Micro Structure of Bitcoin Transaction Process

Gisha George
Department of Computer Science and Applications
St.Mary’s College,
Trichur

Abstract-- Bitcoin is a form of digital currency, created and held electronically which are not printed. Bitcoin is a purely online virtual currency, unbacked by either physical commodities or sovereign obligation; instead, it relies on a combination of cryptographic protection and a peer-to-peer protocol for witnessing settlements. Bitcoin is an online communication protocol that facilitates virtual currency including electronic payments. Since its inception in 2009 by an anonymous group of developers (Nakamoto, 2008), Bitcoin has served approximately 41.8 million transactions between 62.8 million accounts. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. Bitcoin is a complex scheme, and its implementation involves a combination of cryptography, distributed algorithms, and incentive driven behaviour. Moreover, recent developments suggest that Bitcoin operations may involve risks whose nature and proportion are little, if at all, understood. Bitcoin is the world’s first decentralized digital currency, allowing the easy storage and transfer of cryptographic tokens. The purpose of this paper is to provide the necessary technical background for understanding Bitcoin's basic operations. We discuss the micro-structure of the Bitcoin transaction process. The discussion pays special attention to the use of cryptography in the Bitcoin protocol. Specifically, the protocol uses cryptographic algorithms for the security of transactions and for the implementation of distributed maintenance of a public ledger.

I. INTRODUCTION

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed time stamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes. Bitcoin has often been compared to cash as transactions are near-instantaneous and non-refundable. However Bitcoin goes beyond the scope of cash, allowing truly global transactions, processed at the same speed as local ones. It offers a public transaction history and it introduces many new and innovative uses such as smart properties, micropayments, contracts and escrow transactions for dispute mediation.

II. BITCOIN DESIGN PRINCIPLES

Many Bitcoin design principles are familiar from the Internet’s architecture. Bitcoin’s rules were designed by engineers, not lawyers or regulators. Furthermore, Bitcoin emphasizes decentralization. Rather than store transactions on any single server or set of servers, Bitcoin uses a distributed transaction log with mechanisms to reward honest participation, bootstrap acceptance by early adopters, and guard against concentrations of power. Anyone can create an account, without charge and without any centralized vetting procedure or requirement to provide a real name.

III. ENABLING TECHNOLOGIES

The Bitcoin core consists of the protocol (including an opensource reference implementation), many globally distributed computers connected in a peer-to-peer network on top of standard Internet protocols, and the state of the system, which is encoded in a distributed data structure that holds the system’s transaction ledger. The Bitcoin core is surrounded by an ecosystem of agents who use Bitcoin and offer related services, as discussed in subsequent sections. By design, Bitcoin lacks a centralized authority to distribute coins or track who holds which coins. Consequently, the process of issuing currency, verifying validity, and confirming balances is considerably more difficult than in classic bookkeeping systems. The primary innovation in Bitcoin’s design is its ability to perform these functions without a centralized authority. Bitcoins are actually recorded as transactions. For instance, some user Charlie does not simply “hold” three bitcoins. Rather, Charlie participates in a publicly verifiable transaction showing that he received three bitcoins from Bob. Charlie was able to verify that Bob could make that payment because there was a prior transaction in which Bob received three bitcoins from Alice. Indeed, each bitcoin can readily be traced back through all transactions in which it was used, and thus to its start of its circulation. A consequence of decentralized verification and consensus is that all transactions are readable by everyone in records stored in a widely replicated data structure. In general, transactions are ordered recursively by having the input of a transaction (roughly, the source of funds) refer to the output of a previous transaction (e.g., Bob pays Charlie using bitcoin he received from Alice).
A. The Role of Cryptography

Whereas most encryption conceals information from public scrutiny, Bitcoin uses cryptography for the fundamentally different purpose of enforcing system fairness. First, Bitcoin uses private keys to authorize spending money: Only with an account holder’s private key may funds from that account be spent. Digital signatures then allow others to verify that a given message, purportedly spending funds from a given account, in fact occurred with permission from the authorized user of that account. Notice that no centralized bookkeeper is needed; no single party need know all account holders. Rather, the system is open, and verify transactions is decentralized identities, known as a Sybil attack (Douceur, 2002). In response, the Bitcoin protocol makes it costly to submit fake votes. Consistent with the Internet’s open architecture, anyone can connect multiple computers to the Bitcoin system. But voting requires first working to solve a mathematical puzzle that is computationally hard to solve (although easy to verify). Solving the puzzle provides “proof of work”; in lieu of “one person, one vote,” Bitcoin thus implements the principle of “one computational cycle, one vote.”

IV. BITCOIN: TRANSACTIONS

Figure 1 shows a diagram of payments on the Bitcoin users’ network. The nodes are entities and the directed arrows depict payments in bitcoin. As the diagram suggests, the entities transact directly, that is, in contrast to most traditional payment systems where various parties, such as banks, processors, and networks, sit between the payer and payee, there is no designated intermediary in Bitcoin. Each transaction is chronologically recorded in a public ledger, called the block chain, by participants in the network. There is a reward for recording transactions in the block chain, and the participants in the Bitcoin system compete (by solving a computationally intensive cryptographic problem) to make records. A well-defined process, which guarantees consensus, elects the winning participant and the block chain is updated. Importantly, each participant keeps a copy of the ledger, and the consensus of the incremental changes guarantees that these copies are identical. Thus, the verification and the record keeping of transactions is decentralized.

Note:
There are four entities A, B, C and D, transacting directly with each other, i.e. with no intermediary. In addition, the diagram shows the possibility of B transacting with itself. All transactions are chronologically recorded in a public ledger called a block chain.

The Bitcoin transaction process is fairly complex and computer scientists are actively investigating aspects of its security, privacy, distributed control and incentive schemes. For example, although Bitcoin is referred to as a near-instantaneous payment system (on average it takes 10 minutes to process a transaction), some have questioned its suitability for fast payments.

A. The Bitcoin transaction process

We now turn to describe the Bitcoin transaction process. Because cryptographic algorithms have implications for the security and privacy of Bitcoin’s implementation, we start with a brief overview. Then we turn to describe a transaction record on the public ledger. Because the public ledger is the main source of information for the activity in the Bitcoin system, its structure naturally determines the scope of our empirical analysis. Finally, we present the process of executing a payment between two parties using the Bitcoin network.

1. Cryptographic basics.

The Bitcoin transaction process uses cryptography to verify transactions, process payments, and control the supply of bitcoins. The particular cryptographic schemes implemented in the Bitcoin protocol are not new and, in fact, are used in a wide range of information security applications. Because the topic is somewhat esoteric in economic applications and, more importantly, because we
believe that cryptographic and distributed algorithms may have applications to a broader set of economic practices reaching beyond the payment industry, we review at some length the principles of their operation below.

Bitcoin relies on two cryptographic schemes: digital signatures and cryptographic hash functions. Briefly, the former enables the exchange of accurate (payment) instructions between the parties of a transaction, and the latter is used to enforce discipline in writing transaction records in the public ledger. Neither of these schemes is unique to Bitcoin; they are widely used to secure commercial and government communications. For the sake of completeness, we provide a brief outline below.

Figure 2: Public Key Encryption

2. **Digital signatures**

Digital signatures are a way to authenticate a message between a sender and a receiver in a way that ensures:

(i) authentication: the recipient can verify that the message came from the sender,

(ii) non-repudiation: the sender cannot deny sending the message,

(iii) integrity: the message has not been tampered with. The implementation of digital signatures involves public key encryption, where a pair of keys–public and private–are generated with certain desirable properties.

Figure 2 illustrates the process of digitally signing a message (or a unit of data). The “sign” function combines the message with the private key of the sender to produce Signature. The process of obtaining cisor effect signing the message with the identity of the sender, her private key pa. The intended recipient then receives the signed message (the message together with its signature). Before accepting the message, the receiver verifies the authenticity of its sender by comparing the message and the public key of the sender. This is done by the verify function that takes as inputs the signed message (mandc) together with the public key pk and produces a binary output state: accept or reject. The sign and verify functions are publicly accessible.

The Bitcoin protocol employs the above scheme to sign transaction messages. In particular, transaction messages signed with the private key pa and then broadcast to the Bitcoin network. All members of the Bitcoin system can verify that this transaction came from the owner of public key Pk by taking the message m, signature c, and public key pk and running the verification algorithm.

3. **Cryptographic hash function**

In general, a cryptographic hash function takes as input a string of arbitrary length and returns a string with predetermined length. We will refer to the input as message m and the output as hash h.

- **Pre-image resistance.** Given a hash hit is difficult to find a message m such that hash(m) = h.
- **Second pre-image resistance.** Given message m1 it is difficult to find a different message m2 such that hash(m1) = hash(m2). In other words, changing the message leads to changing the hash.
- **Collision resistance.** It is difficult to find two different messages m1 and m2 such that hash(m1) = hash(m2).

Another desirable property of the hash function is that even small changes in message m are likely to change hash h significantly. This makes it very unlikely for someone to be able to infer the content of the message from the hash. In summary, the output of hash functions is very much unpredictable (looks random) although it is deterministic. Bitcoin mainly uses SHA-256, a type of Secure Hash Algorithm (SHA-2) designed by the National Security Agency and published by the National Institute of Standards and Technology.
V. A BITCOIN TRANSACTION

A. Bitcoin ownership and Bitcoin addresses

From a technical point of view, bitcoins reside in what is known in the bitcoin system as bitcoin addresses. The ownership of a particular amount of bitcoins reduces to the capability of sending payments (over the Bitcoin network) from the bitcoin address(es) with which these bitcoins are being associated. The capability of sending payments from Bitcoin addresses is controlled via digital signatures (we introduced above) that involve pairs of a public key $p_k$ and a private key $p_a$. In particular, each bitcoin address is indexed by an unique public ID|an alpha numeric identifier which, in fact, corresponds to the public key $p_k$. The private key $p_a$, which is the counterpart of $p_k$, gives control over the bitcoins held in this address. Specifically any payment (message) involving this address as a sending address has to be signed with the proper private key to be considered valid. In simple words, owning the bitcoins in a given bitcoin address amounts to knowing the private key which corresponds to the public ID (i.e. the key $p_k$) of that address.

At any point in time every bitcoin address is associated with a given bitcoin balance which is, in effect, public information. This is the case because any participant in the Bitcoin network can deduce the bitcoin balances following a given transaction history that is recorded in the public ledger. In particular, every existent or proposed (newly broadcast) transaction can be checked for consistency against the preceding history of transactions i.e. it can be verified that the amounts transacted are available in the corresponding bitcoin addresses.

1. A transaction on the block chain

Entities engage in transactions on the Bitcoin network through a collection of bitcoin addresses, figuratively called their wallet - a set of bitcoin addresses owned by a single entity.

In particular, each transaction record involves one or more sending addresses and one or more receiving addresses together with how much each of these addresses send and receive. Figure 3 reflects this description. In the figure, there are two sending addresses (sending 10 and 55 BTC, respectively) and two receiving addresses (receiving 60 and 5 BTC, respectively).

VI. THE BITCOIN TRANSACTION PROCESS

The Bitcoin transaction process has mechanisms in place which guarantee that (a) the verification of each transaction is distributed among multiple participants in the network, (b) the recording of each transaction is time discretized, i.e. transactions are linearly ordered with consecutive time stamps, (c) the participants in the payment network compete and are rewarded for recording a transaction, and (d) multiple nodes cross-check each transaction record.
A. **Initiating a transaction**

Suppose that Alice would like to send Bob 1 bitcoin using the Bitcoin network. To do that, both Alice and Bob need to have bitcoin addresses. Call these address$_{Alice}$ and address$_{Bob}$. Then Alice needs to issue and (digitally) authenticate a message of the sort

“address$_{Alice}$ is sending address$_{Bob}$ 1 bitcoin.”

Once Alice signs a transaction message, with her private key and broadcasts it, every one on the Bitcoin network can verify that it was Alice who issued the message and the message has not been tampered with. Moreover, as we pointed out earlier, the digital signatures ensure that no one else could have signed this message, i.e. Alice cannot deny having signed it.

**B. Verifying a transaction**

Before executing a transaction (which amounts to recording the transaction on the ledger) the Bitcoin protocol has to verify two aspects of the transaction message: “address$_{Alice}$ is sending address$_{Bob}$ 1 bitcoin”. First, is it Alice who has broadcast the transaction message? As we discussed, the digital signature scheme guarantees that indeed only the owner of the private key for this address could have signed the message. Second, are there enough funds at the sending address to guarantee that the transaction can be completed? Below we discuss how the Bitcoin protocol handles this in a hypothetical scenario, deferring the complexity of the underlying mechanisms for a moment.

Suppose there were a single designated participant who maintains all account balances and receives each transaction request. In addition, suppose that the protocol requires that transactions are accepted sequentially, for example, every day there is at most one transaction accepted for verification and clearance. It would have then been trivial in terms of effort for this designated entity to verify the integrity of the transaction request and the availability of funds, and then proceed to record the transaction. Moreover, the fact that transaction requests are accepted sequentially guarantees that duplicated messages and double spending can be readily detected. Note that this hypothetical scenario does not require the books to be either public or private. More generally, although maintenance of records and verification of transactions are core functions of all electronic payment systems, these functions typically occur through private ledgers maintained by trusted third parties.

Decentralized systems such as Bitcoin replace third party intermediaries and the records kept by them with the public ledger maintained by a distributed information system. In particular, the public ledger. Note that Bob's authorization is not needed for initiating and eventually recording the transaction.

In payment card systems, for example, banks maintain their own records of the balances of their account holders. These banks, in turn, use the functionality and record-keeping systems of payment card networks to exchange information needed to allow the transfer of balances between agents in the system allows for decentralized approach to transaction message verification.

**C. Blockchain update**

After the initial verification of a signed transaction message, a set of participants in the Bitcoin network compete to record the transaction in the block chain. First, the competing nodes group transactions, which have been broadcast since the last record on the block chain, in a block of transactions. The block then is used to define a computationally intensive task (to be discussed below). The winner of the competition is the node who first solves this task. Once the winner is determined, the transaction record is completed. The winning node is entitled to make the record and collect the reward. It remains to describe the computationally intensive task that defines the competition for recording a block of transactions. The task on which the nodes compete builds on one of the cryptographic schemes we discussed above: the hash function. First, a block of newly broadcast transactions is used as an input into the cryptographic hash function to obtain a hash called a digest. This digest together with announce-Jan alphabetic-numeric string—and the hash of the previous block—are input into another hash function that delivers a block chain hash of the new block. The task that nodes need to solve comprises finding a nounce such that the block chain hash of the new block has certain properties. The first competing node to find a desirable nounce broadcasts this information to the rest of the network, and the ledger is updated. This scheme is an implementation of Hash cash, a type of proof-of-work system, whose goal is to ensure that computers use a defined number of computational resources to complete some. The nodes that carry out the proof-of-work process are known in the Bitcoin ecosystem as miners. These miners are incentivized to spend computational resources in this process by an award built into the Bitcoin protocol. For the most part the award is a predetermined amount of newly generated bitcoins. The rest of the award, which currently is of much lower value, is voluntary transaction fees that are paid by the initiators of transactions to the miners in order to process their transactions. The initial idea was that these voluntary fees would replace the coin-generation reward to incentivize miners when that amount goes to zero.

**ACKNOWLEDGEMENT**

Thank you for all my subordinates.

**REFERENCES**

[1] Introduction to data mining with case studies - G.K. GUPTA, Professor of Computer Science, Monash University, Clayton, Australia.