Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies

Florian Tschorsch and Björn Scheuermann

***Abstract*—Besides attracting a billion dollar economy, Bitcoin revolutionized the field of digital currencies and influenced many adjacent areas. This also induced significant scientific interest. In this survey, we unroll and structure the manyfold results and research directions. We start by introducing the Bitcoin protocol and its building blocks. From there we continue to explore the design space by discussing existing contributions and results. In the process, we deduce the fundamental structures and insights at the core of the Bitcoin protocol and its applications. As we show and discuss, many key ideas are likewise applicable in various other fields, so that their impact reaches far beyond Bitcoin itself.**

***Index Terms*—Altcoins, Bitcoin, blockchain, cryptocurrencies, digital currencies, distributed consensus, survey, tutorial.**

I. Introduction

OVER THE past decades, the Internet has witnessed the advent of many bottom-up, grassroots applications which solve problems in a cooperative, distributed manner. A number of these community-driven, non-commercial systems have become well-known and widespread; examples include anonymous communication [1], PGP [2], Hashcash [3], and BitTorrent [4]. In fact, practically applicable solutions have often become available soon after the idea for a certain application had first been conceived. Digital money is an exception from this rule: from the early 1980s the vision of digital money had been around—but it took more than a quarter of a century before a fully distributed solution became reality.

The early attempts to build digital currencies, as described in [5], [6], require a central authority—that is, a bank. Approaches like B-money [7], Karma [8], RPOW [9], and bit gold [10] later came up with the idea to interpret the solution to a cryptographic puzzle—a proof of work—as something valuable. They compared it to a piece of precious metal or a minted coin. This way everybody could become a "digital gold digger", mining money independently from a bank, but still requiring a central instance to maintain ownership records.

In order to completely eliminate the bank, the ledger which accounts for the ownership of coins must also be distributed. However, a fundamental and inherent risk of digital currencies in general—and a distributed currency in particular—is the ability to double spend coins. Since digital copies are trivial, someone could issue two transactions in parallel, transferring the same coin to different recipients. In an online and centralized scenario, the bank is able to detect and prevent the attempt. Accomplishing the same in a distributed setting is far from trivial. The distribution of information and the problem of mutual agreement on a consistent state is a challenge, especially in the presence of selfish and/or malicious participants. It boils down to the Byzantine Generals problem [11]. This insight [12] pushed the idea to employ quorum systems [13]. Quorum systems, as described in [14], accept the possibility of faulty information and the existence of malicious entities in a distributed environment. They introduce the concept of voting. As long as the majority of any chosen subset of peers (quorum) is honest, the correct ledger state can be obtained by election. However, the approach is vulnerable to the Sybil attack [15]: a malicious entity could set up many peers which subvert the election and inject faulty information. Furthermore, it ignores the propagation delays in distributed systems and leads to temporary inconsistencies.

These difficulties were finally overcome by the Bitcoin design [16]. In November 2008 it was announced by Satoshi Nakamoto to the Cryptography mailing list [17]. After its deployment in 2009, Bitcoin quickly became viral. Nakamoto remained active until about 2010, before handing over the project. Until now the true identity of Nakamoto remains unknown and is subject to speculation, e.g., whether the name is real or a pseudonym, or if it in fact represents a group of people. That much is certain: Bitcoin cleverly combines existing contributions from decades of research [3], [14], [18]–[20]. Beyond that, however, it also solved fundamental problems in a highly sophisticated, original and practically viable way: it uses a proof of work scheme to limit the number of votes per entity, and thus renders decentralization practical.

Bitcoin miners collect transactions in a block and vary a nonce until one of them finds the solution to a given puzzle. The block including the solution and the transactions are broadcast to all other entities, and the distributed ledger (the *block chain*) is updated. The ownership of coins can be determined by traversing the block chain until the most recent transaction of the respective coin is found. Forks of the block chain due to malicious manipulations or propagation delays are resolved by considering the "longest" fork (including most of the work) as consensus. Thus, Sybil and—at least to some extent—double spending attacks are mitigated by binding additions to the block chain (votes) to proof-of-work contributions. The proof of work also induces a continuous supply of new coins as a reward (and incentive) for miners. All of this does not require a centralized coordinating authority, and practically demonstrates the feasibility of a distributed digital currency.

Early Bitcoin studies gave a preliminary overview of the system's strengths and weaknesses [21] and compared them

Manuscript received September 3, 2015; revised January 10, 2016; accepted February 14, 2016. Date of publication March 2, 2016; date of current version August 19, 2016.

The authors are with the Department of Computer Science, Humboldt University of Berlin, Berlin 10099, Germany (e-mail: tschorsch@informatik.hu-berlin.de; scheuermann@informatik.hu-berlin.de).

Digital Object Identifier 10.1109/COMST.2016.2535718

to paper and electronic cash [22]. This survey describes and reflects the state of the art in the area of fully distributed digital currencies. Today, this reaches significantly beyond Bitcoin. Yet, Bitcoin is still by far the most widely known system, and it marks the turning point which accelerated the entire research area. We therefore put Bitcoin at the center of our attention, and arrange related and alternative concepts around it. We will start from Bitcoin's proof-of-work concept, from where we explore the technical background and discuss the implications of the central design decisions. Based on a detailed understanding of these aspects, the research area beyond Bitcoin unfolds, so that we iteratively take alternative approaches into the discussion. For instance, this includes alternatives to the proof-of-work scheme or Bitcoin-like distributed consensus schemes for other applications. Many of these approaches result in new currencies, so-called "altcoins", which exist concurrently to Bitcoin.

In order to gain a full technical understanding of Bitcoin as it is used today, scientific literature alone is not sufficient. Many important details can only be found in mailing lists, forum posts, blogs, wikis, and source code—some of them dating back until the 1980s. This survey aims to provide the whole picture. Therefore, we also took these sources into account, to incorporate also those aspects that have previously not been described with scientific rigour. In fact, even though Bitcoin has been recognized controversially and gained media attention due to being used for criminal purposes, from a technical perspective, we perceive a certain beauty in the system, which may not necessarily be visible at a first glance, but which we hope to convey through our description.

The four goals of this survey are: (i) provide an holistic technical perspective on distributed crypto currencies, (ii) explore the design space and expose the implications of certain design decisions, (iii) consolidate and link the broad body of work while distilling the key algorithmic features, and (iv) identify the fundamental ideas which remain independent from specific implementations or temporary idioms of usage.

Likely the closest relative to our article—and worth a pointer in this context—is [23]. The authors outline the key elements of Bitcoin's design and the existing body of work in a condensed form for readers with substantial prior knowledge in the area. They also motivate further research in the field and discuss research challenges. In the article at hand, we address a broader audience by including a tutorial-style introductory part. Furthermore, we include a comprehensive selection from the existing literature for a more in-depth overview. Note that an earlier version of this survey is available as preprint [24].

The remainder of this survey is structured as follows. Section II introduces the basics of Bitcoin and provides a first outline of central concepts, including proof of work and the prevention of double spending. In Section III we then consider security threats and implications. Bitcoin's backbone, the peer-to-peer network, influences virtually every aspect of the currency; we cover it in Section IV. The subsequent Section V discusses the balance between privacy properties and the system's inherent transparency; here, we review many approaches to enhance privacy. In Section VI we revisit the proof-of-work scheme and related topics, and in particular discuss alternative approaches. Finally, Section VII summarizes our key observations and concludes this survey.

II. The Bitcoin Protocol

In this section we will explain the core Bitcoin protocol as originally introduced in [16]. This will pave the ground for more in-depth discussions of specific aspects in subsequent sections. We begin with an abstract and rather simplistic view of a digital currency, which we then iteratively refine. We also sketch the research context of the presented ideas, and, where appropriate, follow the early steps of digital currencies before Bitcoin [5], [6]. However, our discussions are always directed towards the foundations of the Bitcoin protocol and its main idea: the use of proof of work to eliminate the bank and to decentralize and secure the ledger. In particular, this section will successively introduce the basics on mining, the block chain, transactions and scripting.

The Bitcoin developer documentation [25], the Bitcoin wiki [26] and the Bitcoin source code (github.com/bitcoin/bitcoin) constituted valuable sources for the aspects discussed in this section. For a tutorial-like explanation of Bitcoin, we also refer the reader to the blog post [27] and the online course [28].

A. The Starting Point: Centralized Digital Currencies

Assume Alice intends to transfer a coin to Bob. In order to do so—in an extremely naive approach—she could generate a digitally signed contract stating "I transfer one coin to Bob" and announce it publicly. Following Bitcoin terminology, such a contract may be called *transaction* (TX). For the moment, we can consider it as a signed contract, which is verifiable using Alice's public key. It is per se not forgery proof, though, because it can be replayed: if a duplicate copy of the contract appears, it cannot be decided whether Alice tries to fool Bob, whether she (perfectly honestly) aims to transfer a second coin to Bob, or whether Bob performs a replay attack in order to claim multiple coins from Alice's account.

Obviously, to solve such ambiguities, uniquely identifiable coins are necessary. This could be achieved by introducing serial numbers—but where do they come from? We need a trusted source which issues the serials. In a centralized scenario this is what is generically called a *bank*: the bank issues coins with unique serial numbers and maintains a ledger including all ownerships, i.e., the mapping between user accounts and serial numbers.

Transferring a coin would then consist of Alice signing and announcing a transaction of the following form: "I transfer coin #1210 to Bob". Bob verifies the ownership of coin #1210 by consulting the bank. If the transaction is valid and Bob accepts the transaction, the bank updates its ledger. In this moment the owner of the coin changes from Alice to Bob.

This simple, centralized digital currency exemplifies the basic design of the banking model. In fact, it resembles the classical baseline of online electronic payment protocols [5], [6] (even though, of course, they include many clever extensions and additional features). An overview of further technologies in this domain can be found in [29].

Bitcoin aims for a much more ambitious solution, though: one which gets rid of the central bank. To this end, mechanisms are needed to create coins in a distributed setting, and to store and manage the ledger in a distributed way. The key

challenge is to achieve consensus on existing coins and their ownership without a central instance, and without mutual trust relationships between participants.

B. Proof of Work: Decentralizing the Currency

So, how can we eliminate the central bank? Bitcoin solves this in a very pragmatic way: in a sense, everyone is the bank. That is, every participant keeps a copy of the record which would classically be stored at the central bank. We can consider it a distributed ledger reflecting all transactions and ownerships. In Bitcoin, the so-called *block chain* takes the role of this distributed ledger.

However, distributed storage of multiple copies of the block chain opens up new possibilities for Alice to cheat. In particular, Alice could issue two separate transactions to two *different* receivers (say, Bob and Charlie), transferring the *same* coin. This is called *double spending*. If Bob and Charlie verified and accepted the transactions independently (based on their respective local copy of the block chain), this would drive the block chain into an inconsistent state.

In the banking model, double spending is prevented by the usage of serial numbers issued and controlled by the bank. The centralization also prohibits concurrent processing of transactions and enforces a total order. Transferred to the decentralized case, if Bob accepts the transaction and tells everyone else about it *before* Charlie accepts it, though, Charlie would be able to identify the transaction as a double spending attempt. Thus, under the assumption of a synchronous and unjammable broadcast channel, a simple, synchronized distributed ledger is viable. This is the essence of the simplified B-Money proposal [7]. This assumption does not hold in practice, though. Therefore, we have to deal with the undesirable period between issuing a transaction and having everyone informed about it—a prototypical distributed consensus problem.

Bitcoin addresses this problem by, in a sense, letting the entire network verify the legitimacy of the transactions, so that double spending will be noticed by other participants. If and only if a majority of the participants agrees on the existence and legitimacy of the transaction, Bob should accept it. The approach resembles the so-called Byzantine Generals problem [11], [12], i.e., it is related to the challenge of tolerating (intentional) faults in a distributed environment. With the Byzantine Generals problem in mind, the question of false identities arises: an adversary could mount a Sybil attack [15]. That is, Alice could set up many instances all confirming the transaction (thus constituting the "majority"), even though it is, in fact, a double spend. Bob would believe them and accept the transaction.

The Bitcoin protocol makes use of *proof of work* to prevent Sybil attacks. Before verifying a transaction and spreading the news about it, participants have to perform some work to prove they are "real" identities. The work consists of a cryptographic puzzle, which artificially increases the computational cost to verify transactions. Thereby, the ability of verification depends on the computing power, and not on the number of (potentially fake) identities. The underlying assumption is that it is much harder to control the majority of the computing power in the system than it is to control the majority of the identities.

Such proof-of-work schemes have (also before Bitcoin) been used in other areas, for instance against denial of service attacks or spam. Likely one of the best-known examples is Hashcash [3].

New Bitcoin transactions are communicated to all participants in the network. Given they are valid, these transactions are collected to form a so-called *block*. The puzzle used in the proof of work-based distributed validation process consists of calculating a hash of the thus formed block and adjusting a nonce in such a way that the hash value is lower than or equal to a certain *target* value. Once one participant has found such a nonce, the block with the respective nonce will be distributed in the network, and participants will update their local copy of the block chain.

Solving the puzzle is computationally difficult. Bitcoin uses the SHA-256 hash function [30]. Unless the (cryptographic) hash function used for calculating the block hashes is broken, the only fruitful strategy is to try different nonces until a solution is found. Consequently, the difficulty of the puzzle depends on the target value. The lower the target, the less solutions exist, the more difficult the puzzle becomes. If, for instance, the target demands that the (binary) hash begins with 42 zeros, an average of 2^{42} attempts are needed before the puzzle is solved.

Given that all network participants aim to solve the puzzle, the chance of being the first to come up with a solution is proportional to the fraction of the total computing power. Sometimes the analogy of "raffle tickets" is used: the number of tickets for a given participant is proportional to her computing power. The total number of tickets in the raffle wheel is proportional to the total computing power in the system. The more tickets in the raffle wheel, the lower are the chances of winning for a certain user with a given computing power. However, the user can increase her chances by buying more raffle tickets, i.e., by increasing her computing power.

For reasons of stability and reasonable waiting times for transaction validation, the target value is adjusted every 2,016 blocks. It is then re-chosen to meet a verification rate of approximately one block every 10 minutes. Thus, on average, every two weeks ($= 2016 \cdot 10$ min) the target is recalculated. The new target T is given by

$$T = T_{\text{prev}} \cdot \frac{t_{\text{actual}}}{2016 \cdot 10\,\text{min}}$$

where T_{prev} is the old target value and t_{actual} the time span it actually took to generate the last 2,016 blocks. However, the target never changes by more than a factor of four. If 2,016 blocks were generated during a time span shorter than two weeks, this indicates that the overall computing power has increased, so that the proof of work difficulty should also be increased.

In Bitcoin, the term *difficulty* is used in the specific meaning to express how difficult it is to find a hash below a given target. The ratio of the highest possible target and the current target is used as the difficulty measure. The minimum difficulty, that is the maximum allowed target value (2^{224}), is 1. Analogue, the maximum difficulty is when the target value is 1. It has been

noted [31] that the difficulty adjustments yield systematically too fast block creation for exponential hash rate growth (as it is the case in Bitcoin). With this issue in mind, the authors of [31] propose a new difficulty retargeting method.

Let us recap this in the context of our example, where Alice still wants to transfer coins to Bob. When Alice broadcasts her transaction, Bob, Charlie and many others receive it. They all verify its legitimacy based on their local copy of the block chain. Subsequently they enqueue it to the pending transactions they have heard of (that is, they add it to the current block). If Charlie intends to spread his "opinion" that the collection of pending transactions is valid, he first needs to solve the puzzle. Let us assume Charlie is the first participant who solves the puzzle, i.e., the first one to find a nonce for which the hash value meets the target. He then broadcasts the block of transactions together with this nonce. Other participants can verify that the nonce is a valid solution, and hence add the new block to their block chain. At this point, it is considered consensus that Alice's transfer of the coin to Bob is valid, and Bob is the new owner of the respective coin.

But, after all: why should anyone solve this puzzle and waste computation time (thus energy, ergo money) for verifying and certifying other people's transactions? What does Charlie gain from doing so? In order to provide an incentive, the Bitcoin protocol rewards the first participant who provides the proof of work with coins. There are two sources for this reward: *transaction fees* and *mining*. For now, we concentrate on mining and cover transaction fees only briefly. Later on, we get into more details also on the fees.

Mining is the process of adding new blocks to the block chain, because—in addition to securing the ledger—it results in the generation of new coins. Just like precious metals and collectibles, the block has an unforgeable scarcity: recall that parameters are chosen such that there is one successful puzzle solution roughly every ten minutes. This scarcity creates a value, which is backed up by the real-world (computational) resources required to mint it.

Note that mining also provides a controlled and predictable supply of coins, which does not involve a central bank. Bitcoin's precursors [7]–[10] already made this fundamental observation and incorporated it in their designs.

In Bitcoin, the initial block reward was set to 50 coins (50 BTC). Every 210,000 blocks, that is approximately once every four years ($= 210,000 \cdot 10$ min), the reward halves. This happened the first time by the end of November 2012[1]. Since then, the reward for a solved proof-of-work puzzle is 25 BTC. The iterative halving will continue until the mining reward drops below 10^{-8} BTC. This amount is the minimal unit of Bitcoin, also known as *satoshi*.

This event is predicted for the year 2140. The minting of new coins will then stop and all ever existing coins (approximately $21 \cdot 10^6$) will be in circulation. However, due to the transaction fees an incentive to validate new blocks will still remain. Indeed, since the first halving of the block reward, transaction fees have increased substantially. There are exceptions such as different transaction priorities [26, pp. Transaction Fees], but as a rule of thumb the transaction fee is currently 0.1 mBTC/kB, i.e., $0.1 \cdot 10^{-3}$ BTC per kB of the respective raw transaction data. The data size will be rounded up to the next thousand bytes, yielding a fee of 0.1 mBTC for typical transactions, regardless of the amount being transferred. Fees will most likely continue to increase over time and provide the necessary incentive. The relationship of mining rewards and transaction fees is discussed in [32].

[1]https://blockchain.info/rawblock/270670

C. Block Chain

So far, we gave only an abstract explanation of the block chain and denoted it as the distributed ledger. That still hits the spot—but there is more. We will now take a closer look at the structure of the block chain. In particular, we will turn towards the question how Bitcoin keeps the blocks in order and comes to a system-wide consistent consensus.

To determine the ownership of each coin, a total order of blocks (and thus transactions) is desirable. For this reason, blocks include a pointer to the previously validated block in the chain. This is illustrated in Figure 1. The pointer is implemented by including a hash of the preceding block. Consequently, the block chain has the structure of a linked list. The so-called *block height* is the number of blocks from head to tail. The block proves that a particular transaction must have existed at the time to get into the block. In this sense, Bitcoin implements a distributed variant of a timestamp service along the lines of [19].

Because of the continuous mining, the block chain constantly grows. Due to the popularity of Bitcoin in general and gambles such as SatoshiDice (satoshidice.com) in particular, the number of transactions has increased enormously. For instance, bets on SatoshiDice result in two transactions: the stake and the payout (which is at least one satoshi). The winner is determined by a pseudo-random number, which is derived from hashing a daily changing secret and information extracted from the transaction. Their transaction volume peaked in June 2012 with about 62,000 daily transactions. As a consequence, this inflates the block size and results in a non-negligible size of the block chain, currently in the order of tens of gigabytes. Furthermore, the high number of transactions increases the effort of the validation procedure itself. In order to keep the size and the computational effort low, Bitcoin offers a simplified payment verification (SPV) [16] based on Merkle trees [18]. It takes the transactions as leaves and builds a hash tree on top. The root of this tree is a hash value including information from all transactions; this root is included in the block header. The hash tree enables the verification of transactions without the need for a complete local copy of all transactions. Since the root is known and secured through the mining process, branches can be loaded on demand from untrusted sources. Tampering with any transaction would result in different hash values and would thus be detected.

Because block validations are calculated in a distributed way through mining, *forks* can occur: independent block validations can be broadcast almost simultaneously, or while the distribution of one validated block is stalled due to propagation delays. In case of a fork, there are two (or more) different versions

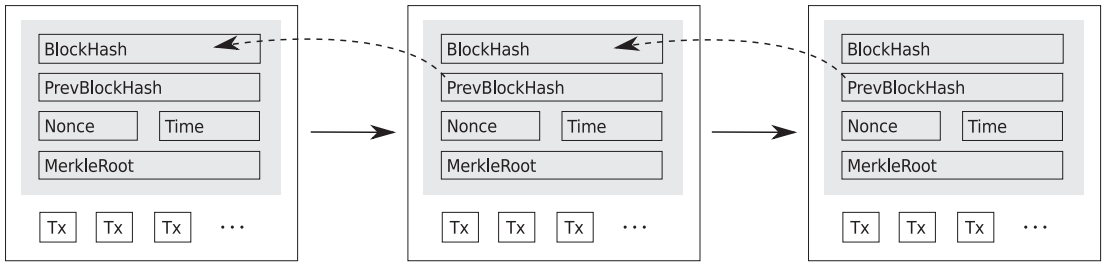


Fig. 1. Simplified block chain.

of the linked list with, potentially, different sets of included transactions. That is, different participants in the system will disagree on the structure of the block chain. Consequently, there might no longer be a consensus on the order of transactions. Hence, ownership is not settled.

Bitcoin solves this issue by a simple, but effective rule: mining is continued on the "longest" locally known fork, that is, the one involving the highest amount of computational effort so far. At some point, miners of one fork will broadcast validations before others. Thus, one of the forks will "overtake" the other and, once it has been propagated, will become the longest fork, i.e., the *main chain*, for all participants. Thereby, distributed consensus is restored.

If, for example, Alice tries to double spend the same coin with Bob and Charlie and shares the two transactions with two separate subsets of miners respectively, the block chain may fork. Eventually, only one fork will survive, that is, the longer fork will be considered the valid block chain. The other fork is then called *orphaned* and the included transactions are nullified. However, valid transactions of one fork may already be part of the other fork, too, or they will be added to the next block of transactions. Assuming Alice's transaction to Bob made it into the valid block chain, the transaction to Charlie will not be considered anymore, because it attempts to double spend coins. Charlie will recognize this situation after the fork is resolved.

Nevertheless, double spending is still possible under certain circumstances. Suppose Alice buys Charlie's car and wants to pay with Bitcoin. Hence she issues and broadcasts a transaction transferring the agreed amount to Charlie. At some point the transaction is included in a block and hooked into the block chain. Eventually the block chain grows, and additional blocks add up as depicted in Figure 2. In return, Charlie hands over the keys to his car. With malicious intentions in mind, Alice creates a conflicting transaction, transferring the coins to another account (e.g., one of her own ones). If she controls enough computing power (more than all honest miners together), she can start a fork and "catch up" with the block chain until her fork becomes longer and thus gets accepted by all others. As a result, she gets her money back. In general, someone who controls more than half of the total computing power can decide which blocks ultimately get accepted in the block chain. Therefore, this attack is commonly referred to as the 51% attack. Of course, the longer back transactions lie, the more blocks need to be caught up until a fraudulent chain gets accepted. This limits adversaries' possibilities to revise the history of transactions. As a rule of thumb, transactions are commonly considered steady after six consecutive block verifications. However, it remains a trade-off, which we will discuss and quantify in Section III.

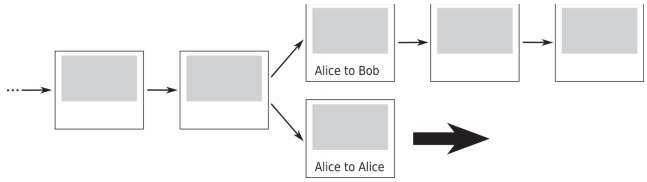


Fig. 2. Double spending (race attack).

D. Transactions

Until now we have not exactly stated what "coins" are in the Bitcoin protocol. In fact, coins as such do not exist: there are only transactions, which elaborately assign ownership rights. Thus, the closest actual equivalent to a coin we can think of is the chain of transactions. This will become clear by having a closer look at Bitcoin transactions and how they are composed.

Before receiving coins, Bob needs a virtual wallet consisting at least of a public/private key pair. Bob's Bitcoin *address* is derived from his public key, by hashing it with SHA-256 first and RIPEMD-160 subsequently, prepending a version number, and appending a checksum for error detection. Addresses are base58-encoded to eliminate ambiguous characters. The purpose of Bitcoin addresses is to shorten and obfuscate public keys. In order to receive payments they are not strictly necessary (one could also use the public key or a secret), but they provide a secure and convenient way. It is recommended to avoid key (and thus address) reuse because it harms security and privacy: in particular, it enables comparison-based attacks on signatures [33] and tracking of coin flows [34], [35]. Instead, a new key and address should be used for each transaction.

Assume Bob sends his Bitcoin address to Alice. Alice uses her wallet to issue a transaction with Bob's address as the destination. Figure 3 schematically depicts a transaction as it could occur when Alice transfers a coin to Bob.

The key elements of a transaction are a hash value as the transaction identifier (TXID) and a list of *inputs* and *outputs*. Alice uses the input to reference a so far unused output of an earlier transaction. More specifically, `prevTxHash` is the hash identifying the previous transaction and `index` is the index of the respective output in that transaction. Each output of a transaction can only be used once as an input in the whole block

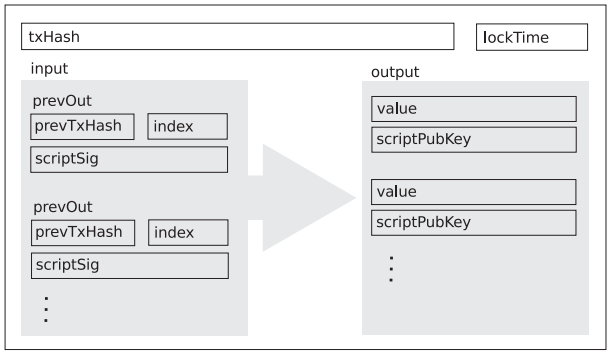


Fig. 3. Transaction.

chain. Referencing the same output again is an attempt to spend the same coin twice (double spending) and thus forbidden. Due to this property, each output of a transaction can be categorized either as an *unspent transaction output (UTXO)* if it has not been referenced by a subsequent transaction so far, or as a *spent transaction output (STXO)*.

In the most basic type of transaction, Alice proves that she is able to mandate over the output referenced on the input side by providing her public key and a signature. For each output, she needs to specify how many coins are to be transferred via this output (`value`) and how to authorize when spending these coins (`scriptKeyPub`); the latter might refer to Bob's Bitcoin address as the destination. The Bitcoin transaction system is much more powerful and flexible, though; this will become clear when we cover the concept of scripting.

It is important to note that the transaction input does not specify how many coins are spent. Because each output of a previous transaction can be used only once, inputs necessarily always use all the coins from the referenced output. Since transactions can have multiple inputs and multiple outputs, this does not restrict Bitcoin: Alice can use an additional output of her transaction to assign part of the coins to her own address, thereby not transferring all the coins from the inputs to others. In this way, Bitcoin implements the idea of *change*.

The sum of all inputs in a standard transaction must be at least as much as the sum of all the outputs. It need not be equal, though: if the input sum is greater than the outputs, implicitly the difference is assigned as transaction fee to the miner validating the block which contains the respective transaction.

The fact that transactions are linked leads us to an inherent and important property of Bitcoin: it is possible to trace transactions back in history. Eventually, doing so will terminate at one out of two possible origins: the *genesis block* or a *coinbase transaction*. Both include special transactions with outputs only.

The genesis block[2] is the origin of the block chain and provides the initial supply of 50 BTC to the system. A coinbase transaction is the much more common origin of a series of transactions. It is the transaction which rewards the miner for validating a block, thereby introducing new coins into the system. Since block chain forks can occur and some blocks will eventually become orphaned, coinbase transactions are locked for at least 100 blocks (i.e., they cannot be spent before 100 subsequent blocks have been verified).

[2]https://blockexplorer.com/b/0

```
scriptPubKey:OP_DUP OP_HASH160 <pubKeyHash>
  OP_EQUALVERIFY OP_CHECKSIG

scriptSig: <sig> <pubKey>
```

Script 1. "Pay-to-PubKeyHash" (P2PKH) script template

```
scriptPubKey: OP_HASH160 <redeemScriptHash>
  OP_EQUAL

scriptSig: [<sig> ...] <redeemScript>
```

Script 2. "Pay-to-PubKeyHash" (P2SH) script template

```
scriptPubKey: <m> <pubKey> [<pubkey> ...] <n>
  OP_CHECKMULTISIG

scriptSig: 0 [<sig> ...]
```

Script 3. *m*-of-*n* multi-signature transaction script template

Since coins as such do not exist in Bitcoin, there are also no serial numbers of coins. The transaction hashes and the reference to the previous transactions take the role of serial numbers as they are used in other digital cash systems. This, finally, also eliminates the need for a bank issuing serial numbers.

E. Scripts

As indicated before, Bitcoin transactions provide much more flexibility than just the simple coin transfers outlined above. In fact, through *scripting* there is a certain degree of programmability what exactly a transaction does. Scripting is realized by a simple stack-based language. It is intentionally designed not to be Turing complete, so that it is easier to handle and unintended side effects can be avoided.

For the following, bear in mind that a coin is only a generic term for a balance determined by a chain of transactions. Recall that each input of a Bitcoin transaction connects to a given, previous output. Each output in a Bitcoin transaction is described by a script. The operations to be performed, potentially along with constants, constitute the so-called `scriptPubKey`. A script expects a number of "arguments", the `scriptSig`. An input which connects to an output must provide the `scriptSig`the respective script. The connection is considered valid when the output's script evaluates to `true` given the `scriptSig` provided in the connecting input.

The probably most essential and most common script of all is "Pay-to-PubKeyHash" (P2PKH). Semantically, a transaction employing P2PKH transfers coins from one or more origin addresses to a destination address. The key idea is to have a script at the output which checks whether the connecting input has been signed with the public key "owning" the coins at the output. Script 1 provides the generic P2PKH script template. Bitcoin scripts are processed from left to right. In its `scriptSig`, P2PKH requires a public key (`pubKey`) which hashes to the

TABLE I
EXEMPLARY P2PKH SCRIPT EXECUTION

	scriptSig (unlocks an output)		scriptPubKey (locks an output)				
Script:	sigBob pubKeyBob		OP_DUP	OP_HASH160	pubKeyBobHash	OP_EQUALVERIFY	OP_CHECKSIG
Stack:					pubKeyBobHash		
			pubKeyBob	pubKeyBobHash	pubKeyBobHash		
		pubKeyBob	pubKeyBob	pubKeyBob	pubKeyBob	pubKeyBob	
	sigBob	sigBob	sigBob	sigBob	sigBob	sigBob	true

specified Bitcoin address (pubKeyHash) and a signature (sig) proving the possession of the respective private key.

Consider Alice's transaction to Bob. Alice would substitute the pubKeyHash token in Script 1 by Bob's Bitcoin address. She would then include the resulting script as one output script in her transaction to Bob, associated with the value she intends to transfer. If Bob wants to spend the coins again, he needs to provide his public key and his signature in the connecting input's scriptSig.

Table I shows the script execution and the state of the stack step by step. Here, pubKeyBob, pubKeyBobHash and sigBob denote Bob's public key, the hash of Bob's public key (i.e., Bob's address) and Bob's signature, respectively. First, scriptSig (the "arguments") from the input and the scriptPubKey (the "code") from the output are concatenated. The first tokens in the concatenated result are sigBob and pubKeyBob. These are constant values; constants are simply pushed to the stack when they appear in a script. OP_DUP duplicates the most recent entry, i.e., pubKeyBob, on the stack. OP_HASH160 hashes the most recent entry twice (SHA-256 and RIPEMD-160) and pushes the result, in this case pubKeyBobHash. In the next step, pubKeyBobHash (as inserted into the script template by Alice) gets pushed to the stack.

OP_EQUALVERIFY verifies the equality of the two topmost stack entries and raises an error if they differ. More generally, the suffix VERIFY as in OP_EQUALVERIFY indicates a combination of two steps, where the second one is equivalent to OP_VERIFY: OP_VERIFY takes the topmost element from the stack and marks the transaction invalid if this element is not true. This step concludes the first important check: whether the correct public key has been provided. The last remaining operation, OP_CHECKSIG, then checks the signature against the public key and pushes true if they match. If this final check also passes, the script legitimates Bob to spend the coins: a transaction is valid if nothing fails and the topmost stack entry upon termination is true.

Output scripts as discussed so far are created by the originator of the transaction, i.e., the payer. However, it might be desirable for the payment receiver to specify the output script, for instance to ensure long-term security. Of course, after receiving payments, receivers could transfer the coins to themselves with a customized output script. This is not really convenient, though, and it incurs additional transaction fees. Therefore, "Pay-to-ScriptHash" (P2SH) transactions were created and admitted as a standard transaction [36]. P2SH enables the receiver to specify a so-called *redeem script* (redeemScript). The hash of the redeem script is transformed into a Bitcoin address-like format [37] and sent to the originator instead of the recipient's Bitcoin address. The hash is included in a generic output script and can be redeemed as specified in Script 2. In principle, the redeem script can be any script, but the transaction is considered as a standard transaction only if the redeem script follows one of the standard "pay-to-x" scripts, e.g., a P2PKH. P2SH also supports future development and makes it easier to introduce and roll out new standard transaction types. The idea of P2SH has been generalized to the "pay-to-contract" protocol in [38].

Scripting in Bitcoin provides a huge variety of ways to spend coins. For instance, distributed contracts with minimal trust become possible. One building block are m-of-n multi-signature transactions [39], which require m valid out of n possible signatures to redeem a transaction. The use cases for m-of-n multi-signature transactions are manifold, e.g., they are used for (but not limited to) deposits, escrow and dispute mediation. A 2-of-3 multi-signature transaction can, for example, be used to realize customer protection via an independent mediator. In such a constellation, coins are locked and neither the buyer nor the seller alone can claim them. If, however, both agree, the buyer could pass a half-signed transaction over to the seller, who is now able to complete the transaction. In case of a dispute, the mediator can side with one of the participants and clear the situation by providing her signature. Another use case is to secure online wallets. If all funds are held in 2-of-2 multi-signature transactions, where one key is not stored in the online wallet, a thief would not be able to rob a wallet by hacking the online wallet provider. Because of their relevance and to get an impression of Bitcoin's advanced scripting capabilities, we take a somewhat closer look here.

Script 3 depicts the generic script template for an m-of-n multi-signature transaction. After pushing the constants to the stack, OP_CHECKMULTISIG takes the integer n first (because after pushing it is the topmost entry), then n pubKey items, subsequently the integer m, and finally m sig items off the stack. Now, in essence, OP_CHECKMULTISIG iterates over public key / signature pairs and executes OP_CHECKSIG. Every time a match is found, the script moves on to the next signature or otherwise tries the next public key. As a consequence, the provided signatures in scriptSig must be in the order of the appearance of their matching signature in scriptPubKey If the m signatures match, the script pushes true to the stack and legitimates the transaction.

Due to a bug in Bitcoin's implementation of OP_CHECKMULTISIG (it pops once too often from

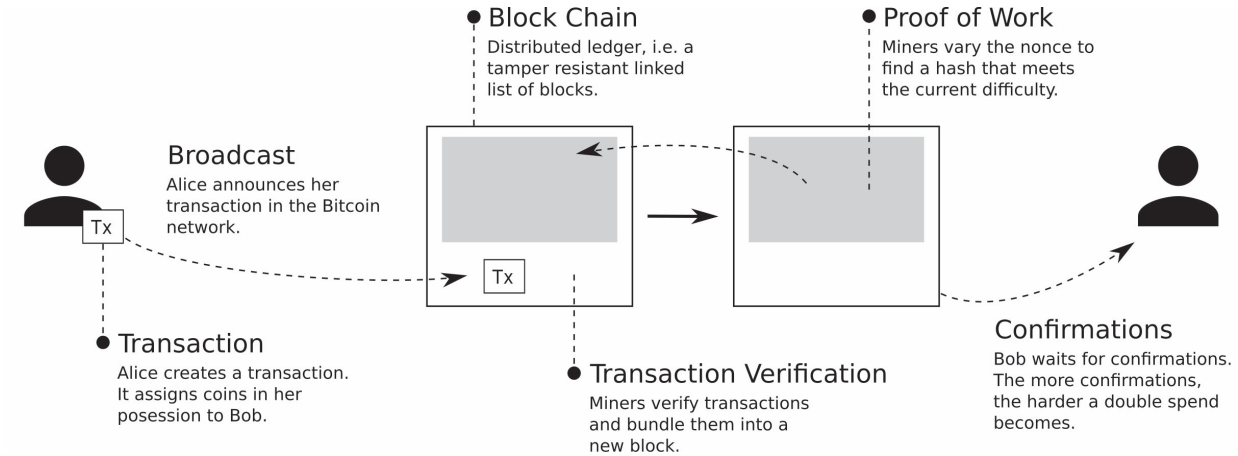


Fig. 4. Bitcoin's building blocks explained.

the stack), it is required to provide one extra value in the `scriptSig`, which is not used. Due to the requirement of maintaining compatibility, this bug cannot be fixed.

An m-of-n script can be realized with P2SH scripts and thus can be specified by the receiver(s). Here, the `scriptPubKey` becomes the redeem script. If $n \leq 3$, the transaction is considered a standard transaction.

Even though Bitcoin's scripting has a limited instruction set, the possibilities are manifold. The above mentioned examples can be considered rather limited and small compared to what is possible. In the remainder of this survey, we will see some clever protocols [40]–[42] which make heavy use of it. Constantly newly developed applications suggest that there is a large dormant, unexplored feature space.

Beyond Bitcoin, the so-called second generation of cryptocurrencies [43], such as Mastercoin (MSC, mastercoin.org), Counterparty (XCP, counterparty.io), and Ethereum (Ether, ethereum.org) implement a new transaction syntax with a fully-fledged (Turing-complete) scripting language [44], [45]. They follow the idea of smart contracts [46] and colored coins [47], which are understood as digital assets. These assets can be used to realize sophisticated financial instruments such as stocks with automatic dividend payouts or to manage and trade physical properties such as cars.

Most of these next-generation coins work on top of Bitcoin's block chain and are therefore called *on-chain currencies*. Since they encode their transactions into Bitcoin's transactions, they lack the validation of transactions by miners, because Bitcoin miners do not "understand" the new transaction types. However, the new protocol layer can build upon Bitcoin's strong foundation and its security. Furthermore, it will increase Bitcoin's value from which both will profit. Sometimes the analogy used to describe the relation between next-generation currencies and Bitcoin is that of HTTP and TCP/IP: HTTP provides a versatile application-layer protocol to the more fundamental transport and network layer. Similarly, the scripting languages are compared to the relation between JavaScript and HTML.

F. Recapitulation

After motivating Bitcoin's design decisions step by step, we will now recap and see how the building blocks work together. Figure 4 breaks down and illustrates the involved steps of a coin transfer from Alice to Bob. First, Alice uses her Bitcoin wallet, i.e., a collection of private keys, to create a transaction. The transaction script proves that Alice is in the possession of the referenced coins and assigns the specified amount to Bob's Bitcoin address. She broadcasts the transaction to let everybody else, in particular miners, convince themselves of the legitimacy. Miners bundle her and many other transactions in a block and attempt to find the respective proof of work, i.e., to solve the cryptographic puzzle by altering the nonce. Blocks refer to previous blocks and therefore not only confirm the legitimacy of all included transactions but also all previous transactions. With every new block that is a confirmation of Alice's transaction, Bob becomes more and more confident about its validity.

The enormous success of Bitcoin attracted a large number of users. The majority of Bitcoin users seems to be classifiable as geeks, investors, ideologists, or criminals [48]. The groups are not mutually exclusive, but there is an ideological divergence: while libertarians conceive it as an alternative currency independent from state power, others grasp it as a decentralized payment system that challenges power structures within the realm of finance [49].

Anyway, in order to use Bitcoin, the by far easiest way is to buy coins from an exchange. To this end, one deposits money to an account at the exchange, in any currency supported by the exchange. The deposit can be used to trade with other users by placing so-called "buy" and "sell" orders. Buy orders are offers to buy a certain amount of coins in exchange for another currency at a maximum price. Sell orders are offers to sell a certain amount of coins at a minimum price. The exchange back-end can execute orders according to the *order book*, if the price of a buy order is at least as high as the price of a sell order. The Bitcoin price increased rapidly since it became more popular and known to a wider audience [50]. About five years after Bitcoin's launch, the exchange rate surpassed the mark

TABLE II
COMPARISON OF BANKING MODEL AND BITCOIN

	Banking Model	Bitcoin
regulation/oversight	central bank	consensus
transaction verification	centrally	consensus
money creation	loans	mining
money supply	virtually unlimited	finite supply
value of money	exchange rate	proof of work, supply and demand, trust
money transfer	mediated, reversible	direct, non-reversible
privacy	implementation-dependent	somewhat anonymous
fees	account charge, transaction charge	virtually constant transaction charge
transaction delay	theoretically instantaneous, practically in the order of days	in the order of tens of minutes

TABLE III
BITCOIN ATTACK VECTORS AND VULNERABILITIES

Attack Vector	Description	Sec.
wallets	vulnerable to theft [54], [55]	III-A
key recovery	recovering private keys due to weak randomness [33], [56]	III-A
51% attack	achieves optimal Byzantine resilience, i. e., $2f + 1$ resilience [57]	III-B, V-D
double spending	double spending is and will always be possible [58]	III-B
block withholding	used for double spending [59], [60] and for selfish mining [61]	III-B, III-D
transaction malleability	altered TXIDs [62] to make sb. believe transactions have been failed [63]	III-C
timejacking	used to isolate peers [64] and to drift mining difficulties [65]	III-D
netsplit	facilitates double spends with more than one confirmation [66]	IV-B
scalability	depends on propagation delays [67] and fork resolving strategies [68]	IV-D
centralization	weakens the resilience of the currency [69], [70]	IV-D, V-E
DoS	peer blacklisting can be used to mount denial of service attacks [71], [72]	IV-E
transaction history	block chain analysis might reveal trade relationships [73]–[75]	V-B

of $1,000 per bitcoin. The price dynamics have been a controversial topic, though, keeping various research disciplines busy [51]–[53]. Nevertheless, Bitcoin has turned many early adopters into millionaires and still comprises a billion dollar economy.

From a technical point of view the Bitcoin design decentralizes the common banking model. In Table II we compare both approaches. Certainly, there are pros and cons on both sides. However, Bitcoin turned the typical conception of digital money upside down. In the following sections we will dig deeper in to the technical details and the respective implications.

III. SECURITY

In this section, we discuss security risks and security implications of the Bitcoin protocol and system design. Since Bitcoin is a digital currency with a notable market value, motives to exploit weaknesses for profit are ubiquitous. Beyond double spending, the attack vectors include key recovery and transaction malleability, for example. Table III gives an overview of potential vulnerabilities of which we will discuss the majority in this section. The most fundamental fear, though, remains the so-called 51% attack. During its discussion we will also have the opportunity to explore some elementary system properties of Bitcoin.

A. Wallets and Cryptography

In order to use Bitcoin, the first thing a user needs is a wallet. The wallet holds a public/private key pair, which is the best approximation of the user's account. Thus, obviously, it is essential to take protective means to secure the wallet [26, pp. securing your wallet].

Common Bitcoin terminology distinguishes a variety of wallet types, such as software, hardware, paper, brain and online wallets. Software wallets are one of the most common ways to use Bitcoin. For a software wallet, a locally running Bitcoin instance is necessary. The Bitcoin developer team release a reference implementation of the Bitcoin protocol (bitcoin.org). It is a full client which processes the whole block chain. However, there are many alternative implementations such as Armory (bitcoinarmory.com) or Electrum (electrum.org), which offer additional features. Online wallets such as blockchain.info or Coinbase (coinbase.com) are another popular way to participate. They either manage the wallet centrally, or they follow a hybrid approach where the wallet is stored encrypted and most operations are performed on the client side in the browser. All software and online wallets are inherently prone to security problems because an attacker gaining access to a targeted machine can also obtain access to the user's wallet.

The term hardware wallet summarizes a class of approaches which follow the idea of using a separate device that usually operates offline. Since the device is not directly connected to a network, it becomes much harder for an attacker to gain access. For an example see [55]. More advanced and secure ways (at least if done right) are paper and brain wallets. A paper wallet stores the keys holding coins offline as a physical document. This way they are comparable to cash money. A brain wallet takes it a step further and stores keys in the user's mind by memorizing a passphrase. The passphrase is turned into a private key, from which the public key and the Bitcoin address are derived with Bitcoin's standard hashing and

key derivation algorithms. To avoid dictionary or brute-force attacks, the phrase must be sufficiently long and must have a very high level of entropy.

We already noted that multi-signature transactions can be used to increase the security of wallets. For example BitGo (bitgo.com) offers online wallets with 2-of-3 multi-signature transactions. In the same manner, threshold signatures can be used to impede theft and add two-factor security to wallets [54], [76]. The idea comes directly from secret sharing [77]: the secret, in this case the private key, is split into shares. Any subset equal to or greater than a predefined threshold is able to reconstruct the secret, but any subset that is smaller gains no information about the secret. The main property of threshold signatures is that the key is never revealed. Participants directly construct a signature. This way, very much like multi-signatures, threshold signatures can be used to require m-of-n shares in order to sign a transaction. However, threshold signatures look like regular P2PKH transactions in the block chain, because they mutually construct a single transaction signature. They are, consequently, indistinguishable from the majority of transactions and thus conceal the details of access control. Multi-signature transactions, on the other hand, can be signed independently and do not require multiple rounds of interaction. The advantages and disadvantages of both approaches are discussed in detail in [54], [76].

In order to secure transactions, the Bitcoin protocol makes heavy use of elliptic curve cryptography [78], [79]. For transaction signatures, the elliptic curve digital signature algorithm (ECDSA) as standardized by NIST [80] is used, parametrized by the `secp256k1` curve defined by [81]. For example, take the standard P2PKH transaction script. The user needs to provide her public key and her signature to prove ownership. To provide a signature, the user chooses a per-signature random value, which must be kept secret and must not be used for more than one transaction. Otherwise, the secret key can be computed from the signature. Even partially bit-wise equal random values suffice to derive the private key [56]. Thus, it is essential for the security of ECDSA to use unpredictable and distinct per-signature randomness for every signature. The authors of [33] inspected the block chain for instances of repeated signature nonces for the same public key. They found that 158 public keys reused the signature nonce in more than one signature, making it possible to derive private keys. For all these public keys, the remaining balance is negligibly small (smaller than the transaction fees needed to transfer them). However, one single address claimed coins from 10 of the vulnerable accounts (in sum over 59 BTC) from March to October 2013. The coins appear to have been stolen by this address. In [33], the authors traced the incident back and found that one cause was the incorrectly seeded random number generator of blockchain.info's JavaScript client.

Thefts due to hacked systems, buggy software or incorrect usage are probably the greatest security risk in Bitcoin. As we will see, there are more examples which confirm this view. However, the most prominent type of attack is double spending which we already touched in the previous section, and which we will now re-consider in more detail.

B. Double Spending

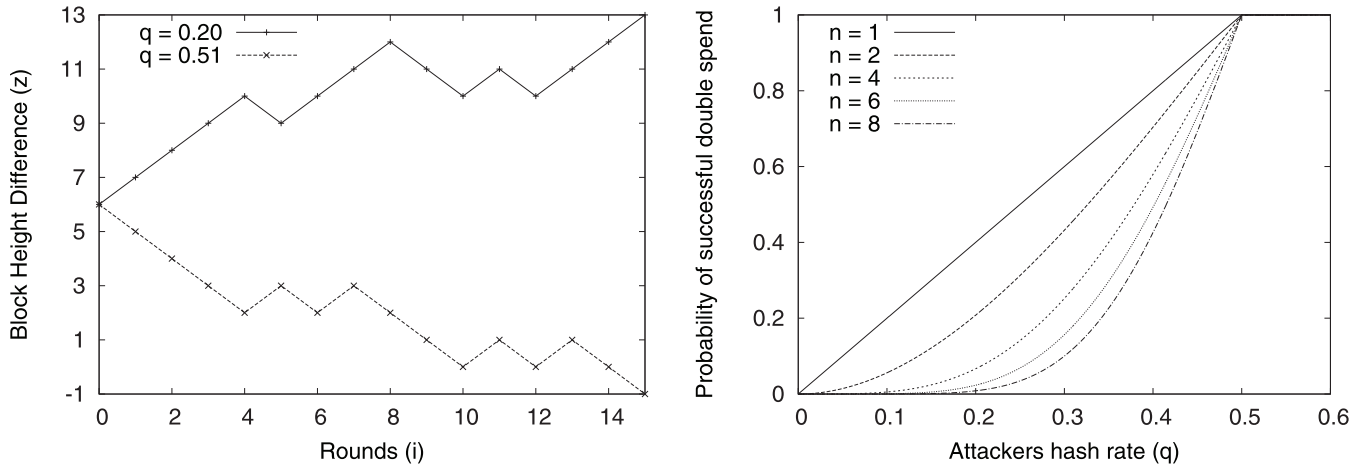
In an online scenario with a centralized bank and with coins that are distinguishable (e.g., by serial numbers), double spending as discussed before is trivially detectable. However, early digital currencies often also considered offline scenarios [6], which made it impossible to contact the bank to authorize the transaction. This made double spending a major issue, even if a central authority existed. Generally, the Bitcoin setting is an online scenario (though offline transactions have been considered, too [82], [83]). However, Bitcoin doesn't have a bank—and the distributed ledger opens up other possibilities for double spending.

The two generally conceivable ways to deal with double spending are (i) detecting it after the fraud actually happened and identifying the adversary for prosecution, or (ii) trying to prevent it. The above mentioned early digital currency approaches followed the first path: they accepted the possibility of double spends and required randomized parts of identifiers in the transactions. In case of double spending, the bank could assemble these parts afterwards to identify the adversary. The first approaches to mitigate double spends used the help of third parties in witness or quorum mechanisms [10], [84], [85]. These approaches are similar to Bitcoin's approach, but still come with the major flaw of being vulnerable to Sybil attacks.

Bitcoin protects against double spending through the rule that only previously unspent transaction outputs may be used in the input of a follow-up transaction, where this rule is enforced during transaction propagation and mining, and where the order of transactions is determined by their order in the block chain. This boils down to a distributed timestamping [19] and consensus algorithm [13], [14], which in turn can be understood as the Byzantine Generals problem [11], [12]. To protect from Sybil attacks [15], Bitcoin couples this to a random oracle, i.e., the proof of work. Thus, the capabilities of an adversary are limited by his computational power.

The authors of [57] modeled the Bitcoin protocol along the lines of a Byzantine consensus algorithm. They showed that it indeed reaches consensus. In particular, under the assumption of synchronous communication Bitcoin achieves optimal Byzantine resilience, so-called $2f + 1$ *resilience*, even in the presence of adversaries. This means the system is safe as long as the honest nodes n prevail the adversaries f by the ratio of $n > 2f + 1$. In case of Bitcoin, the network is resilient to adversaries controlling less than half of the computational power. In the next paragraphs we will assess this property in detail and consider how such an attack manifests in the block chain.

Recalling what has been said before on block chain forks and re-gaining consensus, an attacker can exploit this mechanism to mount a double spend attack along the lines of the example given in the previous section. A more generic blueprint for such a double spend includes the following steps: (i) broadcast a regular transaction (e.g., paying for a product), (ii) secretly mine on a fork which builds on the last block and includes a conflicting transaction which uses the same outputs as in step (i), but pays the attacker instead of the seller, (iii) wait until the seller is confident (i.e., receives enough confirmations) and



(a) Random walk simulation ($z_0 = 6$).

(b) Probability of successful double spending.

Fig. 5. Hash rate-based double spending analysis based on the results from [16], [58].

hands the product over, (iv) as soon as the secret fork is longer than the public chain, broadcast the respective blocks. Because the secret branch is longer, the network will consider it as the valid main block chain. The regular transaction becomes invalid and cannot (even when broadcast by the seller) be included in a block anymore. Accordingly, the longest chain rule has been criticized by [86]. The author notes that it actually tries to solve two distinct problems, namely which blocks and which transactions should be accepted. He suggest to employ separate rules.

In order to assess the success conditions for this type of double spend attacks, let us take a look how to model the race between the benign and the fraudulent block chain. As in [16], [58], we describe it as a binomial random walk. Assume that the hash rates and therefore the difficulty remain constant. Further assume the probability that an honest node finds the next block is p and the probability that an attacker finds the next block is $q = 1 - p$. We denote the difference in heights between the fraudulent and the benign block chain by z. Whenever a block is found, z changes by either $+1$ for a benign block or by -1 for a fraudulent block. Thus z is given by

$$z_{i+1} = \begin{cases} z_i + 1 & \text{with probability } p \\ z_i - 1 & \text{with probability } q. \end{cases}$$

We are interested in the question whether z will ever become -1, which implies that the attacker surpassed the benign block chain and successfully mounted a double spend. Analogously to the results presented in [58], Figure 5a exemplarily shows the two possible outcomes in a random walk simulation. We can draw the conclusion: if $q > p$, i.e., if the attacker controls more than the half of the total hash rate, he will succeed in catching up (for $i \to \infty$). The attacker's success is independent of the number of confirmations. This particular double spending attack is called the $> 50\%$ (commonly referred to as 51%) attack.

The situation is comparable to the Gambler's Ruin Problem [87], which considers the probability of a player ending up without money in a coin-flipping game given the initial credit. For arbitrary probabilities p and q of the possible outcomes in a single iteration, it can be shown that the probability q_z of experiencing gambler's ruin having started with z credits yields

$$q_z = \begin{cases} 1 & \text{if } z < 0 \text{ or } q > p \\ (q/p)^z & \text{if } z \geq 0 \text{ and } q \leq p. \end{cases}$$

In case of Bitcoin, q_z is the probability of the attacker ever catching up from z blocks behind the benign block chain. While for $z < 0$ (the attacker already is ahead of the benign block chain) and $q > p$ (the attacker controls the majority of the overall hash rate) the attacker's success is certain, for the case $z \geq 0$ and $q \leq p$ the probability of success decreases exponentially with z.

Now, what is the probability of a successful double spend *while* honest miners are finding new blocks and hence new confirmations? Remember, the rule of thumb suggests to wait for six confirmations before accepting a transaction. Therefore, assume that the attacker has to deliberately wait for n confirmations, that is, let the benign chain continue to grow by n additional blocks. Meanwhile, though, the attacker is able to produce (not yet published) blocks in the fraudulent fork, the number of which we denote by m. The original Bitcoin paper [16] assumes that m follows a Poisson distribution. More accurately, [58] models the probability of m as a negative binomial variable $P(m)$. Furthermore it is there assumed that the attacker pre-mined a block before initiating the attack, hence $z = n - m - 1$. It follows that the probability of a successful double spend equals

$$\begin{aligned} r &= \sum_{m=0}^{\infty} P(m) \cdot q_z \\ &= \begin{cases} 1 & \text{if } q \geq p \\ 1 - \sum_{m=0}^{n} \binom{m+n-1}{m} (p^n q^m - p^m q^n) & \text{if } q < p. \end{cases} \end{aligned} \quad (1)$$

We visualized the results of equation (1) for various numbers of confirmations n in Figure 5b. Clearly, the higher the number of confirmations, the lower the probability of a successful double spend. The success probability converges to one when the attacker's hash rate approaches the 50% threshold. As [58]

concludes from the results, double spending is possible with *any* hash rate of the attacker, and there is *no* number of confirmations that can reduce the success probability to zero: an attacker with less than 50% of the total computational power is able to perform a double spend by brute force and sufficient luck. A 51% attack will definitely lead to success. In this case, the attacker is able to claim all block rewards for himself, reject transactions and include only those he likes. This will likely drive miners off, which in turn increases the attacker's share and strengthens his position. Thus, the 51% attack is considered the worst-case scenario, because it will probably destroy the Bitcoin network. For this reason it is also called the Goldfinger attack [69].

Traders accepting transactions immediately without any confirmation (i.e., zero confirmation) are particularly exposed to double spending. The authors of [88] analyzed double spending attacks for such fast payments and demonstrated their feasibility. According to their results, it is possible for clients who are not miners to cheat. In order to mount a zero-confirmation attack, the attacker sends a transaction directly to the seller and broadcasts a double-spend transaction in another corner of the network at the same time. If the attacker is lucky enough, the double-spend transaction will make it into the main block chain which is recognized by the seller too late. In particular, an adversary can exploit block chain forks due to the simultaneous adoption of client versions to perform such double-spending attacks [89].

By secretly pre-mining a block, the attacker can increase the chances of success. In every block, the attacker includes a self payment (this will become the double-spend transaction). If he solves the proof of work, he suspends broadcasting and initiates a trade referring to the same coins. The seller (and even the network) will consider the transaction valid. As soon as the trade is completed, the attacker broadcasts the prepared block, which includes the double-spend transaction and thus takes precedence over the other one. This attack was first described by Finney [60] and is hence known as the Finney attack. The general strategy is also referred to as *block withholding*, which also finds use beyond double spending [90], [91].

The fixes to zero-confirmation attacks are implemented since the beginning of Bitcoin: "just wait for confirmations". However, even when waiting for a confirmation, an attacker can employ strategies to increase the chances of success. The Vector76 attack [59] is an example of a 1-confirmation attack. Again, the attacker pre-mines and withholds a block, but this time includes a deposit transaction to the target (e.g., an exchange service) in this block. If the block is ready, the attacker waits for a block announcement and quickly sends the pre-mined block directly to the target. The target and probably some miners will consider the pre-mined block as the main chain. Thus, the deposit transaction has one confirmation. In response, the attacker requests a withdrawal. If the attacker's fork of the block chain survives, the withdrawal will settle. If the other fork survives, however, the deposit is part of an orphaned block and hence invalidated. If additionally the withdrawal does not use the same coins as the deposit (i.e., it does not refer to the outputs from the deposit), then it will still be valid and now in the possession of the attacker. The required behavior is not uncommon for exchanges.

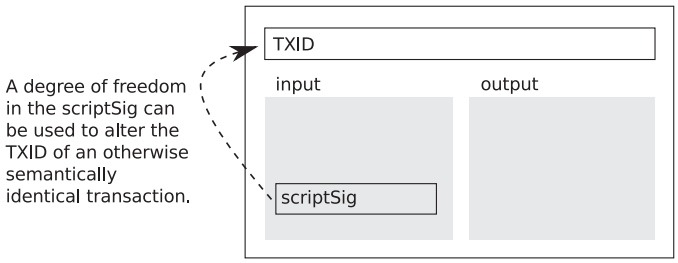


Fig. 6. Transaction malleability.

The fix—again—consists of waiting for more confirmations. However, sellers (or exchanges) can also take some other precautions, like not accepting inbound connections, which we will detail when talking about the Bitcoin peer-to-peer network and its relay patterns in Section IV. For now, we conclude that race attacks for double spending cannot be eliminated entirely. Therefore, each participant of the Bitcoin network needs to trade off the risk and choose to wait for an appropriate number of confirmations. On the other side, there is a trade-off for the attacker, too, who also needs to consider the costs and benefits: if the attack fails, block rewards for pre-mined blocks will be lost. To compensate for the risk, it is therefore necessary to double spend a certain minimum amount.

Even when successful, the block chain allows to recognize double spendings and to identify the tainted coins [70]. The victim will likely keep an eye on these coins and track their flow. Other traders might not be willing to accept tainted coins, because they will always be associated with a fraud. This led to blacklisting and whitelisting considerations. [92] provided first thoughts on quantifying and predicting the risks that are involved.

C. Transaction Malleability

Originally, *transaction malleability* refers to a bug in the Bitcoin protocol, which makes it possible to change the TXID without invalidating the transaction. Recall the anatomy of a transaction as depicted in Figure 6: it includes references to previous transactions (inputs) with a respective redeem script (`scriptSig`) and specifies one or multiple destinations (outputs). Each transaction can be uniquely identified by its TXID, which is a hash of the transaction data, including the redeem script(s).

The signature in a script, however, does not cover the same data as the hash which forms the TXID. In particular, it does not cover the redeem script. The rationale behind this design is that signing the script would imply signing the signature itself, which is obviously impossible. Instead, during signature generation, Bitcoin replaces all redeem scripts by a dummy script consisting of a single `OP_0` (this operation pushes an empty string on the stack). This substitution is not applied when calculating the TXID, though. As a consequence, it becomes possible to modify the transaction by substituting the redeem script by another valid (yet different) one. As a result, the signature remains valid, but the TXID changes.

For instance, a redeem script can be changed without invalidating it by pushing additional data to the stack prior to the data expected by the script of the connected output. In particular, as revealed in [63], it was common practice for exploits to substitute the push operations by zero-padded alternative push operations, thereby preserving the semantics, but altering the TXID. But also the signature itself is vulnerable, because OpenSSL tolerates variations in the encoding of signatures. A list of known sources of malleability, including respective transaction validity rules to tackle the issue, is provided by [62].

Transaction malleability is, of course, not desired. However, per se it does not cause any damage. An attacker can exploit the behavior, though, and make someone believe a transaction has failed, even though it later on gets confirmed. This becomes particularly relevant when targeting exchanges. Exchanges let users buy and sell coins for fiat money or altcoins and hence hold a significant amount of coins. They act as wallet providers to the effect that users who wish to trade need to provide a deposit.

A transaction malleability attack against an exchange proceeds as follows: (i) the attacker withdraws coins from an exchange and (ii) as soon as the attacker receives the respective withdrawing transaction issued by the exchange, he rebroadcasts the altered version of this transaction with a different TXID. One of the two transactions eventually makes it into the block chain. Due to propagation delays and precautions the attacker can take, there is a chance that the modified transaction wins over the original withdrawal. If the exchange relies on TXIDs only, it will not find the withdrawal transaction in the block chain and believe the withdrawal has failed. As consequence, the attacker may withdraw again (and again).

Considered from this angle, the transaction malleability attack can be thought of as a variant of a double spending [63]. In contrast to a typical double spend, however, the attacker is the receiving and not the spending party. The success of the attack depends on a number of constraints, i.e., the malleable transaction must be confirmed and the exchange must check for TXIDs only. The authors of [93] design a malleability-resilient "refund" transaction which does not require any protocol modifications.

We can conclude exchanges are a point of failure in an otherwise highly distributed environment. Therefore additional means of protection, such as cloud providers to protect from distributed denial of service (DDoS) attacks [94], are often employed.

Double-spending attempts (including transaction malleability exploits) in general can only be observed while the colliding transactions are in circulation. Afterwards, only by parsing the block chain, it is not possible to identify successful instances. How exchanges implement the withdrawal process and whether they are truly vulnerable often remains unclear. Therefore, [63] define a transaction malleability attack as successful if the altered transaction gets confirmed. The authors observed transaction activities on the Bitcoin network since January 2013 and identified 28,595 incidents of which approximately 20% were successful. They add up to 64,564 BTC which potentially got stolen.

Bitcoin's reference implementation is (and was) not affected, because it also tracks the respective unspent transaction outputs (i.e., UTXOs) and takes them as an indication for a successfully issued transactions. Some exchanges, though, used a custom implementation and were apparently vulnerable. For example Mt. Gox—a popular exchange in the early days of Bitcoin—released a statement that they were affected by transaction malleability attacks and that it is the cause for halting withdrawals and freezing accounts. The authors of [63] found a strong correlation between the press releases and the attack rate. However, if Mt. Gox stopped withdrawals as stated, it cannot be the root cause of their shutdown, because the majority of attacks occurred after the announcements: only 421 transactions adding up to approximately 1,800 BTC were potentially stolen before. The results rather suggest that the press releases motivated imitators to exploit the vulnerability elsewhere.

Due to the huge coin volume, exchanges are exposed to heist either by external attackers—or the operator itself. In order for an exchange to proove that it is in control of sufficient reserves without actually unveiling all Bitcoin addresses, protocols such as [95] can be used. As [96] find by modeling the risk coin holders face from exchange failures the transaction volume is an indicator whether or not an exchange is likely to close. They also confirm the intuitively obvious: less popular exchanges are more likely to close than popular ones, but popular exchanges are more likely to suffer from security breaches.

D. Pooled Mining

As pointed out before, Bitcoin must strive to maintain a structure in which no entity controls more than half of the computational power. Most of the time in Bitcoin's history, this was the case. However, being the first to successfully verify a block (i.e., being the first to find a valid nonce) happens only with a very small probability. Therefore, the payoff for *solo mining* is extremely bursty: a significant reward—but only very seldom. Miners therefore more and more group into *mining pools*. In a mining pool, multiple miners contribute to the block generation conjointly. Each participant searches parts of the nonce space for a valid nonce. In case one of them is successful, the profit is shared. Therefore, each participant get continuous small rewards, instead of seldom, large ones. Multiple different payout functions are used for sharing the profits in mining pools [90].

From the security perspective, the trend to form mining pools raised concerns: a mining pool centrally aggregates computational power of miners who should, according to the key design idea behind Bitcoin, guarantee a valid distributed quorum through independent participation. A look at the block chain reveals that regularly multiple consecutive blocks are mined by a single mining pool. It already happened a few times that big mining pools such as GHash.io approached the critical threshold of 51% of the network's hash rate [97]. And even if a single mining pool does not exceed the critical threshold by itself, coalitions are able to do so.

There are several options to tackle the problem. Actually, it is in the own interest of each miner to keep the distributed

ecosystem intact. Therefore, the easiest solution is that miners by themselves switch to other mining pools so as to reasonably redistribute the power. As it turned out in the past, this works surprisingly well: calls by the community to switch mining pools were heard and the pools themselves started to support this movement [98].

An engineering approach to the issue is to decentralize the mining pool. Even if a decentralized mining pool gains more than half of the computational power, this power cannot be exploited due to the lack of a central coordinating entity. P2Pool (p2pool.in) is a decentralized mining pool which builds a peer-to-peer network of miners. It creates a new block chain, called *share chain*. The blocks of the share chain are valid Bitcoin blocks, but with a lower difficulty, so that every 30 seconds a new block is generated. If a P2Pool peer finds such a block, it gets broadcast, verified by others, and added to the share chain in similar manner as in Bitcoin itself. This continues until a peer finds a block that also meets Bitcoin's mining difficulty. The respective block is broadcast in the Bitcoin network and the reward is distributed among the P2Pool clients according to the share chain. Since the share chain blocks are required to include a valid coinbase transaction, which pays the miners according to their shares (i.e., the previously found blocks in the share chain), a successful miner cannot claim the reward for herself alone. P2Pool has some weaknesses, though, such as additional complexity and significant resource consumption, which might be the reason why it is not as popular as its centralized counterparts.

The authors of [99] tackle the issue of large mining pools by proposing a non-outsourceable proof of work, which provides a *disincentive* to join mining pools, i.e., distributing work to untrusted servers implies the risk of losing the mining reward. It turns out that [99] formalizes and extends the security notion used in Permacoin [100]. The approach aims at eliminating mining pools, and thus all mentioned (and the following) related issues. More discussion on that topic can be found in [97].

Miners (and mining pools) compete with each other: their chance of winning is proportional to their computational power. However, rogue miners can achieve an unfairly high share by attacking the mining process. The typical intent behind these attacks is to weaken competitors with the aim to gain higher revenue. For that reason, mining pools are the second-most popular target of distributed denial of service attacks in the Bitcoin ecosystem [94]. The trade-off between attacking or investing to gain an advantage can be expressed by rational game-theoretic models [101], [102].

But miners can also exploit the mining process itself to gain an advantage: instead of directly announcing mined blocks, miners keep their discovery private and establish a private chain. If the public chain approaches the length of the private chain, the rogue miner broadcasts his chain to catch up. This way miners intentionally force a block chain fork and initiate a block race. The key idea is to let honest miners waste their power by mining on the public chain, so as to increase the own chances of winning on subsequent blocks. The strategy is widely known as *selfish mining* [61]. More generally, the attack vector is called *block withholding* [91] or *block discarding* [103]. It can also be used for various other attacks, which infiltrate and sabotage competing mining pools [90], [104]. Please note that selfish mining can be considered a global attack as it increases transaction approval time and facilitates double spending, whereas the latter (as well as the previously mentioned Finney attack) is a targeted attack. Nevertheless, they all use the block withholding, but details vary—such as the way blocks are withheld, under what conditions they are released, and for what purpose.

In [61], the authors formally analyzed the incentives for selfish mining and showed that selfish miners obtain a revenue larger than their relative share. The success and profitability heavily depends on the selfish miner's share q of hash rate and the fraction of honest miners that choose to mine on the private chain after broadcasting. The latter is denoted by γ and often depends on network properties (i.e., who hears which block first). In particular, [61] made the observation that selfish mining is profitable if

$$\frac{1-\gamma}{3-2\gamma} < q < \frac{1}{2} \quad . \tag{2}$$

Since selfish (or adversarial) miners who control more than half of the hash rate asymptotically always win the race and are able to catch up with public chains, we are interested in the case $q < 0.5$ only. For $\gamma \approx 1$, which implies that (almost) all honest miners favor the private over the public chain, selfish mining is profitable for virtually all shares q. In the other extreme case of $\gamma \approx 0$, where (almost) all honest miners disregard the private chain, the profitability threshold of selfish mining equals a share of at least $1/3$. That is, miners with more than one third of the computational power can increase their revenue by following the selfish mining strategy. Note that, depending on γ, the threshold ranges between 0 and $1/3$ and thus is substantially lower than the usually considered critical hashing power of $q > 0.5$. Solo miners are unlikely to deliver such a performance nowadays, but mining pools are very well able to do so. The lower bound given by the left-hand side of (2) can be considered a security metric: the higher this security threshold, the higher the fraction of the total computational power that is necessary to exploit selfish mining.

The true current value of γ (and thus of the security threshold) is unknown. However, as [105] show, the value of γ quickly increases with variability of the propagation delay. By mounting eclipse attacks, i.e., isolating parts of the network, an adversary is likely able to push γ closer to one and thus to lower the security threshold significantly. Therefore, [61] propose to relay all blocks that are received within a certain timespan and to select the fork to mine on randomly. As a result, half of the honest miners will choose the private block, which fixes γ at 0.5. This yields a security threshold of 0.25. [106] raises the threshold to 0.32 which renders selfish mining ineffective. Their mitigation is called *freshness preferred*; it suggests to choose the most recent block (according to its timestamp). The DECOR+ protocol [107] aims at eliminating the incentive for selfish mining completely. Yet, freshness preferred, for example, assumes unforgeable and accurate timestamps, which is not easy to achieve [64], [65].

Bitcoin peers maintain a network time, which is the median of time samples from their neighbors. It is secured from arbitrary manipulation by allowing at most a deviation of 70 minutes from the system time. For the sake of triple modular redundancy ("never go to sea with two chronometers; take one or three"), the user is asked to double check the time. Nevertheless, an adversary is able to slow down or to speed up nodes within a tolerance range of 70 minutes. This attack is known as *timejacking* [64]. An advanced attacker can use timejacking to isolate a miner. By speeding up the majority of clocks while slowing down the target's clock, the attacker can achieve a difference of 140 minutes. Since the network time is used to validate blocks, the attacker can generate a "poison pill" block with a custom timestamp, which is accepted by the majority but rejected by the target. As a result, the target sticks to the previous chain and continues mining on this part, whereas the majority of the network has moved on. All newly generated blocks are immediately rejected by the target. Timejacking can be considered a form of denial of service attack, but it also facilitates double spending. Furthermore, it can be used to influence the mining difficulty calculation [65]. The proposed solutions include to tighten the tolerance ranges, to use NTP [108], or to use trusted peers for time sampling only [64].

As we will see next, most of the attacks discussed in this section are possible because of Bitcoin's network structure. In particular, we will see that significant propagation delays and scalability issues of the network are often the root causes.

IV. Network

In this section, we will take a closer look at how Bitcoin organizes the distributed network of peers. In particular, we will consider the Bitcoin protocol, the resulting relay patterns and their implications on information propagation. Furthermore, we provide an outlook on Bitcoin-inspired network applications and services, such as alternative domain name and messaging systems.

Bitcoin uses an unstructured peer-to-peer network based on persistent TCP connections as its foundational communication structure. In general, unstructured overlays are easily constructed and robust against high churn (change-and-turn) rates, i.e., against frequently joining and leaving peers. From existing research, it is known that unstructured overlays like, for instance, Gnutella [109] do not scale well [110], [111]. Searching for files in unstructured file sharing overlays, for instance, requires flooding requests in the network, so that each peer receiving and forwarding a query can check against the locally known data items. This causes significant overhead due to the massive number of copies of each query, and because of the need to maintain state information about seen messages for duplicate suppression. The load on each peer grows linearly with the system size. In order to reduce the amount of relaying, the scope of queries is often limited to a certain number of hops in peer-to-peer file sharing systems—at the cost of imperfect coverage: not every query reaches every peer.

The Bitcoin network has aims which differ from those of peer-to-peer file sharing systems. In Bitcoin, the aim is not to find specific files or data items, but to distribute information as fast as possible to reach consensus on the block chain. Limiting the scope of message propagation is therefore not an option. Clearly, this raises concerns regarding Bitcoin's ability to scale to higher transaction rates while still processing transactions rapidly.

A. Experimenting With the Bitcoin Network/Protocol

Studying the Bitcoin network and the interplay of nodes poses a challenge. By now, there are a few possibilities to approach to this task. One way is to connect to the mainnet, i.e., the live Bitcoin network, or the testnet [25]. The testnet is a global playground to experiment with the Bitcoin protocol and its scripting capabilities. It uses a separate, distinct block chain, and so-called *faucets* provide coins for free. Apart from a few minor parameter alterations, e.g., for faster block generation, the testnet mimics the mainnet and runs the same code as Bitcoin peers. Both approaches can be used to interact with or observe, usually with a highly connected passive peer, the network.

In contrast, local testing environments provide more control. Built into the Bitcoin reference software is a regression test mode (regtest). It can generate blocks on demand and create "private" coins with no real-world value. By doing this, it provides a safe harbor for testing new features. A similar approach is the bitcoin-testnet-box (github.com/freewil/bitcoin-testnet-box). Both have been designed for situations where interaction with random peers and blocks is not desired.

Simulation environments such as simbit [112] and Shadow [113] aim at simulating large-scale Bitcoin networks, while keeping full control over all components. Both are event discrete simulators. Simbit implements the functions of a Bitcoin reference client and miner in a simplified way. The Bitcoin plug-in for Shadow directly executes the Bitcoin software inside the simulation framework. However, [114] argues that executing the expensive block chain interactions and cryptographic operations inhibits the scalability of experiments. Therefore, they base their simulation environment on handpicked parts of the Bitcoin client only to benefit from both scalability through abstraction as well as from high accuracy by realistic client behavior.

In the remainder of this section, we will see some of the presented approaches in action. Apart from valuable insights, this should provide an overview of the available methodology to analyze the Bitcoin network.

B. Joining and Maintaining the Network

Every peer in the Bitcoin network aims to maintain a minimum of eight connections in the overlay. That is, the peer actively tries to establish additional connections if this number is underrun. The number of eight connections can be significantly exceeded if incoming connections are accepted by a Bitcoin peer; usually a network participant does not handle more than 125 connections at a time (`maxconnections`). By default, peers listen on port 8333 for inbound connections. When peers establish a new connection, they perform an application layer handshake, consisting of `version` and `verack`

messages. The messages include a timestamp for time synchronization, IP addresses, and the protocol version. Since Bitcoin version 0.7, IPv6 is supported.

In order to detect when peers have left, Bitcoin uses a soft-state approach. If 30 minutes have been passed since messages were last exchanged between neighbors, peers will transmit a heartbeat message to keep the connection alive. If 90 minutes have passed without any incoming message, the client will assume that its counterpart is offline. Bitcoin peers also keep track of not directly connected peers in the network. They maintain a list of recently active peers, including their IP address and a timestamp. Every peer broadcasts its own IP address in an `addr` message every 24 hours through the overlay. The absence of the message from a certain peer is interpreted as a sign that the respective peer is now offline. Exchanging `addr` messages (during bootstrapping and later on) is the common way to explore the network.

Besides unsolicited reception of `addr` messages, peers can ask neighbors for additional peers by sending a `getaddr` message. The response (`addr`) contains a random selection of 23% (but not more than 1,000) peers from the responder's list of recently active peers. (It seems that there are no particular reasons for the choice of these numbers.) Note that this list does not only include peers directly connected to the originator of the list, but also peers it heard of recently. Thus, retrieving `addr` messages does not reveal the structure of the network without additional effort. In fact, it is a design goal of the Bitcoin network implementation to obfuscate the topology and to make sure that (local) attackers cannot fill up a peer's neighbor table with compromised IP addresses. Otherwise it would facilitate eclipse attacks, where an attacker monopolizes or at least dominates the environment of a node, therefore controlling the message flow between this node and the remainder of the network. In the context of Bitcoin, this is also often called a *netsplit*. An attacker can exploit this to generate an independent, inconsistent view of the network (and the block chain) at the attacked node. This enables double spends with more than one confirmation. The authors of [66] demonstrate the feasibility of eclipse attacks on the Bitcoin network and discuss the countermeasures. Nevertheless, since peers get regular updates and maintain all received participant information, every peer has a relatively broad view of the peers in the network.

Whenever receiving an `addr` message, peers consider relaying address information for messages with a maximum of ten addresses only. If the timestamp associated with the information about a peer is not older than 10 minutes, the peer decides to relay the respective address. Depending on the reachability of a peer, i.e., whether the advertised IP lies within a reachable network, the address is forwarded to either two neighbors or one. This promotes peers with public IP addresses more than peers with private addresses, based on the conjecture that peers with public IPs are more likely to accept incoming connections. The decision which neighbors will receive the address information is determined by deterministic randomness, that is, based on pseudorandom decisions using a fixed seed. Peers maintain state of already advertised IP addresses to avoid repeated advertisements. The seed changes every 24 hours. Addresses designated for the same neighbor are collected in a new `addr` message and relayed in a batch. About every 100 ms, a neighbor is randomly selected (the so-called "trickle node") and the queued addresses are flushed. This mechanism induces an additional random delay per hop during address propagation.

Bitcoin peers use three methods of finding neighbors during bootstrapping: DNS, IRC, and asking neighbors. Since Bitcoin version 0.6, DNS is the default bootstrapping mechanism. The software is shipped with built-in hostnames of seed nodes, the IP addresses of which are resolved via DNS. The DNS servers are run by volunteers and return a set of recently active peers. The usage of IRC, where IP addresses are encoded in the nicknames, is replaced by DNS bootstrapping. Besides, the client asks its neighbors for a list of available peers as introduced above.

In a study from November 2013 to January 2014, the authors of [115] asked a set of initial peers for information about other peers they know, by sending a `getaddr` to these peers. For every previously unknown peer thus discovered, they repeated the procedure and asked them for peers, too. In the first round they already discovered 111,475 IP addresses. After 37 rounds during the 37 days of the study, they discovered 872,648 distinct IP addresses in total. Geolocation lookups revealed that they are spread all over the world. Most of these peers are located in the US (22%) and China (14%). However, considering the number of Internet users in the respective countries, the Netherlands and Norway show the highest adoption rates. The discovered peers in each round show a significant overlap. However, most of them were gone after five days and only 5,769 were online throughout the whole period. Note that some of the peers have dynamic IP addresses and therefore may appear to be more unstable than they really are. In [116] respective statistics on AS level are provided. The online service Bitnodes (getaddr.bitnodes.io) estimates the size of the Bitcoin network and maps the global distribution of reachable nodes on a regular basis.

All reveal the dimension of the Bitcoin network, but do not provide information about the topology. In [117] a technique called AddressProbe, that discovers peer links, is developed. By issuing `getaddr` to a preferably large set of peers, they take a snapshot of the network and infer from the included timestamps how nodes learned from each other to map connected peers. It highly depends on implementation details of the Bitcoin client, i.e., how timestamps for known peers are updated. The results confirm that the majority of peers have a node degree of 8–12, which resembles the default parameters. However, a significant number of peers exceed the maximum number of 125 connections by a factor of up to 80 and are persistent over time. These extremely high-degree nodes include other benign measurement studies, mining pools, and wallet services. Investigating the resulting connection graph indicates that the Bitcoin network is not purely random. In particular community structures are visible, which suggests that Bitcoin's join procedure has an influence on the topology.

C. Transaction and Block Propagation

Based on the unstructured overlay as discussed so far, information about new transactions and blocks is spread to the

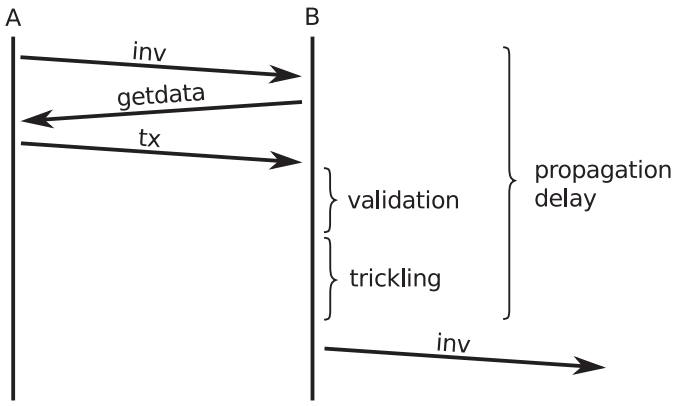


Fig. 7. Transaction propagation.

peers in order to form the distributed consensus. The mechanism is simple: messages are flooded through the network. Let us revisit our example where Alice wants to issue a transaction. Where we focused on the semantics and the transaction and block chain structure before, we now take a closer look at the exchanged messages. The message flow is illustrated in Figure 7. Assume Alice constructed a valid transaction. Before broadcasting the actual transaction data including all details of inputs and outputs, she sends an inventory (`inv`) message stating "I know about new transactions" to all of her neighbors. This message contains a list of transaction hashes (TXIDs), but not the actual transaction data.

Alice's neighbors will request data from specific transactions in a separate `getdata` message, if these transactions are so far unknown to them. This pull-based communication mechanism reduces the load on the network by avoiding unnecessary, redundant transmissions of transaction records. In response to a `getdata` message, Alice sends the respective transaction record. After Alice's neighbors verified the transaction, they will make it available to all their neighbors in the same manner as Alice did, starting with an `inv` message.

Messages, in general, are flushed periodically about every 100 ms. However, transaction relaying takes place by "trickling" messages out. Bitcoin randomly selects with a probability of 1/4 the transactions for an `inv` message and stalls the remaining transactions. Every neighbor gets a different set of randomly chosen transactions, each about 1/4 of the currently available set. Only the randomly selected "trickling node" (cf. `addr` message relaying) gets all transactions immediately. The other neighbors either get it later or already got it from another neighbor. Trickling reduces the overhead and at the same time makes traffic analysis more difficult, in a similar manner as mixes do in mix networks [1]. It also helps to conceal the originator of a transaction. However, since every 100 ms a random batch is flushed, an additional delay in the order of some hundreds of milliseconds is induced to the propagation of transactions. Therefore, trickling in Bitcoin is, in fact, counterproductive to the aim of propagating information as fast as possible. It trades off overhead and privacy against fast transaction propagation.

Peers keep track of the transactions that they have already seen, but "forget" them after a while if they do not make it into the block chain. Alice, as the originator of her transaction, is responsible for its distribution. She might hence need to re-broadcast it if the transaction did not get into the block chain, to make sure it gets considered in the next block.

By observing the forwarded messages from a highly connected peer, [118] revealed three distinct relay patterns. With about 91% of all observed instances, the most common relay pattern involves lots of peers relaying a transaction only once. Since clients keep track of seen transactions and relay only new ones, this is exactly what one would expect. The second relay pattern involves a transaction received once or multiple times from a single peer. This is not very common (3%); it occurs when invalid transactions are broadcast and hence not relayed. The third relay pattern involves a transaction relayed by multiple peers and re-relayed by at least one of them (6%). The reason behind the occurrence of this pattern is that transaction originators are responsible for their transactions and might need to re-broadcast if they get forgotten.

The insights into transaction propagation also help to increase the resilience against fraudulent users paying with Bitcoin. For example, assume Alice wants to buy a snack and pay with Bitcoin. Further assume that Alice is very hungry and wants the snack asap, without waiting for the commonly expected six confirmations (about one hour). On the other hand, the merchant wants to make sure that it is safe to hand over the product without fearing the risk of double spending (we discussed the risk of double spending in such fast payment scenarios before, see also [88]). With this storyline in mind, the authors of [119] developed propagation strategies for merchants to realize fast payments. From the merchant's perspective, the key observation is that Alice should not be the only source of information for this transaction. Quite in contrast: the merchant should not accept incoming connections and connect to a preferably large sample of peers. Thus, Alice is likely not able to send transactions directly to the merchant and therefore forced to broadcast the transaction. In addition, the merchant should not relay transactions. As long as he is connected to at least one honest peer, he will receive potentially fraudulent transactions and is able to recognize the double spending.

Another (not implemented) proposal is to use Bitcoin's `alert` messages, which are aggressively flooded, to signal a double spending attempt [88]. The intuition is that even when the attacker is able to fool the merchant, some (honest) peers will see the colliding transactions. They can then broadcast alerts immediately. Thus, by considering these strategies and waiting for a small listening period, the merchant makes sure that the majority of the Bitcoin network has received the transaction. Additionally he probably received Alice's transaction more than once from his neighbors. If there is no attempt to double spend, the risk of fraud has been reduced. Nevertheless, a cost-benefit trade-off remains.

The propagation of validated blocks is analogous to the propagation of transactions. A miner who has successfully solved the proof-of-work broadcasts an inventory message to all neighbors first. The full block is transferred upon request only. Peers receiving a new (unseen) block will relay it in the same manner. The period from receiving an inventory message for a new

block until forwarding the announcement to all other neighbors induces a propagation delay, which consists of the time it takes to announce, request, transmit and validate the block (or transaction). In case of blocks, the validation includes the validation of each transaction and hence access to the block chain. In order to reduce the propagation delay, trickling is not used for blocks. However, an adversary can exploit Bitcoin's static download timeouts to delay transaction and block propagation [71]. That is, a Bitcoin peer accepts 2 minutes download time for a transaction and 20 minutes for a block, before a timeout fires. Since peers request a data object only from a single peer, typically the first peer from which a new announcment has been received, an adversary can stall propagation by (i) being the first one to announce new transactions or blocks to its peers but (ii) not answering their requests. In order to satisfy (i), the adversary can for example relay announcments immediately without actually verifying the data. As shown in [71], the propagation time can even be further extended under reasonable circumstances.

The induced propagation delay has implications on the Bitcoin protocol. In [67], the authors analyzed the information propagation in the Bitcoin network. They connected to a large sample of nodes in the network as observer, i.e., without actively relaying messages. They registered the arrival times of block hashes in `inv` messages from these nodes. The probability density function of times since the first block was received shows an exponential distribution, with a median of about of 6.5 seconds and a mean of 12.6 seconds. The distribution shows a long-tail behavior with 5% of the nodes still not having received the block after 40 seconds. The authors also discuss the relationship between the propagation delay and the probability of block chain forks. Obviously, due to the significant propagation delay, forks in the block chain become more likely. Thus, they conclude that if the amount of transactions and/or the network size increases, propagation delays will grow and, consequently, the rate of block chain forks will increase, too. This has an important impact on the resilience of Bitcoin against malicious nodes [120]. In order to mitigate the threat, a modified message exchange behavior has been proposed [67]. It aims to reduce the propagation delay by pipelining the block propagation, and by splitting the validation into checking for a valid nonce first and validating all transactions later on. However, this introduces new attack vectors, allowing adversaries (or everybody else) to flood `inv` messages through the whole network without providing a valid block or transaction.

In summary, the key determinant for information propagation in the Bitcoin network is the unstructured overlay network and its characteristics. As the network grows, its diameter will increase respectively. The authors of [67] showed the impact in a rather extreme experiment by deploying a highly connected peer (approximately 3,500 neighbors) that acts as relaying hub in the live Bitcoin network. Their client actively tried to connect to every peer from the address list, reducing the distance between any two nodes to, ideally, two hops only. As a consequence, the block chain fork rate dropped from 1.69% to 0.78%—but at the cost of bandwidth requirements peaking at around 100 MB/s. This reveals a pressing issue of the Bitcoin network today: its scalability.

D. Scalability

The main objective of the peer-to-peer network in Bitcoin is to quickly distribute the information into every part of the network. Variations in the propagation mechanisms directly affect the formation of the distributed consensus and thus the security of Bitcoin. In general, inconsistent states, i.e., block chain forks, are undesirable, because they facilitate double spending. However, the Bitcoin network is faced with scalability issues. Especially network bandwidth, network size and storage requirements pose challenges.

Bitcoin's wiki states that the protocol is capable of much more than the current transaction rate [26, pp. Scalability] and is thus able to scale to higher demands. Currently, Bitcoin has an artificial maximum block size of 1 MiB, which limits the number of transactions per block and therefore also the growth rate of the block chain. This limit is enforced to prevent from inflating the block chain before the Bitcoin protocol is capable of handling more transactions. Consider for example a single-input, single-output "pay-to-PubKey" (P2PK) transaction, which has a size of 166 bytes and is thus one of the smallest standard transactions. A back-of-the-envelope calculation results in a theoretical upper bound of approximately 10 transactions per second (tps). A more conservative and realistic assumption would be to consider P2PKH transactions with at least two inputs (to merge previous outputs) and two outputs (one for change). Accordingly, Bitcoin is capable of a transaction rate of approximately 4 tps. Alternatively, the block generation interval could be shortened, which implies that the proof-of-work difficulty would have to be adjusted accordingly. As discussed before, though, close-to-simultaneous block validations by different miners lead to block chain forks. Therefore, shorter block creation intervals come at the price of a higher chance of block chain forks.

Either way, scaling to higher transaction rates will eventually consume more resources. For example, to handle a rate of 2,000 tps, a block size of more than half a gigabyte and an Internet connection of approximately 1 MiB/s is required. As stated in [121], a higher transaction rate (which is inevitable if Bitcoin really poses an alternative to the banking model) will eventually demand a super peer-based overlay structure (as in later versions of Gnutella [122]) in order to handle the load. We can observe some evidence of this trend—and the emergence of super peers in the Bitcoin network. For instance, the study of [115] found that from 1,300 connected peers, 20 forwarded more than 70% of both transactions and blocks first. Therefore, [123] suggests to explicitly introduce a hierarchical network structure, which consists of super peers (i.e., miners), full nodes (e.g., exchanges) and wallet nodes (e.g., online wallets or thin clients).

Full nodes (or *full chain clients*) download and verify all blocks starting from the genesis block. This is the most secure mode of operation. Even though not strictly necessary for a client, full nodes participate in the P2P network and help to propagate information. Alternatively, *thin clients* which use the *simplified payment verification (SPV)* [16] can be used. A thin client needs the block headers only and requests transactions on demand. As illustrated in Figure 8, the block header

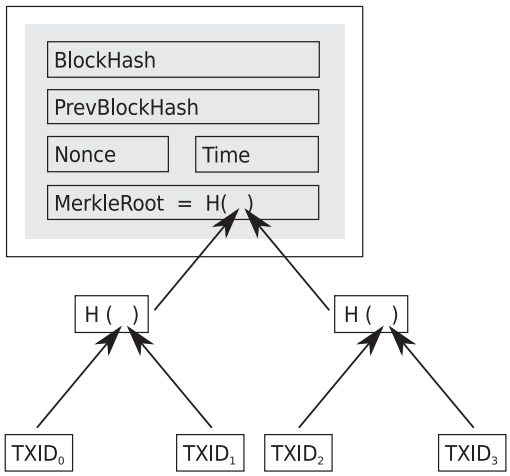


Fig. 8. Merkle tree.

incorporates a Merkle root [18], which secures the transactions of that particular block by constructing a hash tree over the TXIDs: transaction hashes are paired and hashed. Hashes without a partner are hashed by themselves. This is hierarchically repeated until a single hash remains, the Merkle root. It allows clients to verify that a transaction is part of a block by starting at the respective leaf and traversing the branches up to the root. If the final hash equals the Merkle root, the transactions must be part of the block. For the verification, thin clients request a list of (some) intermediary hashes from full nodes, but they do not need the complete block with all transaction data. Since the block headers including the Merkle root are secured, valid intermediate hashes cannot be faked easily. Thus, the approach can reliably verify the existence of transactions. Their absence, however, can be faked by answering with invalid hashes.

Clients can reduce the risk by sampling from multiple nodes. Yet, eclipse attacks are of course possible. In addition to security issues, requesting specific transactions from full nodes has important privacy implications: from the requested transaction, a full node might infer the owner of the coins. To limit the information leak, Bitcoin employs a Bloom filter [124] (a probabilistic data structure) to obfuscate requests [125]. Clients express their request as a Bloom filter and send it to the full node. All transactions which match the pattern given by the Bloom filter are sent to the thin client. The inherent false positive rate of Bloom filters is used to adjust the desired level of privacy at the expense of some additional overhead.

Thin clients mitigate some of Bitcoin's scalability issues by relying on the data provisioned by full nodes. A consequent step in this direction would be to separately store the raw transaction data, and to include transaction hashes in blocks only. Indeed some altcoins such as Dogecoin (DOGE, dogecoin.com) follow this approach. The approach still requires the distinction between thin clients and full nodes. In particular, full nodes still need to store all data. Even though thin clients employ techniques to limit the necessary trust in others, they subvert Bitcoin's core intent of rigorous decentralization. In a sense, the resulting structure resembles the banking model [121].

The authors of [126] intentionally break with Bitcoin's design philosophy and propose a system that makes cryptocurrencies more palatable to traditional banks and governments. The approach, namely RSCoin, envisages a central bank which primarily controls the money supply, but relies on a distributed set of so-called mintettes to verify transactions and prevent double spending. By doing this, they eliminate the wasteful proof of work and yield a scalable distributed ledger-based system. While this approach promotes centralization, let us turn towards other approaches which tackle the root cause of Bitcoin's scalability issues.

A fundamental bottleneck is the sheer size of the block chain. Since Bitcoin version 0.8, transactions and block indices are stored with LevelDB instead of the previously used Berkeley DB. This improvement increased the performance of synchronization and block verification, which used to be a bottleneck before. Nevertheless, the storage issues remain.

Therefore, the author of [127] disassembles the block chain and isolates three key components. First, the block chain manages ownership records and thus implicit account balances. Second, it helps the network coordinating transactions. Third, the linked blocks and the proof of work secure the ledger. For each function, he suggests a data structure which takes the responsibility of the respective function, with the overall aim of substituting and slimming down the block chain. The account balances are tracked in a so-called account tree. It combines a binary radix tree and Merkle hashing with UTXOs as leafs. The roots of the radix tree and the Merkle tree become part of the block header. This ensures integrity of the ownerships and supports quick address lookups. In order to periodically group transactions and update the ledger, a component analogous to the block chain is necessary. However, due to the account tree it becomes possible to discard old blocks. Thus, the proposed solution is to keep a few hundreds of blocks in a so-called mini block chain only. Therefore, inputs and outputs of transactions do not point to other transactions anymore. Instead, they point to addresses in the account tree and are thus implicitly linked. Simply discarding old blocks weakens the security, though. The solution is similar to the thin clients' strategy: a proof chain with block headers only. All three data structures together use less space but provide the same functionality. The design is not meant to substitute the live Bitcoin system: migrating the complete block chain seems impossible. An alternative currency, named Cryptonite (XCN, cryptonite.info), employs the proposed mini block chain scheme.

Even if we assume Bitcoin to be able to adapt to higher loads, there are additional limitations on the transaction rates [68]. Especially delayed block propagation and Bitcoin's security assumptions restrict transaction rates more than the limits imposed by, for example, bandwidth requirements. A fact noted in [67] and [68] is that attempting to increase either the block creation time or the block size not only increases the bandwidth requirements, but also adversely affects the protocol. If the block that has been verified is not propagated rapidly, the probability of a fork increases. Bitcoin may be able to resolve forks, but frequent conflicts still waste valuable resources. Obviously, larger blocks imply longer propagation times and thus increase the risk of forks. [68] used the data set of [67] and revealed a linear dependency between the block size and the propagation delays in the Bitcoin network. By extrapolating from the data

set, they found that it takes 0.066 s per KiB to reach half of the nodes in the network.

Higher block generation rates will likewise result in more frequent conflicting blocks. The authors of [68] provide estimates of transaction rates as a function of the block size and the block propagation delay with regard to delays and security guarantees. Bitcoin's security heavily depends on the assumption that the time it takes to propagate blocks is significantly shorter than the block generation time. Thus, with an increasing transaction rate it becomes more and more likely that attacks are possible for an attacker controlling less than 50% of the overall hash rate. In an (optimistic) estimate, [68] assumed an unlimited block size, a transaction size of 0.5 KiB, and an adversary controlling 40% of the network's hash rate. Furthermore, they used the propagation delay factor of 0.066 s per KiB from above. The resulting upper bound on the transaction rate is approximately 40 tps.

As an optimization, [68] suggest to alter the mechanism to resolve block chain forks. The basic observation is that orphaned blocks are still valid blocks, i.e., solve the crypto puzzle, which can contribute to the block chain's irreversibility. Therefore, also the computational effort that was necessary to mine blocks that became orphaned should make a fork "heavier". That is, instead of the "longest" block chain, the fork with the "heaviest" subtree should be taken as a metric to resolve conflicts. It exploits the work that was already invested and enhances the security of their ancestor. It is thus possible to increase the transaction rate under the same security constraints.

Alternatively, [42] propose a new payment protocol that reduces the number of transactions committed to the block chain and hence also reduces the load. They use micropayment channels [26, pp. Contracts] as a building block to create a duplex micropayment channel (DMC) protocol. Micropayment channels are established as a shared account between two parties with a credit limit that can be transferred in total and a time limit that specifies the lifetime. The setup consists of two transactions, a 2-of-2 multi-signature transaction and a time-locked refund, whereof only the multi-signature transaction is broadcast. The sender can incrementally replace the time-locked refund by a new version, which refunds a smaller fraction and sends the remaining amount to the receiver. Either when the deadline approaches or the limit is exhausted, the most recent refund is broadcast and becomes valid. As a result the block chain is typically only involved during the setup and closure phase of the channel. The authors of [42] extend the simple micropayment channels and introduce the concept of invalidation trees, which enables the possibility to reset the channel. Duplex payments are thus able to cancel each other out by resetting the channel accordingly. The authors envisage long-lived point-to-point payment channels between payment service providers, which route transfers between users, possibly over multiple hops. However, one has to be aware that this may raise privacy concerns.

We can conclude that the general scalability issues of unstructured overlays combined with the issues induced by the Bitcoin protocol itself remain. Some practical, pragmatic solutions appear able to keep Bitcoin in a working state for the foreseeable future. However, many of the results suggest that scalability remains an open problem. A summary of the most prevalent issues is provided by [128]. The considerations also raise the question whether Bitcoin is (and can remain) a decentralized currency [69], [70], [129].

E. Deanonymization

Tracking message flows does not only help to understand the network, it also discloses user information. As noted in [121], by controlling a hub connected to all peers, it is possible to learn the IP address of any transaction originator: assuming that the transaction is not forwarded by an online wallet provider, the originator is likely also the issuer of the transaction. This breaks the pseudonymity of transactions. The relay patterns identified in [118] confirm the expected behavior. Inspired by [121], the authors used their insights and developed heuristics to match transactions to IP addresses, even if the observing hub is not fully connected. During their study of five months, they were able to link 1,162 Bitcoin addresses to IP addresses while being connected to a median of 2,678 peers.

Internet anonymity services like Tor [130] provide a solution to this privacy issue by concealing the originating IP. Tor decouples sender and receiver information by employing the onion routing protocol [131] along a circuit of relay nodes. The IP address of the source node is thereby hidden, the destination of the connection sees only the address of the last Tor node along the circuit (the *exit node*). Therefore, the Bitcoin client is able to tunnel the traffic through Tor via the SOCKS interface.

However, [72] point out that it is possible for an attacker to trigger a ban of Tor connections to the Bitcoin network. They exploit Bitcoin's denial-of-service protection, which blacklists misbehaving nodes under certain circumstances. Whenever a Bitcoin peer receives malformed messages, it increases a penalty score for the respective IP address. If the score passes a threshold, the IP is banned from connecting to this Bitcoin peer for 24 hours. One possibility for a simple, small message which is malformed in the sense of this mechanism is to send blocks with an empty transaction list. An attacker could use a Tor circuit for each pair of Tor exit node and Bitcoin peer, and mount a straightforward denial-of-service attack by getting the Bitcoin peers to blacklist all Tor exit IP addresses. In a similar way, other proxy services can be banned from the Bitcoin network. Such an attack involves many connections and large amounts of traffic, but nevertheless seems feasible. Bitcoin over Tor in general and mounting the mentioned denial-of-service attack in particular introduces additional attack vectors, such as eclipse attacks by banning Tor from benign Bitcoin peers only or man-in-the-middle attacks by blacklisting benign exit nodes from Bitcoin peers [132].

But even when using anonymized connections, it is possible to map the originator of transactions. The observation that a peer's set of neighbors can serve as a fingerprint was made in [72]. Recall that clients usually connect to eight peers and advertise their addresses in the network by broadcasting it to all neighbors. The authors call the eight peers (which apparently accept incoming connections) the client's *entry nodes*. Clients maintain connections to entry nodes as long as they

remain reachable. Thus, it can be assumed that the fingerprint is stable. If an adversary is already connected to the network, he will receive the address announcement, too. An adversary can exploit this fact and create a fingerprint for an IP address by connecting (ideally) to all Bitcoin servers and logging the set of peers that forward the IP address. These peers are likely the entry nodes for the respective IP. However, due to the "trickling" of `addr` messages, an adversary will see a fraction of the entry nodes only. This and timing effects can result in false positives. In the next step, the attacker is able to map transactions to entry nodes and thus also to the originator of the transaction. If the transaction is relayed by a subset of the entry nodes, it can be linked to the respective client. In detail, this is tricky because of network latency and trickling, but as the authors show in their experimental results, the attack still has a significant success rate (about 11% of all transaction could be disclosed).

The proposed mitigation strategy from [72] suggests to rotate outbound connections, for instance after every transaction, so as to blur the fingerprint. This proposal started a discussion [133] that resembles many arguments also used in a very different context, namely the entry selection policy for the Tor anonymity network [134]–[136]. The arguments include that rotating entry nodes periodically will lead to a higher probability of selecting a malicious entry node. Sticking to a stable set of entry nodes reduces this risk. Eventually, as for Tor, it will be necessary to differentiate with respect to assumed adversary capabilities, to clearly state the attacker model, and to trade off the implications of any defense.

F. Botnets

Botnets are a distributed formation of processes connected to a network. Illegal botnets run on systems without the knowledge of their operator. They have access to local files, network resources, and are able to run arbitrary programs. In most cases they communicate with a botmaster over a so-called command and control (C&C) channel. The botmaster uses it to seed new instructions to and to collect information from the bots. There are several approaches, such as IRC, Tor, or distributed hash tables (DHT), to realize the C&C channel. It has been shown, that the block chain can be used as C&C infrastructure by encoding instructions in transaction scripts [137]. The approach benefits from Bitcoin's resilience.

Botnets are often used with the purpose of making money, including phishing and sending spam emails, but also distributed denial of service attacks. Thus, it was only a matter of time until botmasters would discover crypto currencies as an additional source of income. The authors of [138] perform a case study on an early adopter, the Miner Botnet (first activities date back to December 2010). Technically, the botnet is not state of the art, but at this early time it was distinguished by its mining capabilities. In particular, worker bots perform benchmarks on the compromised system and retrieve detailed information on graphic cards to initialize the mining software. The worker bots connect to proxy bots who collect the results of their work. The proxy bots run the standard Bitcoin client software and connect to a randomly selected mining pool from a hard-coded list. Every 20 minutes, proxy bots post their wallet holding the minted coins to the C&C server. The geographical distribution of the Miner botnet clusters around the countries Ukraine, Russia, Poland, Romania, and Belarus, which is likely due to the spreading strategy adopted by the botnet owner.

The authors of [139] termed the above mentioned approach *proxied pool mining*. By investigating several other botnets, they identified additional strategies, which they called *direct pool mining* and *dark pool mining*. As the name implies, with direct pool mining, botnets do not need a proxy and directly connect to a mining pool. The approach is very simple and does not require a separate proxy infrastructure, but it also has some disadvantages. Mining pools can easily detect botnet mining, because of the large number of miners with relatively smaller hash rates, all sharing the same account. Proxied pool mining can be detected, too, but masks the worker bots and has the flexibility to quickly switch to a new proxy if banned. With dark pool mining, the botnet hosts its own mining pool to which workers connect. The mining pool server consequentially connects to the Bitcoin network. The earnings for direct and proxied pool mining flow constantly due to the public mining pools. Dark pool mining will result in bursts of earnings. Throughout most of 2012 and the first quarter of 2013 it was absolutely profitable to run a mining botnet, even considering the prices charged (in dark corners of the Internet) for hiring a botnet [139]. In addition botnets can make use of techniques such as [140], [141] to accelerate mining with non-custom hardware, i.e., CPUs and GPUs.

Since botnet mining exploits mostly unused resources and hence does not interfere with most other typical botnet activities, it can be expected that mining remains profitable for large botnets. But why break into other people's systems if we can use free resources? The authors of [142] asked this question and used free cloud services to develop a cloud-based mining botnet. The main challenge was to automate the process, especially generating "credible" email addresses, to acquire a significant amount of bots, i.e., free accounts. In their tests, they were able to aggregate computing power worth thousands of dollars per week.

G. Bitcoin-Inspired Network Applications

Apart from revolutionizing the area of digital currencies, Bitcoin also inspired other applications, most notably many network applications. Examples include but are not limited to a decentralized domain name system [143], abuse prevention of cloud services [144], or anonymous and distributed messaging [145]. In the following, we will highlight two examples which build upon a fundamental insight into the role and properties of the block chain.

Since the early days of computer networks, naming services played an important role. Generally speaking, naming services map keys to values. DNS, which translates domain names to IP addresses, is probably the most well-known one.

Zooko Wilcox-O'Hearn conjectured [146] that when designing a naming service, one can choose only two out of the three properties "distributed", "secure", and "human-meaningful". Examples include OpenPGP public key fingerprints, which are secure and decentralized, but not human meaningful. Domain

names, in contrast, are meaningful and can be considered secure, but they are managed centrally. The conjecture that building a system incorporating all three properties is infeasible became known as Zooko's triangle.

Bitcoin breathed new life into the feasibility discussion. The late Aaron Swartz described a naming service based on Bitcoin's protocol [147], which defies Zooko's triangle. He leverages the decentralized block chain as a key-value storage. Instead of assigning coins to addresses, he proposes to translate meaningful names to addresses. In his design, the proof-of-work scheme secures the mapping stored in the block chain in the very same way in which Bitcoin secures the transactions. Roughly at the same time, a Bitcoin-based naming service was discussed in [148], and only a few months later Namecoin [143] was announced. The authors of [149] also provide additional background information on the development history.

Namecoin (NMC, namecoin.info) is an alternative approach to DNS, coordinating .bit domains. It shares the codebase with Bitcoin and inherits its properties. The mining process is therefore identical to Bitcoin, but starts with a fresh genesis block and consequently creates on its own block chain. For the most part, Namecoin extends the Bitcoin protocol to handle additional information (such as domain names) and introduces three new types of transactions: `name_new`, `name_firstupdate` and `name_update`. Assume Alice wants to register example.bit. First, she needs to broadcast a special pre-order transaction of type `name_new`. It consist of a sufficiently high network fee (currently 0.01 namecoins) as input and a `name_new` output script which includes the encrypted domain name. Please note: at this point the domain is not yet owned by Alice or anyone else. Thus, it is still possible to issue another `name_new` transaction with the same domain name, for example when losing the necessary key to successfully connect to the output script. After a mandatory waiting period of 12 blocks, Alice broadcasts the actual registration in a `name_firstupdate` transaction. It publicly announces the domain name in plaintext and assigns the ownership. Updates need to be performed every 36,000 blocks (approx. 250 days) at the latest by issuing a `name_update` transaction, otherwise the domain expires.

The initial pre-ordering prevents others from quickly registering the same domain name when seeing the registration. The 12 blocks waiting period provides time to broadcast the registration and to anchor it in the block chain. The network fee's purpose is to prevent from massive pre-ordering. Once used in a pre-order, the fee gets destroyed and cannot be used for normal payments anymore. Thus, domain names are, in a sense, attached to "special" coins, which can, however, still be exchanged and traded through updates. Indeed, updates are basically normal transactions referring to the previous update. They enable, for instance, IP address updates and domain transfers. In Namecoin, every user can become her own domain registrar. However, the system is not strictly limited to domains. For example CertCoin [150] proposes a authentication system based on Namecoin.

In principle, any type of data can be registered (also in Bitcoin), as long as it follows the protocol specification. So-called *Null Data transactions* (cf. Script 4) allow to encode small, arbitrary data into the block chain. Interestingly, [33] found values which do not appear to correspond to valid cryptographic key pairs; they seem to encode ASCII characters. On the downside, encoding arbitrary data into the block chain impels block chain inflation.

```
scriptPubKey: OP_RETURN <data>
```

Script 4. Null data transaction script template

Bitmessage [145] takes the idea and implements an anonymous, distributed, and encrypted messaging protocol. The protocol is quite different from Bitcoin (and Namecoin), though. First of all, there is no block chain, because it is not a design goal to store all messages forever. Instead, Bitmessage is considered a best-effort service, which asks peers to save messages for two days only. In order to be sure that messages are successfully received, an acknowledgment mechanism is implemented. If an acknowledgment is missing, the sender re-broadcasts the message with exponential backoff intervals. This way, Bitmessage addresses the problem of block chain inflation.

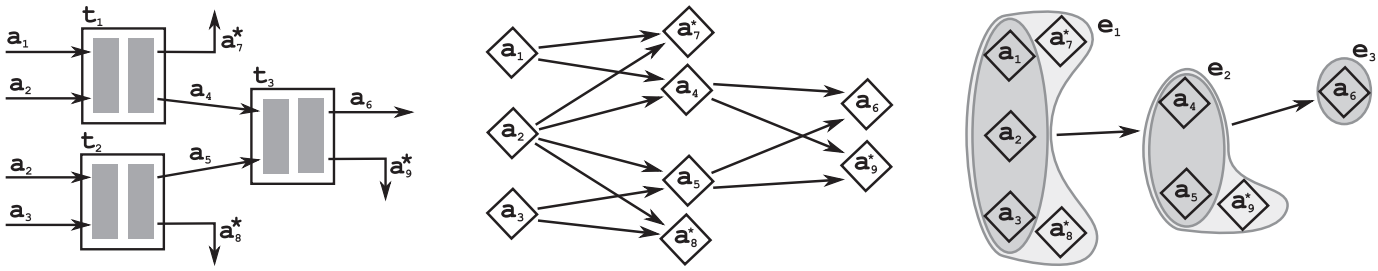
Before broadcasting a message, the sender needs to provide a valid proof of work with the message. This is very similar to Hashcash [3] and limits spam and DoS attacks. The difficulty is adjusted according to the message size. Like transactions and blocks, messages are flooded through an unstructured overlay network. This mixes all circulating messages of all users, making it difficult to link sender and receiver. In addition, messages are encrypted with the recipient's public key and have no visible addresses attached. Therefore, every peer needs to decrypt every received message to check if it is the intended recipient.

V. Privacy

The original Bitcoin paper briefly describes privacy considerations: in contrast to traditional banking—that is, trusted third party models which limit the accessible trading information—Bitcoin's block chain publicly reveals all transaction data. The public addresses in the block chain, though, intend to provide pseudonymity, so that this openness of the transaction history does not automatically imply identifiability. To support this feature, a new key pair (and thus a new address) should be used for each transaction. In this sense, Bitcoin clients use so-called *change addresses* (sometimes also called *shadow addresses*) by default, which are generated for each transaction and receive the change of the transaction on the output side.

However, as [16] already points out and as we know from privacy and social network research [151]–[153], even when hiding behind multiple pseudonyms, these can be linked and often reveal identifying information. Along these lines, there is a significant body of research on the analysis of Bitcoin's publicly available block chain [34], [73]–[75], [89], [154]–[157].

In the following, we will outline the methodology most block chain analysis approaches follow (Section V-A), before we then summarize interesting results obtained thereby (Section V-B). Subsequently, we describe current practices and research insights when it comes to increase Bitcoin's level of privacy (Section V-C).



(a) Transaction Graph (b) Address Graph (c) Entity Graph

Fig. 9. Block chain analysis.

A. Methodology of Block Chain Analyses

The reader might have noticed from previous sections that in Bitcoin there is no such thing like a "from" attribute in a transaction. A single, isolated transaction does not state an originator. Transactions refer to previous outputs only. By following this reference, we may infer something from their destination and consider it as originator of the referring transaction. Consider transaction t_3 from Figure 9a for example, which sends coins to address a_6 (assume a_9^* is the change address). From the destination address a_4 of transaction t_1 we may say that t_3 is "from" a_4. Thus, even though block explorers often display a "from" attribute as if it was encoded in the transaction they truly infer it from the "last sent-to" address. Since transactions can have numerous inputs and outputs (as it is the case for t_3), it is, strictly speaking, not even a single "last sent-to" address but rather it should be termed "all last sent-to" addresses. Therefore, in order to conduct an analysis of the block chain, pre-processing steps are necessary, including the construction of several graphs, namely transaction, address and entity graphs. Let us take a closer look at these steps (which are illustrated in Figure 9) and the possibilities to link Bitcoin users.

a) Transaction Graph: The most straightforward step is to construct a *transaction graph* $\mathcal{T}(T, L)$, where T is the set of transactions in the block chain and L is the set of directed assignments (i.e., transaction output-input relations) between these transactions. Each assignment $l \in L$ carries a number of coins C_l. Inherently, transactions have a total order defined by the block chain, so, as [73] noted, there cannot be any loops in $\mathcal{T}$.

b) Address Graph: From the assignments in the transaction graph, we can infer an origin-destination pair of Bitcoin addresses. This will be possible at least for most standard transactions such as P2PKH. Based on these relations, we can derive an *address graph* $\mathcal{A}(A, L')$, where A is the set of all Bitcoin addresses and L' is the set of directed assignments, but this time connecting addresses rather than transactions. Optionally, we can make $\mathcal{A}$ a multigraph and add a timestamp as an attribute to each $l \in L'$ so as to distinguish between multiple assignments between the same pair of addresses. Please note that some assignments will not yield an origin-destination pair. For example, coinbase blocks have no origin address (i.e., no input) and point to one destination address (i.e., one output) only.

c) Entity Graph: The next step aims at grouping addresses which *probably* belong to the same user. Based on a number of heuristics, which are either directly derived from the Bitcoin protocol or reflect common practices, a so-called *entity graph* can be constructed. The entity graph $\mathcal{E}(E, L'')$ consists of a set E of entities, where each $e \in E$ is a disjoint subset of addresses A. Like [34], we use the neutral term entity here to express the possibility of errors and the missing ground-truth knowledge about real ownerships.

The most widely accepted heuristic is to assume that all input addresses of a given transaction belong to the same entity. Based on this heuristic, we can cluster the transitive closure of this property over all transactions. If, for example, $a_1, a_2 \in A$ are the inputs of one transaction $t_1 \in T$ and $a_2, a_3 \in A$ of another transaction $t_2 \in T$, then we may conjecture that a_1, a_2, a_3 all belong to the same entity.

In [75], a second heuristic is introduced, which also clusters completely *new* addresses on the output side to the input entity, assuming that such an address is the change address. In particular, consider two output addresses $a_i^*, a_j \in A$ where a_i^* is an address which never before appeared in the block chain and will never be re-used to receive payments, and a_j is an address which was part of at least one previous transaction. In this case, a_i^* is assumed to be the change address and belongs to the same entity as the input addresses. The authors of [74] argue that due to mining pools or gambling sites, it is common to issue transactions to multiple different users with probably more than one new address. Hence they refined the heuristic, adding the condition that it should only be applied if there is only one *single* new address a_i^* in the transaction. Furthermore, they also excluded self-changes and coinbase transactions from the clustering.

In general, these and other heuristics take advantage of typical idioms of use and thus are prone to errors in case of unconventional Bitcoin applications. False positives in the clustering process can join addresses into huge entities which actually do not belong together. This has been observed in [74], leading the authors to further refinements. Mostly by manual inspection they identified usage patterns induced by services such as SatoshiDice. SatoshiDice sends payouts back to the same address. If a user spent coins from a change address, the address would receive another input which invalidates the one-time receive property of a change address. They used this observation to clean up their heuristic from false positives.

Independent from this particular case, idioms of use constantly change. For example, the community recommends not only to use a fresh address as the change address, but also a fresh receiving address. The rule of thumb is: use a fresh address whenever possible. However, there is also an approach with the opposite intention, i.e., enriching transactions with a so-called *marker address* (a. k. a. *green address*) to link the transaction to an entity [158]. This and related proposals [159] can be used to leverage from existing trust relationships so as to accept transactions quicker, for example. In addition, new techniques such as CoinJoin [160], where different users join in a single transaction, alter the usage patterns. Thus, heuristics must consider these changes, i.e., they must constantly be refined and adapted. Some heuristics might even hold true for a segment of the block chain only, while a certain usage pattern was common.

d) Ownership: Mapping addresses and thus entities to identities finally requires side channels. Some addresses, e.g., from WikiLeaks or Silk Road, are publicly known. Many services, like online stores or exchanges, expect the user to identify before using the service. Others can be detected by using web crawlers searching social networks (like, for instance, bitcointalk.org) for Bitcoin addresses (in the users' post signatures, for example) as it was done in [35], [73]. The software BitIodine [161] offers an automated analysis framework. Using similar means as described above, it parses the block chain, constructs the respective graphs, uses heuristics for clustering, and links addresses to users by adding side channel information.

Another approach is to match IP addresses. Publicly available data sets from Bitcoin faucets, which give out coins for free, are used in [73]. These services save and publish the IP address of the recipients to prevent abuse. A more rigorous way is to exploit the information that can be revealed by observing the network. In particular, as explained in Section IV, it is possible to correlate transaction originators to IP addresses. Based on the techniques presented in this section, transactions can be linked with the Bitcoin address and thus also with the IP address. If the linked Bitcoin address is part of an entity cluster, the whole cluster with all involved transactions is deanonymized.

B. Block Chain Analysis Results

Based on the methods described above, a number of interesting and useful insights on the use of Bitcoin and the flow of transactions can be gained. In this section we will give a brief summary.

In [73] and [35], transactions and entities of interest are identified and their relationships are illustrated. The PageRank algorithm [162] to find "important" entities is used in [35]: entities with more "references" (i.e., a higher number of incoming transactions) are ranked higher, as well as entities referenced by entities with a high rank. With this method, [35] identified the addresses of SatoshiDice and the FBI as particularly interesting. In contrast, [73] started from known addresses such as WikiLeaks and visualized their neighborhood. This way they (directly or indirectly) linked entities to their donations and revealed that donations were forwarded to other addresses.

The graphs allow to track coins along a sequence of transactions and to reveal patterns. Popular strategies to divert large amounts of coins (e.g., from thefts) are to create long chains of transactions with branches and (re-)collections [34], [73], [74]. Such a practice can be used to obscure coin flows. Noteworthy is a pattern termed *peeling chain* [74], which was observed in multiple studies: a single address starts with a large bitcoin amount. In a transaction, a small fraction is "peeled off" and transferred to a change address. This procedure is repeated, potentially hundreds of times. The peeled-off amounts often reside in *saving accounts* and often have never since been moved [34]. Sometimes, small amounts are aggregated to a large amount, forming the starting point for another peeling chain. Through careful analysis, it was possible to expose the meaningful recipient of the Bitcoin transactions. In a similar maneuver from a theft in 2011, the attempt to lay a false trail was revealed [73]. After the theft, coins were transferred to an address which is associated with the hacker group LulzSec. The thief most probably tried to draw the attention to somebody else; the analysis did not reveal evidence for any other relationship between LulzSec and the thief. More transaction patterns are described by [163]. More types of scams and their prevalence are investigated by [157].

Coins residing in saving accounts are often called *dormant coins* [34], [154]. They are moved only occasionally, if at all. One famous example is the wealth of Dread Pirate Roberts (DPR), the operator of Silk Road, the biggest online marketplace for drugs and much more (sometimes also "amazon.com of illegal drugs"). The FBI was able to seize only a small fraction of his coins; the rest still resides in saving accounts [156].

In general, the degree of anonymity of an entity can be expressed through a set of entities within which it is indistinguishable. The bigger this so-called *anonymity set*, the stronger the anonymity. In [154], it is assumed that dormant entities, which are currently not active, do not increase the anonymity set. Thus, when taking a certain point in time into consideration, the number of active entities is a better estimate.

Their analysis reveals a scale-free distribution (power law) of active days (i.e., days with cash flow) for the entities. Consequently, there is a large number of entities active for one day only, but also many single entities active for long periods. According to the findings, in order to blend into a large anonymity set, the aim is to create a "small" entity (i.e., small number of associated addresses), and to be active for a short time only.

The consensus of all aforementioned contributions is that there exist means to link information in Bitcoin's block chain. This makes Bitcoin not as private as it is often assumed. Quite in contrast: it is probably the most transparent trading system ever built. The block chain is a huge record, which enables everybody to evaluate all transactions.

C. Enabling Privacy

Even though privacy is not an inherent property of Bitcoin, it is strongly associated with it. Hence, it is often used for purposes where sender and/or receiver intend to remain

anonymous. Dread Pirate Roberts is cited in an interview after his arrest with the statement that Silk Road would not have been possible without Bitcoin [164]. Besides, there is a strong desire to create an anonymous digital currency. In this section, we discuss some of the best-practice techniques and proposals, which enable (more) privacy either within Bitcoin or in related digital currency systems.

In order to prevent block chain analysis techniques from succeeding, decoupling of information about the sender and the receiver is required. In analogy to mix networks for network anonymity like Tor (which, as discussed above in Section IV-E, decouple sender and receiver addresses in communication), mixing services for Bitcoin transactions—*money laundry services*—can be constructed. Indeed, there are many parallels between these fields.

The easiest way for gaining anonymity in Bitcoin is a third-party approach, comparable to a single-hop anonymization proxy in anonymous communication: a trusted third party gets coins (including a tip), with the request to transfer the coins to a given destination address. Due to the extremely large trading volume, the popular dice gamble SatoshiDice could leave the impression of being a good way to obscure transactions and to launder coins (even when losing every now and then). As noted by [74], the winnings are tied to the wager transaction, though. Thus, a block chain analysis would be able to follow the flow. In order to avoid this, the coins need to be juggled around by the third party in such a way that incoming and outgoing transactions cannot be linked.

Indeed such services exist. They all follow similar principles: transactions are routed through a shared wallet, so as to break the chain of trackable transactions. Assume Alice wants to send a bitcoin to Bob. Alice sends the bitcoin to a new Bitcoin address generated by the mixing service. The mixing service aggregates coins received from all its users to re-distribute them again. Some services use randomness, i.e., they split the amount into smaller random chunks and transfer them after random intervals. The user can schedule the transactions and provide time constraints. This way, as indicated in Figure 10, rather than receiving the bitcoin directly from Alice, Bob will receive it from others, which ideally will not reveal a relationship between Alice and Bob. An experimental analysis of three services, namely Bitcoin Fog (bitcoinfog.com), BitLaundry (bitlaundry.com) and Send Shared by blockchain.info[3] is contributed in [165]. There it is confirmed that most of them indeed obscure the transaction, but they still have issues and leak links. The most important reason is the sometimes low usage volume and, in consequence, the small anonymity set. If this happens and no reserve assets exist in the mixing services' pool, it will likely use the just-received coins next.

Sometimes a *taint analysis* as provided by blockchain.info[4] is used to evaluate the anonymity provided by a mixing service. It describes which fraction of coins received by a Bitcoin address can be traced back to another address. The more "tainted" the chain of transactions is, the stronger the linkage between the involved addresses remains. The only untainted coins are freshly minted coins from the coinbase transaction. However, taint analyses are not widely accepted, because they do not provide much information about the anonymity of a mixing service. Due to the lack of a good measure, the authors of [166] define the so-called *taint resistance*. They use the Matthews correlation coefficient (MCC) to express the accuracy an adversary obtains by linking inputs and outputs of a single transaction.

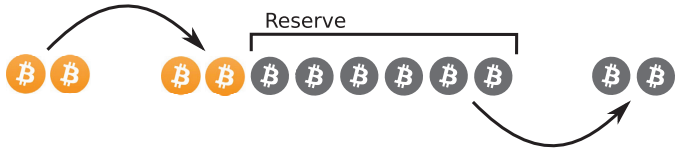


Fig. 10. The principle of Bitcoin mixing services.

The discussion reminds of the early years of anonymous communication [1] and the subsequent research on mixing services [167]–[170]. Aspects and techniques such as trust, observability, timing correlation, batching, dummy traffic and many more play a central role in this field just as in coin mixing services. However, the case of Bitcoin reveals two significant differences: a major trust problem and a predominant global adversary. Both characteristics will be discussed in the next paragraphs.

With respect to trusting a single mix, the same holds for network anonymity and coin mixing: the mix is always able to resolve the mapping between sender and receiver. But as long as the service is trustworthy and nobody else has access to their servers, plausible deniability remains. So, what to do if the mixing service is *not* trustworthy? The standard answer is: concatenate multiple mixes in a cascade. Even if individual mixes are compromised, as long as there is at least one honest mix, anonymity can be expected. (In theory at least: there exist attacks where it is sufficient to control a subset of mixes [169], [171], [172].) However, the trust problem in Bitcoin has a dimension that does not exist in network anonymity: since Bitcoin deals with monetary values, trust also means to put stock in somebody else's hands. This is, of course, not entirely different from data forwarding, because data also has a value, especially when it includes passwords or personal information. For this reason, data is typically secured by cryptographic means before handing them over to a mix. An adversary "running away with the encrypted data" can be considered acceptable, as long as the cryptography is strong enough, i.e., the encrypted data is worthless for an untrustworthy mix. From Bitcoin's perspective, transferring coins means changing the ownership in an irreversible way. At this point, the mix (who might be malicious) is—by the protocol—the legitimate owner of the coins. Thus, he could spend them for whatever he likes. This monetary aspect should not be underestimated, as it amplifies the trust problem with mixing services.

An adversary with a global view of the network has long been considered unlikely in the field of network anonymity. Even though it is now no longer considered that unlikely by all [173], such an adversary remains a very strong assumption. Bitcoin, in contrast, inherently does have such global observers: the block

[3]The mixing service Send Shared was dropped by blockchain.info. Their new service Shared Coin follows a different strategy, which we will cover later in this section.

[4]https://blockchain.info/taint/1dice6GV5Rz2iaifPvX7RMjfhaNPC8SXH

chain is publicly available. In both, network anonymity and Bitcoin anonymity, we can distinguish between passive (honest but curious) and active adversaries, but the adversary models are different.

A mixing service design named Mixcoin is proposed in [174]. The design is not entirely different from the previously deployed mixing services, but pays particular attention to the implications of parameter choices such as mixing and transaction fees in the face of different adversary models. If not considered carefully, fees add a "tag" (in a sense) to the transaction and help tracking the path. Mixcoin also includes a reputation-based approach for accountability, which is expected to reduce the probability of thefts. The authors of [175] extend the Mixcoin protocol by applying blind signatures [5] to prevent the mix from learning input-output mappings: users provide inputs and cryptographically blinded outputs. The mix signs the blinded outputs in return. Now, users can anonymously reconnect and reveal their "unblinded" output to the mix, which can verify that the outputs were signed in advance.

CoinJoin [160] is an approach which tries to go further in the sense that it aims to securely prevent theft, while at the same time providing privacy and being fully compatible with the Bitcoin protocol. It exploits the fact that multiple inputs of a transaction are independent from each other. For transaction verification, every input needs a valid signature, where the signatures do not necessarily need to stem from the same user. Thus, it is possible that users agree on a set of inputs and outputs and independently sign the transaction without the risk of theft. In order to blend in, all outputs in a CoinJoin transaction need to send the same amount of coins. The anonymity in a single transaction is limited by the number of outputs, but it can be significantly improved by concatenating CoinJoin transactions. Even relaxing the conditions and simply joining casually in transactions (i.e., without caring for the output volumes) impedes block chain analyses. In fact, it breaks the fundamental heuristic from Section V-A (inputs of a transaction belong to the same entity). As another side effect, per-user transaction fees are reduced, making joint transactions cheap. However, the devil is in the detail: unless very carefully implemented, e.g., allowing only certain coin denominations and taking special care of fees, it is possible to link inputs and outputs easily [166], [176], [177].

Besides, CoinJoin has two major weaknesses: (i) it needs to manage the collection of signatures, which involves the risk of additional privacy leaks, and (ii) participants can mount a denial-of-service attack by stalling joint transactions.

Regarding (i), users need to negotiate all transaction details in advance, construct the transaction, collect the respective signatures and finally broadcast the transaction in the Bitcoin network. The negotiation could be done informally—on IRC, for example—or in a more structured way using a specialized distributed protocol. The easiest way, of course is to employ a central entity, i.e., a server, which takes control. This basic idea of CoinJoin is implemented and offered as an online service named Shared Coin (sharedcoin.com) where blockchain.info takes the role of the central instance. There is also a decentralized implementation for Bitcoin named Coinmux (coinmux.com). Dash (DASH, dashpay.io), which was formely known as Darkcoin, is an altcoin which offers CoinJoin-like transactions natively [178].

Independent from using a centralized vs. decentralized or a formal vs. informal way of negotiation, some instances will invariably learn the mapping of input and output addresses. In the decentralized case, all participants will know the mapping of their allies. In the centralized case, the server will know the mapping of all participants. As [160] sketched, blind signatures can help to solve this issue. First approaches in these directions can be found in [179].

CoinShuffle [180] is a decentralized approach which tackles the former problem by constructing a chain of participants and using layered cryptography in a similar manner as in mix networks [1]. CoinShuffle participants send their transaction destination—encrypted in layers—along the chain of participants. In each intermediate step, the respective participant removes a layer of encryption. Additionally, each participant adds his designated destination, likewise encrypted in layers. The last participant of the chain receives the full list of destinations from its predecessor, removes the final encryption layer from all of them, and finally adds his own destination. The transaction can now be constructed and signed as proposed by the CoinJoin protocol. Note that the last peer of the chain of participants cannot link individual destinations. Likewise, intermediate peers cannot link destinations because they are encrypted.

With respect to (ii) from above, a user committing her intention to participate in a joint transaction, but later on not signing it, can stall the successful conclusion of the transaction. Blacklisting users deemed malicious may help, but comes with the bitter taste of false positives. However, ideas presented by [181] might mitigate the problem: the authors develop a primitive called composite signatures, which is based on aggregate signatures [182]. Initially composed of a masking key, it allows to incrementally add new signatures to the composite signature. The advantage over CoinJoin is that input and output addresses need not be known in advance. The composite signature can rather be passed around, making it more robust against DoS. Since the aggregation process is irreversible—that is, it is hard to compute individual signatures based on the composite signature—the approach provides plausible deniability. This requires modifications to the Bitcoin protocol, though: it changes the way signatures and references are computed and verified.

Approaches such as the fair exchange protocol by [21] and CoinSwap by [41] continue to reduce the necessary mutual trust and thus also enable anonymous peer-to-peer mixing. They make use of Bitcoin's scripting features, i.e., multi-signature and hash-locked transactions. A number of related Bitcoin-based commitment protocols can be found in [183], [184]. The authors of [185] support this trend and present a discovery mechanism by publishing "advertisements" in the block chain, which thwarts Sybil and DoS attacks.

The general idea of CoinSwap [41], for example, is that Alice and the mixing service build a 2-of-2 multi-signature transaction with Alice's coins. The mixing service and Bob build another 2-of-2 multi-signature transaction with the mixing service's coins. These transactions are announced publicly. The

respective refund transactions are time-locked and held back for safety, in case one party vanishes. Next, Alice and the mixing service as well as Bob and the mixing service each construct and exchange redeem transactions for the multi-signature transactions. Both redeem transactions are additionally hash-locked by the *same* secret (which comes from Bob). Thus, both of them can be redeemed by the respective participants as soon as the secret is known. This ensures that if Bob gets paid, the mixing service gets paid, too. Once the mixing service becomes confident that it gets paid, it can release the multi-signature. The same applies to Alice. In the end, successful CoinSwap transactions are not distinguishable from standard multi-signature transactions.

The anonymity set of CoinSwap consists of all 2-of-2 multi-signature transaction published at roughly the same time. Since Alice could also play the role of Bob in the protocol, CoinSwaps can be chained. Every CoinSwap requires four transactions and rather complex staged phases. As mentioned, it can also be used to exchange (or mix) coins in a peer-to-peer fashion. CoinJoin, in comparison, is less complex, but also has a limited anonymity set, namely the number of participants in a single transaction. However, both approaches seem to have a place: CoinJoin could be used (opportunistically) to increase overall privacy for everyone, and CoinSwap could achieve stronger anonymity when desired, at the cost of additional transactions.

Instead of developing means of usage which increase the privacy, there are also approaches which extend the Bitcoin protocol or propose altcoins with native untraceable transaction support. The aforementioned Darkcoin [178] is one example. Another approach builds upon non-interactive zero-knowledge proofs [186]. Zerocoin [187] is a protocol extension to Bitcoin by which Alice can prove to others that she owns a bitcoin and is thus eligible to spend *any* other bitcoin. First she produces a secure commitment, i.e., the zerocoin, which is recorded in the block chain so that others can validate it. In order to spend a bitcoin, she broadcasts a zero-knowledge proof for the respective zerocoin, together with a transaction. The zero-knowledge proof protects Alice from linking the zerocoin to her. Still, the other participants can verify the transaction and the proof. Instead of a linked list of Bitcoin transactions, Zerocoin introduces intermediate steps. Unfortunately, even though Zerocoin's properties may seem appealing, it is computationally complex, bloats the block chain and requires protocol modifications. However, it demonstrates an alternative, privacy-aware approach.

An extension of Zerocoin is presented by [188]. The authors developed additional means to also hide the coin volume of transactions and Bitcoin addresses. A fully-fledged altcoin design named Zerocash with strong privacy guarantees was presented in [189]. It takes the zero knowledge approach from Zerocoin, but improves it both in terms of functionality and efficiency.

Another altcoin approach is CryptoNote [190], which denotes a protocol and technology framework. An actual deployment of CryptoNote is Bytecoin (BCN, bytecoin.org). CryptoNote aims for the same two major privacy features as Zerocoin and its extensions: unlinkable transactions and untraceable payments. Unlinkable transactions help hiding the balance of a Bitcoin address. In Bitcoin, users are able to achieve this by always using a fresh address. However, as the existing results based on block chain analyses underline, if the public address is know (as with WikiLeaks or Silk Road, for example), the account balance can be determined. CryptoNote utilizes the basic idea of the Diffie-Hellman exchange protocol [191] to derive one-time key pairs for each transaction. These key pairs are generated on demand by the respective parties, without previous interaction. In particular, the sender uses the recipient's public address and generates a one-time public key to which the coins are sent. In addition, the sender adds half of the Diffie-Hellman handshake to the transaction. The receiver can use this half and its original private key to compute the private key required to redeem the transaction.

In order to further increase the difficulty of tracing payments and coin flows, CryptoNote uses *ring signatures* [192]. Ring signatures secure a message like any digital signature, but can be produced by any member of a group. Unlike group signatures, ring signatures make it infeasible to determine which member of the group signed the message. Every member can compute a ring signature on a message using their own private key and the group's public keys. For CryptoNote this means: when signing a transaction, in addition to the output he owns, the sender selects multiple other outputs of foreign transactions with the same amount (i.e., outputs she does not necessarily own). She then joins them as a single input. From the public keys of all outputs and her own private key, the sender creates the respective ring signature for the input. The validity of the transaction only implies that one of the group members has signed the transaction and spends a coin, but not which coin exactly. This is significantly different from Bitcoin, because only one of the selected outputs can actually be spent, not all of them. It increases the resistance against analysis of the block chain by providing multiple plausible paths to follow. Every consecutive transaction amplifies the effect by adding additional cash flow options.

However, such a scheme raises questions regarding double spending. In particular, if it is not possible to determine which coin has been spent, how can attempts of double spending be detected? CryptoNote tackles this issue by employing *traceable ring signatures* [193]: if somebody uses a private key more than once to create a signature, this can be detected, because every transaction also holds a so-called *key image*. If the same key image reappears, it means the one-time private key has been used more than once. This indicates double spending. Therefore, every peer keeps track of the previously seen key images. As with Zercoin, though, the increased privacy level comes at the price of a bloated block chain and more complex operations.

VI. Proof-of-X (PoX) Schemes

For attempts to paraphrase the Bitcoin protocol and to give a generalized description of its purpose, probably notions such as "consensus", "distributed" and "verification" come to mind. All of these are closely related to the role of proof of work in the Bitcoin design. In the following, we will dig deeper into this aspect. This exposes challenges which are sometimes much more subtle than the ones we saw before (like double

spending and scalability issues), but which likewise are of substantial importance. In response to these additional challenges, many alternative protocols have been proposed, forking from the Bitcoin protocol and implementing their own currency. We already mentioned examples such as Dogecoin, Darkcoin, and Bytecoin. But there are many more altcoins, and we will highlight a few in this section.

A. Reaching Consensus—The Byzantine Generals Problem

From a general perspective, Bitcoin works towards a consensus in a distributed manner and replicates the state network-wide. In order to guarantee fault tolerance, some redundancy is necessary. The amount of redundancy depends on the failure types. Consider, for example, three entities holding a value. Assume that a single entity fails: it always returns the same, wrong value. By comparing the answers, it is easy to identify the failing entity and to decide on the true value. Two entities would not suffice, an analogous situation would result in a conflict. In general terms, in the presence of f failures, the network needs $n \geq 2f + 1$ entities to tolerate the failures.

However, failures in a broader sense can also be random or malicious. These failures are called Byzantine failures, after the famous Byzantine Generals problem [11]. The original problem description considers the case of n generals trying to mutually agree via messengers on a common battle plan. However, f of the generals are traitors and try to thwart the agreement. The situation is comparable to a distributed system which aims to reach consensus. The Byzantine Generals problem with synchronous and reliable communication reaches consensus as long as $n \geq 3f + 1$ is satisfied [11]. In case of asynchronous communication, the Fischer-Lynch-Paterson (FLP) proof shows that an asynchronous and deterministic consensus protocol cannot tolerate any failures at all [194]. Later, [195] refined the results and revealed the dependency on the system properties process synchronicity, communication delay (bounded or unbounded), message order, and transmission method (point-to-point or broadcast). An overview of the first decade of this broad field is given by [196], [197].

The topic kept research busy. Some contributions relaxed the conditions in order to overcome the impossibility results. Non-deterministic consensus protocols, for example, provide solutions to the asynchronous case [198]. While consensus becomes possible due to the randomness, the approach leaves a (small) chance of failing. Others replaced the requirement of each entity to commit to a final decision by accepting that each entity has a current view (or "opinion") that may change as execution proceeds [199]. This yields the concept of "stabilizing consensus".

All of this comes quite close to what we see in the Bitcoin protocol: it makes heavy use of randomness in the mining process and re-adjusts it regularly. Furthermore, Bitcoin deliberately omits a final and fixed ownership attribution[5]. Instead, it uses a rule of thumb: after (typically) six confirmations, transactions are considered settled. Convergence is achieved via the longest chain rule.

A popular example which borrows directly from the results of Byzantine agreement is Ripple (XRP, ripple.com). Ripple takes a different direction and relies on a set of trusted "authorities" to build consensus. It implements a round-based consensus algorithm with final decision making. The final decision results in a so-called "last closed ledger" which represents the current state of all accounts. Ripple's consensus algorithm achieves $5f + 1$ resilience [200].

Another condition is the timing model, which describes the message propagation in the network. In the synchronous communication case, messages arrive after a certain fixed time span. Any message that takes longer is considered a failure. Protocols for the synchronous case explicitly rely on timing assumptions; they often proceed in discrete rounds. As numerous impossibility results show, solutions are often only possible for the synchronous case. In the much more general asynchronous timing model, no assumptions are made on the relative rate of execution or message delivery. As [201] points out, the asynchronous timing model might not be realistic, because it is unlikely that messages take longer than a certain threshold (even though this threshold could well be very high). However, protocols for the asynchronous case—where they exist—are very generic and work irrespectively of the system's condition.

Thus, the system designer is left with two bad choices. The fact that Bitcoin allows the blocks' timestamp to deviate only within a certain range hints at the assumption of a synchronous network model. The 10 minutes block creation time was, in the first place, chosen as a trade-off between confirmation time and the amount of work wasted due to chain forks. But it also ensures to reach every corner of the network even in the face of prolonged propagation times. It therefore, in a sense, synchronizes the network (loosely).

In addition to the already mentioned conditions, the Bitcoin network is, due to its structural properties which support anonymity, of unknown size. In the face of Byzantine failures, this additional condition makes the problem harder. Malicious entities can set up fake identities which subvert the election and inject faulty information, i.e., they can mount a Sybil attack [15]. In Bitcoin, the proof-of-work requirements tackle this vulnerability by artificially increasing the cost of a vote. This approach originates from the attempts to combat spam [3], [202]. In fact, the idea to use it in the context of Byzantine agreement protocols has been proposed before Bitcoin already [203]. Yet, even though the possibility of Sybil attacks had been considered there, the size of the network was assumed to be known; otherwise, the assumptions are comparable to those behind Bitcoin.

Thus, in principle, all the puzzle pieces required to build a consensus protocol similar to Bitcoin were there. The similarity of the problem and the advances in the field were recognized [12]. The idea to employ Byzantine agreement protocols such as [14] to the area of distributed digital currencies paved the ground [13]. Even design proposals and prototypes existed [7]–[10]. Eventually, in 2008, time was ready and Bitcoin appeared.

In summary, we can say that Bitcoin tackles the Byzantine Generals problem from a practical angle. Nakamoto himself

[5]By now, Bitcoin in fact has checkpoints, which are once in a while hard-coded into the software and mark an irreversible block height in the block chain. Checkpoints were introduced by Satoshi Nakamoto later and are not part of the original design.

compared the protocol design to this particular problem [204]. As also discussed in [205], Bitcoin balances viability and security and seems to have found a sweet spot. It suggests that Bitcoin underlies the assumptions of a synchronous network of unknown size, relaxes the deterministic constraint and takes eventual consistency as adequate. In [57] a fault tolerance of $2f + 1$ is derived under these assumptions, where f is the total hash power of malicious miners (Byzantine failures). This meets the intuitions and the analyses of the 51% attacks: as long as more than half of the hash power is controlled by honest miners, the network will eventually reach consensus, even in the presence of malicious miners. However, as [120] add to this view, Bitcoin meets the theoretical fault tolerance only as long as the assumption of synchronicity holds. Thus, information propagation amongst honest peers is essential, especially when the malicious miners' hash power approaches the critical threshold; otherwise the system becomes fragile and insecure.

B. Proof of Work—the Monopoly Problem

Proof of work is a key component of Bitcoin. Inherently, any task suitable as a basis for proof-of-work schemes needs to be difficult to solve, but trivial to verify. It often boils down to a random process of trying to find a solution to a puzzle—like a (partial) hash collision.

Bitcoin's precursors B-money [7], Karma [8], RPOW [9] and Bit Gold [10] already incorporated a proof-of-work scheme in one way or the other. In all these cases, the motivation was to consider the solution to the puzzle as a scarce and valuable good, like "gold". RPOW is a centralized approach, which uses reusable proof of work as token money. Coins are minted by a server in return to a proof of work. The coins are reusable and transferable, while the central server checks for validity. B-money decentralizes the process by assuming a synchronous unjammable broadcast channel. Transactions are issued by signing a contract, which is broadcast so that everybody knows of it. Alternatively, a trusted set of servers can be employed to keep track of the ledger. In a similar way, Karma implements a distributed currency by maintaining a so-called bank set. Karma also considered the effect of inflation and deflation and proposed means to adjust money creation. Probably Bit Gold is the most advanced approach of all precursors, as it chains the proof of work, uses the last entry to create the next challenge and adjusts the difficulty. However, it also relies on a quorum of hosts/addresses rather than a quorum of computing power. It is thus vulnerable to Sybil attacks. Finally, it was the Bitcoin protocol to combine Sybil resistance and coin minting by a sophisticated proof-of-work scheme.

Originally, the paradigm of proof of work is "one-CPU-one-vote" [16]. Bitcoin uses a CPU-bound function (i.e., SHA-256 [30]) as the basis for its proof-of-work scheme. Miners are by nature rational profit seekers. Their mining costs consist of expenses for mining hardware and ongoing energy cost. They strive to reach the break-even point as quickly as possible, to make as much profit as possible. The first miners used computers with ordinary CPUs to solve the proof of work. Even though CPUs are extremely versatile, the versatility comes at the expense of limited speed. Miners therefore quickly sought for faster solutions to dominate the competition and to make more profit.

Mining operations are highly parallelizable. Some graphics processors (GPUs) are therefore able to compute the repeated hash operations much faster and much more energy efficient than any CPU. GPU mining quickly replaced CPU mining. Bitcoin's popularity picked up pace and pushed the competition even more. The fact that CPU-bound hash functions are suitable for hardware acceleration [206] received attention. Thus, it was only a matter of time until hardware-based mining solutions became available—first based on reconfigurable logic (Field-Programmable Gate Arrays, FPGAs) and subsequently based on application-specific integrated circuits (ASICs). FPGAs and especially ASICs significantly increased the speed and efficiency of mining. Since then, only ASICs (if at all) are economically viable for bitcoin mining. They achieve hash rates in the order of one terahash per second. In [207], [208] the story of Bitcoin hardware and its energy footprint is told in detail. Recent observations and optimizations [209], [210] will probably continue to push the hash rates even higher in the future.

Following the increasing computational power, Bitcoin adjusts the difficulty, i.e., the target value, to maintain the ten-minute-per-block target rate. This behavior can be seen in Figure 11, which we generated by parsing the block chain and calculating a moving average of the block confirmation time (plotted on the left y-axis) for a small part of the block chain. We can observe a repeated decrease of the confirmation time, which implies that the total hash rate of all participants increases. Every 2016 blocks, Bitcoin adjusts the difficulty of the proof of work, which is plotted on the right y-axis. Only very seldom in the history of Bitcoin it happened that the difficulty was adjusted downwards. Most often it increases.

Overall the difficulty follows an exponential growth, as Figure 12 shows. Please note the logarithmically scaled y-axes. Since the difficulty is continuously adjusted to the hash rate, the data line in this plot can be interpreted as either of these: the hash rate according to the left y-axis, or the difficulty according to the right y-axis.

The use of specialized mining equipment increases the voting power per entity. This development subverts the proof-of-work paradigm and therefore implies a threat. In particular, it reduces the democratic basis by suppressing "small" miners. As a consequence, the trust in Bitcoin degrades.

In Bitcoin, we can take the idiom "rich gets richer" literally: it has been shown that the wealth of rich users increases faster than the wealth of users with low balance [211]. Additionally, there is an alarming trend that the power of a small group of miners significantly exceeds the power that all other users contribute [70]. This raises the question whether Bitcoin is still truly a decentralized currency or if it is shifting towards the centralized banking model which it originally questioned.

During the early steps of proof-of-work (i.e., Hashcash) and before Bitcoin, the imbalanced capabilities of systems were already identified as a possible issue. This was considered inherent to CPU-bound functions. In order to recover the situation, the idea to employ memory-bound functions instead was introduced. The approach is to incorporate large amounts

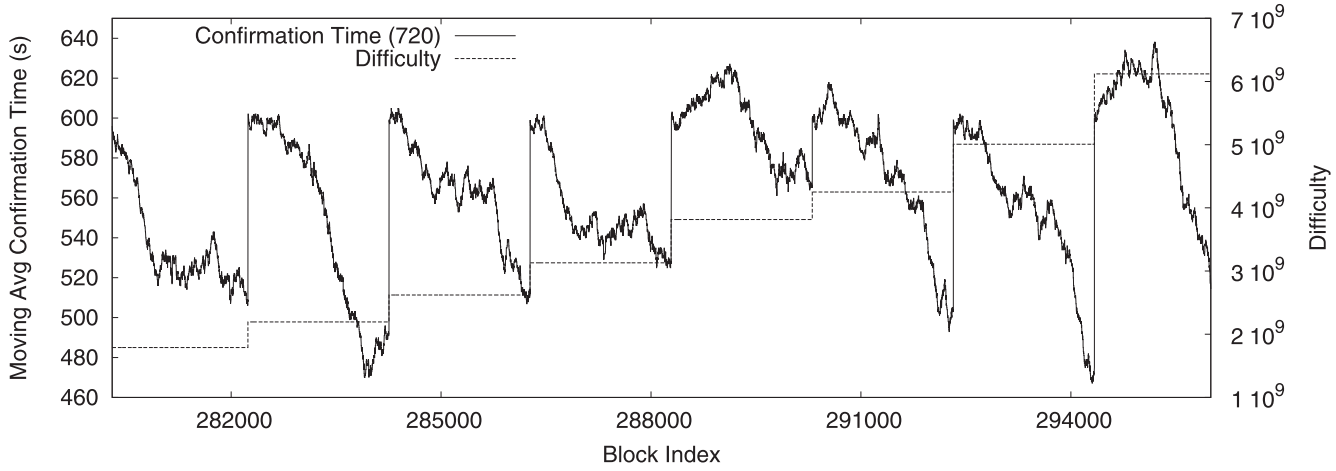


Fig. 11. Moving average of the confirmation time and difficulty calculated from the block chain.

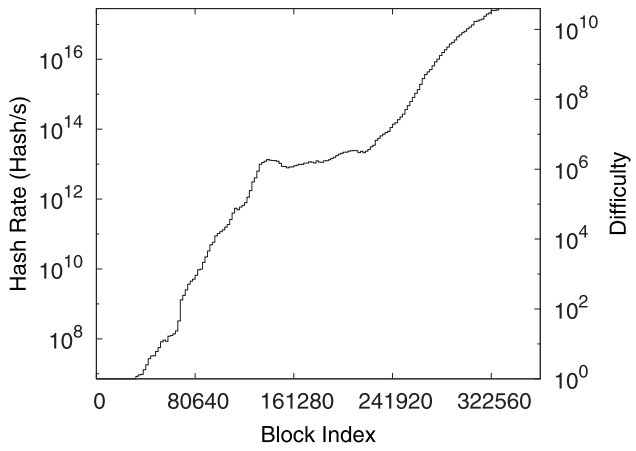


Fig. 12. Hash rate and difficulty obtained from the block chain (logscaled y-axes).

of (unpredictable) memory access operations in the proof of work calculations, so that these constitute the dominant factor. Hence, solving the proof of work is limited by the memory access time, not by the CPU speed. The underlying assumption is that the differences between users with regard to memory access speed are inherently much smaller than the differences with respect to computing power. Memory-bound functions had been proposed in the context of spam prevention before [212], [213].

In the context of Bitcoin, functions such as scrypt [214] and CryptoNight [190] have been discussed. In a corresponding proof-of-work scheme, memory-intensive operations are added to the hashing operations. The intention is to foster more evenly distributed power among the user base, to avoid the emergence of a monopoly. Unfortunately, scrypt—which is probably the most popular alternative proof-of-work scheme, and is used, e.g., by Litecoin (LTC, litecoin.org)—still enables the use of specialized mining devices. The appearance of more energy-efficient GPU-based mining brought a significant increase of Litecoin's hash rate. Moreover, most alternative hash functions are rather immature and not as well analyzed as, for example, SHA-256. Therefore, concerns about possible future weaknesses remain. In general, there are discussions whether ASIC-resistant proof of work can exist at all [215], [216].

Another fundamental criticism of proof of work in general and Bitcoin in particular is that it wastes computational power (and thus energy) without any intrinsic value. Contributions which try to alter this situation are NooShare [217], Primecoin [218] and Permacoin [100]. NooShare proposes the scheduling of arbitrary Monte-Carlo simulations as a proof of work. Primecoin (XPM, primecoin.io) requires miners to find long chains of prime numbers, so-called Cunningham chains. Permacoin realizes distributed storage by requiring so-called proofs of retrievability, that is, access to local storage. All three approaches provide an added value besides securing the block chain. However, other difficulties arise then, such as fine-tuning the difficulty and preventing reuse of earlier results. For example, in case of Primecoin, the length of a prime chain does not naturally imply a suitable difficulty metric. Chains of eight primes may be a hundred times harder to find than chains of seven primes. Primecoin solves this issue by using Fermat's primality test to construct an approximately linear difficulty metric for a given chain length. Even though Primecoin is considered a CPU-only currency (since finding prime chains appears to be inefficient on GPUs), doubts along the same lines as mentioned earlier exist [219], and first GPU-based miners are already available.

For completeness, we briefly mention some altcoins which also rely on proof of work. We have already mentioned Litecoin as an adopter of scrypt as the underlying hash function. Dogecoin is another popular altcoin which uses scrypt. Both are Bitcoin forks (and thus use the same code base), but have faster confirmation times of 2.5 minutes and 1 minute, respectively. Dogecoin also has a much higher coin supply and a higher reward per block. Therefore, it is gaining traction as a microdonation system.

Not deployed, but nevertheless appealing are the ideas of MAVEPAY [220] and FawkesCoin [221]. As the names indicate, they build upon MAVE [222] and the Guy Fawkes signature protocol [223], which substitute Bitcoin's elliptic curve DSA (ECDSA). FawkesCoin, for example, constructs a digital currency with only symmetric cryptography. Due to

the symmetry property, signatures can be used securely only once. Hence, FawkesCoin requires to use a fresh address for every transaction (which, however, is also recommended for Bitcoin anyway). In contrast, MAVEPAY uses digital signature algorithms with selectable security thresholds and thereby reduces resource demands.

C. Proof of Stake—Towards Solving Incentive Problems

Even though Bitcoin vividly shows that a digital currency based on proof of work is viable, weaknesses still exist. The participants of Bitcoin pay the miners via a mechanism of inflation to secure the currency. Nevertheless, the future when the block reward declines over time remains unclear. Approximately every four years (i.e., every 210,000 blocks) the block reward halves. After the first reward halving, we can observe a slight dip in the difficulty, implying that miners left the network. If the controlled supply of coins continues as specified, approximately in the year 2032 the reward will be less than 1 BTC, and in the year 2140 it will be down to zero. According to [86], this kind of deflation is a self-destruction mechanism. It puts the security of crypto currencies at risk by driving off miners. Whether the transaction fees will suffice to compensate the decreasing reward and to provide the necessary incentive for miners remains unclear and is controversially discussed [69].

The relationship between the miners' strategy and the mining reward follows a trade-off, which can be modeled using game theory [224]. Once the miner finds a solution, she needs to make sure to propagate the information before others claim the next block to get the reward. The transactions to include in a block are chosen by the miner. We can assume that their number has no effect on the complexity of the proof of work, but that a higher number increases the time to reach consensus: the more bytes the block contains, the more time it takes to broadcast it through network. And the more transactions a block holds, the more time it takes to verify its validity. On the other hand, the more transactions there are in a block, the bigger the reward. According to [224], there is a unique Nash equilibrium, i.e., a point where no participant can gain an advantage from changing her strategy. Interestingly, at this Nash equilibrium miners will not include any transaction at all in their blocks. Obviously, this would render Bitcoin practically useless, which hurts miners as well. The Nash equilibrium shifts as soon as transaction fees increase or the block reward significantly decreases. This suggests that transaction fees might provide an incentive.

However, there is a problem with decreasing rewards, which boils down to the tragedy of the commons [225]. Tragedy of the commons is a game theoretic term which describes the phenomenon that taking individually, independently optimized (and thus most likely selfish) actions reduce the peer group's long-term gain by depleting a common resource. Known examples come from areas such as environmental pollution, fishing resources and road traffic.

The relevance to Bitcoin is multifaceted [226]. From the users' perspective, it is in the interest of all users to provide an incentive for miners and to pay transaction fees in order to maintain a secure network. However, each individual user's (selfish) interest is to let others pay the fees. Users might therefore start to issue transactions without fees. If the majority acts this way, mining becomes unprofitable, and miners will give up. From the miners' perspective, there is another tragedy of the commons problem. On one hand, their group interest is to have users pay high fees. Thus, all miner's could mutually agree to expect a certain fee per transaction and only then consider the respective transaction valid. On the other hand, the cost of including a transaction in a block is negligibly small. Thus, each miner gains a personal advantage by simply including every transaction with a fee, independent from the actual amount. This might lead to continuously lower fees, up to the point where mining is not lucrative anymore. In both cases, miners will turn away and thus gaining a monopoly becomes easier. Again, there is a risk for the currency's security.

Questioning proof of work as a basis and looking for alternatives lets us revisit the fundamental requirements which need to be fulfilled: first, the block generation must be somehow "expensive", and individual miners shall not be able to gain an overproportionally high ability to mint coins. Second, consensus must eventually be reached; there must be a common rule to resolve forks and to determine the main block chain. Third, it must be forgery proof. The latter is a general requirement for currencies, which must hold here, too.

It turns out that *coin age* is a viable alternative to proof of work. Coin age is defined as the currency amount times the holding period [227]. For example, if Alice transfers two coins to Bob and Bob held the coins for 90 days, the coin age is 180 coin-days. When Bob spends the two coins, the coin age he accumulated is destroyed.

The idea to use the coin age to define the reward is known as *proof of stake* [227] (PoS). It is, for example, implemented in Peercoin (PPC, peercoin.net). Mining a proof-of-stake block requires to construct a so-called *coinstake block* (named after Bitcoin's coinbase transaction). In a coinstake transaction, owners send coins in their possession to themselves and add a predefined percentage as their reward. Analogue to proof of work, a hash value below or equal to a target value is required to successfully mint a block. In contrast to proof of work (and Bitcoin), the difficulty is individually determined: it is inversely proportional to the coin age. Because the hash is—except for a timestamp—calculated on static data, there is no way for miners to use their computational power to solve the puzzle faster than others. In particular, there is no nonce which can be modified. Instead, every second the timestamp changes and miners have a new chance of finding the solution. If they find a solution, they broadcast the block including the coinstake transaction. The coinstake transaction assigns the reward to the miner, but also resets the coin age. Of course, new coin age can subsequently be accumulated again, slowly increasing the chances of solving the puzzle next time.

One can think of coin age in proof of stake the same way as of computing power in proof of work. A huge pile of old coins is equivalent to a powerful ASIC mining rig. But there are key differences: the "power" is independent from computing power. Instead, it depends on the deposit. Thereby, proof of stake provides an answer to the criticism that proof of work wastes energy. Unlike Primecoin, which tries to put an intrinsic

value into the proof of work, proof of stake eliminates the high energy consumption altogether. It shifts from a highly competitive tournament to a raffle-like scheme, with repeatedly occurring new chances for all participants. In addition, miners destroy the coin age by claiming the reward; they do not keep it for the next round. This gives others the chance to "win the raffle", too.

These properties mitigate the risk of monopoly in the tragedy of the commons problem. Note that the voting power is more equally distributed. Thus, "rich gets richer" is complemented by "poor gets richer" [228], meaning every participant can provide a proof of stake, thus help to secure the block chain and in return get a reward in proportion to their holding.

Besides, exploiting a proof of stake-based currency seems much more expensive. In contrast to proof of work, where the longest block chain survives, proof of stake declares the block chain with the highest total sum of destroyed coin age as the main chain. In order to perform an attack similar to the 51%-attack, an attacker must hold a huge amount of coins, which even when destroying the coin age suffices to gain more than half of the odds. It is assumed that the cost for gaining the majority of computing power in a proof-of-work scheme (e.g., for hardware) is smaller than the cost for buying enough coins in a proof-of-stake setting. However, there are also objections to this claim [229], suggesting that the attack would be anticipated and thus coins would be ditched, which reduces the attacker's costs. Nevertheless an attacker holding lots of coins would suffer severely from ruining the currency, which probably reduces the incentive to do so in the first place.

For practical purposes, proof of stake is proposed to complement proof of work and to become the dominant factor when the proof of work block rewards subside, as, e.g., Peercoin. Yet, there are also entirely proof of stake-based altcoins, such as Nextcoin (NXT, nxt.org).

Derivatives—such as transactions as proof of stake (TaPoS) [230] and delegated proof of stake (DPoS) [231]—are supposed to mitigate the monopoly problem, and at the same time to make the system more secure by collecting votes from a larger base. We will cover the details of the problems which motivated these (and other) directions in the next section.

D. Proof of Activity—Incentivize Active Participation

Proof of stake shows an alternative to proof of work, but it comes with a number of limitations. And actually there is another tragedy of the commons problem, which affects proof of stake likewise.

The authors of [232] emphasize the goal of information propagation in Bitcoin and compare it to the 2009 DARPA Network Challenge: on the date of the 40th anniversary of the Internet, DARPA announced a challenge in which competing participants tried to find red weather balloons across the US. MIT's winning strategy [233] consisted of recruiting hunters and offering a reward. However, they recognized that this is another challenge by itself, so they offered an additional reward for recruiters of balloon finders. This way they created an incentive to spread the word. In fact, the additional reward is necessary because each additional hunter competes with other hunters in the proximity, i.e., each additional participant reduces the others' chances of finding the balloon.

From the miners' perspective, the situation in Bitcoin is not different, especially when the block reward decreases and the transaction fees should compensate. This reveals another tragedy of the commons [226]: a miner has an incentive to keep any transaction including a fee for itself. Eventually, the miner will not relay the transaction, so as to reduce competition. Instead of rewarding transaction fees to the miners, Peercoin destroys the fees in order to eliminate the incentive to not cooperate [227].

But proof of stake has some more limitations: it entirely depends on the coin age, which can be accumulated by holding coins only, and can be claimed in a coinstake transaction to oneself. Coins spent in regular transactions assigning coins to others also destroy the coin age, but are not considered in the proof-of-stake raffle. Thus, hoarding coins is encouraged; [234] therefore talks of *collectibles* rather than currencies.

The major weakness, though, is that coin age accumulates even when the node is not connected to the network. It suffices when nodes come online occasionally and wait for their reward, only to go offline again afterwards. This behavior will result in a more bursty reward distribution than in the case where nodes remain online all the time, but stakeholders most likely will accept that. The lack of a sufficient number of online nodes, though, facilitates attacks.

Any reward scheme which tries to incentivize in one or the other sense must pay attention to Sybil attacks [232]. For example, MIT's strategy in the DARPA challenge was vulnerable, because balloon hunters could set up false identities as recruiters to increase their finder's reward. In the following, we summarize two extensions [226], [234] which incorporate proof of stake and provide an advanced reward scheme. Related approaches which avoid the usage of proof of stake exist, too [235].

In [234] the author follows the idea that a higher activity produces a healthier economy. He identifies the problem that coin age is a linear function of time. In practice, Peercoin implements an upper and a lower bound of coin age to mitigate some of the mentioned problems. However, changing the increment function to an exponential decay function, for example, would have a profound impact. In such a setting, the increment rate of the coin age decreases with time and asymptotically converges to zero. Parameterizing the decay constant allows for a deliberate specification of the function's half-life time. This changes the incentive: a fresh coin accumulates coin age much faster, up to a fixed value. The intention is to reduce the resistance to trade coins and to encourage users to stay online. It is conceivable to employ other functions, such as non-monotonic and/or periodic functions. That would imply to punish hoarding coins even more, or to reflect a seasonal pattern. The basic idea is termed *proof of stake velocity* and is implemented in Reddcoin (RDD, reddcoin.com).

The approach by [226] is to directly reward active peers for their contribution. The idea is to raffle a fraction of the proof-of-work block reward among all active nodes, while their stake determines the amount of raffle tickets, i.e., their chances of winning. It is thus a combination of proof of work and proof of

stake. In detail, miners mine "empty" blocks only. If they solve the proof-of-work puzzle, they broadcast it in the network as before. Everybody receiving the block derives N deterministic pseudorandom ticket numbers from it. The first $N-1$ most lucky stakeholders sign the block with their respective private key and broadcast the signature. If the N-th most lucky stakeholder sees the block, she creates a wrapper, includes the block, all transactions, the $N-1$ signatures, adds her own signature and broadcasts the wrapped block. Others will consider it as a legitimate extension of the block chain if the block and the lucky stakeholders are valid. Finally the transaction fees are shared by stakeholders and the miner.

In order to determine the N lucky stakeholders, the pseudorandom number is interpreted as an index in the list of all so far minted satoshis. Finding the user in possession of the satoshi is done by a procedure called "follow-the-satoshi". Everybody can verify it by inspecting the block chain and following the satoshi from the coinbase transaction up to the address currently holding it. Please note that this is much like proof of stake, with the difference that the coin age is irrelevant. Alice holding two coins has twice as high a chance to be picked as Bob holding one coin. The decision to share the transaction fees as reward among the stakeholders and not, for example, the entire block reward is rooted in the observation which we pointed out earlier: a high reward for the stake incentivizes undesirable coin hoarding. The small fees are considered a nice bonus, but not an incentive for hoarding.

The underlying concept is to reward active peers which are online. If one of the lucky stakeholders is offline, he will not be able to respond and to add her signature. Hence, the block cannot be completed. At some point, there will be another miner solving the proof of work, drawing N different stakeholders. The difficulty is adjusted according to the hash rate and the fraction of active peers. The concept is accordingly called *proof of activity* (PoA) [226]. It rewards stakeholders who participate rather than punishing passive stakeholders. The proof-of-work component is inevitable to make the system converge and to provide a rule to resolve forks. Moreover, it is necessary to throttle the speed of picking the lucky stakeholders. Proof of activity improves security: besides a huge amount of computational power, an attacker needs a significant amount of stake to double spend.

In some ways, proof of activity is a core component of peer-to-peer networks. The BitTorrent protocol [4], for example, uses a built-in incentive mechanism for direct reciprocity ("tit-for-tat"). The effectiveness of this approach has been shown many times [236], [237]. As we have explained before, the Bitcoin network follows a different goal, i.e., fast block propagation ("gossip") and not file sharing ("exchange"). Therefore, we can conceive proof of activity as indirect reciprocity.

E. Proof of Publication—Provable Commitments

After looking at various proof-of-X schemes, let us close the circle and come to another achievement of computing history which apparently influenced the Bitcoin design, namely secure timestamping. A timestamping service provides timestamps for digital documents, which securely keep track of the creation and modification time of the document. There are many timestamping schemes, such as PKI-based centralized services, where documents and timestamps are hashed and secured by the private key of the timestamping server. However, the server can easily backdate documents by hashing and signing a previous timestamp. Thus, the approach comes with the premise of trusting the timestamping server.

In order to tackle this issue, [19] developed so-called linked timestamps. Each timestamp certificate includes a hash of the previous one. This ensures a total order of documents, even if inaccurate clocks are in place. Furthermore, it hardens fake certificates, because it is not possible to retroactively hook documents in the linked chain of timestamps.

As already noted in [19], it is possible to distribute the process of secure timestamping. Instead of relying on a single server, it is favorable to consult multiple instances. The hash of the document can be interpreted as a k-tuple of server IDs to request certificates from. However, a vulnerability to Sybil attacks shows up again, and the problem in general is very closely related to the Byzantine Generals.

Once again, this is where Bitcoin steps in: Bitcoin also references previous transactions and links blocks, but it also provides Sybil resilience. In fact, it is essential for a transaction system to determine the order of actions. Since Bitcoin's proof-of-work mechanism constantly readjusts the difficulty to meet the target of one block every 10 minutes, the protocol can also be considered a distributed secure timestamping service, where the timestamp accuracy is roughly the block generation time.

The authors of [40] come to a similar conclusion and propose a carbon dating commitment protocol based on Bitcoin, namely CommitCoin. The idea is, in a more general context, also known as *proof of publication* and comes in various manifestations. In the case of CommitCoin, a Bitcoin address is generated which encodes the information of a respective document. Other use cases include coin tosses [238], lotteries [239], or decentralized poker [240], This works without a central entity and without the need to trust each other, that is, secure multi-party computations (MPC). MPC enables such use cases, however, comes with the caveat that it cannot enforce payouts or compensation. Cryptocurrencies are, therefore, a natural choice for combining MPC with money: players bet coins by issuing elaborate transactions, i.e., commitments, while still not trusting each other or any kind of third party. Such protocols are not limited to gambling and generalizations exist [183], [241].

Proofs of publication require a number of complex steps to encode data or operations while preserving the involved coins. However, intentional coin destruction can also be used for sound purposes. At the beginning, especially with currencies relying on proof of stake, the problem of how to bootstrap a new currency exists. Bitcoin, for example, (and many other proof of work-based currencies) have a genesis block. Other altcoins, such as Counterparty or Mastercoin[6], bootstrapped by using the idea of *proof of burn*. By "burning" coins of one

[6]Strictly speaking, Mastercoin did not use proof of burn. It rather used a so-called exodus address, which was a regular Bitcoin address and funded the development of the currency. On a more abstract level, though, it follows the same idea.

currency in a verifiable but unspendable way, coins of another currency can be generated and assigned. At first sight, burning coins might seem to be a harsh primitive of commitment, but it can be considered as expensive, just like a proof of work.

This property makes proof of burn a very well viable tool for migration. Simple protocol changes such as invalidating an old transaction type might involve a *soft fork*, but generally remain backward compatible. Older clients will continue to accept transactions which are considered invalid by new software releases. In order to enforce the changes, the majority of the miners must upgrade. Miners that do not upgrade may waste computing power by generating blocks that will be rejected by others. On the other hand, miners have a handle to oppose unwilling upgrades as long as the majority refuses.

Changes to core components such as the block structure, difficulty rules, or the set of valid transactions are much more difficile and often involve a *hard fork*. Since it makes previously invalid transactions or blocks valid, it requires all users and miners to upgrade. Otherwise, two different coins with two different rule sets emerge. Both, soft and hard forks show another fundamental property of cryptocurrencies: miners not only vote on the state of the block chain, but also vote on the underlying rule set.

Sometimes, changes can be implemented in such a way that new transaction types appear to older clients like a previously already valid transaction type, as it was done with P2SH transactions. If this is not possible, proof of burn steps in and provides a way of moving from one chain to another. The authors of [242] take it one step further: why not send coins not only to addresses within one block chain, but also to concurrent block chains? As a result, they developed so-called *side chains*. Similar to proof of burn, coins are sent to a special output. Thereby, they are not destroyed, but only "immobilized" until somebody can prove they are no longer being used elsewhere. This adds a form of reversibility to the proof of burn. In order to make this work for Bitcoin, a new validation rule would have to be introduced, though, which would require at least a soft fork.

Similar to proof of burn, other provable commitment protocols such as proof of bandwidth or proof of retrievability can be used to repay expenses as it was proposed in the context of Tor [243]–[245] or to realize a decentralized file storage [100].

VII. Summary of Observations and Future Research Directions

After our extensive characterization of Bitcoin and its related approaches, it is time to take a look back and summarize our lessons learned, before we discuss future research directions and the next generation of Bitcoin.

We exposed the agreement on and maintenance of an unforgeable, but distributed ledger—the block chain—which holds all assignments ever created—the transactions—and makes them verifiable to everyone. Bitcoin is considered a secure timestamping service and a practical solution to the Byzantine Generals problem. In order to achieve consensus, Bitcoin accepts the risk of failure. In particular, double spends (or race attacks) are and will always be possible. The risk, though, can be minimized and is subject to a personal trade-off.

The transparency of the system is a fundamental aspect to achieve verifiability, but likewise it introduces an omnipresent global attacker model. Therefore, we can conclude Bitcoin is anything but private. Nevertheless, it can hide identities and the efforts to strengthen this property continue. The attempts and techniques recall the discussion on anonymity networks. However, it also brings up commitment schemes such as zero knowledge proofs and gives them a whole new "playground". Thus, we see the starting point of a symbiotic effect between different areas.

Probably one of the most outstanding contributions of Bitcoin is the degree of decentralization which was previously deemed impossible. The ingenious concept of mining, may it be based on proof of work, proof of stake or something else, secures the ledger and eventually stabilizes the consensus. It binds "votes" to something "expensive" and incentivizes to "pay" for it by holding out the prospect of a reward, which at the same time controls the money supply of the digital currency. Without mining, fake identities would be able to subvert the consensus and destroy the system. Because of this crucial point, we can conclude that 51% attacks are the worst-case scenario. Furthermore, the mining monopoly threatens the decentralization.

The previously listed observations and features are often considered to be the most innovative parts of Bitcoin. Certainly, the balance of security and privacy features with a transparent and verifiable transaction process are contributing factors of Bitcoin's popularity. However, only in combination with one of the most distinctive features, namely the scripting capabilities, the depth of possibilities becomes evident. The instruction set may be limited, but it is still a powerful tool to realize sophisticated transactions and contracts. This trend is further followed by a second generation of cryptocurrencies with a fully-fledged scripting language. Yet the possibilities are barely explored.

For the future it remains unclear whether Bitcoin can and will stay as robust as it is today. Especially the scalability of the network and the subsiding rewards are pressing and need to be addressed. At the moment both apparently work well enough. In case of the peer-to-peer network, though, one can already observe symptoms of degradation, such as a long-tail distribution of the information propagation delay. However, Bitcoin's security assumptions rely heavily on the fast propagation of transactions and blocks. Thus, in order to scale to more participants and higher transaction rates the network needs to be able to handle the load. In case of the subsiding mining rewards the research community is unsure whether this poses a real problem or if fees are able to provide the necessary incentive. So far, we discussed a huge body of approaches which aim to be a solution to issues in Bitcoin. Some of them are deployed as an altcoin or an additional service. We provide a summary in Table IV, where we also point to the respective papers and the section(s) where we discussed them. Yet it remains unclear which alternative approach is most promising to actually improve Bitcoin, and which will survive in practice.

All the altcoins can be considered as a huge testing environment, from which Bitcoin can borrow in the future to address weaknesses. Bitcoin is constantly evolving and remains under development. It established the so-called Bitcoin improvement proposal (BIP) design documents as a way to introduce new

TABLE IV
SUMMARY OF ALTCOINS AND EXTENSIONS

	Approach	Distinct Feature (incl. References)	Sec.
Precursor	B-Money	Mining reward proportional to proof of work difficulty; requires a broadcast channel [7]	II-B, V-D, V-E
	Bit Gold	Chained proof of work [10]; Byzantine-resilient quorum [13]	III-B, V-D, V-E
	Karma	Distributed currency maintained by a bank set [8]	V-E
	RPOW	Centralized (reusable) proof of work exchange/ bank [9]	V-E
Altcoins	Bitshares (BTS)	Delegated proof of stake [231]	V-F
	Bytecoin (BCN)	Implements CryptoNote [190], which aims for unlinkable and untraceable transactions	V-C, V-E
	Counterparty (XCP)	Colored coin; used proof of burn	V-H, V-H
	Cryptonite (XCN)	Implements the mini block chain scheme [127]	IV-D
	Dash (DASH)	Formerly known as Darkcoin; implements native CoinJoin-like transactions [178]	V-C
	Dogecoin (DOGE)	Block payload holds TXIDs only; fast block generation	IV-D, V-E
	Litecoin (LTC)	Uses scrypt [214] to foster distributed power among miners	V-E
	Mastercoin (MSC)	Colored coin; exodus address	V-H
	Nextcoin (NXT)	Entirely proof of stake based	V-F
	Peercoin (PPC)	Identified coin age as alternative measure; proof of stake [227]	V-F
	Primecoin (XPM)	Proof of work with intrinsic value i. e. prime chains [218]	V-E
	Reddcoin (RDD)	Proof of stake velocity [234]	V-E
	RSCoin	Centrally controlled money supply with distributed verification [126]	IV-D
	Ripple (XRP)	Implements a novel Byzantine agreement protocol [200]	V-D
	Zerocash	Full-fledged altcoin, carrying on the ideas of Zerocoin [189]	V-C
Altchains	Bitmessage	Secure messaging service [145]	IV-G
	Ethereum (Ether)	Turing complete smart contract processing [44], [45]	II-E
	Namecoin (NMC)	Key-value storage; realizes decentralized domain name coordination [143]	IV-G
	Permacoin	Decentralized file storage; proposes proof of retrievability [100]	V-E
Protocols / Extensions	CoinJoin	Uses multi-signature transactions to enhance privacy [160]	V-C
	CoinShuffle	Decentralized protocol to coordinate CoinJoin transactions [180]	V-C
	CoinSwap	Enables P2P-based trustless mixing [41]	V-C
	CommitCoin	Secure timestamping protocol [40]	V-H
	Mini block chain	Identifies individual block chain components [127]	IV-D
	Mixcoin	Mixing with accountability [174]	V-C
	Zerocoin	Unlinkable and untraceable transactions by employing zero knowledge proofs [187]	V-C

features to Bitcoin. If a BIP finds the mutual consent of the community, it becomes accepted. However, since some of the proposed changes are more invasive than others, migration is an important point.

In summary, in this survey we studied the broad field of Bitcoin, its characteristics and related concepts. In particular, we investigated the protocol's foundations, including the role of proof of work, and their relationship to security and network aspects. By doing so, we provided a holistic technical perspective on distributed currencies. Bitcoin and the huge zoo of altcoins constitute a highly dynamic and certainly not yet fully understood field of research, in which manyfold open research questions with very high practical relevance remain to be answered. It will certainly be highly interesting to follow the future developments in this dynamic field.

ACKNOWLEDGMENT

The authors would like to thank Daniel Cagara for the discussions on this topic and for sharing his practical experience. We also like to thank the Bitcoin community for valuable feedback on the preprint of this paper. Finally, we express our gratitude to the anonymous reviewers and the editor in chief for their constructive, detailed and very helpful feedback.

REFERENCES

[1] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 211–219, Feb. 1981.
[2] P. R. Zimmermann, *The Official PGP User's Guide*. Cambridge, MA, USA: MIT Press, 1995.
[3] A. Back, "Hashcash—A denial of service counter-measure," Tech. Rep., Aug. 2002 [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf
[4] B. Cohen, "Incentives build robustness in BitTorrent," in *Proc. 1st Workshop Econ. Peer Peer Syst. (P2PEcon'03)*, Jun. 2003, pp. 68–72.
[5] D. Chaum, "Blind signatures for untraceable payments," in *Proc. 2nd Conf. Adv. Cryptol.*, Aug. 1982, pp. 199–203.
[6] L. Law, S. Sabett, and J. Solinas, "How to make a mint: The cryptography of anonymous electronic cash," *Amer. Univ. Law Rev.*, vol. 46, no. 4, 1996.
[7] W. Dai. (1998). *B-Money* [Online]. Available: http://www.weidai.com/bmoney.txt
[8] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, "KARMA: A secure economic framework for peer-to-peer resource sharing," in *Proc. 1st Workshop Econ. Peer Peer Syst. (P2PEcon'03)*, Jun. 2003.
[9] H. Finney. (2004). *Rpow* [Online]. Available: http://cryptome.org/rpow.htm
[10] N. Szabo. (2005). *Bit Gold* [Online]. Available: http://unenumerated.blogspot.de/2005/12/bit-gold.html
[11] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.
[12] N. Szabo, "Advances in distributed security," 2003 [Online]. Available: http://szabo.best.vwh.net/distributed.html
[13] N. Szabo, "Secure property titles with owner authority," 1998 [Online]. Available: http://nakamotoinstitute.org/secure-property-titles/
[14] D. Malkhi and M. Reiter, "Byzantine quorum systems," *Distrib. Comput.*, vol. 11, no. 4, pp. 203–213, 1998.
[15] J. Douceur, "The Sybil attack," in *Proc. 1st Int. Workshop Peer Peer Syst.*, Mar. 2002, pp. 251–260.
[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008 [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[17] S. Nakamoto. (2008, Nov.). *Bitcoin P2P e-Cash Paper* [Online]. Available: https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

[18] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Proc. 7th Conf. Adv. Cryptol. (CRYPTO'87)*, Aug. 1987, pp. 369–378.

[19] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptol.*, vol. 3, pp. 99–111, 1991.

[20] H. Massias, X. S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirement," in *Proc. 20th Symp. Inf. Theory Benelux (SITB'99)*, May 1999.

[21] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better—How to make bitcoin a better currency," in *Proc. 16th Int. Conf. Financial Cryptogr. Data Secur. (FC'12)*, Mar. 2012, pp. 399–414.

[22] D. Drainville, "An analysis of the bitcoin electronic cash system," Univ. Waterloo, Waterloo, ON, Canada, Canada, Tech. Rep., Dec. 2012.

[23] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Proc. 36th IEEE Symp. Secur. Privacy (SP'15)*, May 2015, pp. 104–121.

[24] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IACR Cryptology ePrint Archive, Tech. Rep. 2015/464, 2015.

[25] (2014). *Bitcoin Developer Documentation* [Online]. Available: https://bitcoin.org/en/developer-documentation

[26] (2014). *The Bitcoin Wiki* [Online]. Available: https://en.bitcoin.it/wiki

[27] M. Nielsen. (2013, Dec.). *How the Bitcoin Protocol Actually Works* [Online]. Available: http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

[28] A. Narayanan, J. Bonneau, E. Felten, and A. Miller. (2015). *Bitcoin and Cryptocurrency Technologies* [Online]. Available: https://www.coursera.org/course/bitcointech

[29] N. Asokan, P. A. Janson, M. Steiner, and M. Waidner, "The state of the art in electronic payment systems," *IEEE Comput.*, vol. 30, no. 9, pp. 28–35, Sep. 1997.

[30] D. Eastlake III and T. Hansen. (2011, May). *US Secure Hash Algorithms (SHA and SHA-Based HMAC and HKDF), RFC 6234 (Informational), Internet Engineering Task Force* [Online]. Available: http://www.ietf.org/rfc/rfc6234.txt

[31] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer Peer Netw. Appl.*, 2015.

[32] K. Kaskaloglu, "Near zero bitcoin transaction fees cannot last forever," in *Proc. Int. Conf. Digit. Secur. Forensics*, Jun. 2014, pp. 91–99.

[33] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur. (FC'14)*, Mar. 2014, pp. 157–175.

[34] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Proc. 17th Int. Conf. Financial Cryptogr. Data Secur. (FC'13)*, Apr. 2013, pp. 6–24.

[35] M. Fleder, M. Kester, and S. Pillai, "Bitcoin transaction graph analysis," Massachusetts Institute of Technology (MIT), Computer Systems Security, Tech. Rep. 6.858, 2013.

[36] G. Andresen, "BIP 16: Pay to script hash," Jan. 2012 [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki

[37] G. Andresen, "BIP 13: Address format for pay-to-script-hash," Oct. 2011.

[38] I. Gerhardt and T. Hanke, "Homomorphic payment addresses and the pay-to-contract protocol," Computing Research Repository, Tech. Rep. abs/1212.3257, 2012.

[39] G. Andresen, "BIP 11: M-of-N standard transactions," Oct. 2011.

[40] J. Clark and A. Essex, "CommitCoin: Carbon dating commitments with bitcoin," in *Proc. 16th Int. Conf. Financial Cryptogr. Data Secur. (FC'12)*, Mar. 2012, pp. 390–398.

[41] G. Maxwell. (2013, Oct.). *CoinSwap: Transaction Graph Disjoint Trustless Trading* [Online]. Available: https://bitcointalk.org/index.php?topic=321228.0

[42] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Proc. 17th Int. Symp. Stabilization Safety Secur. Distrib. Syst.*, Aug. 2015, pp. 3–18.

[43] J. R. Willett, "The second bitcoin," White Paper, Tech. Rep., 2013 [Online]. Available: https://sites.google.com/site/2ndbtcwpaper/2ndBitcoinWhitepaper.pdf

[44] G. Wood, "ETHEREUM: A secure decentralised generalised transaction ledger," Tech. Rep., 2014 [Online]. Available: http://gavwood.com/Paper.pdf

[45] E. Project, "A next-generation smart contract and decentralized application platform," 2014 [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[46] N. Szabo, "The idea of smart contracts," 1997.

[47] M. Rosenfeld, "Overview of colored coins," Tech. Rep., 2012 [Online]. Available: https://bitcoil.co.il/BitcoinX.pdf

[48] A. Yelowitz and M. Wilson, "Characteristics of bitcoin users: An analysis of Google search data," *Appl. Econ. Lett.*, vol. 22, no. 13, 2015.

[49] J. Bohr and M. Bashir, "Who uses bitcoin? An exploration of the bitcoin community," in *Proc. 12th IEEE Conf. Privacy Secur. Trust (PST'14)*, Jul. 2014, pp. 94–101.

[50] M. Matta, I. Lunesu, and M. Marchesi, "Bitcoin spread prediction using social and web search media," in *Proc. Workshop Deep Content Anal. Techn. Pers. Intell. Serv. (DeCAT'15)*, Jun. 2015.

[51] L. Kristoufek, "What are the main drivers of the bitcoin price? Evidence from wavelet coherence analysis," *PLoS ONE*, vol. 10, no. 4, Apr. 2015.

[52] D. Garcia, C. J. Tessone, P. Mavrodiev, and N. Perony, "The digital traces of bubbles: Feedback cycles between socio-economic signals in the bitcoin economy," Computing Research Repository, Tech. Rep. abs/1408.1494, 2014.

[53] D. Shah and K. Zhang, "Bayesian regression and bitcoin," Computing Research Repository, Tech. Rep. abs/1410.1231, 2014.

[54] S. Goldfeder, J. Bonneau, E. W. Felten, J. A. Kroll, and A. Narayanan, "Securing bitcoin wallets via threshold signatures," Tech. Rep., 2014 [Online]. Available: http://www.cs.princeton.edu/~stevenag/bitcoin_threshold_signatures.pdf.

[55] T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, "Bluewallet: The secure bitcoin wallet," in *Proc. 10th Int. Workshop Secur. Trust Manage.*, Sep. 2014, pp. 65–80.

[56] N. Howgrave-Graham and N. P. Smart, "Lattice attacks on digital signature schemes," *Des. Codes Cryptogr.*, vol. 23, no. 3, pp. 283–290, 2001.

[57] A. Miller and J. J. LaViola, Jr., "Anonymous Byzantine consensus from moderately-hard puzzles: A model for bitcoin," Computer Science, Univ. Florida, Gainesville, FL, USA, Tech. Rep., Apr. 2014 [Online]. Available: http://tr.eecs.ucf.edu/id/eprint/78

[58] M. Rosenfeld, "Analysis of hashrate-based double spending," Tech. Rep., 2012 [Online]. Available: https://bitcoil.co.il/Doublespend.pdf

[59] Vector67. (2011). *Fake Bitcoins?* [Online]. Available: https://bitcointalk.org/index.php?topic=36788.msg463391\#msg463391

[60] H. Finney. (2011). *Best Practice for Fast Transaction Acceptance—How High is the Risk?* [Online]. Available: https://bitcointalk.org/index.php?topic=3441.msg48384\#msg48384

[61] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur.*, Mar. 2014, pp. 436–454.

[62] P. Wuille, "BIP 62: Dealing with malleability," Mar. 2014 [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki

[63] C. Decker and R. Wattenhofer, "Bitcoin transaction malleability and MtGox," in *Proc. 19th Eur. Symp. Res. Comput. Secur. (ESORICS'14)*, Sep. 2014, pp. 313–326.

[64] corbixgwelt. (2011, May). *Timejacking & Bitcoin* [Online]. Available: http://culubas.blogspot.de/2011/05/timejacking-bitcoin_802.html.

[65] B. Cohen. (2014, Nov.). *An Attack on the Timestamp Semantics of Bitcoin* [Online]. Available: http://bramcohen.com/2014/11/03/an-attack-on-the-timestamp-semantics-of-bitcoin

[66] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *Proc. 24th USENIX Secur. Symp. (USENIX Secur.'15)*, Aug. 2015, pp. 129–144.

[67] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Proc. 13th IEEE Int. Conf. Peer-to-Peer Comput. P2P'13*, Sep. 2013, pp. 1–10.

[68] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *Proc. 19th Int. Conf. Financial Cryptogr. Data Secur. (FC'15)*, Jan. 2015, pp. 507–527.

[69] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proc. 12th Workshop Econ. Inf. Secur.*, Jun. 2013.

[70] A. Gervais, G. Karame, S. Capkun, and V. Capkun, "Is bitcoin a decentralized currency?" in *Proc. 35th IEEE Symp. Secur. Privacy (SP'14)*, May 2014, pp. 54–60.

[71] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, "Tampering with the delivery of blocks and transactions in bitcoin," in *Proc. 22nd ACM Conf. Comput. Commun. Secur. (CCS'15)*, Oct. 2015, pp. 692–705.

[72] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *Proc. 21st ACM Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 15–29.

[73] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and Privacy in Social Networks*. New York, NY, USA: Springer, 2013, pp. 197–223.

[74] S. Meiklejohn *et al.*, "A fistful of bitcoins: Characterizing payments among men with no names," in *Proc. 13th ACM SIGCOMM Conf. Internet Meas. (IMC'13)*, Oct. 2013, pp. 127–140.

[75] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *Proc. 17th Int. Conf. Financ. Cryptogr. Data Secur.*, Apr. 2013, pp. 34–51.

[76] S. Goldfeder *et al.*, "Securing bitcoin wallets via a new DSA/ECDSA threshold signature scheme," Tech. Rep., 2015 [Online]. Available: http://www.cs.princeton.edu/stevenag/threshold_ sigs.pdf.

[77] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[78] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. 5th Conf. Adv. Cryptol.*, Aug. 1985, pp. 417–426.

[79] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[80] P. Gallagher and C. Kerry. (2013, Jul.). *Federal Information Processing Standards (FIPS) Publication 186-4: Digital Signature Standard (DSS)* [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[81] D. R. L. Brown. (2010). *SEC 2: Recommended Elliptic Curve Domain Parameters*, Standards for Efficient Cryptography Group (SECG) [Online]. Available: http://www.secg.org/sec2-v2.pdf

[82] A. Dmitrienko, D. Noack, A. Sadeghi, and M. Yung, "On offline payments with bitcoin (poster abstract)," in *Proc. 1st Workshop Bitcoin Res. (BITCOIN'14)*, Mar. 2014, pp. 159–160.

[83] T. Ruffing, A. Kate, and D. Schröder, "Liar, liar, coins on fire!: Penalizing equivocation by loss of bitcoins," in *Proc. 22nd ACM Conf. Comput. Commun. Secur.*, Oct. 2015, pp. 219–230.

[84] I. Osipkov, E. Y. Vasserman, N. Hopper, and Y. Kim, "Combating double-spending using cooperative P2P systems," in *Proc. 27th Int. Conf. Distrib. Comput. Syst. (ICDCS'07)*, Jun. 2007, p. 41.

[85] J.-H. Hoepman, "Distributed double spending prevention," in *Proc. 15th Int. Workshop Secur. Protocols (SPW'07)*, Apr. 2007, pp. 152–165.

[86] N. T. Courtois, "On the longest chain rule and programmed self-destruction of crypto currencies," Computing Research Repository, Tech. Rep. abs/1405.0534, 2014.

[87] W. Feller, *An Introduction to Probability Theory and Its Applications*. New York, NY, USA: Wiley, 1957.

[88] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proc. 19th ACM Conf. Comput. Commun. Secur. (CCS'12)*, Oct. 2012, pp. 906–917.

[89] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Capkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, pp. 2:1–2:32, 2015.

[90] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," Computing Research Repository, Tech. Rep. abs/1112.4980, 2011.

[91] N. T. Courtois and L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency," Computing Research Repository, Tech. Rep. abs/1402.1718, 2014.

[92] M. Möser, R. Böhme, and D. Breuker, "Towards risk scoring of bitcoin transactions," in *Proc. 1st Workshop Bitcoin Res. (BITCOIN'14)*, Mar. 2014.

[93] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "On the malleability of bitcoin transactions," in *Proc. 2nd Workshop Bitcoin Res.*, Jan. 2015, pp. 1–18.

[94] M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of denial-of-service attacks in the bitcoin ecosystem," in *Proc. 1st Workshop Bitcoin Res. (BITCOIN'14)*, Mar. 2014, pp. 57–71.

[95] G. G. Dagher, B. Bünz, J. Bonneau, J. Clark, and D. Boneh, "Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges," in *Proc. 22nd ACM Conf. Comput. Commun. Secur. (CCS'15)*, Oct. 2015, pp. 720–731.

[96] T. Moore and N. Christin, "Beware the middleman: Empirical analysis of bitcoin-exchange risk," in *Proc. 17th Int. Conf. Financial Cryptogr. Data Secur.*, Apr. 2013, pp. 25–33.

[97] I. Eyal and E. G. Sirer. (2014, Jun.). *How to Disincentivize Large Bitcoin Mining Pools* [Online]. Available: http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools/

[98] N. Hajdarbegovic. (2014, Jan.). *Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack*, Coindesk [Online]. Available: http://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/

[99] A. Miller, A. E. Kosba, J. Katz, and E. Shi, "Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions," in *Proc. 22nd ACM Conf. Comput. Commun. Secur. (CCS'15)*, Oct. 2015, pp. 680–691.

[100] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in *Proc. IEEE 35th Symp. Secur. Privacy (SP'14)*, May 2014, pp. 475–490.

[101] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against bitcoin mining pools," in *Proc. 1st Workshop Bitcoin Res. (BITCOIN'14)*, Mar. 2014, pp. 72–86.

[102] A. Laszka, B. Johnson, and J. Grossklags, "When bitcoin mining pools run dry: A game-theoretic analysis of the long-term impact of attacks between mining pools," in *Proc. 2nd Workshop Bitcoin Res. (BITCOIN'15)*, Jan. 2015, pp. 63–77.

[103] L. Bahack, "Theoretical bitcoin attacks with less than half of the computational power (draft)," IACR Cryptology ePrint Archive, Tech. Rep. 2013/868, 2013.

[104] I. Eyal, "The miner's dilemma," in *Proc. 36th IEEE Symp. Secur. Privacy (SP'15)*, May 2015, pp. 89–103.

[105] 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," Computing Research Repository, Tech. Rep. abs/1505.05343, 2015.

[106] E. Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur. (FC'14)*, Mar. 2014.

[107] S. D. Lerner. (2014, May). *Decor+* [Online]. Available: https://bitslog.wordpress.com/2014/05/07/decor-2/

[108] D. Mills, J. Martin, J. Burbank, and W. Kasch. (2010, Jun.). *Network Time Protocol Version 4: Protocol and Algorithms Specification, RFC 5905 (Proposed Standard), Internet Engineering Task Force* [Online]. Available: http://www.ietf.org/rfc/rfc5905.txt

[109] (2003). *The Annotated Gnutella Protocol Specification v0.4* [Online]. Available: http://rfc-gnutella.sourceforge.net/developer/stable/

[110] Q. Lv, S. Ratnasamy, and S. Shenker, "Can heterogeneity make Gnutella scalable?," in *Proc. 1st Int. Workshop Peer Peer Syst. (IPTPS'02)*, Mar. 2002, pp. 94–103.

[111] Y. Chawathe, S. Ratnasamy, L. Breslau, N. Lanham, and S. Shenker, "Making Gnutella-like P2P systems scalable," in *Proc. Conf. Appl. Technol. Archit. Protocols Comput. Commun. (SIGCOMM'03)*, Aug. 2003, pp. 407–418.

[112] EB3full. (2014, May). *simbit—P2P Network Simulator* [Online]. Available: https://bitcointalk.org/index.php?topic=603171.0

[113] A. Miller and R. Jansen, "Shadow-bitcoin: Scalable simulation via direct execution of multi-threaded applications," in *Proc. 8th Workshop Cyber Secur. Exp. Test*, Aug. 2015.

[114] T. Neudecker, P. Andelfinger, and H. Hartenstein, "A simulation model for analysis of attacks on the bitcoin peer-to-peer network," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM'15)*, May 2015, pp. 1327–1332.

[115] J. A. D. Donet, C. Pérez-Sola, and J. Herrera-Joancomartı, "The bitcoin P2P network," in *Proc. 1st Workshop Bitcoin Res. (BITCOIN'14)*, Mar. 2014, pp. 87–102.

[116] S. Feld, M. Schönfeld, and M. Werner, "Analyzing the deployment of bitcoin's P2P network under an AS-level perspective," in *Proc. 5th Int. Conf. Ambient Syst. Netw. Technol. (ANT'14)*, June 2014, pp. 1121–1126.

[117] A. Miller *et al.*, "Discovering bitcoin's public topology and influential nodes," Tech. Rep., May 2015 [Online]. Available: https://cs.umd.edu/projects/coinscope/coinscope.pdf

[118] P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in bitcoin using P2P network traffic," Mar. 2014, pp. 469–485.

[119] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten, "Have a snack, pay with bitcoins," in *Proc. 13th IEEE Int. Conf. Peer Peer Comput. (P2P'13)*, Sep. 2013, pp. 1–5.

[120] J. A. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Proc. 34th Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT'15)*, Apr. 2015, pp. 281–310.

[121] D. Kaminsky (2011, Aug.). *Black OPS of TCP/IP*, Black Hat USA, 2011 [Online]. Available: http://dankaminsky.com/2011/08/05/bo2k11/

[122] T. Klingberg and R. Manfredi. (2002, Jun.). *Gnutella 0.6* [Online]. Available: http://rfc-gnutella.sourceforge.net/src/rfc-0/_6-draft.html

[123] S. L. Reed, "Bitcoin cooperative proof-of-stake," Computing Research Repository, Tech. Rep. abs/1405.5741, 2014.

[124] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[125] M. Hearn and M. Corallo, "BIP 37: Connection bloom filtering," Oct. 2012 [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki

[126] G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," IACR Cryptology ePrint Archive, Tech. Rep. 502, 2015.

[127] J. Bruce, "The mini-blockchain scheme," Tech. Rep., Jul. 2014, Rev. 2 [Online]. Available: http://cryptonite.info/files/mbc-scheme-rev2.pdf

[128] N. T. Courtois, P. Emirdag, and D. A. Nagy, "Could bitcoin transactions be 100x faster?," in *Proc. 11th Int. Conf. Secur. Cryptogr. (SECRYPT'14)*, Aug. 2014, pp. 426–431.

[129] B. Laurie, "Decentralised currencies are probably impossible but let's at least make them efficient," Tech. Rep., 2011 [Online]. Available: http://www.links.org/files/decentralised-currencies.pdf

[130] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proc. 13th USENIX Secur. Symp. (USENIX Security'04)*, Aug. 2004, pp. 303–320.

[131] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding routing information," in *Proc. 1st Int. Workshop Inf. Hiding (IHW'01)*, May 1996, pp. 137–150.

[132] A. Biryukov and I. Pustogarov, "Bitcoin over Tor isn't a good idea," in *Proc. 36th IEEE Symp. Secur. Privacy (SP'15)*, May 2015, pp. 122–134.

[133] Bitcoin Development Mailing Lists. (2014). *Outbound Connections Rotation* [Online]. Available: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-August/006502.html

[134] L. Øverlier and P. Syverson, "Locating hidden servers," in *Proc. 27th IEEE Symp. Secur. Privacy (SP'06)*, May 2006, pp. 100–114.

[135] T. Elahi, K. Bauer, M. AlSabah, R. Dingledine, and I. Goldberg, "Changing of the guards: A framework for understanding and improving entry guard selection in Tor," in *Proc. ACM Workshop Privacy Electron. Soc. (WPES'12)*, Oct. 2012, pp. 43–54.

[136] R. Dingledine, N. Hopper, G. Kadianakis, and N. Mathewson, "One fast guard for life (or 9 months)," in *Proc. 7th Workshop Hot Topics Privacy Enhancing Technol. (HotPETs'14)*, Jul. 2014.

[137] S. T. Ali, P. McCorry, P. H.-J. Lee, and F. Hao, "Zombiecoin: Powering next-generation botnets with bitcoin," in *Proc. 2nd Workshop Bitcoin Res. (BITCOIN'15)*, Jan. 2015, pp. 34–48.

[138] D. Plohmann and E. Gerhards-Padilla, "Case study of the miner botnet," in *Proc. 4th Int. Conf. Cyber Conflict (CYCON'12)*, Jun. 2012, pp. 1–16.

[139] D. Y. Huang *et al.*, "Botcoin: Monetizing stolen cycles," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS'14)*, Feb. 2014.

[140] J. Heusser. (2013, Feb.). *SAT Solving—An Alternative to Brute Force Bitcoin Mining* [Online]. Available: https://jheusser.github.io/2013/02/03/satcoin.html

[141] J. A. Dev, "Bitcoin mining acceleration and performance quantification," in *Proc. 27th IEEE Can. Conf. Elect. Comput. Eng. (CCECE'14)*, May 2014, pp. 1–6.

[142] R. Ragan and O. Salazar. (2014, Aug.). *Cloudbots: Harvesting Crypto Coins Like a Botnet Farmer*, Black Hat USA [Online]. Available: http://www.http://slideshare.net/rob.ragan/cloudbots-harvesting-crypto-currency-like-a-botnet-farmer

[143] Vinced. (2011, Apr.). *Namecoin—A Distributed Naming System Based on Bitcoin* [Online]. Available: https://bitcointalk.org/index.php?topic=6017.0

[144] J. Szefer and R. B. Lee, "Bitdeposit: Deterring attacks and abuses of cloud computing services through economic measures," in *Proc. 13th IEEE/ACM Int. Symp. Cluster Cloud Grid Comput. (CCGRID'13)*, May 2013, pp. 630–635.

[145] J. Warren, "Bitmessage: A peer-to-peer message authentication and delivery system," Tech. Rep., Nov. 2012 [Online]. Available: https://bitmessage.org/bitmessage.pdf

[146] Z. Wilcox-O'Hearn (2010, Jan.). *Names: Distributed, Secure, Human-Readable: Choose Two* [Online]. Available: http://web.archive.org/web/20011020191610/http://zooko.com/distnames.html

[147] A. Schwartz. (2011, Jan.). *Squaring the Triangle: Secure, Decentralized, Human-Readable Names* [Online]. Available: http://www.aaronsw.com/weblog/squarezooko

[148] Kiba. (2010, Dec.). *BitDNS Bounty (3500 BTC)* [Online]. Available: https://bitcointalk.org/index.php?topic=2072.0

[149] D. Barok, "Bitcoin: Censorship-resistant currency and domain system for the people," Networked Media, Piet Zwar Institute, Rotterdam, The Netherlands, Tech. Rep., Jul. 2011.

[150] C. Fromknecht, D. Velicanu, and S. Yakoubov, "CertCoin: A namecoin based decentralized authentication system," Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep., 6.857 Class Project, May 2014.

[151] A. Narayanan and V. Shmatikov, "De-anonymizing social networks," in *Proc. 30th IEEE Symp. Secur. Privacy (SP'09)*, May 2009, pp. 173–187.

[152] L. Backstrom, C. Dwork, and J. Kleinberg, "Wherefore art thou R3579X?: Anonymized social networks, hidden patterns, and structural steganography," in *Proc. 16th Int. World Wide Web Conf. (* WWW'07*)*, Apr. 2007, pp. 181–190.

[153] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proc. 29th IEEE Symp. Secur. Privacy (SP'08)*, May 2008, pp. 111–125.

[154] M. Ober, S. Katzenbeisser, and K. Hamacher, "Structure and anonymity of the bitcoin transaction graph," *Future Internet*, vol. 5, no. 2, pp. 237–250, 2013.

[155] A. Baumann, B. Fabian, and M. Lischke, "Exploring the bitcoin network," in *Proc. 10th Int. Conf. Web Inf. Syst. Technol. (WebDB'04)*, Apr. 2014, pp. 369–374.

[156] D. Ron and A. Shamir, "How did dread pirate roberts acquire and protect his bitcoin wealth?" in *Proc. 1st Workshop Bitcoin Res. (BITCOIN'14)*, Mar. 2014, pp. 3–15.

[157] M. Vasek and T. Moore, "There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams," in *Proc. 19th Int. Conf. Financial Cryptogr. Data Secur. (FC'15)*, Jan. 2015, pp. 44–61.

[158] J. Vornberger, "Marker addresses: Adding identification information to bitcoin transactions to leverage existing trust relationships," in *Proc. 42nd GI Jahrestagung (INFORMATIK'12)*, Sep. 2012, pp. 28–38.

[159] D. Vandervort, "Challenges and opportunities associated with a bitcoin-based transaction rating system," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur. (FC'14)*, Mar. 2014, pp. 33–42.

[160] G. Maxwell. (2013, Aug.). *Coinjoin: Bitcoin Privacy for the Real World* [Online]. Available: https://bitcointalk.org/index.php?topic=279249.0

[161] M. Spagnuolo, F. Maggi, and S. Zanero, "Bitiodine: Extracting intelligence from the bitcoin network," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur. (FC'14)*, Mar. 2014, pp. 457–468.

[162] L. Page, S. Brin, R. Motwani, and T. Winograd, "The pagerank citation ranking: Bringing order to the web," Stanford InfoLab, Tech. Rep. 1999-66, Nov. 1999.

[163] D. Ferrin, "A preliminary field guide for bitcoin transaction patterns," in *Proc. Texas Bitcoin Conf.*, 2015.

[164] A. Greenberg. (2013, Aug.). *An Interview With a Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A)*, Forbes Magazine [Online]. Available: http://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/

[165] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," Sep. 2013.

[166] S. meiklejohn and C. Orlandi, "Privacy-enhancing overlays in bitcoin," in *Proc. 2nd Workshop Bitcoin Res. (BITCOIN'15)*, Jan. 2015, pp. 127–141.

[167] G. Danezis, R. Dingledine, and N. Mathewson, "Mixminion: Design of a type III anonymous remailer protocol," in *Proc. 24th IEEE Symp. Secur. Privacy (SP'03)*, May 2003, pp. 2–15.

[168] U. Möller, L. Cottrell, P. Palfrader, and L. Sassaman, "Mixmaster Protocol—Version 2," IETF Internet Draft, Jul. 2003.

[169] A. Serjantov, R. Dingledine, and P. Syverson, "From a trickle to a flood: Active attacks on several mix types," in *Proc. 5th Int. Workshop Inf. Hiding (IHW'02)*, Oct. 2002, pp. 36–52.

[170] C. Diaz and A. Serjantov, "Generalising mixes," in *Proc. Privacy Enhancing Technol. Workshop (PET'03)*, Mar. 2003, pp. 18–31.

[171] J.-F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in *Proc. Int. Workshop Des. Privacy Enhancing Technol. Des. Issues Anonymity Unobservability (PET'00)*, Jul. 2000, pp. 10–29.

[172] P. Syverson, G. Tsudik, M. Reed, and C. Landwehr, "Towards an analysis of onion routing security," in *Proc. Int. Workshop Des. Privacy Enhancing Technol. Des. Issues Anonymity Unobservability (PET'00)*, Jul. 2000, pp. 96–114.

[173] A. Johnson, C. Wacek, R. Jansen, M. Sherr, and P. Syverson, "Users get routed: Traffic correlation on Tor by realistic adversaries," in *Proc. 20th ACM Conf. Comput. Commun. Secur. (CCS'13)*, Oct. 2013, pp. 337–348.

[174] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur. (FC'14)*, Mar. 2014, pp. 486–504.

[175] A. M. F. B. Blindcoin Blinded, "Luke Valenta and Vrendan Rowan," in *Proc. 2nd Workshop Bitcoin Res. (BITCOIN'15)*, Jan. 2015, pp. 112–126.

[176] K. Atlas. (2014). *Coinjoin Sudoku* [Online]. Available: http://www.coinjoinsudoku.com

[177] Michael_S (bitcointalk.org). (2014, May). *Why Coinjoin, as Used in Darkcoin, Does not Bring Full Anonymity* [Online]. Available: http://www.scribd.com/doc/227369807/Bitcoin-Coinjoin-Not-Anonymous-v01

[178] E. Duffield and K. Hagan, "Darkcoin: Peer-to-peer crypto-currency with anonymous blockchain transactions and an improved proof-of-work system," Mar. 2014 [Online]. Available: http://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf

[179] W. Ladd, "Blind signatures for bitcoin transaction anonymity," Tech. Rep., 2013 [Online]. Available: http://wbl.github.io/bitcoinanon.pdf

[180] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in *Proc. 7th Workshop Hot Topics Privacy Enhancing Technol. (HotPETs'14)*, Sep. 2014, pp. 345–364.

[181] A. Saxena, J. Misra, and A. Dhar, "Increasing anonymity in bitcoin," in *Proc. 1st Workshop Bitcoin Res. (BITCOIN'14)*, Mar. 2014, pp. 122–139.

[182] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proc. 22nd Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT'03)*, May 2003, pp. 416–432.

[183] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Fair two-party computations via bitcoin deposits," in *Proc. 1st Workshop Bitcoin Res. (BITCOIN'14)*, Mar. 2014, pp. 105–121.

[184] I. Bentov and R. Kumaresan, "How to use bitcoin to design fair protocols," in *Proc. 34th Annu. Conf. Adv. Cryptol. (CRYPTO'14)*, Aug. 2014, pp. 421–439.

[185] G. D. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-resistant mixing for bitcoin," in *Proc. 13th ACM Workshop Privacy Electron. Soc. (WPES'14)*, Nov. 2014, pp. 149–158.

[186] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications," in *Proc. 20th Annu. ACM Symp. Theory Comput. (STOC'88)*, May 1988, pp. 103–112.

[187] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Proc. 34th IEEE Symp. Secur. Privacy (SP'13)*, May 2013, pp. 397–411.

[188] E. Androulaki and G. O. Karame, "Hiding transaction amounts and balances in bitcoin," in *Proc. 7th Int. Conf. Trust Trustworthy Comput. (TRUST'14)*, Jun. 2014, pp. 161–178.

[189] E. Ben-Sasson *et al.*, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. 35th IEEE Symp. Secur. Privacy (SP'14)*, May 2014, pp. 459–474.

[190] N. van Saberhagen, "Cryptonote v2.0," Tech. Rep., Oct. 2013 [Online]. Available: https://cryptonote.org/whitepaper.pdf

[191] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[192] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT'01)*, Dec. 2001, pp. 552–565.

[193] E. Fujisaki and K. Suzuki, "Traceable ring signature," in *Proc. 10th Int. Conf. Pract. Theory Public-Key Cryptogr. (PKC'07)*, Apr. 2007, pp. 181–200.

[194] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *J. ACM*, vol. 32, no. 2, pp. 374–382, 1985.

[195] D. Dolev, C. Dwork, and L. Stockmeyer, "On the minimal synchronism needed for distributed consensus," *J. ACM*, vol. 34, no. 1, pp. 77–97, 1987.

[196] N. Lynch, "A hundred impossibility proofs for distributed computing," in *Proc. 8th ACM Symp. Principles Distrib. Comput. (PODC'89)*, Aug. 1989, pp. 1–28.

[197] J. Turek and D. Shasha, "The many faces of consensus in distributed systems," *IEEE Comput.*, vol. 25, no. 6, pp. 8–17, Jun. 1992.

[198] J. Aspnes, "Randomized protocols for asynchronous consensus," *Distrib. Comput.*, vol. 16, nos. 2–3, pp. 165–175, 2003.

[199] D. Angluin, M. J. Fischer, and H. Jiang, "Stabilizing consensus in mobile networks," in *Proc. 2nd Int. IEEE Conf. Distrib. Comput. Sensor Syst. (DCOSS'06)*, Jun. 2006, pp. 37–50.

[200] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Tech. Rep., 2014 [Online]. Available: https://ripple.com/files/ripple_consensus_whitepaper.pdf

[201] M. K. Aguilera, "Stumbling over consensus research: Misunderstandings and issues," in *Replication*. New York, NY, USA: Springer, 2010, pp. 59–72.

[202] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Proc. 13th Conf. Adv. Cryptol. (CRYPTO'93)*, Aug. 1993, pp. 139–147.

[203] J. Aspnes, C. Jackson, and A. Krishnamurthy, "Exposing computationally-challenged Byzantine impostors," Dept. Comput. Sci., Yale Univ., Tech. Rep. YALEU/DCS/TR-1332, Jul. 2005.

[204] S. Nakamoto. (2008, Nov.). *Re: Bitcoin P2P e-Cash Paper* [Online]. Available: https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html

[205] A. Miller. (2012, Aug.). *Bitcoin Theory (Byzantine Generals and Beyond)* [Online]. Available: https://bitcointalk.org/index.php?topic=99631.0

[206] R. Chaves, G. Kuzmanov, L. Sousa, and S. Vassiliadis, "Cost-efficient SHA hardware accelerators," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 16, no. 8, pp. 999–1008, Aug. 2008.

[207] M. Bedford Taylor, "Bitcoin and the age of bespoke silicon," in *Proc. 8th Int. Conf. Compilers Archit. Synth. Embedded Syst. (CASES'13)*, Sep. 2013, pp. 1–10.

[208] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *Proc. 25th IET Irish Signals Syst. Conf. (ISSC'14)*, Jun. 2014, pp. 280–285.

[209] N. T. Courtois, M. Grajek, and R. Naik, "The unreasonable fundamental incertitudes behind bitcoin mining," Computing Research Repository, Tech. Rep. abs/1310.7935, 2013.

[210] N. T. Courtois, M. Grajek, and R. Naik, "Optimizing SHA256 in bitcoin mining," in *Proc. 3rd Int. Conf. Cryptogr. Secur. Syst. (CSS'06)*, Sep. 2014, pp. 131–144.

[211] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, "Do the rich get richer? An empirical analysis of the bitcoin transaction network," Computing Research Repository, Tech. Rep. abs/1308.3892, 2013.

[212] C. Dwork, A. Goldberg, and M. Naor, "On memory-bound functions for fighting spam," in *Proc. 23rd Annu. Int. Cryptol. Conf. (CRYPTO'03)*, Aug. 2003, pp. 426–444.

[213] M. Abadi, M. Burrows, M. Manasse, and T. Wobber, "Moderately hard, memory-bound functions," *TOIT ACM Trans. Internet Technol.*, vol. 5, no. 2, pp. 299–327, May 2005.

[214] C. Percival, "Stronger key derivation via sequential memory-hard functions," in *Proc. Tech. BSD Conf. (BSDCan'09)*, May 2009.

[215] M. Hearn. (2014, Jul.). *Mining Decentralisation: The Low Hanging Fruit*, Bitcoin Foundation [Online]. Available: https://bitcoinfoundation.org/2014/07/03/mining-decentralisation-the-low-hanging-fruit/

[216] B. D. M. Lists. (2014). *ASIC-Proof Mining* [Online]. Available: http://sourceforge.net/p/bitcoin/mailman/bitcoin-development/thread/53B714A8.1080603@codehalo.com/

[217] A. Coventry, "Nooshare: A decentralized ledger of shared computational resources," Tech. Rep., Apr. 2012 [Online]. Available: http://web.mit.edu/alex_c/www/nooshare.pdf

[218] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," Tech. Rep., 2013 [Online]. Available: http://primecoin.io/bin/primecoin-paper.pdf

[219] Koooooj. (2013, Nov.). *Good News for Primecoin: One Such Coin That Exists Today That Will Actually Never Have ASICS Developed for it is Primecoin* [Online]. Available: http://redd.it/1ra887

[220] S. D. Lerner, "MAVEPAY, a new lightweight payment scheme for peer to peer currency networks," Tech. Rep., Apr. 2012 [Online]. Available: https://bitslog.files.wordpress.com/2012/04/mavepay1.pdf

[221] J. Bonneau and A. Miller, "Fawkescoin: A cryptocurrency without public-key cryptography," in *Proc. 22nd Int. Workshop Secur. Protocols (SPW'14)*, Mar. 2014.

[222] S. D. Lerner, "MAVE, new lightweight digital signature protocols for massive verifications," Tech. Rep., Apr. 2012 [Online]. Available: https://bitslog.files.wordpress.com/2012/04/mave1.pdf

[223] R. Anderson, F. Bergadano, B. Crispo, J.-H. Lee, C. Manifavas, and R. Needham, "A new family of authentication protocols," *ACM Oper. Syst. Rev.*, vol. 32, no. 4, pp. 9–20, 1998.

[224] N. Houy, "The bitcoin mining game," GATE, Univ. Lyon, Tech. Rep. halshs-00958224, Mar. 2014.

[225] G. Hardin, "The tragedy of the commons," *Science*, vol. 162, no. 3859, pp. 1243–1248, 1968.

[226] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," in *Proc. 9th Workshop Econ. Netw. Syst. Comput. (NetEcon'14)*, Jun. 2014, pp. 34–37.

[227] S. King and S. Nadal, "Ppcoin: peer-to-peer crypto-currency with proof-of-stake," Tech. Rep., Aug. 2012 [Online]. Available: http://peercoin.net/assets/paper/peercoin-paper.pdf

[228] S. King. (2013, Oct.). *Peercointalk's Community Interview With Sunny King #1* [Online]. Available: http://www.peercointalk.org/index.php?topic=2216.0

[229] N. Houy, "It will cost you nothing to 'kill' a proof-of-stake crypto-currency," *Econ. Bull.*, vol. 34, no. 2, pp. 1038–1044, 2014.
[230] D. Larimer, "Transactions as proof-of-stake," Tech. Rep., Nov. 2013.
[231] D. Larimer. (2014). *Delegated Proof-of-Stake (DPOS)*, bitshares [Online]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/
[232] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On bitcoin and red balloons," in *Proc. 13th ACM Conf. Electron. Commerce (EC'13)*, Jun. 2012, pp. 56–73.
[233] G. Pickard *et al.*, "Time critical social mobilization: The DARPA network challenge winning strategy," Computing Research Repository, Tech. Rep. abs/1008.3172, 2010.
[234] L. Ren, "Proof of stake velocity: Building the social currency of the digital age," Tech. Rep., Apr. 2014 [Online]. Available: http://www.reddcoin.com/papers/PoSV.pdf
[235] G. Paul, P. Sarkar, and S. Mukherjee, "Towards a more democratic mining in bitcoins," in *Proc. 10th Int. Conf. Inf. Syst. Secur. (ICISS'14)*, Dec. 2014, pp. 185–203.
[236] D. S. Menasché, L. Massoulié, and D. F. Towsley, "Reciprocity and barter in peer-to-peer systems," in *Proc. 29th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM'10)*, Mar. 2010, pp. 1505–1513.
[237] C. Aperjis, R. Johari, and M. J. Freedman, "Bilateral and multilateral exchanges for peer-assisted content distribution," *IEEE/ACM Trans. Netw.*, vol. 19, no. 5, pp. 1290–1303, Oct. 2011.
[238] A. Back and I. Bentov, "Note on fair coin toss via bitcoin," Computing Research Repository, Tech. Rep. abs/1402.3698, 2014.
[239] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on bitcoin," in *Proc. IEEE 35th Symp. Secur. Privacy (SP'14)*, May 2014, pp. 443–458.
[240] R. Kumaresan, T. Moran, and I. Bentov, "How to use bitcoin to play decentralized poker," in *Proc. ACM 22nd Conf. Comput. Commun. Secur. (CCS'15:)*, Oct. 2015, pp. 195–206.
[241] R. Kumaresan and I. Bentov, "How to use bitcoin to incentivize correct computations," in *Proc. ACM 21st Conf. Comput. Commun. Secur. (CCS '14)*, Nov. 2014, pp. 30–41.
[242] A. Back *et al.* (2014, Oct.). "Enabling blockchain innovations with pegged sidechains," Tech. Rep. [Online]. Available: http://www.blockstream.com/sidechains.pdf
[243] M. Ghosh, M. Richardson, B. Ford, and R. Jansen, "A torpath to torcoin: Proof-of-bandwidth altcoins for compensating relays," in *Proc. 7th Workshop Hot Topics Privacy Enhancing Technol. (HotPETs'14)*, Jul. 2014.
[244] R. Jansen, A. Miller, P. Syverson, and B. Ford, "From onions to shallots: Rewarding tor relays with tears," in *Proc. 7th Workshop Hot Topics Privacy Enhancing Technol. (HotPETs'14)*, Jul. 2014.
[245] A. Biryukov and I. Pustogarov, "Proof-of-work as anonymous micropayment: Rewarding a tor relay," in *Proc. 19th Int. Conf. Financial Cryptogr. Data Secur. (FC'15)*, Jan. 2015, pp. 445–455.

Florian Tschorsch received the B.S. and M.S. degrees in computer science (with a focus on computer networks as major and cultural studies as minor subject) from Heinrich Heine University (HHU), Düsseldorf, Germany, in 2009 and 2010, respectively. He is currently a Researcher with Humboldt University of Berlin, Berlin, Germany. His research interests include anonymity networks in general and their transport protocol design in particular. Lately, digital currencies attracted his growing interest as well. For the period of his Master's studies, he received a scholarship from HHU Düsseldorf and the state of North Rhine-Westphalia.

Björn Scheuermann received the B.S. degree in mathematics and computer science and the Diploma degree (German M.S. equivalent) in computer science from the University of Mannheim, Mannheim, Germany, in 2004, and the Ph.D. degree in computer science from Heinrich Heine University, Düsseldorf, Germany, in 2007. He became a Junior Professor with Heinrich Heine University in 2008. He is a Professor and the Chair of Computer Engineering with Humboldt University of Berlin, Berlin, Germany. After positions of Associate Professor and the Head of the Telematics Group, University of Würzburg, Würzburg, Germany, and an Associate Professor of Practical Computer Science/IT Security with the University of Bonn, Bonn, Germany, he joined Humboldt University in October 2012. His research interests include performance, design, and security aspects of computer networks. Within this field, he works, for instance, on digital currencies, performance aspects of privacy-preserving communication, and network hardware design (Photo: (c) WISTA Management GmbH).