Chapter 2
Financial Data, Blockchain, Decision-Making and Quality of Experience

2.1 Financial Data, Blockchain and Game Theory

Blockchain is a technology that enables cryptocurrency, such as bitcoin (the most popular cryptocurrency). Cryptocurrency, in general, is a digital payment system that does not rely on banks as intermediary nodes to complete monetary transactions, but instead it is a peer-to-peer digital payment system that can enable anyone to participate in monetary transactions, e.g. to send and receive payments. Game theoretic philosophy is a core aspect of blockchain design.

2.1.1 Financial Data and Blockchain

Cryptocurrencies, and blockchain as their underlying technology, have revolutionized the transaction of funds, as well as the potentialities of blockchain in how people, organizations and societies can function and conduct business (DiNizo 2018). When it comes to blockchain-based digital currencies (and cryptocurrencies), bitcoin (Nakamoto 2008) has been the most prominent (Abramova and Böhme 2016). In that context, blockchain technology acts as a decentralized (with peer-to-peer (P2P) networks) and encrypted security system for a distributed ledger; a chain of data blocks each of which keeps track and record of (cryptocurrency) transactions. Each block records a crypto hash for the block before it (hence, a "chain"), the transaction data and a timestamp (Du et al. 2019). Pairs of public and private keys compose a public key infrastructure (PKI) which enables the secure transfer of data (Abramova and Böhme 2016) and where the chained blocks prevent the tampering of the previously manifested transactions (Beck et al. 2018).

Blockchain allows for the creation of autonomous, self-governing and self-regulating infrastructure (Chapron 2017; Wörner et al. 2016), overwriting the need

J. Antoniou, O. Tringides, *Effects of Data Overload on User Quality of Experience*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-031-06870-6_2

of supporting traditional financial institutions and authorities who would normally act as a trusted mediating third party or centralized authority (being government or private financial institutions) (Aste et al. 2017; Barrett et al. 2016) (Fig. 2.1).

As financial transactions and trading activities are dependent on trust (Tang 2018), for blockchain technology's application in the financial sector, trust is paramount, as the execution of payment transactions must be secure (Kshetri 2018). Blockchain is thus particularly fitting for the context of decentralized environments, where parties (humans or devices) lack mutual trust (Lindman et al. 2017). Cryptocurrencies (with blockchain) enable mutually mistrusting entities to perform financial transactions without relying on a central trusted third party while offering a transparent and integrity-protected data storage (Nakamoto 2008). As a result of decentralization of blockchain applications, it reduces the risks and challenges of both privacy and trust (Lindman et al. 2017).

In the blockchain, once an element becomes part of the blockchain, it cannot be altered, thus providing an indisputable record of past transactions.

Blockchain is open source and thus transparent for everyone; this is an important factor of trust, as malicious code cannot be added into it.

For transactions, each user on a blockchain has a blockchain address (a unique alphanumeric address), and they can decide to keep it secret or open to others (Tapscott and Tapscott 2017), helping them preserve their anonymity. There isn't any centralized financial institution that stores users' private information (Zheng et al. 2018).

Distributed ledgers record transactions automatically and in real time, reducing the possibility of fraud (Rennock et al. 2018), where replication among all network members allows for each transacting members to check transaction history, and thus the blockchain can be managed effectively (Pereira et al. 2019) without the need of a third party (Tapscott and Tapscott 2017). This reduces uncertainty, insecurity and ambiguity in transactions, among all network participants (Nærland et al. 2017).

In a given blockchain network, a consensus mechanism aims to bring a unified agreement on the validation of all transaction records within the network, given the absence of a central authority (Chang et al. 2020).

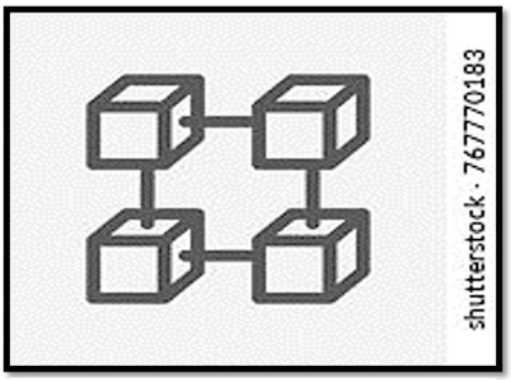

Fig. 2.1 Blockchain is a transparent technology making it a trusted technology. (This photo by unknown author is licensed under CC BY Creative Commons Attribution 3.0 Unported)

A main advantage (and main driver) of this trusted self-regulating setup is the reduction of transaction costs (Karafiloski and Mishev 2017). This is largely because it reduces the need to rely on trusted third parties (Iansiti and Lakhani 2017), as reliance on a centralized third party for the safety of one's assets is no longer required (Tama et al. 2017). Beyond the decrease of the cost of trading, the time for a transaction is also decreased, again because it removes the need of handling by a trusted third party (Staples et al. 2017), using P2P directly instead. This is contrasted with the traditional financial environment, where, for example, a commercial bank is responsible for maintaining ledgers and executing transactions (Hull et al. 2016) and a central bank is required to verify each transaction (Zheng et al. 2018). As with the distributed system, the copy of the ledger is present with all its members; thus, the distributed trust offered by blockchain technology removes the need of any trusted third party or authority to facilitate, verify or approve transactions.

Although so far the majority of applications of blockchain has been for payment transactions, beyond that, it is becoming a core technology in the FinTech sector (Du et al. 2019) and at the same time extends its potential in further financial, commercial (Underwood 2016) and social contexts. This is because blockchain, by providing a secure audit trail that cannot be tampered or corrupted, allows people to build trust faster and has the potential to change (global) financial infrastructures (Pilkington 2016). Thus, blockchain can be used in other various financial services, such as digital assets (Peters et al. 2015), as blockchain can assert and manage asset ownership and contracts (Mattila 2016).

Further advantages of blockchain are facilitating the automation and streamlining of processes and removing manual back office labour (Walker et al. 2016). Blockchain technology is resilient, as it is not prone to any sort of major attacks. Members in a blockchain network can implement conditions and rules in the form of smart contracts (algorithmic programs), where they can automatically execute transactions (Tapscott and Tapscott 2017).

Blockchain facilitates validated, tamper-resistant transactions that are consistent across the network participants (Beck et al. 2018), maintaining that the database is complete, distributed and unalterable (Yoo 2017). Blockchain can give users confidence that no record of transactions has been altered either deliberately (e.g. hacking or fraud) or accidentally (e.g. due to technical fault) (Beck et al. 2018).

The development of blockchain technologies and applications is ongoing and still faces challenges until they reach maturity: challenges such as efficiency in mining (the issue of power consumption and the resulting carbon footprint) especially when it comes to scalability, as well as issues of privacy and security (where the need and question of legal regulation are important challenges (Tu and Meredith 2015) in order to enhance secure, ethical and smart application).

2.1.2 Blockchain and Game Theory

Game theory's basic philosophy is to study different models of strategic decision-making. The aim of the blockchain technology is to motivate anonymous nodes to collaborate for the common good of the network. To motivate the nodes to follow such decision-making, strategic decision-making must be employed. The goal is to design systems so that everyone acting in their own self-interest will help the network instead of being harmful to it. The *prisoner's dilemma* game model is an appropriate game theoretic model to showcase how this can be achieved.

The prisoner's dilemma is basically a model of a game, where two players must decide whether to cooperate with their opponent or whether to defect from cooperation. Both players make a decision without knowing the decision of their opponent, and only after the individual decisions are made, these are revealed. There is a story behind the model, which goes something like this:

> Two suspects are arrested by the police. Since the policemen have insufficient evidence for their conviction, they separate the two suspects and offer them a deal. If one testifies against the other, i.e. defects, and the other remains silent, i.e. cooperates, the betrayer goes free, and the silent one goes to prison for 10 years. If they both remain silent, they both go to prison but only for 6 months on a minor charge. If they both testify against each other, they both go to prison for 5 years. Each suspect must choose whether to testify or whether to remain silent.

The specific example has several considerations. Mutual cooperation has a reward for both of them receiving the least harsh punishment. However, such decision entails the risk that in case one of the players defects, then the other player will receive the harshest punishment. Given the risk of cooperation, it is very tempting to defect because if the opponent cooperates, then defecting will result in the best payoff with no punishment. If both defect, the punishment is still not the harshest one. The decision-making process is a selfish one. Each player will consider what the other player will do. If the other player cooperates, then defecting is the best strategy as it will result in no punishment. If the other player defects, then the best strategy is to also defect to avoid the harshest punishment. So, given this reasoning, both players will defect receiving an average punishment. However, this is not the best possible outcome for the game since if they cooperated they would get away with the least harsh punishment.

The desirable cooperative behaviour must be somehow motivated so that the players' selfish but rational reasoning results in the cooperative decision. The above description of the game is based on a one-shot game model of the prisoner's dilemma, i.e. the players have to decide only once – no previous or future interaction of the two players affects this decision. Cooperation may evolve, however, from playing the game repeatedly with the same opponent. This is referred to as the *iterated prisoner's dilemma,* which is based on a repeated game model with an unknown or infinite number of repetitions. The decisions at such games, which are taken at each repetition of the game, are affected by past actions and future expectations, resulting in strategies that motivate cooperation. The way motivation may be

encouraged in such games will be analysed also with respect to the blockchain context. Remember that the goal when modelling the blockchain interaction is to motivate cooperation, such that selfish nodes make decisions that will help the blockchain network.

2.1.2.1 Introducing the Blockchain Scenario

The blockchain technology is basically, as the name implies, a *chain of blocks.* These blocks contain information and represent a digital ledger, where transactions are recorded. This ledger is open to anyone and is not kept by an intermediary authority, like a bank. With regard to this ledger, note that once data has been recorded inside a blockchain, it is quite hard to alter it. The type of data that can be stored in any block depends on the type of blockchain. A very popular type of blockchain is the *bitcoin* blockchain, and the type of data stored is transaction details, e.g. payment receiver, payment transmitter, number of coins, etc. Blockchain uses a peer-to-peer network, and everyone is allowed to join. Once someone joins, they get a full copy of the blockchain, which they can validate.

The validation of blocks uses hashes. A hash is the outcome of a hashing algorithm that aims in essentially producing a unique value for any piece of data, which can act as its identity. Since hashes cannot be reversed, one cannot reconstruct a piece of data from access to its hash. However, since a hash is a unique identity for the piece of data that it represents, it can be used to show that a file has not been altered or tampered with, by keeping the original hash of a file and regenerating it for validation.

In the blockchain environment, what we end up with is a system where everyone's history is a series of blocks, also known as a *chain*, and the blocks may not be independent of each other, but each one is validated using hashes. We also have *miners*, which are nodes that are completing the necessary computational work to validate these blocks, by working on succeeding in proposing the next valid block. Each clock is not only associated with its own hash, which can show if any changes to the block have been made, but is also associated with the hash of the previous block. This information is part of each block's header's metadata. In fact, all blocks are made of a header and a body, the body containing a set of transactions.

Therefore, a chain of validated blocks is created, resulting in a secure technology option for transactions. Because of this chain of hashes, changing a block in the chain will result in changing the block's hash. Since the next block will have the hash of the previous block before the change, if a block is changed, then all subsequent blocks are going to become invalid. But what if there is tampering with a block and the intruder manages to tamper with subsequent blocks and fix the hashes? To mitigate such problems, another defence mechanism that blockchains have is the *proof of work,* which manages to slow down the creation of new blocks (to deter intruders from managing to complete changing blocks quickly).

When a new block is created and validated by a *miner*, the block is sent to everyone in the network. Then everyone verifies that the block has not been tampered

with. If this is verified, then this block is added on the blockchain. This is achieved in a distributed manner, i.e. everyone participating in the blockchain network has a copy of the blockchain and adds the validated and verified block on their own copy of the blockchain. Overall, the blockchain network participants must have consensus on the validity of a block, e.g. if a block has been tampered with, it will be rejected.

Miners in a blockchain network are special nodes on the peer-to-peer network that create new blocks by collecting transactions and putting them in the newly created block. A valid block carries a reward, but to avoid for one powerful miner overtaking the blockchain network, after reaching a preset number of blocks, the reward is decreased repeatedly until it becomes zero. Of course, there are other incentives to motivate miners to continue creating blocks even when the reward is decreased, for example, the transaction fees, which are much smaller than a reward but continue to increase in contrast to the decreasing reward.

There are a lot of miners in the blockchain network, and all miners are competing with one another as they are all trying to validate blocks and receive rewards. However, rewards are only recognized on the longest new chain of blocks to be added on the main blockchain. So, there is a competition between the miners that has to do with who will first manage to validate the next blocks for the blockchain and publish it. For miners to succeed in ending up with the longest chain, they may be tempted to hide some aspects of their computational work in order to publish a longer chain of blocks which will have priority over other chains. The network participants will need to verify the longest chain and the miner will receive the reward.

Therefore, in the process of *mining,* miners have a choice to be honest or dishonest about their progress with the block validation. Consider the blockchain environment, where miners simultaneously work on validating their blocks and get them published on the main blockchain so that they can receive the reward. This system can only work if the miners are honest and can share the rewards in the long term.

In order to have the longest chain of blocks, a miner will need to employ a lot of computational power. The risk here is for a dishonest miner to acquire disproportionately large amounts of computational resources in order to alienate the competition and end up with the longest chain. This would give the specific miner increasing power in the network. This should be avoided because this could end up destroying the peer-to-peer basis of the network, which should not have any powerful authority handling transactions, but the work should be shared among peers.

Game theory will help us understand how such situation can be avoided.

2.1.2.2 The Blockchain Scenario Game

In order to model the blockchain scenario as a game, we need to define the different elements of the game model, i.e. the players, the actions available to the players, their payoffs from taking these actions, etc.

Consider that the miners are the players of the game. Each one of the miners has their own set of transactions that they have mined. Out of their set of transactions,

each miner has to decide which of these transactions to include in their block. The final decision may have to do with the monetary reward, e.g. deciding to include those transactions that carry larger transaction fees. Another decision that a miner has to make is to choose which block to mine on top of. Remember that the new block has to be added to the main blockchain, so it needs to include the hash of the previous block that it will be added to. Once the block is validated, the miner has to decide whether to publish the block immediately or withhold it so that a longer chain can be created. In this model, all the miners are mining blocks at the same time, so they cannot know the length of the chains that competing miners are working towards, before such chains are published.

In any case, there is a cost that comes with playing the game, which is the cost of mining, including the fixed cost of having specialized hardware to be able to mine, but also the day-to-day costs of carrying out the work of mining and validating blocks. Nevertheless, if a miner manages to publish their block, then the miner will receive a block reward. In addition to the block reward, the miner gets the transaction fees from all the transactions that were included in the published block (decided by the miner as mentioned above). Therefore, modelling this game must consider a payoff of rewards minus costs. A miner would be motivated to play the game only if the rewards are larger than the costs.

External factors may also affect the game play, for instance, we may consider that this is a network and network latency must be considered as a source of delay in finding out about published blocks even if the other miners are honest.

To model this interaction, we are inspired by the prisoner's dilemma game model, where we have cooperation versus defection, and we follow the idea by replacing the notion of cooperation with the notion of honesty and the notion of defection with the notion of dishonesty.

Let's consider that we have two miners, $\boldsymbol{m_1}$ and $\boldsymbol{m_2}$, that will be competing in the blockchain scenario game, competing on who will be the first to publish and verify their block or their chain of blocks. The two miners are working on their blocks simultaneously and will make their validated blocks available at timings such that they will both be verified at the same time. Both $\boldsymbol{m_1}$ and $\boldsymbol{m_2}$ aim to become richer, which can happen from receiving rewards and transaction fees that are larger than the costs incurred for mining. Table 2.1 illustrates the game.

The rows in Table 2.1 indicate the actions and payoffs for Miner 1 ($\boldsymbol{m_1}$), whereas the columns in the table indicate the actions and payoffs for Miner 2 ($\boldsymbol{m_2}$). The decision that $\boldsymbol{m_1}$ has to make is to be either honest or dishonest about the new block. When $\boldsymbol{m_1}$ is honest, the costs incurred are a fixed amount of costs c for one block validation, where **c** includes both the cost of the mining hardware and the daily use of resources needed to support mining. If $\boldsymbol{m_2}$ is also honest, then $\boldsymbol{m_1}$ and $\boldsymbol{m_2}$ will

Table 2.1 The blockchain scenario game

	Miner 2 is honest	Miner 2 is dishonest
Miner 1 is honest	***{(0.5r-c), (0.5r-c)}***	***{(0.2r-c), (0.8r-C)}***
Miner 1 is dishonest	***{(0.8r-C), (0.2r-c)}***	***{(0.5r-C), (0.5r-C)}***

share success with each other. In the case of mutual honesty, each miner ends up receiving the rewards about **50%** of the time. If m_2 is dishonest, then the cost will not change for m_1, but the reward will decrease as the dishonest player will receive the reward most of the time; we indicate this with a *20–80* split favouring the dishonest player. Note that the dishonest player m_2 will incur higher costs, C, where $C > c$. The costs will be greater because of the multiple resources that need to be committed in order for m_2 to be able to work on multiple blocks, but we consider that, overall, the additional rewards are much more than the additional costs.

Now let's consider that m_1 is dishonest and working on more than one block. Then the costs incurred, C, as discussed above, will be greater because of the multiple resources that need to be committed in order for m_1 to be able to work on multiple blocks. If m_2 is also dishonest, then the two miners will share the reward: each miner receiving the reward about **50%** of the time. However, the cost incurred will be larger this time resulting in an overall payoff that is less than the payoff that the two miners would share if they were both honest. In case that ***m2*** is honest, then ***m1*** will receive the majority of the reward with an 80–20 split, favouring ***m1*** (but still with the increased costs). The behaviour, costs and rewards are also similar for m_2, represented by the columns in Table 2.1. The payoff tuple in each cell of Table 2.1 represents the following values: *(payoff for m_1, payoff for m_2)*.

In this *blockchain scenario* game, each miner must consider their options in terms of actions and decide on what their strategy is. Considering all possible strategies, a *dominant strategy* is a strategy that will have the largest payoff no matter how other miners behave. In order for the blockchain technology to succeed, the dominant strategy should be one of cooperation between the miners, i.e. decisions and actions that are based on honesty, regardless of what everyone else is doing.

Given that what we want to motivate is honest behaviour, even if we cannot achieve a dominant strategy of cooperation, we should at least aim for a *Nash equilibrium* that motivates honesty. A Nash equilibrium is when none of the players have any incentive to change state, no matter what their opponent does.

Let's return to the model presented in Table 2.1.

When playing a blockchain scenario game, each miner must decide whether to be honest or whether to be dishonest, assuming that each miner does not know what the other miner will decide. The decision of each miner is based on the following reasoning: if m_1 or m_2 believes that the opponent will be honest, then the best option is to be dishonest because even though higher costs will be incurred, the rewards will be much higher making up for the costs. By being dishonest while the opponent is honest, a player has an opportunity to maximize the payoff. On the other hand, if m_1 or m_2 believes that the opponent will be dishonest, then, the best option will be to also be dishonest in order for the rewards to be eventually shared *50–50* (even with the increased cost that comes with the dishonest decision). In fact, in the game depicted in Table 2.1 , it appears as though being honest will give less payoff while being dishonest will give more payoff. Having no other information and being asked to make this decision once, the best response strategy for both players is to be dishonest.

However, the blockchain scenario is not just about making one decision for a single interaction but in considering the infinite horizon of repeated interactions between the miners. In that case, a more accurate model to consider is *the iterative blockchain scenario* game model presented next.

2.1.2.3 The Iterative Blockchain Scenario Game

We have considered the blockchain scenario game where the interacting miners must decide whether to be honest or dishonest with their fellow miners. Inspired by the prisoner's dilemma game, we have illustrated a game model that elaborates the payoffs from honest and dishonest decisions of miners when simultaneously waiting for the verification of their blocks. We have shown that the game model favours dishonesty because the payoffs will be higher for a once-off decision. However, the blockchain technology system is an environment that supports continuous interaction and favours repeated simultaneous mining and block publishing. Therefore, we will proceed to model a repeated, also known as an *iterative*, game model for this scenario.

An iterative game makes it possible for the miners to consider the continuous relationship with other miners and consider the benefits of sharing the rewards honestly in the long run, incurring the least amount of costs. In the game model itself, the decisions of the miners consider the complete previous history of their opponents. This gives the opportunity to the miners interacting multiple times to reward each other for honesty or to punish each other for dishonesty.

The strategies that employ such punishments or rewards are called trigger strategies. A trigger strategy is a strategy that changes in the presence of a predefined trigger; it dictates that a player must follow one strategy until a certain trigger is activated. Once the trigger is activated, then the player will follow a different strategy, for the rest of the game. One of the most popular trigger strategies is the grim trigger strategy, which dictates that the player participates in the relationship in a cooperative manner, but if dissatisfied for some known reason, then the previously cooperating player leaves the relationship forever. Therefore, in the case of our example, renewing the honest relationship and, thus, the fruitful interaction between miners participating in the iterative blockchain scenario game is contingent upon the actions of the miners.

Other than the grim strategy, in cases of such iterative interactions, we may consider other less harsh reactions to a trigger. For instance, another strategy used to elicit honest decisions from an opponent is for a player to mimic the actions of his opponent, giving the opponent the incentive to play cooperatively, since in this way he will be rewarded with a similar mirroring behaviour. This strategy is referred to as tit-for-tat strategy. If both miners in our blockchain scenario example decide to interact honestly, either using the grim strategy or the tit-for-tat strategy, then none of the two players will have an incentive to change their strategy because honesty will result in the highest payoffs in the long term. Therefore, we have a Nash equilibrium between the two miners. The cooperative equilibrium is only motivated

because of the repetition of the interaction and the consideration of future payoffs. However, we will need to model the interaction with these strategies to show that such interaction between cooperative trigger strategies results in an equilibrium, which is a desired solution for the game.

The following section presents in detail the resolution of the iterative blockchain scenario game, including any equilibria that may result from the strategies.

Resolution of the Iterative Blockchain Scenario Game

We will model the blockchain scenario game as an iterative game in order to demonstrate an equilibrium solution. We have two miners, m_1 and m_2, making decisions about honesty or dishonesty with regard to their blocks. Both players will make their first decision simultaneously, but since the relationship is continuing beyond the first stage, both will know whether the opponent was honest or dishonest in that first play, and based on that, they can decide how to act in future interactions. Let's assume that m_1 decides to be honest. If m_2 also decides to be honest, the payoff to m_2 will be $0.5r-c$, where r represents the reward for the block (with probability 0.5) and c represents the minimum mining cost incurred. Otherwise, m_2 can decide to be dishonest with payoff $0.8r-C$, where r has a higher probability of 0.8, but the costs incurred are also higher and represented by C, where $C > c$. Simultaneously, the payoff to m_1 will be $0.5r-c$ if m_2 is honest and $0.2r-c$ if m_2 is dishonest, with the same reward r, and costs C and c as previously explained. In the case that m_1 is dishonest, then if m_2 is honest, the payoff to m_2 will be $0.2r-c$, and the payoff to m_1 will be $0.8r-C$. But if m_2 decides to also be dishonest, then the payoff to m_2 will be $0.5r-C$ and to m_1, $0.5r-C$.

In following interactions, both nodes have the option to continue their behaviour, whether this is being honest or being dishonest or to switch behaviours. Let's consider the *grim* strategy and the *tit-for-tat* strategy described previously. The *grim* strategy implies that a game player will cooperate with the opponent but will leave the interaction forever if there is any non-cooperative behaviour from the opponent. This is not convenient for the iterative blockchain scenario game because the miners want to continue mining. So, we will select the *tit-for-tat* strategy for the miners in our game model, as their cooperative strategy. As a reminder, the *tit-for-tat* strategy is a strategy by which a miner is always honest, unless the opponent is dishonest; in which case, the honest miner will switch to dishonesty for one round and return back to honesty, until such behaviour is detected again. Similarly, we can define a corresponding non-cooperative strategy to compare. In fact, the non-cooperative strategy will be presented as a counter-option to the *tit-for-tat* strategy.

Therefore, the analysis of the iterative blockchain scenario game considers the interactions between the two miners, where both miner m_1, and miner m_2 employ the *tit-for-tat* strategy as their cooperative strategy. Note that by the term *cooperative strategy*, we refer to the miners' intention to be honest with each other but also use a trigger in their strategy as a defence mechanism in case the opponent is dishonest.

To better highlight the benefit of using a cooperative strategy, we will also define non-cooperative strategies as alternative options for the two miners to use. We can first consider the *cheat-and-leave* strategy. The *cheat-and-leave* strategy is defined so as to allow the miner employing this the choice to be non-cooperative, dishonest, behaviour. With this strategy, the dishonest miner, either $\boldsymbol{m_1}$ or $\boldsymbol{m_2}$, would leave the interaction after being dishonest, in order to avoid any future interaction. To avoid any future interaction would mean for $\boldsymbol{m_1}$ or $\boldsymbol{m_2}$ to stop mining, which is not desired by the miners in any case. Therefore, we will reject the *cheat-and-leave* strategy as an option for the non-cooperative strategy that can be used by the miners.

A better non-cooperative strategy to consider is the *cheat-and-return* strategy. The *cheat-and-return* strategy is not so strict, as it gives the opportunity to the miner, who wants to be dishonest, to initialize dishonest behaviour but not discontinue mining, instead to return back to the interaction to accept the punishment, so that the interactions can continue. We will examine the *cheat-and-return* strategy as a strategic option for the two miners and compare the long-term use of a non-cooperative strategy to the long-term use of a cooperative strategy, such as the *tit-for-tat* strategy.

Our iterative game model considers a number of repeated interactions with an unknown horizon. We will treat this as an infinite repetition model because we cannot know if or when the last interaction between the miners will take place. The payoffs for the game are the summation of payoffs for each round of the game, as these are defined in Table 2.1.

Therefore, we must consider and compare different sequences of payoffs, and in order to compare such sequences of payoffs in repeated games, we need to use the idea of the present value of a payoff sequence to help us quantify the overall payoffs from different strategies, e.g. trigger strategies over the whole game. The present value is the total payoff that a player is willing to accept currently instead of waiting for the future payoff; the present value is based on a discount factor. Basically, a player in a repeated game is willing to accept a smaller payoff in the current play that would be worth more in the future.

The rate by which the current payoff would increase in the future can be defined as $\boldsymbol{\alpha}$. Therefore, if a player's payoff in the next iteration were equal to 1, currently, the payoff the player would be willing to accept would be equal to $\frac{1}{1+\alpha}$. Note that if there exists a probability that the interaction between the two miners will not continue in the next iteration, then we must also introduce this probability into the model. Given that there is always the possibility that the two miners will not synchronously publish their blocks in the future, we must admit that such probability exists.

Let the probability of no future interaction be equal to $\boldsymbol{p}$. Given $\boldsymbol{p}$, the payoff that one of the miners is willing to accept currently would be equal to $\boldsymbol{\delta} = \frac{1-p}{1+\alpha}$, where $\boldsymbol{\delta \in [0, 1]}$ and can also be referred to as the discount factor. Therefore, given a payoff $\boldsymbol{X}$ in the next interaction, the present value of the interaction currently is equal to $\boldsymbol{\delta} \cdot \boldsymbol{X}$. Now, this only considers the next interaction between the two miners. However,

we want to consider a repeated set of interactions with an unknown horizon, which implies that the model should be equivalent to that of an infinite game. Hence, for an infinitely repeated game, the present value includes the discounted payoff of all future interactions of the game.

Let the payoff from the current interaction between the two miners to be equal to 1. Then, the additional payoff a miner is willing to accept for the next interaction is equal to $\boldsymbol{\delta}$. For the interaction following that, the payoff would be equal to $\boldsymbol{\delta \cdot \delta}$, i.e. $\boldsymbol{\delta^2}$, then to $\boldsymbol{\delta^3}$, to $\boldsymbol{\delta^4}$ and so on. Thus, the present value for the complete game is equal to $\boldsymbol{1 + \delta + \delta^2 + \delta^3 + \delta^4 + \text{etc}}$. We can use the sum of an infinite geometric series to calculate this sum to be equal to $\frac{1}{1-\delta}$. Now, if the payoff is not equal to 1 but to a variable X payable at the end of each interaction, then the present value in an infinitely repeated game is equal to $\frac{X}{1-\delta}$. Note that if we were interested in only studying a specific number of interactions, the sum for a finite geometric series of $\boldsymbol{n}$ repetitions is equal to $\frac{X \cdot \left(1-\delta^n\right)}{1-\delta}$.

Given that we are examining an infinitely repeated game, then we must find an equilibrium, not just in any one stage of the game, but we must find an equilibrium for the game, i.e. a set of strategies that the players follow throughout the game path such that when receiving the corresponding payoffs, the players have no incentive to change these strategies. When a strategy allows a player to play the best response to the opponent's strategy after every sequence of past actions such that the player will receive a higher payoff than any other strategy would give, then we have found the *subgame perfect* strategy. When all players play their *subgame perfect* strategies, then we have an equilibrium in the repeated game, known as a *subgame perfect equilibrium*.

Let's investigate the different game profiles. Let the two players, miners $\boldsymbol{m_1}$ and $\boldsymbol{m_2}$, have a choice between a cooperative and a non-cooperative strategy, i.e. between an honest and a dishonest behaviour. Consider that to demonstrate an honest behaviour, both the miners, $\boldsymbol{m_1}$ and $\boldsymbol{m_2}$, can employ the *tit-for-tat* strategy, and to demonstrate a dishonest behaviour, $\boldsymbol{m_1}$ and $\boldsymbol{m_2}$ can employ the *cheat-and-return* strategy. Since both miners demonstrate the same behaviour and have the same choices, it is sufficient to show that honest behaviour is the best response strategy for any one of the players to achieve subgame perfect equilibrium in the game.

Best Response Strategy

Let's assume a history of cooperative moves in the past from both miners and compute the present value of any future payoffs for one of the two miners at a given point in time. Let $\boldsymbol{m_1}$ employ the *tit-for-tat* strategy. Then, $\boldsymbol{m_2}$ could either employ the *cheat-and-return* strategy, i.e. decide to demonstrate dishonesty, or decide to also play the *tit-for-tat* strategy, i.e. continue to demonstrate honest behaviour.

If $\boldsymbol{m_2}$ decides to be honest, then $\boldsymbol{m_1}$'s present value of the future payoffs equals to:

$$\frac{X}{1-\delta}, \text{ where } X = \boldsymbol{0.5r - c}.$$

Thus, the present value of the future payoffs to both m_1 and m_2 will be $\frac{0.5r - c}{1 - \delta}$ as a result of this interaction.

Since the *tit-for-tat* strategy is inherently cooperative, then unless there is any dishonest behaviour by any of the players, they will both continue to be honest for the entire game. In fact, there will not be any dishonest action because both employ the same strategy, which introduces honest actions in every interaction unless provoked; so, there will not be any provocation. The payoff will continue to be the same in every interaction, and we can find the present value of the infinite sum of payoffs to be as shown above.

If m_2 decides to be dishonest and employ the *cheat-and-return* strategy at any interaction of the game, then the payoff to m_1 will be different. Let's calculate the corresponding present value for m_1, when m_2 decides to be dishonest. Note that in the first interaction, m_1 is honest but m_2 is dishonest; therefore, there is only a *0.2* probability of getting the reward r while still incurring the standard mining costs. Once m_1 discovers about m_2's dishonesty, the decision is to also exhibit dishonest behaviour. Thus, m_1 is dishonest in the second interaction as a punishment to m_2, whereas m_2 has returned to cooperative and honest behaviour. This time, m_1 has a probability of *0.8* of collecting the reward r, but the costs increase to C. From the third interaction onwards, they return to honest behaviour.

Thus, if m_2 decides to be dishonest, then m_1's present value of the future payoffs equals to:

$$(0.2r - c) + (\delta \cdot 0.8r - C) + \left(\delta^2 \cdot \frac{0.5r - c}{1 - \delta}\right)$$

Similarly, m_2's present value of the future payoffs will be:

$$(0.8r - C) + (\delta \cdot 0.2r - c) + \left(\delta^2 \cdot \frac{0.5r - c}{1 - \delta}\right)$$

To show that it is worth being dishonest, we must show that the present value of the future payoffs that m_2 receives when being dishonest is greater than the present value of the future payoffs that m_2 receives when being honest. Consider the following:

$$(0.8r - C) + \delta \cdot (0.2r - c) + \delta^2 \cdot \left(\frac{0.5r - c}{1 - \delta}\right) > \frac{0.5r - c}{1 - \delta}$$

Solving for δ, we get the following:

$$(0.8r - C) + \delta \cdot (0.2r - c) > -\delta^2 \cdot \left(\frac{0.5r - c}{1 - \delta}\right) + \frac{0.5r - c}{1 - \delta}$$

$$(0.8r - C) + 0.2r\delta - c\delta > -\delta^2 \cdot \left(\frac{0.5r - c}{1-\delta}\right) + \frac{0.5r - c}{1-\delta}$$

$$(0.8r - C) + 0.2r\delta - c\delta > \left(1 - \delta^2\right) \cdot \left(\frac{0.5r - c}{1-\delta}\right)$$

$$(0.8r - C) + 0.2r\delta - c\delta > (1-\delta) \cdot (1+\delta) \cdot \left(\frac{0.5r - c}{1-\delta}\right)$$

$$(0.8r - C) + 0.2r\delta - c\delta > (1+\delta) \cdot (0.5r - c)$$

$$\frac{0.8r}{0.5r - c} - \frac{C}{0.5r - c} + \frac{\delta(0.2r - c)}{0.5r - c} > (1+\delta)$$

$$\frac{0.8r}{0.5r - c} - \frac{C}{0.5r - c} - 1 > (\delta) - \frac{\delta(0.2r - \mathrm{c})}{0.5r - c}$$

$$\frac{0.8r - C}{0.5r - c} - 1 > \delta\left(1 - \frac{0.2r - \mathrm{c}}{0.5r - c}\right)$$

$$\frac{\dfrac{0.8r - C - 0.5r + c}{0.5r - c}}{\dfrac{0.5r - c - 0.2r + c}{0.5r - c}} > \delta$$

$$\delta < \frac{0.3r - C + c}{0.3r}$$

Therefore, it is a good idea to be dishonest if δ satisfies this inequality because that is when the reward will be greater than the cost, given the present value of the future payoffs for both honest and dishonest behaviours.

Consider the values $-C + c$ and remember that $C > c$, which means that $-C + c$ returns a negative value. Consequently, $0.3r - C + c$ is less than $0.3r$, and the fraction is less than 1 as expected (if $0.3r - C + c$ is positive). If the costs are higher than a third of the reward, the result will be negative, and since a discount factor cannot be negative, then we can conclude that it is *never* a good idea to be dishonest when the costs are higher than a third of the reward (given our probability assumptions when modelling the game). If the costs are less, then we get a positive value between 0 and 1 for δ. Since we are using the summation to find the present value of the payoffs, then the closer to one δ is, the higher the present value will be. In our example, this will happen if the costs are minimized. However, since mining does need to invest in resources and thus it is inevitable to incur specific costs, then our model shows that the miners are motivated towards honest behaviour that can give the higher payoffs in the duration of a repeated game of interactions, with an unknown horizon.

2.2 Summary and Conclusions

This chapter focuses on financial data, specifically on blockchain, a technology that enables cryptocurrency. An example of a popular cryptocurrency that we refer to in the chapter is bitcoin. We approach the idea of cryptocurrency more generally as a digital payment system that does not rely on banks as intermediary nodes to complete monetary transactions. We investigate the system's peer-to-peer approach for digital payment and how it can enable anyone to send and receive payments.

We recognize that game theoretic philosophy is a core aspect of blockchain design, and we propose a model for the process of mining. In the process of mining, miners have to create and publish blocks, and within those steps, they can decide to be honest or dishonest about their progress with the block validation. In fact, game theory has to do with decision-making and motivation for specific decisions, and it is important in this particular example because the blockchain system can only be effective if there is motivation for the miners to continue participating, in our case, when miners are honest and can share the rewards in the long term.

The reason that the system must motivate honesty and cooperation is because a dishonest miner risks to acquire a disproportionately large amounts of computational resources in order to alienate the competition and end up with the longest chain of blocks. This would give a single miner increasing power in the blockchain network. This should be avoided because this could end up destroying the peer-to-peer basis of the network, which should not have any powerful authority handling transactions, but the work should be shared among peers.

The game theory model helps us understand how such situation can be avoided, by modelling an iterative game between the miners, that makes it possible for miners to consider the continuous relationship with other miners, instead of their own egoistic short-term gain. The model motivates consideration of the benefits of sharing the rewards honestly in the long run, incurring the least amount of costs. To reinforce the iterative nature of the model, the decisions of the miners are modelled to consider the complete previous history of their opponents. This gives the opportunity to the miners interacting multiple times to reward each other for honesty or to punish each other for dishonesty. Since mining does need to invest in resources and thus it is inevitable that the miners will incur specific costs, then our model shows that the miners are motivated towards honest behaviour.

References

Abramova S, Böhme R (2016) Perceived benefit and risk as multidimensional determinants of bitcoin use: a quantitative exploratory study. In: The 37th international conference on information systems, 1–20

Aste T, Tasca P, Matteo TD (2017) Blockchain technologies: the foreseeable impact on society and industry. Computer 50(9):18–28

Barrett M, Oborn E, Orlikowski WJ (2016) Creating value in online communities: the socio-material configuring of strategy, platform, and stakeholder engagement. Inf Syst Res 27(4):704–723

Beck R, Müller-Bloch C, King JL (2018) Governance in the blockchain economy: a framework and research agenda. J Assoc Inf Syst 19(10):1020–1034. https://doi.org/10.17705/1jais.00518

Chang V, Baudier P, Zhang H, Xu Q, Zhang J, Arami M (2020) How blockchain can impact financial services – the overview, challenges and recommendations from expert interviewees. Technol Forecast Soc Chang 158:120166., ISSN 0040-1625. https://doi.org/10.1016/j.techfore.2020.120166

Chapron G (2017) The environment needs crypt-governance. Nature 545:403–405

DiNizo AM Jr (2018) From Alice to Bob: the patent eligibility of blockchain in a post-CLS bank world. 9 Case W. Res. JL Tech. & Internet 1 (2nd), [Online]. Available from: https://scholarlycommons.law.case.edu/jolti/vol9/iss1/2. Accessed 4 Apr 2020

Du W, Pan SL, Dorothy E, Leidner DE, Yinga W (2019) Affordances, experimentation and actualization of FinTech: a blockchain implementation study. J Strateg Inf Syst 28:50–65

Hull R, Batra VS, Chen YM, Deutsch A, Heath FFT, Vianu V (2016) Towards a shared ledger business collaboration language based on data-aware processes. In: Sheng QZ, Stroulia E, Tata S, Bhiri S (eds) ICSOC 2016, LNCS, pp 18–36. https://doi.org/10.1007/978-3-319-46295-0_29936

Iansiti M, Lakhani KR (2017) The truth about blockchain. Harv Bus Rev 95(1):118–127

Karafiloski E, Mishev A (2017) Blockchain solutions for big data challenges: a literature review. The 17th international conference on smart technologies (The IEEE EUROCON), 763–768

Kshetri N (2018) 1 blockchain's roles in meeting key supply chain management objectives. Int J Inf Manag 39:80–89

Lindman J, Rossi M, Tuunainen VK (2017) Opportunities and risks of blockchain technologies in payments: a research agenda. In: The 50th Hawaii international conference on system sciences, 1533–1542

Mattila J (2016) The blockchain phenomenon. In: The blockchain phenomenon. Berkeley Roundtable of the International Economy. Available at: https://ideas.repec.org/p/rif/wpaper/38.html

Nærland K, Müller-Bloch C, Beck R, Palmund S (2017) Blockchain to rule the waves: nascent design principles for reducing risk and uncertainty in decentralized environments. The 38th International Conference on Information Systems, pp 1–16

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Pereira J, Tavalaei MM, Ozalp H (2019) Blockchain-based platforms: decentralized infrastructures and its boundary conditions. Technol Forecast Soc Change 146:94–102. https://doi.org/10.1016/j.techfore.2019.04.030

Peters G, Panayi E, Chapelle A (2015) Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective. J Financ Perspect 3(3):1–25

Pilkington M (2016) Blockchain technology: principles and applications. Research handbook on digital transformations, chapter 11. https://doi.org/10.4337/9781784717766

Rennock, M-JW, Cohn, A, Butcher JR (2018) Blockchain technology and regulatory investigations. Pract Law. February/March 2018, pp. 35–44, Litigation

Staples M, Chen S, Falamaki S, Ponomarev A, Rimba P, Tran AB, Weber I, Xu X, Zhu J (2017) Risks and opportunities for systems using Blockchain and smart contracts. In: Data61. CSIRO, Sydney. https://doi.org/10.4225/08/596e5ab7917bc

Tama BA, Kweka BJ, Park Y, Rhee KH (2017) A critical review of blockchain and its current applications. Int Conf Electr Eng Comput Sci 2017:109–113

Tang Y (2018) How fintech changes our live? [Online]. Available from: https://mp.weixin.qq.com/s/1RdTkI9q4NlMrdxNqQFO2w. Accessed 10 Apr 2022

Tapscott A, Tapscott D (2017) How blockchain is changing finance. Harv Bus Rev. [Online] Available from: https://hbr.org/2017/03/how-Blockchain-is-changing-finance. Accessed: 5 Apr 2020

Tu KV, Meredith MW (2015) Rethinking virtual currency regulation in the bitcoin age. Wash Law Rev (Seattle 1962) 90(1):271–347

Underwood S (2016) Blockchain beyond bitcoin. IEEE/ACM Trans Networking 59(11):15–17
Walker MJ, Burton B, Cantara M (2016). Hype cycle for emerging technologies identifies three key trends that organizations must track to gain competitive advantage. Gartner. Available at: https://www.gartner.com/en/newsroom/press-releases/2016-08-16-gartners-2016-hype-cycle-for-emerging-technologies-identifies-three-key-trends-that-organizations-must-track-to-gain-competitive-advantage. Accessed 10 Apr 2022
Wörner D, von Bomhard T, Schreier YP, Bilgeri D (2016) The bitcoin ecosystem: disruption beyond financial services? In: The twenty-fourth European conference on information systems, 1–16
Yoo S (2017) Blockchain based financial case analysis and its implications. Asia Pac J Innov Entrep 11(3):312–321. https://doi.org/10.1108/APJIE-12-2017-036
Zheng Z, Xie S, Dai HN, Chen X, Wang H (2018) Blockchain challenges and opportunities: a survey. Int J Web Grid Serv 14(4):352–375. https://doi.org/10.1504/IJWGS.2018.095647