How Much Should I Double Spend My Bitcoin? Game theory of Quantum Mining

Zhen Li[1] and Qi Liao[2] ✉

[1] Department of Economics and Management, Albion College, USA zli@albion.edu
[2] Department of Computer Science, Central Michigan University, USA
liao1q@cmich.edu

Abstract. Quantum computing as an inevitable technology can revolutionize many aspects of our society. One potential impact is on cryptocurrency such as Bitcoin, which relies on proof-of-work mining to secure the underlying blockchain protocol. Miners empowered by quantum computers will have superior computational power to win the competition. The quantum advantage jeopardizes the security and trustworthy of cryptocurrency and the transaction validation process by taking over a majority of the network's computing power, known as a 51% attack. Fraudulent Bitcoin transactions in the form of double spending can happen, and the emerging quantum miner could enable double spending and benefit from it. How much double spending is optimal without causing too much "inflation"? What shall be the optimal strategy of the first quantum miner facing the competition from other quantum miners? What are the implications of having one or multiple quantum miners to the security of the Bitcoin network? We conduct a novel game theoretic and economic analysis to address these questions. Simulation illustrates that quantum miners would have to collude to gain from double spending in a quantum competitive environment. The distribution of cryptocurrency between quantum miners and classical miners and how cost-effective classical miners are can affect the profitability and the sustainability of double spending as well as the collusion of quantum miners. Intensified quantum competition will decrease the chance of collusion and eventually make the Bitcoin network secure again. The critical point of quantum popularity that will eliminate double spending is found.

Keywords: Game Theory · Quantum Computing · Cryptocurrency · Bitcoin · Quantum Mining · Double Spending · Collusion · Cybersecurity · Economics

1 Introduction

Cryptocurrency such as Bitcoin is a decentralized digital currency and payment system based on classical cryptographic technologies which works without a central administrator such as a central bank in traditional currencies. The Bitcoin network operates on the Proof-of-Work (PoW) consensus mechanism to ensure the integrity of the network, allowing for secure and transparent peer-to-peer transactions without the need for intermediaries.

It is generally believed that Bitcoin is cryptographically protected against malicious modifications. The techniques used in cryptocurrency blockchains make them virtually unhackable if the networks are powerful enough to outpace hackers. However, in theory, Bitcoin can be subject to the so-called "51% attack." A malicious miner or a group of miners who control more than half of the network's mining can launch an attack on the blockchain network. Attackers could use their dominant computing power to alter the blockchain like interrupting the recording of new blocks by preventing other miners from completing blocks. Large miners could freeze any users' funds, erase past transactions, or launch other attacks like reversing transactions to double spend tokens.

With the current status of computation, it is nearly impossible to launch a successful 51% attack on a cryptocurrency like Bitcoin with a large participation rate. A recent report [20] suggests that the current state of security in Bitcoin makes 51% attacks economically unfeasible. However, the situation could change with the recently rapid development of quantum computers. Quantum computing is a cutting-edge computing paradigm that harnesses the principles of quantum mechanics known as quantum bits (qubits) to perform computations. The superposition and entanglement property of qubits as well as quantum gates and quantum algorithms will put the early adopters of quantum computers in an advantageous position also known as "quantum supremacy" where quantum computers can solve the complex problems that classical computers cannot solve.

The emerging technology of quantum computing may impose credible threat on the security of the Bitcoin network. When it comes to Bitcoin mining, miners equipped with quantum computers (i.e., quantum miners) can have incomparable advantage over classical miners in procuring mining rewards and rewriting blockchain history. Although quantum computers are not powerful enough yet [10], and researchers have suggested that 51% attacks on Bitcoin by quantum computers may not be possible until 2028, recent evidence indicates it could happen sooner [13]. With the superior computing power that no one can compete with, the first-moving quantum miner certainly has the potential to benefit from the advantageous computing power such as gaining from double spending.

Double spending can be viewed as digital equivalent of a perfect counterfeit. Intuitively, double spending of Bitcoin benefits the attacker but at a cost of deteriorating Bitcoin value. As the number of tokens increases with the attacker's double fake spending, the value of Bitcoin is eroded partially due to increased currency supply and inflation, and also due to trust in the network being damaged which may eventually destroy Bitcoin. Such dilemma imposes a constraint on the attacker's scale of double spending. What is the optimal double spending scale that is considered "healthy" without destroying Bitcoin? In addition, we believe the first quantum miner's monopolistic superior computing power will not last forever. Once quantum computing is available to one Bitcoin miner, it is only a matter of time until others with quantum computing will join, too. With multiple quantum miners, none would have the 51% computing power to double spend alone. What is the best strategy of the first quantum miner facing emerging quantum competition? How is the situation change with intensifying

quantum competition? What are the implications of the popularity of quantum computing on the sustainability and the security of the Bitcoin network?

To address these questions, this study conducts a novel game theoretic analysis on double spending strategies by quantum miners. It explores the appearance and evolution of quantum computing in the Bitcoin network focusing on the quantum miners' incentive to double spend. We first develop an economic model to find the equilibrium Bitcoin price using the supply and demand analysis of the Bitcoin market. We further explore the effects of double spending on the Bitcoin price and the economic well-being of various participants in the Bitcoin market. We develop a game theory model to study the strategic actions by the first quantum miner and other miners from whom more quantum miners emerge. Our work compares the first quantum miner's choices with and without quantum competition. The modeling analysis indicates that the first quantum miner can initially benefit from exercising the superior computing power to double spend. Once facing quantum competition, all quantum miners (including the first quantum miner) have solid financial incentives to collude with no motivation to cheat. Nevertheless, the likelihood of collusion keeps falling with intensified quantum competition. The collusion between quantum miners eventually breaks down, and the Bitcoin network would once again become immune to 51% attacks. We find that there are two critical break points of collusion or the ending points of double spending, one relates to the percentage of Bitcoin in possession of the first quantum miner, and the other relates to the percentage of the Bitcoin mining population that are quantum miners.

We believe this is the first research examining the implications of quantum competition on the Bitcoin network. An important insight is that the threat of quantum computing on Bitcoin security may be limited and short-lived. The first quantum miner and the subsequent quantum miners must walk a fine line to balance the benefit and the cost of double spending and share the profit of double spending. The first quantum miner can benefit from double spending using the superior computing power, but it is extremely difficult, if ever possible, to make double spending profit long-lasting. Collusion is a necessary condition for quantum miners to double spend in a competitive environment. Although quantum miners have the incentive to collude, the profitable and sustainable range of double spending shrinks with spreading quantum computing. In case the first quantum miner holds a large share of Bitcoin in circulation, the emergence of another quantum miner is sufficient to terminate double spending.

2 Background and Related Work

Bitcoin, as a decentralized cryptocurrency, operates by motivating participants to act in a way that benefits the entire network that involves various game situations, e.g., allocating computational power to mining [3], competing for mining rewards [16] and transaction fees [12], etc. Research suggests competition in Bitcoin mining increases energy consumption and may not be socially desirable

[14]. Game theory has been applied to the security and trust in the bitcoin networks including 51% attacks and double spending [4,17,25].

Consensus networks like PoW were created to prevent double spending in blockchain-based crypocurrencies [6] but this consensus is only reliable with the assumption that no single miner can hold more than 50% of the network's computational power. Quantum computing promises to have exponential speedup far surpassing classical computers [1] and is expected to impose threats on both the technical and the financial security of Bitcoin [8,13]. Even a single quantum miner with relatively low cartographical computing power can act strategically to manipulate the blockchain network [2].

Double spending is the most straightforward way to monetize the ability of breaching the 50% threshold to launch an attack on blockchain networks [21]. In theory, a double spending attack at any proportion of computing power can be made profitable [9]. It has been suggested that double spending can be prevented by costly mining and delaying settlement [5]. Technical countermeasures include the Proof-of-Stake (PoS) and other algorithms alternative to the PoW algorithm to enhance Bitcoin security [19,24]. Possible solutions and preventive measures are also studied considering the threats a quantum-capable attacker could impose on blockchain networks [10,11,23]. Researchers are taking measures to tackle the quantum challenge. A structured literature review [10] provides insights on weighing up the dangers of quantum computing and the countermeasures.

Quantum computing can also change the way classical games are played. If classic games are played on a quantum computer or played by a quantum computer, the games become quantum games. The emerging quantum computing has had a profound impact on the research domain in the context of multi-agent games [22]. The quantum advantage allows quantum players to have a distinct advantage over classical players to achieve higher payoffs at equilibrium [7]. Economic incentives were analyzed for both quantum and regular miners for optimal double spending [15].

Our research is related to existing literature on the incentive mechanisms of the bitcoin network and the quantum threat on bitcoin security on a novel angle: it focuses on the competition between quantum miners on top of the competition between quantum miners and classical miners. It applies game theory and economic principles to the security of bitcoin networks. To the best of our knowledge, this is the first game theoretic study exploring the threat of quantum computing on bitcoin networks in a quantum competitive environment.

3 An Economic Model of Bitcoin Market

In this section we establish a Bitcoin pricing model to explore the impacts of double spending on bitcoin value. For easy reference, Table 1 provides a list of major variables used in the paper and their brief definitions.

Table 1: Symbols and Definitions

Symbol/Variable	Definition
$\overline{B}$	capped Bitcoin maximum supply
B_0	units of Bitcoin rewarded to classical miners
D	double spending scale by the 1st quantum miner in case of monopoly and by both quantum miners in case of duopoly
D_1	double spending scale by the 1st quantum miner in case of duopoly
D_2	double spending scale by the 2nd quantum miner in case of duopoly
P_B	equilibrium Bitcoin price without double spending
P_D	equilibrium Bitcoin price with double spending
EP_B	expected Bitcoin price without double spending
EP_D	expected Bitcoin price with double spending
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 demanded for transaction purpose
S	units of Bitcoin demanded for speculative purpose
RR	required rate of return on Bitcoin investment
R	expected rate of return on Bitcoin investment
N	classical miner population
C	per-classical-miner operating cost of participation in Bitcoin network

3.1 The quantity analysis of Bitcoin as a medium of exchange

A medium of exchange is an intermediary instrument within an economy which is used primarily to facilitate transactions. Bitcoin already operates as a medium of exchange and Bitcoin in circulation satisfies the quantity equation

$$P_B T V = P Y \tag{1}$$

where P_B is the unit price of Bitcoin, T is the quantity of Bitcoin used as a medium of exchange, V is the velocity of Bitcoin that is a measurement of the rate at which one unit of Bitcoin is being transacted for goods and services in a time period, P is the price level of goods and services traded in Bitcoin, and Y is the units of goods and services traded in Bitcoin. Equation (1) is an identity that holds true by definition, similar to the quantity equation of money defined in economics.

From (1), the transaction demand for Bitcoin is

$$T = \frac{PY}{P_B V} \tag{2}$$

3.2 Supply and demand analysis of the Bitcoin market

The supply and demand analysis is the natural framework to learn insights about price determination. Here we apply the supply and demand analysis to the Bitcoin market to find the equilibrium Bitcoin price. In particular, the supply of Bitcoin comes from block mining which will eventually be fixed at $\overline{B}$, the designed maximum of Bitcoin. The supply of Bitcoin is exogenous to the model. The demand for Bitcoin includes both the transaction demand for payment purpose and the speculative demand for financial investment purpose. The quantity of Bitcoin demanded for transaction purpose is T as in the quantity analysis of Bitcoin. Bitcoin is also demanded for speculative purpose. Let S be the units of Bitcoin demanded for such purpose. The Bitcoin market equilibrium (without double spending) is

$$\overline{B} = \frac{PY}{P_B V} + S \tag{3}$$

where the right-hand-side is the combined demand for Bitcoin consisting of the transaction demand from (2) and the speculative demand.

Solving (3), the equilibrium Bitcoin price is

$$P_B = \frac{PY}{(\overline{B} - S)V} \tag{4}$$

As shown, Bitcoin price is increasing in the speculative demand for Bitcoin and decreasing in the supply of Bitcoin.

The key determining factor of the speculative demand for Bitcoin is the expected rate of return on Bitcoin investment ($R = \frac{EP_B - P_B}{P_B}$), which may or may not be equal or above the required rate of return (RR) holders desire to receive from Bitcoin investment. As in the finance literature, RR is defined as the minimum return an investor will accept for an investment as compensation for a given level of risk. We assume Bitcoin market participants have a common RR to hold Bitcoin for speculative purpose.

Given expected Bitcoin price, if $R < RR$ at the current Bitcoin price, the speculative demand for Bitcoin decreases and the Bitcoin price starts to fall until R rises to RR. If $R > RR$ at the current Bitcoin price, the speculative demand for Bitcoin increases and the Bitcoin price starts to rise until R falls to RR. In the steady state of the Bitcoin market, the rate of return on Bitcoin investment is equal to the required return, and the current Bitcoin price and the expected Bitcoin price have the following relationship:

$$EP_B = (1 + R)P_B \tag{5}$$

where $R = RR$.

In summary, the equilibrium of the Bitcoin market has two-fold meanings:

- The total Bitcoin supply is equal to the total Bitcoin demand including both the transaction demand and the speculative demand for Bitcoin (3).
- The expected rate of return on Bitcoin investment is equal to the required rate of return at the current market price of Bitcoin (5).

The latter implies that in Bitcoin market equilibrium, the market participants have a common expectation to see the Bitcoin price to grow by R each period.

Combining (3) and (5), we solve for the units of Bitcoin demanded for speculative purpose:

$$S = \overline{B} - \frac{PY(1+R)}{EP_B V} \tag{6}$$

In (6), $\overline{B}$, P, Y, R and V are all predetermined. There is a one-to-one correspondence between the expected future price of Bitcoin and the speculative demand for Bitcoin. As EP_B increases, S increases. As $EP_B \to 0$, $S \to 0$.

3.3 The impact of increased Bitcoin supply (double spending) on the Bitcoin market

Suppose the supply of Bitcoin increases from $\overline{B}$ to $\overline{B} + D$. The new Bitcoin market equilibrium satisfies the following two conditions:

$$P_D = \frac{PY}{(\overline{B} + D - S)V} \tag{7}$$

$$EP_D = (1+R)P_D \tag{8}$$

modified from (3) and (5).

Since the expected rate of return remains at R once the Bitcoin market reaches the new equilibrium, the speculative demand for Bitcoin stays the same as (6). As P, Y and V are all exogenous to the model and S stays unchanged, (7) indicates that an increase in Bitcoin supply apparently decreases the market value of Bitcoin, i.e., $P_D < P_B$. The increase in Bitcoin supply also decreases the expected price of Bitcoin, i.e., $EP_D < EP_B$ comparing (5) and (8).

The increased Bitcoin supply is fully absorbed into the transaction demand for Bitcoin with $P_B T = P_D(T+D)$, according to the quantity analysis of Bitcoin.

The economic impact of an increase in Bitcoin supply implies that the increase in the quantity of Bitcoin waters down the value of Bitcoin. The purchasing power of Bitcoin decreases but the speculative attractiveness of Bitcoin can be conserved so long as speculators receive the same expected rate of return equalling their required rate of return.

How is double spending compared to an authentic increase in Bitcoin supply? Double spending means that the same units of Bitcoin could potentially be spent multiple times. Successful double spending of Bitcoin essentially increases the use of Bitcoin for transaction purpose by the amount of double spending and reaches a total transaction demand for Bitcoin from T to $T + D$ where D is the scale of double spending, which represents both the increased transaction demand for Bitcoin and the increased supply of Bitcoin, keeping the Bitcoin market remain balanced with unchanged speculative demand for Bitcoin.

3.4 Double spending can be a self-destructive process

Different from increasing the money supply by printing money, the increase in the Bitcoin supply due to double spending is temporary. According to the quantity equation of Bitcoin (1), two scenarios may occur following a successful double spending at constant T, V and P.

Scenario 1: Y is largely unaffected, i.e., the need to use Bitcoin to make payments remains the same. In this case, the Bitcoin price will bounce back to the pre-double-spending level.

Scenario 2: Y decreases, e.g., when double spending makes fewer sellers willing to accept Bitcoin. In this case, the Bitcoin price will stay below the pre-double-spending level.

Scenario 1 is likely to be the case if double-spending does not diminish the need of Bitcoin to make payment. In practice, Bitcoin is often used for underground payments and illegal transactions, for ransomware payments, for governments to evade embargoes, etc. Such needs of Bitcoin is not economic per se and may not be sensitive to the changing market value of Bitcoin. In this case, the value of Bitcoin can self-recover after the temporary damage caused by double spending.

In contrast, the damage of double spending to the market value of Bitcoin is long-lasting in Scenario 2 when the deteriorating value of Bitcoin effectively decreases people's desire or ability to use Bitcoin to buy goods and services. If double spending continues, the Bitcoin price would keep falling and eventually, there could be no need to use Bitcoin to pay and Bitcoin would be worthless and become nonexistent. In other words, double spending can be a self-destructive process that leads to the extinction of Bitcoin, as depicted in Scenario 2.

4 Game Theory of Double Spending By Quantum Miners

As the economic analysis shows, there are both benefits and costs when a quantum miner double spends. We capture the dilemma using a stylized game to study the financial incentive for the first quantum miner to double spend strategically, in absence and with the appearance of subsequent quantum miners. Specifically, we explore the first quantum miner's decision-making in case of "monopoly" (when the first quantum miner is the only quantum miner) and "duopoly" (when there is a subsequent quantum miner).

Suppose initially there are one quantum miner (referred to as the "first quantum miner") and N non-quantum miners (referred to as "classical miners"). Without loss of generality, we assume all the miners are also Bitcoin users and investors in the Bitcoin market. The strategic interaction is between the first-moving quantum miner and classical miners from whom a subsequent quantum miner may emerge. All the parties are money driven.

To focus on the themes, we make the following assumptions to highlight several key features of the Bitcoin protocol and to simplify the situation:

- All miners participate the Bitcoin network with free entry and exit.

- There are no transaction rewards. Miners' welfare is measured by the market value of possessed Bitcoin.
- The total Bitcoin is fixed. Upon acquisition of quantum computing, the first quantum miner wins all mining competition and receives all remaining Bitcoin rewards.
- All classical miners have the same computational power thus their possession of Bitcoin and the mining cost are identical.
- Only quantum miners have the computing power to double spend. Quantum miners have the same computing power.
- Quantity of goods and services traded in Bitcoin is constant but units of Bitcoin needed to buy an item fluctuates with the Bitcoin price.

The unique features of the first quantum miner imply that the miner can act like the monetary authority controlling the supply of Bitcoin by managing double spending. When exercising the superior ability to double spend, the quantum miner has to do the cost-benefit analysis. For classical miners nonetheless, the inferior computing power disables them from winning the mining competition but they reserve the freedom of leaving the Bitcoin network.

The game proceeds as follows: The first quantum miner chooses the scale of double spending, which determines the current "money supply" of Bitcoin and hence the price of Bitcoin. Classical miners choose whether to exit the Bitcoin market. In a quantum competitive environment additionally, the subsequent miner determines whether to counter double spending.

Since all miners are money driven, the welfare effects of their decision-making determine their actions. The first quantum miner's choice of double spending is the key. Although the game is not modeled as a Stackelberg game, the first quantum miner can be viewed as the leader and the game can be solved using backward deduction starting from the classical miners' and the subsequent quantum miner's decision-making.

In the following analysis, we begin with the welfare analysis and the finding of game solutions in absence of quantum competition. We then discuss the situation in a quantum competitive environment.

4.1 Welfare impact of double spending

Double spending by the first quantum miner affects the welfare of all the miners.

Welfare impact of double spending on the first quantum miner Using the defined variables in Table 1, the units of Bitcoin held by the first quantum miner is $(\overline{B} - B_0)$. Specifically we define D, the double spending scale, as the number of tokens held by the quantum miner the miner uses to double spend once. We ignore the possibility of multiple double spending to make the model traceable and manageable. With this definition, $(\overline{B} - B_0)$ sets the upper bound on the double spending scale of the first quantum miner.

At the moment of double spending, the market value of Bitcoin is P_B so that the quantum miner gains an amount of $P_B D$. As double spending decreases the

market value of Bitcoin, the cost of double spending for the quantum miner is $(P_B - P_D)(\overline{B} - B_0)$. Taking into consideration both the benefit and the cost of double spending, the net welfare gain the first quantum miner receives is

$$\Pi = P_B D - (P_B - P_D)(\overline{B} - B_0) \tag{9}$$

Welfare impact of double spending on classical miners The loss to classical miners come from the decreased value of Bitcoin caused by double spending. For classical miners as a whole, their total loss is

$$(P_B - P_D)B_0 \tag{10}$$

which is equally shouldered by classical miners.

4.2 Finding profitable and sustainable double spending

The monopolistic quantum miner has the following constraints when making the rational choice of double spending:

- The upper bound of double spending is the monopolistic quantum miner's possession of Bitcoin.
- The quantum miner's net gain is non-negative.
- The Bitcoin network is resilient to double spending "attack" launched by the quantum miner, i.e., classical miners do not exit the Bitcoin network.

The three constraints correspond to the following three math relations:

$$0 \leq D \leq (\overline{B} - B_0) \tag{11}$$

$$P_B D - (P_B - P_D)(\overline{B} - B_0) \geq 0 \tag{12}$$

$$P_D \frac{B_0}{N} \geq C \tag{13}$$

where B_0/N is the holding of Bitcoin by an individual classical miner and C is the per-classical-miner's operating cost that includes the hardware cost, electricity, etc. Classical miners have the financial incentive to support the Bitcoin network as long as the remaining value of Bitcoin exceeds the cost of participating in the network. Although the initial investment in quantum computing is significant, once in operation, the fast quantum computing power largely saves the mining cost. Therefore, for simplicity, the operating cost of the quantum miner is not included. Adding quantum miners' cost function to the model will not change model conclusions. Indeed, it will strengthen the model conclusions by reducing the profit margin of quantum computing.

From (12), double spending is profitable for the first quantum miner at

$$D \geq \frac{(P_B - P_D)(\overline{B} - B_0)}{P_B} \tag{14}$$

Combined with (11), the profitable double-spending satisfies

$$\frac{(P_B - P_D)(\overline{B} - B_0)}{P_B} \leq D \leq (\overline{B} - B_0) \tag{15}$$

Combining (7) and (13), the sustainable double spending falls in the following range to keep classical miners stay in the Bitcoin network:

$$D \leq \frac{PYB_0}{NCV} + S - \overline{B} \tag{16}$$

Combining (15) and (16), we have the final specification of the range of double spending the first quantum miner shall pursue to make double spending both profitable and sustainable:

$$\frac{(P_B - P_D)(\overline{B} - B_0)}{P_B} \leq D \leq min\{(\overline{B} - B_0), \frac{PYB_0}{NCV} + S - \overline{B}\} \tag{17}$$

4.3 The impact of quantum competition

Naturally the first quantum miner can be the monopolistic quantum miner only for a certain time. Eventually subsequent quantum miners will occur. How will quantum competition change various miners' decision-making?

Subsequent quantum miner's choice Since all quantum miners are assumed to have the same computational power, if there are more than one quantum miner in the Bitcoin network, no individual miner could reach the threshold to launch a 51% attack. With the computational power compatible with the first quantum miner, the second quantum miner needs to choose if to use the power to prevent the first quantum miner from double spending. If yes, the market value of the Bitcoin held by the second quantum miner is $P_B \frac{B_0}{N}$; If not, the second quantum miner's welfare is $P_D \frac{B_0}{N}$. Apparently, the second quantum miner would be better off to prevent the first quantum miner from double spending. In other words, although the second quantum miner does not have the ability to double spend successfully, he/she still benefits from possessing the computational power to protect the Bitcoin network against double spending. Remaining classical miners benefit as well.

The insight learnt is that when there are multiple quantum miners in the Bitcoin network, the network can be resistent to 51% attacks.

The first quantum miner's choice facing quantum competition Since no individual miner, quantum or classical, would be able to double spend successfully acting alone, the first quantum miner is worse off for sure facing quantum competition. To double spend, the first quantum miner would have to collude with the subsequent quantum miner.

Collusive quantum miners In principle, the two quantum miners can collude to double spend. They jointly choose how much to double spend and share the net gains. Suppose the first quantum miner double spends D_1 and the second quantum miner double spends D_2. They face the following constraints:

$$0 \leq D_1 \leq (\overline{B} - B_0) \tag{18}$$

$$0 \leq D_2 \leq \frac{B_0}{N} \tag{19}$$

$$P_B D_1 - (P_B - P_D)(\overline{B} - B_0) \geq 0 \tag{20}$$

$$P_B D_2 - (P_B - P_D)\frac{B_0}{N} \geq 0 \tag{21}$$

$$P_D \frac{B_0}{N} \geq C \tag{22}$$

Of above, the first two equations limit the feasible range of double spending by each quantum miner, the second two guarantee that double spending is profitable for the quantum miners, and the last serves to keep classical miners from exiting the Bitcoin market. Solving these inequalities, the common ranges that satisfy all of the constraints are

$$\frac{(P_B - P_D)(\overline{B} - B_0)}{P_B} \leq D_1 \leq (\overline{B} - B_0) \tag{23}$$

$$\frac{(P_B - P_D)\frac{B_0}{N}}{P_B} \leq D_2 \leq \frac{B_0}{N} \tag{24}$$

$$D_1 + D_2 \leq \frac{PYB_0}{NCV} + S - \overline{B} \tag{25}$$

There can be various combinations of $\{D_1, D_2\}$ that make double spending profitable and sustainable. We will use simulations to illustrate the sets of solutions and the impacts on the first quantum miner when facing quantum competition.

5 Simulation Analysis And Numerical Examples

In this section, we parameterize the model and illustrate the profitability, feasibility and sustainability of double spending by the first quantum miner and the plausible collusion between quantum miners. Due to lack of transparency in the Bitcoin network regarding Bitcoin ownership and transactions, it is hard to find data sources to assign values to the variables. We look for publicly available data and assign values with the priority of having the relative values meaningful rather than having the values match the real-world data.

5.1 Assigning values to variables

Bitcoin was designed from its inception to have a capped supply of 21 million tokens. Bitcoin has a history of fluctuating and ever-increasing price. Starting at a price of zero when it was introduced in 2009, the Bitcoin price reached over $70,000 in May 2024. The price jumps and fluctuations generally reflect investor enthusiasm, demand, and supply. The historical record of Bitcoin shows the market certainly has not yet shown the steady state. The actual data on Bitcoin supply, demand and price may not be a good fit for this simulation purpose.

As for the number of people participating in the Bitcoin market, the exact number of Bitcoin miners is difficult to determine due to the decentralized and anonymous nature of the network. Estimates suggest that there are tens of thousands of active miners worldwide. As of March 2024, there are just over 46 million Bitcoin wallets holding at least $1 of value. Around 40% of Bitcoin ownership falls into identifiable categories, including exchanges, miners, governments, balance sheets of public companies, and dormant supply [18].

We choose an approach to use hypothetical parameter values along with the scaling-down of some realistic data to simulate the effects of double spending. We assume there are initially 1 quantum miner and 100 classical miners. The first quantum miner holds 10% of the total Bitcoin. The total supply of Bitcoin is fixed at $2,000$, of which the first quantum miner holds 200 and each classical miner holds 4.5. In the Bitcoin market equilibrium, 70% Bitcoin is demanded for speculative purpose and 30% is for transaction purpose. That is, the values of the parameters are set as $N = 100$, $\overline{B} = 2,000$, $B_0 = 1,800$, $S = 1,400$, $T = 600$. We also set $P = 1$, $V = 2$ and $Y = 12,000$.

5.2 The case of no quantum competition

At the specified parameters, the initial Bitcoin price is 10 from (4). From (7), The relationship between double spending and the Bitcoin price is

$$P_D = \frac{6,000}{600 + D} \tag{26}$$

In absence of quantum competition, the first quantum miner's choice of profitable and sustainable double spending, from (17), is defined by

$$20(10 - P_D) \leq D \leq min\{200, (\frac{120,000}{C} - 600)\} \tag{27}$$

Replacing P_D in (27) with (26), we can find all the profitable and sustainable scale of double spending the first quantum miner can choose from:

$$20(10 - \frac{6,000}{600 + D}) \leq D \leq min\{200, (\frac{120,000}{C} - 600)\} \tag{28}$$

At $C = 150$, $(\frac{120,000}{C} - 600) = 200$. Such cost can be called the "accommodation cost." If the operating cost of classical miners is no higher than the

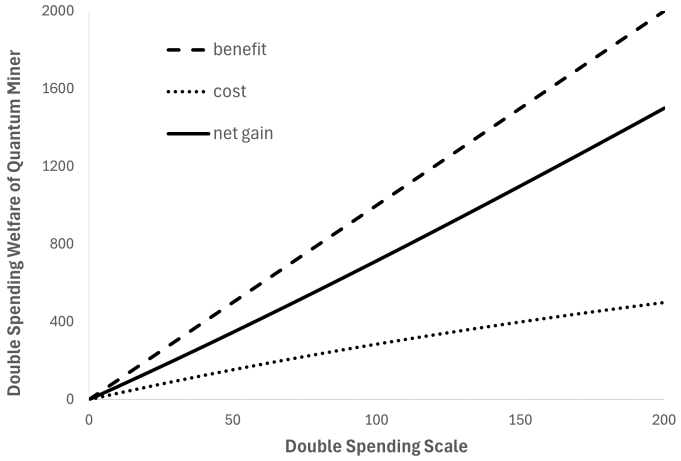

Fig. 1: The welfare effects of double spending (i.e., benefit, cost and net gain) for the monopolistic quantum miner when the miner holds 10% of total Bitcoin. As shown, the net gain of double spending is increasing in the level of double spending. The optimal strategy is to double spend to the upper bound of the profitable and sustainable range of double spending.

accommodation cost, the first quantum miner would be able to double spend all the possessed Bitcoin. Otherwise, the first quantum miner would have to limit the actual double spending at a level below the quantity of possessed Bitcoin. The implication is that the efficiency of classical miners can be beneficial to quantum miners. As cost-effective classical miners are more likely to remain in the Bitcoin network, the quantum miner has more flexibility to double spend.

The first quantum miner's net gain of double spending is

$$\Pi = 10D - 200(10 - \frac{6,000}{600 + D}) \tag{29}$$

which is the difference between the benefit and the cost of double spending.

Figure 1 illustrates how the benefit, the cost and hence the net gain of the first quantum miner changes with the scale of double spending when the first quantum miner holds 10% of total Bitcoin. As shown, both the benefit and the cost increase with the scale of double spending. At the specified parameters, the benefit increases faster than the cost so that the optimal level of double spending is the highest possible double spending that is feasible and sustainable. In other words, the first quantum miner will double spend to the limit of the feasible and the sustainable range.

The ever positive and increasing net gain of double spending at any level of double spending is largely due to the small share of Bitcoin in the possession of the quantum miner whose double spending does not significantly affects Bitcoin supply or Bitcoin price. What if the quantum miner holds a big share of Bitcoin? As an extension of the simulation, we keep other parameters unchanged but

assume the first quantum miner holds 60% of total Bitcoin or 1,200 Bitcoin tokens.

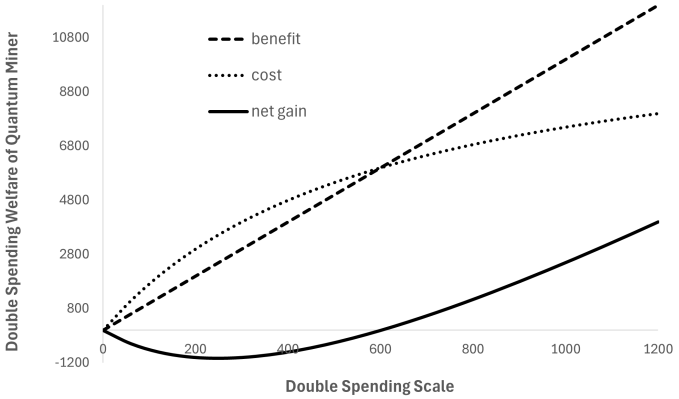

Fig. 2: The welfare effects of double spending (i.e., benefit, cost and net gain) for the monopolistic quantum miner when the miner holds 60% of total Bitcoin. As shown, the net gain of double spending initially falls before it starts rising. When the monopolistic quantum miner holds a large share of total Bitcoin, the miner has to double spend beyond a threshold to make double spending profitable.

Figure 2 illustrates how the benefit, the cost and hence the net gain of the first quantum miner changes with the level of double spending when the first quantum miner holds 60% of total Bitcoin. As shown, the benefit and the cost still increase with the level of double spending, which is true regardless anyway, but the cost is increasing faster than the benefit initially. Therefore when the quantum miner's holding of Bitcoin is a large share of total Bitcoin in circulation, the miner has to double spend beyond a certain threshold to make double spending profitable. In this numerical example, the threshold is $D = 600$, as can be solved from (14).

To generalize, assuming classical miners are sufficiently efficient, i.e., $C \leq 150$, so that the upper bound of double spending by the quantum miner is the Bitcoin held by the quantum miner. The range of profitable and sustainable double spending at various possession of Bitcoin by the quantum miner is illustrated in Figure 3. Double spending would be profitable and sustainable so long as the quantum miner chooses to double spend within the range. For most part, the width of the range is constant at 600. This is largely because of the model assumptions that lead to a proportional change in the Bitcoin price along with an increase in the Bitcoin supply. If we factor in other considerations such as psychological (e.g., the lost confidence of Bitcoin users when the quantum miner holds more Bitcoin), the range may start narrowing when the Bitcoin holding by the quantum miner reaches a certain level.

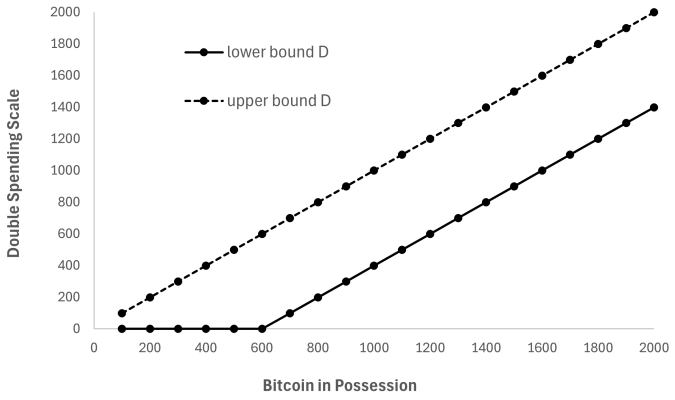

Fig. 3: The range (lower/upper bounds) of the profitable and sustainable scale of double spending for the monopolistic quantum miner at various levels of Bitcoin in possession. The actual double spending by the miner has to fall within such boundary.

5.3 Quantum mining collusion in a competitive environment

Now we look at the duopolistic competition and collusion between the first quantum miner and a subsequent quantum miner. Jointly, there are three constraints imposed on the two quantum miners' choice of double spending:

$$20(10 - P_D) \leq D_1 \leq 200 \tag{30}$$

$$1.8(10 - P_D) \leq D_2 \leq 18 \tag{31}$$

$$D_1 + D_2 \leq \frac{120,000}{C} - 600 \tag{32}$$

Previous simulations show that the net gain of double spending is increasing in the scale of double spending beyond a threshold (0 or above). An individual quantum miner would want to double spend at the maximum, which would only be possible if $C \leq 147$, in which case $D_1 = 200$ and $D_2 = 18$, and the quantum miners would easily form a coalition. Neither party would have an incentive to deviate. Note the accommodation operating cost of classical miners is smaller at the presence of multiple quantum miners, implying that the prerequisite for the optimal collusion between quantum miners is the improved efficiency of classical miners. The more efficient classical miners are, the more likely for more quantum miners to form an optimal coalition.

Nevertheless, if $C > 147$, not all quantum miners can reach the maximum possible double spending. The quantum miners would have to compromise and each chooses a scale of double spending that is below their upper bound.

Suppose $C = 160$, then $D_1 + D_2 \leq 150$ from (32), i.e., the combined double spending must be no higher than 150. The first quantum miner has to bargain with the subsequent quantum miner to coordinate double spending.

What are the subsequent quantum miner's options? There are three possibilities:

- Do nothing. The welfare effect on the subsequent quantum miner is $-(P_B - P_D)\frac{B_0}{N} = -36$.
- Do not collude but use the quantum power to prevent the first quantum miner from double spending. The welfare effect is 0.
- Collude to share the net gain of double spending with the first quantum miner. The welfare effect is $10D_2 - 36$.

Apparently, the subsequent quantum miner's best strategy is to collude if given an assigned share of double spending $D_2 \geq 3.6$. In this double spending game, both quantum miners have no incentives to cheat. On one hand, the net gain is increasing in the scale of double spending so the parties have no incentives to under spend. On the other hand, since the agreed-upon allocation of double spending satisfied $D_1 + D_2 = 150$. One party's over spending would push classical miners exit the Bitcoin market hence killing the Bitcoin network. Unless the quantum miner is extremely myopic, the quantum miner would limit double spending to make classical miners stay. The numerical example shows that when facing the quantum competition, quantum miners have an incentive to collude, and their coalition is stable.

At $B - B_0 = 200$, the range of profitable and sustainable double spending is $0 \leq D_1 \leq 200$, as shown in Figure 3. The first quantum miner certainly benefits from collusion that makes double spending possible. Nevertheless, as the number of subsequent quantum miner reaches 42, it would no longer be possible to find any feasible allocation of double spending to enable collusion. There will be no more double spending. $N^* = 42$ is the critical quantum popularity that will effectively terminate double spending. In other words, in this numerical example, when quantum computing reaches about 40% of the mining population, no quantum miners can successfully double spend no matter how collusive and collaborative they are.

In Figure 4, we illustrate the critical quantum mining penetration rate in relevance to the Bitcoin possession by the first quantum miner at $C = 160$, i.e. $D_2 \geq 0.2\frac{B_0}{100}$, holding $D_1 = 0$ for the purpose of simulating the feasibility of quantum mining collusion. Quantum mining penetration rate is measured by quantum miners as a percentage of the mining population. The critical penetration rate is a break point of double spending beyond which double spending disappears. Figure 4 shows that the distribution of circulating Bitcoin between the first quantum miner and classical miners is essential. At first, at low levels of Bitcoin in possession of the first quantum miner, an increase in the Bitcoin holding by the quantum miner increases the room of quantum mining collusion. The more classical miners hold Bitcoin, the short-lived is double spending. Nevertheless, beyond the turning point of the curve, an increase in the fist quantum miner's holding of Bitcoin decreases the likelihood of collusion and eventually,

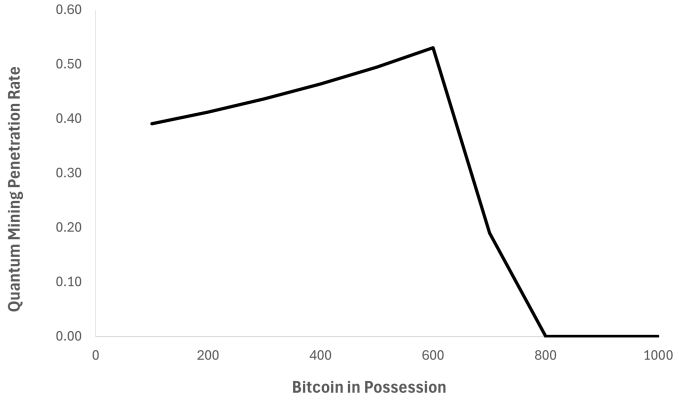

Fig. 4: The critical (maximum) penetration rate of quantum mining to enable collusion among quantum miners. For example, at the turning point 600 Bitcoin possession (30% of total Bitcoins), quantum miners may still collude if quantum mining does not exceed 53% among all mining processes.

quantum competition totally disables double spending practice in the Bitcoin network. If the first quantum miner holds a certain amount of circulating Bitcoin (around 780 in the simulation), there is no more room to collude with subsequent quantum miners even at $D_1 = 0$.

In other words, collusion between quantum miners is not always feasible. We have to combine Figures 3 and 4 to find the mutually beneficial shares of double spending between the first quantum miner and the subsequent quantum miners. At $B - B_0 = 800$ for example, the lower bound of the first quantum miner's double spending is 200, which exceeds 150. The first quantum miner will not be able to share double spending with the subsequent quantum miner who will prevent the first quantum miner from double spending. The line in Figure 4 depicts critical quantum penetration to disable double spending. The intersection of the line and the x-axis is the break point of Bitcoin possession by the first quantum miner to make double spending possible facing quantum competition. Beyond the point, the appearance of just another quantum miner will suffice to terminate double spending practice. Although different parameters will change the numerical values of quantum mining profit, the critical penetration rate, etc., they do not affect the model conclusions.

6 Conclusion and Future Work

The appearance of quantum computing imposes a fundamental threat to the survival of cryptocurrencies such as Bitcoin. Early adopters of quantum computing will have unprecedented advantage over traditional miners and exercise the superior computing power to launch 51% attacks on the Bitcoin network such as profiting from double spending. This paper conducts the economic and game

theoretic analysis of the interconnections between emerging quantum computing and cryptocurrency security. The research explores the effects of double spending and quantum computing competition on the welfare of the Bitcoin market participants and the overall security of the Bitcoin network. A stylized game is developed to explore the strategic interactions between Bitcoin miners with a focus on the decision-making by the first quantum miner in absence and with quantum competition from subsequent quantum miners.

The research results suggest that in absence of quantum competition, the first quantum miner, as the money-driven monopolistic quantum miner, shall choose the level of double spending in a sustainable range that is profitable to the monopolistic quantum miner and also provides sufficient financial incentives to encourage the network participation of classical miners. The appearance of subsequent quantum miners makes the first quantum miner worse off. Facing quantum mining competition, quantum miners have to collude to successfully double spend. Simulations illustrate that the key factors determining the profitability and the sustainability of double spending in a quantum competitive environment are the distribution of Bitcoin between the first quantum miner and other miners and the intensity of quantum competition. Most interestingly, the thresholds and critical turning points of collusion among quantum miners were identified in simulations.

Notable findings also indicate the cost effective classical miners are beneficial to quantum miners. The early quantum miners' holding of Bitcoin is a double-edged sword. The increased holding of Bitcoin by the first quantum miner can make double spending more profitable and longer-lived but only up to a certain point. Increased penetration rate of quantum mining and presence of quantum competition will eventually terminate double spending practice and make the Bitcoin network secure again. To that end, we recommend and encourage quantum competition. Future research is necessary to implement quantum security measures against quantum-based double spending practice before its self-healing.

References

1. Arute, F., Arya, K., Babbush, R., et al.: Quantum supremacy using a programmable superconducting processor. Nature **574**, 505–510 (October 23 2019)
2. Bailey, B., Sattath, O.: 51% attack via difficulty increase with a small quantum miner. arXiv (2403.08023) (March 2024)
3. Bertucci, C., Bertucci, L., Lasry, J.M., Lions, P.L.: Mean field game approach to bitcoin mining. arXiv (2004.08167) (April 2020)
4. Breiki, H.A.: Trust evolution game in blockchain. In: Proceedings of 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA). Abu Dhabi, United Arab Emirates (December 05-08 2022)
5. Chiu, J., Koeppl, T.V.: The economics of cryptocurrency: Bitcoin and beyond. Canadian Journal of Economics **55**(4), 1762–1798 (November 2022)
6. Chohan, U.W.: The double spending problem and cryptocurrencies. SSRN (January 6 2021)
7. Eisert, J., Wilkens, M., Lewenstein, M.: Quantum games and quantum strategies. Physical Review Letters **83**(15), 3077–3080 (October 11 1999)

8. Holmes, S., Chen, L.: Assessment of quantum threat to bitcoin and derived cryptocurrencies. IACR Cryptol. ePrint Arch. **2021**, 967 (2021)
9. Jang, J., Lee, H.N.: Profitable double-spending attacks. Applied Sciences **10**(23) (2020)
10. Kappert, N., Karger, E., Kureljusic, M.: Quantum computing - the impeding end for the blockchain? In: Proceedings of Pacific Asia Conference on Information Systems (PACIS). Dubai, UAE (June 2021)
11. Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., Trushechkin, A.S., Yunusov, R.R., Kurochkin, Y.V., Lvovsky, A.I., Fedorov, A.K.: Quantum-secured blockchain. Quantum Science and Technology **3**(3), 35004 (May 31 2018)
12. Kim, D., Ryu, D., Webb, R.I.: Determination of equilibrium transaction fees in the Bitcoin network: A rank-order contest. International Review of Financial Analysis **86** (March 2023)
13. Kim, Y., Eddins, A., Anand, S., Wei, K.X., van den Berg, E., Rosenblatt, S., Nayfeh, H., Wu, Y., Zaletel, M., Temme, K., Kandala, A.: Evidence for the utility of quantum computing before fault tolerance. Nature **618**, 500–505 (2023)
14. Li, Z., Liao, Q.: Toward socially optimal bitcoin mining. In: Proceedings of 5th IEEE International Conference on Information Science and Control Engineering (ICISCE). Zhengzhou, China (July 20-22 2018)
15. Li, Z., Liao, Q.: Is quantum computing the bitcoin terminator? In: Proceedings of the 30th Americas Conference on Information Systems (AMCIS). pp. 1–10. Salt Lake City, Utah (August 15-17 2024)
16. Li, Z., Reppen, A.M., Sircar, R.: A mean field games model for cryptocurrency mining. Management Science **70**(4) (June 2023)
17. Liu, Z., Luong, N.C., Wang, W., Niyato, D.T., Wang, P., Liang, Y.C., Kim, D.I.: A survey on applications of game theory in blockchain. ArXiv (1902.10865) (2019)
18. Moore, W.O.: Demystifying bitcoin's ownership landscape. Grayscale (November 30 2023)
19. Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T., Dutkiewicz, E.: Proof-of-Stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. IEEE Access pp. 85727–85745 (June 26 2019)
20. Nuzzi, L., Waters, K., Andrade, M.: Breaking BFT: Quantifying the cost to attack Bitcoin and Ethereum. SSRN (February 15 2024)
21. Pinzón, C., Rocha, C.: Double-spend attack models with time advantange for bitcoin. Electronic Notes in Theoretical Computer Science **329**, 79–103 (2016)
22. Pérez-Antón, R., Sánchez, J.I.L., Corbi, A.: The game theory in quantum computers: A review. International Journal of Interactive Multimedia and Artificial Intelligence (September 2023)
23. Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M.F., Knottenbelt, W.J.: Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack. Royal Society Open Science **5:180410** (2018)
24. Tas, E.N., Tse, D., Gai, F., Kannan, S., Maddah-Ali, M.A., Yu, F.: Bitcoin-enhanced Proof-of-Stake security: Possibilities and impossibilities. In: Proceedings of 2023 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA (May 21-25 2023)
25. Zaghloul, E., Li, T., Mutka, M.W., Ren, J.: Bitcoin and blockchain: Security and privacy. IEEE Internet of Things Journal **7**(10), 10288–10313 (2020)