BLOCKASTICS

Stochastic models for blockchain analysis

Pierre-O Goffard

March 28, 2022

Chapter 1

Introduction

A blockchain is a distributed ledger made of a sequence of blocks maintained by achieving consensus among a number of nodes in a Peer-to-Peer network. The blockchain technology has attracted a lot of interest after the advent of the bitcoin cryptocurrency in 2008, see Nakamoto [2008]. Since then, the blockchain concept has been used to develop decentralized systems to store and maintain the integrity of time-stamped transaction data across peer-to-peer networks. Besides the creation of a digital currency, blockchain applications include the sharing of IT resources, the registration of authentication certificate or the implementation of smart contracts.

A blockchain is

- Decentralized as it is maintained by a network. Nodes can be light or full nodes. Light nodes are blockchain users that broadcast transactions, full nodes are in charge of verifying and recording the transactions, see Figure 1.1.

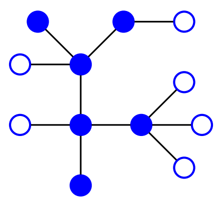


Figure 1.1: A network made of full nodes (blue) and light nodes (white)

  - A local copy is stored by each full node which grants security
  - The governance is not handled by a central authority

- Public or private. In public blockchain anyone can access the data, in private blockchain reading access is restricted.

- permissionned or permissionless. In permissionless blockchain, anyone can join the network as a full node.

- Immutable. Altering the information written in the blockchain is made difficult if not impossible.
- Incentive compatible. The process of reaching consensus is costly to the full nodes who must be compensated for their hard work.

The consensus protocols, at the core of the blockchain technologies, are the focus of these lecture notes. The goal is to evaluate consensus protocol according to three dimensions

1. Efficiency: The amount of data being processed per time unit
2. Decentralization: The fairness of the distribution of the decision power among the nodes
3. Security: The likelihood of a successful attack on the blockchain

Because consensus protocols involve random components, stochastic modelling is required to assess a blockchain system within the Efficiency/Decentralization/Security trilemma in Figure 1.2. As it is hard to improve one dimension without negatively impacting the other two, trade-offs

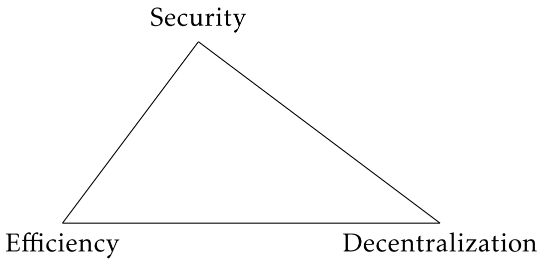


Figure 1.2: The blockchain trilemma

must be made. We will see how to use classical models of applied probability, including urn, epidemic, graph, queue and risk models, to provide numerically tractable indicators to quantify the efficiency, decentralization and security of blockchain systems. These indicators will then allow us to carry out sensitivity analysis with respect to the model parameters to optimize and improve blockchain implementations.

The main application of blockchain systems today is undoubtedly cryptocurrencies, the most well known of which being the bitcoin introduced by Nakamoto [2008]. Public and permissionless blockchain, like the bitcoin one, must be associated to a cryptocurrency. Indeed, to add a block to the bitcoin blockchains the full nodes compete to solve a cryptrographic puzzle using brute force search algorithm. The first node (referred to as a miner) who finds a solution, appends the next block and collects a reward expressed in cryptocurrency. Assuming this reward is worth something, it offsets the operational cost which is essentially the electricity consumed to run the computers 24/7. A cryptocurrency must be equipped with following features

1. No central authority (Decentralized network)

2. Ledger to record all the transactions and coin ownership (the blockchain)

3. A coin generation process (block finding reward)

   $\hookrightarrow$ It creates an incentive compatible system to the full nodes

4. Ownership can be proved cryptographically, a wallet is secured with a public/private key system

5. Transactions can be issued by an entity proving ownership of the cryptographic unit through the private key

6. The system cannot process more than one transaction associated to the same cryptographic unit. It must be robust to double spending attack in which a fraudster is issuing two conflicting transactions to recover the funds she already spent

This charcaterization is given by Lansky [2018]. Cryptocurrencies draw their fundamental value from the fact that they

- provide transaction anonymity
- provide a reliable currency in certain regions of the world
- permit money transfer worldwide at low fare
- do not require a thrusted third party

An important implication of this architecture is disintermediation, it creates an environment where multiple parties can interact directly and transparently. Blockchain is therefore immediately relevant to banks and financial institutions which incur huge middlemen costs in settlements and other back office operations. Decentralized finance (DeFi) offers a new financial architecture that is non-custodial, permissionless, openly auditable, pseudo-anonymous and with potential new capital efficiencies. It extends the promise of the original bitcoin whitepaper Nakamoto [2008] of non-custodial transaction to more complex financial operations, see the SoK of Werner et al. [2021].

Blockchain is a research topic of interest to many communities. Computing science distributed ledger technologies (synonymous with blockchains) rely on distributed algorithms and enable cooperation within a peer-to-peer network. Linking blocks and checking the authenticity of data uses cryptographic functions which is another field of computer science. The establishment of an incentive system within a network of individuals adopting a strategic behavior naturally leads to problems of game theory similar to those solved by economists. The discussion on the nature of new financial assets such as crypto-currencies, utility tokens and non-fungible tokens, is also at the center of the concerns of researchers in finance and monetary economics.

We focus here on the use of mathematics to optimize blockchain systems which makes our problems very close to those encountered in operations research. These notes are organized as follows. Chapter 2 presents the various consensus algorithms. Chapter 3 focuses on the security aspects. In Chapter 3, we take a look at decentralization in Chapter 4. We close on efficiency with Chapter 5.

Chapter 2

Consensus protocol

Transactions flow through the network of full nodes. After reviewing them, the full nodes must agree on the transaction that will be recorded in the next block. to do this, an algorithm must be designed so that consensus is reached. A consensus protocol must be based on one of the scarce resources available to the network peers which include

- bandwidth
- computational power
- storage

The first solution that comes to mind for reaching consensus is a majority vote based on a message exchange system. This solution has been proposed by Lamport et al. [1982] within the famous "Byzantine general problem". A voting system inside a large network involves a colossal number of messages exchanged leading to the consumption of all the bandwidth, the failure of some nodes by denial of service and delays in the synchronization of the network. Practical solution like the celebrated Practical Byzantine Fault Tolerance (PBFT) presented in Göbel et al. [2016] have been implemented in some blockchain systems. Despite these advances, a change in methods was needed to accommodate a network that could grow indefinitely.

Nakamoto [2008] solved this scaling problem by proposing a system based on the election of a leader. The Proof-of-Work (PoW) protocol appoints a leader based on its computing resources. Each node competes to solve a puzzle with a brute force search algorithm. The first node who is able to propose a solution append the next block. The search for a solution, referred to as mining, is associated with an operational cost borne by the nodes which is compensated by a reward expressed in the native blockchain cryptocurrency. The surge in cryptocurrency prices has led to a rush in block mining, leading to a major spike in the electricity consumption and electronic waste generation of blockchain networks. The blockchain network consumes as much electricity as countries the size of Thailand at the time of the writing. The need for a more environmentally friendly consensus protocol therefore becomes pivotal. The use of data storage has been implemented within the Filecoin project of Protocol Labs [2017] via the Proof-of-Space (PoSp) and its variant like the Proof-of-Spacetime protocol. A leader is chosen depending on how much data she currently stored or for how long some data has been stored. Proof-of-Space (PoSp) is seen as a fairer and greener alternative by blockchain enthusiasts due to the general purpose nature of storage and the lower energy cost required by storage. The fact that most storage resources are owned by companies offering cloud storage solution poses a threat to the decentralized nature of the distributed ledger. The Proof-of-Interaction (PoI) protocol, proposed by Abegg et al. [2021], takes as leader the first node that is able to contact and obtain a response from a random sequence of nodes. This is a bandwidth-based alternative that is more scalable than majority voting. Along with bandwidth, computing power, and storage, a new resource has emerged with the advent of cryptocurrencies as a medium of exchange. The Proof-of-Stake protocol, described by Saleh [2020], selects a node with a probability proportional to the number of cryptocoins it holds.

This chapter is organized as follows. Section 2.1 gives a brief description of the voting based ways to get consensus by reviewing the "generals" problem. Section 2.2 goes through the leader based consensus protocols, including PoW in Section 2.2.1, PoSp in Section 2.2.2, PoI in Section 2.2.3, and PoS in Section 2.2.4.

2.1 Voting system

The problem of reaching consensus in a peer-to-peer network via a majority vote has been abstractedly compared to generals who must agree on a common battle plan. We start from the simple two general case before moving on the the situation of interest with several ones.

2.1.1 Two generals problem

Two generals wish to attack a city but they must agree on a timing to attack a city. They communicate via a messenger who must cross enemy territory at the risk of being intercepted. The first general G_1 sends a message to the second one G_2 saying

```
"I will attack tomorrow at dawn"
```

For the attack to succeed, both generals must attack at the same time. Because their communication medium is unreliable, then G_1 must await confirmation from G_2 in order to attack. If G_1 does not receive confirmation then she will not attack. G_2 is aware of that and respond

```
"I will follow your lead"
```

G_2 does not know whether the message went through and must wait for confirmation. This creates an infinite loop of messages and response, as on Figure 2.1. The two general problem is deemed unsolvable from a theoretical point of view and corresponds to a situation where two

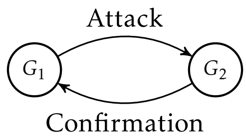


Figure 2.1: Message and confirmation loop

nodes communicate through an unreliable link. A practical solution for generals is to send many messengers hoping that at least one of them will succeed. This is only a thought experiment leading to the several general problem.

2.1.2 Byzantine General problem

The blockchain network contains more than two nodes, these nodes must agree on the transactions to confirm. In a permissionless blockchain the nodes do not trust each other. The problem of the previous section generalizes to more than two generals, assuming that some generals are traitors which corresponds to faulty nodes in the network. This problem is referred to as The "Byzantine general problem" and was coined by Lamport et al. [1982]. Assume that $n > 2$ generals must agree on a common battle plan for instance "Attack" (A) or "Retreat" (R) and that they can only communicate by two party messages. Denote by $m(i,j)$ the message sent by general i to general j. Each general j receives $n-1$ messages and applies a function f to determine the course of action, for instance

$$f(\{m(i,j);\ i = 1,\dots,n\}) = \begin{cases} A, & \text{if } \sum_{i=1}^{n} \mathbb{I}_{m(i,j)=A} > n/2, \\ R, & \text{else.} \end{cases}$$

If there are no traitors, each general is communicating the same value to all the peers and consensus is reached as in Figure 2.2a. If one general is traitor, then he might not communicate the same value to all the generals and no consensus can be reached. It is the case for G_4 in Figure 2.2b. To handle such a situation, roles are given to the general. One of them become the leader and the other are the lieutenants. We aim at finding an algorithm such that

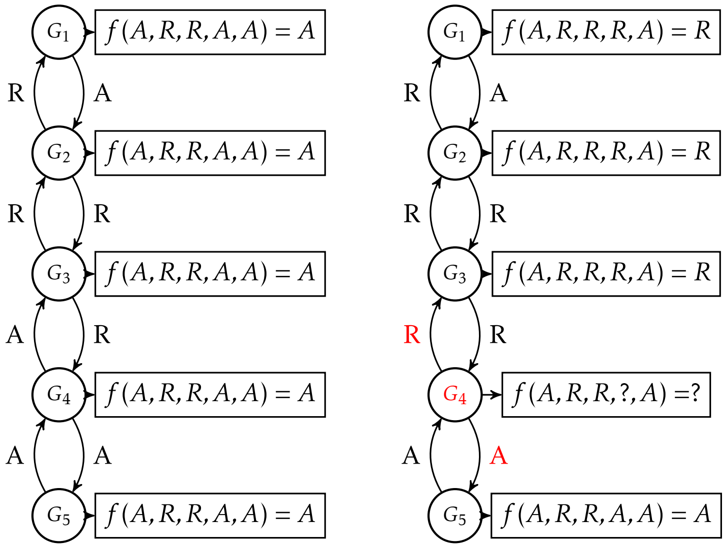
C1 All the loyal lieutenants obey the same order

C2 If the commanding general is loyal, then every loyal lieutenants obey the order he sends

A first result from Lamport et al. [1982] is the following

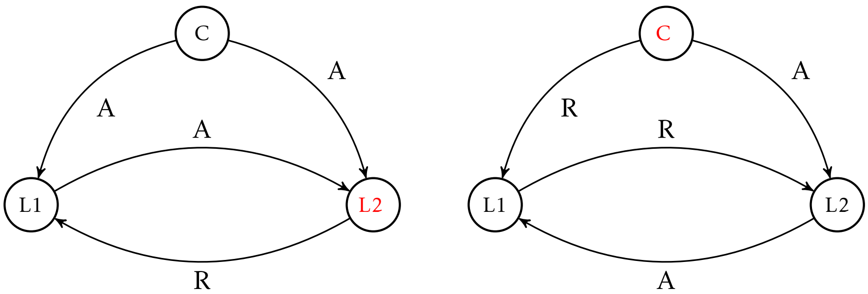
Theorem 1. *There are no solution to the Byzantine General problem for $n < 3m+1$ generals where m is the number of traitors.*

Proof. Consider the situation where $n = 3$ and $m = 1$. The traitor is either the commander or one of the lieutenants as shown in Unfortunately for Lieutenant 2, there is no way for her to tell apart the situation pictured in Figure 2.3a and Figure 2.3b and therefore no way to ensure both C1 and C2. We prove the result for $n > 3$ by contradiction. Assume that there is a way to verify



(a) No traitor (b) One traitor

Figure 2.2: Majority vote with or without a traitor



(a) Commander is loyal (b) Commander is a traitor

Figure 2.3: Majority vote with or without a traitor

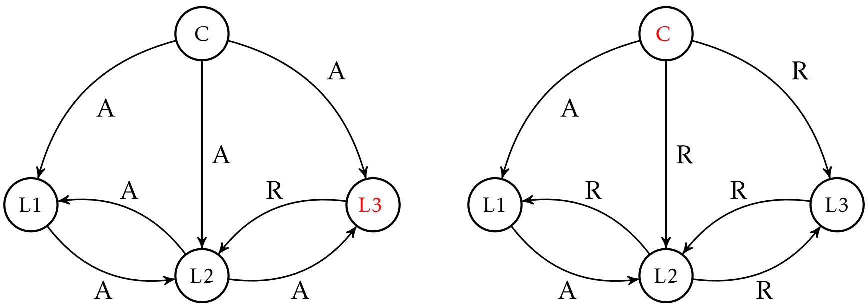
both C1 and C2 with $3 < n < 3m + 1$. We then construct a solution with generals by having one general simulate the commander plus at most $m - 1$ generals, and the other two simulating at most m generals. One of the generals gather all the traitors and is therefore a traitor. The other two are loyal generals as they only simulate loyals general. We have built a solution with three generals that we know is impossible. □

Now we need an algorithm that allows $n > 3m + 1$ generals to deal with m traitors. The 'Oral Message' algorithm denoted by OM(m) and summarized in Algorithm 1 can handle m traitors if the number of generals verifies $n > 3m + 1$. Before looking into the theoretical justification of OM(m), let us illustrate the algorithm with an example.

Example 1. *Consider the situation where* $n = 4$ *and* $m = 1$ *shown in Figure 2.4. If the commander is loyal then one of the lieutenant is a traitor, see Figure 2.4a. The commander gives the order to attack to all the lieutenant* 3 *tells the other that she heard retreat from the commander. The loyal lieutenants*

Algorithm 1 The Oral message algorithm OM(m)

if $m = 0$ **then**;
    for $i = 1 \to n-1$ **do**
        Commander sends $v_i = v$ to lieutenant i
        Lieutenant i set their value to v
    end for
end if
if $m > 0$ **then**;
    for $i = 1 \to n-1$ **do**
        Commander sends v_i to lieutenant i
        Lieutenant i uses OM(m-1) to communicate v_i to the $n-2$ lieutenants
    end for
    for $i = 1 \to n-1$ **do**
        Lieutenant i set their value to $f(v_1, \ldots, v_{n-1})$
    end for
end if



(a) Commander is loyal

(b) Commander is a traitor

Figure 2.4: Illustration of the OM(m) algorithm in the case where $n = 4$ and $m = 1$.

then apply the map f to agree on their value

$$f(A, A, R) = A,$$

which coresponds to the order the commander sent, hence IC1 and IC2 are satisfied. If the commander is a traitor as in Figure 2.4b, then he sends conflicting order to the lieutenant but after communicating the value they received to each other finally agree on the following value

$$f(A, R, R) = R,$$

hence IC1 is satisfied and IC2 can be ignored since the commander is a traitor.

Theorem 2. *Algorithm OM(m) satisfies conditions IC1 and IC2 if $n > 3m + 1$.*

Proof. The proof follows from simple induction.

First assume that the commander is loyal. For $m = 0$, the commanders simply sends the value v to all the lieutenants and IC2 holds. Assume that OM$(m-1)$ works when the commader is loyal. The commander sends v to all the lieutenants. The lieutenants then applies $OM(m-1)$. Because $n-1 > 2k+m-1$, then it follows from the induction hypothesis that each loyal lieutenants get the value v for each of the loyal lieutenants j. The loyal lieutenants $n-1-m > 2k-1 > m$ outnumber the traitorous lieutenants and therefore set their value to

$$f(v_1, \dots, v_{n-1}) = v,$$

and both IC1 and IC follow.

Let us assume that the commander is a traitor, we only have to worry about IC1 in that case. There are at most m traitors and the commander is one of them. We therefore have $m-1$ traitors among the lieutenants. Since the total number of lieutenants exceeds three times the number of traitors $n-1 > 3m > 3(m-1)$ then by applying OM$(m-1)$ all the loyal lieutenants receive the same vector of values $v_1, \dots, v_{n-1}$, agree on the same value

$$f(v_1, \dots, v_{n-1}) = v,$$

which leads to the verification of IC1. □

The main problem associated to this Oral message algorithm is the number of messages is n^{m+1} which is prohibitive for large values of n and m. A celebrated algorithm, called Practical Byzantine Fault Tolerance (PBFT) has been developped later on by Castro and Liskov [1999] but still not fast enough to enable the infinite growth of the network associated to public and permissionless blockchains.

2.2 Leader system

The scalability issue can be solved by opting for a leader based mechanism instead of a majority vote mechanism. The protocols presented in this section use computational power, storage and bandwidth to elect a leader each time a new block must be appended to the blockchain.

2.2.1 Proof-of-Work

The bitcoin blockchain relies on a consensus protocol based on computational power called Proof-of-Work (PoW), presented in Nakamoto [2008]. A block consists of

- a header
- a list of "transactions" that represents the information recorded through the blockchain.

The header usually includes

- the date and time of creation of the block,

- the block height which is the index inside the blockchain,
- the hash of the block
- the hash of the previous block.

The hash of a block is obtained by concatenating the header and the transactions in a large character string thus forming a "message" denoted by m, to which a hash function h is applied.

Definition 1. *A hash function is a function that can map data of arbitrary size to fixed-sized values,*

$$h : \{0,1\}^* \mapsto \{0,1\}^d$$

The hash functions used in blockchain applications must be cryptographic, i.e.

- quick to compute
- one way
- deterministic

Remark 2.2.1. *It must be nearly infeasible to generate a message with a given hash value or to find two messages with the same hash value. A small change in the message should change dramatically the hash value so that the new hash value appears to be uncorrelated to the previous hash,*

$$\text{if } m_1 \approx m_2 \text{ then } h(m_1) \neq h(m_2).$$

We will not expand on how to build such a cryptographic hash function, we refer the interested reader to the work of Al-Kuwari et al. [2011].

In the bitcoin blockchain as well as in many other applications, the standard is the SHA-256 function which converts any message into a hash value of 256 bits. The latter is usually translated into a hexadecimal digest, for instance the hash value of the title of the present manuscript reads as

`98b1146926548f6b57c43474577 13ff2f035beda9c93f12fbc9b202e9c512e80`.

Mining a block means finding a block hash value lower than some target which can only be achieved by brute force search thanks to the properties of cryptographic hash functions. In practice, the search for an appropriate hash value, referred to as a solution, is done by appending a nonce to the block message before applying the hash function. A nonce is a 32 bits number, drawn at random by miners until a nonce resulting in a proper block hash value is found. For illustration, consider the block in Figure 2.5.

The hash value in decimal notation is $1.43e^{76}$ while the maximum value for a 256 bits number is $2^{256} - 1 \approx 1.16e^{77}$. We refer to the latter as the maximal target and denote it by T_{max}. The Proof-of-Work protocol sets a target $T < T_{\text{max}}$ and ask miners to find a nonce such that the hash value of the block is smaller than T. Practitioners would rather talk about the *difficulty* which is defined as $D = T_{\text{max}}/T$. If the difficulty is one, any hash value is acceptable. Increasing the

```
Block Hash: 1fc23a429aa5aaf04d17e9057e03371f59ac8823b1441798940837fa2e318aaa
Block Height: 0
Time:2022-02-25 12:42:04.560217
Nonce:0
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 0}, {'sen
der': 'Satoshi', 'recipient': 'Pierre-O', 'amount': 5, 'fee': 2}]
Previous block hash: 0
Mined: False
--------------
```

Figure 2.5: A block that has not been mined yet.

difficulty reduces the set of allowable hash values, making the problem harder to solve. A hash value is then called *acceptable* if its hexadecimal digest starts with a given number of zeros. If we set the difficulty to 2^4, then the hexadecimal digest of the hash of the block must start with at least 1 leading zero, making the hash value of the block in Figure 2.5 not acceptable. After completing the nonce search we get the block in Figure 2.6. Note that it took 5 attempts to find this nonce. The number of needed trials is geometrically distributed with parameter $1/D$, which means that with a difficulty of $D = 2^4$ it takes on average 16 trials. The protocol adjusts the difficulty automatically every 2,016 block discoveries so as to (globally) maintain one block discovery every 10 minutes on average. The time between two block discoveries depends on the number of hash values computed by the network at a given instant. At the time of writing, the network computes 182.58 Exahashes per second and the difficulty is 27,967,152,532,434.[1] For an exhaustive overview of the mining process in the bitcoin blockchain, we refer the reader to the book of Antonopoulos Antonopoulos [2017, Chapter 10]. As each trial (of the system) for mining a block is independent of the others and leads to a success with very small probability, the overall number of successes is binomially distributed and will be very well approximated by a Poisson random variable. This justifies the Poisson process assumption made in the sequel to model the block arrival and the reward collecting processes. Empirical studies of the block inter-arrival times data tend to confirm this hypothesis, see the work of Bowden et al. Bowden et al. [2020]. The information recorded in a public blockchain may be retrieved by anyone and can be accessed through a blockchain explorer such as blockchain.com, the content of the block of height #724724 may be viewed through the following link block content.

```
Block Hash: 0869032ad6b3e5b86a53f9dded5f7b09ab93b24cd5a79c1d8c81b0b3e748d226
Block Height: 0
Time:2022-02-25 13:41:48.039980
Nonce:2931734429
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 0}, {'sen
der': 'Satoshi', 'recipient': 'Pierre-O', 'amount': 5, 'fee': 2}]
Previous block hash: 0
Mined: True
--------------
```

Figure 2.6: A mined block with a hash value having on leading zero.

[1] Source: bitcoinblockhalf.com

2.2.2 Proof-of-SpaceTime

2.2.3 Proof-of-Interaction

2.2.4 Proof-of-Stake

Chapter 3

Security of blockchain systems

3.1 Double-spending in PoW

3.1.1 Random walk model

Double spending probability

Double spending time

3.1.2 Counting process model

Double spending probability

Double spending time

3.2 Blockwitholding in PoW

3.3 Nothing-at-stake in PoS

Chapter 4

Decentralization of blockchain system

4.1 Decentralization in PoS

Rich get richer? Polya's urn

4.1.1 Average stake own by each peer

4.1.2 Distribution of the stakes

4.2 Decentralization in PoW

4.2.1 Mining pools and reward systems

4.2.2 Mining pool risk analysis

Chapter 5

Efficiency of blockchain systems

5.1 A queueing model with bulk service

5.2 Latency and throughputs computation

Bibliography

Jean-Philippe Abegg, Quentin Bramas, and Thomas Noël. Blockchain using proof-of-interaction. In *Networked Systems*, pages 129–143. Springer International Publishing, 2021. doi: 10.1007/978-3-030-91014-3_9.

Saif Al-Kuwari, James H. Davenport, and Russell J. Bradford. Cryptographic hash functions: Recent design trends and security notions. Cryptology ePrint Archive, Report 2011/565, 2011. https://ia.cr/2011/565.

Andreas Antonopoulos. *Mastering Bitcoin*. O'Reilly UK Ltd., July 2017. ISBN 1491954388. URL https://www.ebook.de/de/product/26463992/andreas_antonopoulos_mastering_bitcoin.html.

R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor. Modeling and analysis of block arrival times in the bitcoin blockchain. *Stochastic Models*, 36(4):602–637, jul 2020. doi: 10.1080/15326349.2020.1786404.

Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, page 173–186, USA, 1999. USENIX Association. ISBN 1880446391. URL https://dl.acm.org/doi/10.5555/296806.296824.

J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation*, 104:23–41, 2016.

Protocol Labs. Filecoin: A decentralized storage network. *White paper*, 2017. https://filecoin.io/filecoin.pdf.

Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, pages 382–401, July 1982. URL https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/.

Jan Lansky. Possible state approaches to cryptocurrencies. *Journal of Systems Integration*, 9(1): 19–31, jan 2018. doi: 10.20470/jsi.v9i1.335.

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Available at https://bitcoin.org/bitcoin.pdf, 2008. URL `https://bitcoin.org/bitcoin.pdf`.

Fahad Saleh. Blockchain without waste: Proof-of-stake. *The Review of Financial Studies*, 34(3): 1156–1190, jul 2020. doi: 10.1093/rfs/hhaa075.

Sam M. Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt. Sok: Decentralized finance (defi), 2021.