a Fast Quantum Computing Attack," *Royal Society Open Science* (5): 180410.