2023/2024 S2

Bitcoin II

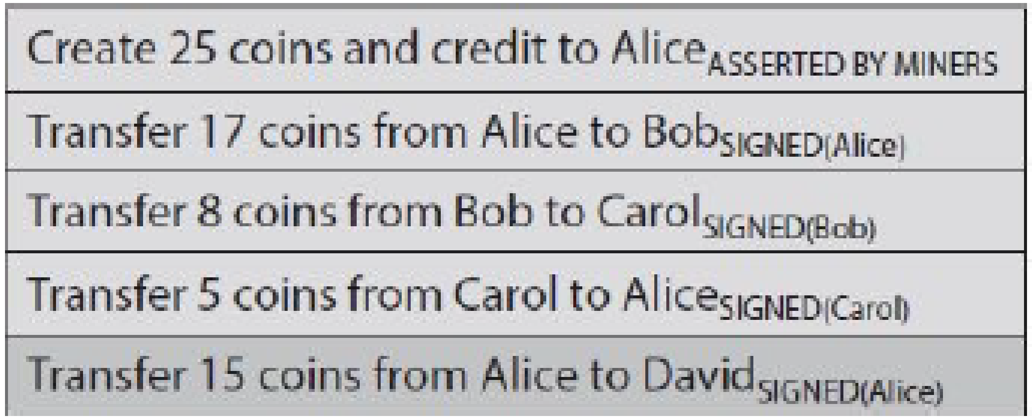
Dr. Hui Gong (h.gong1@westminster.ac.uk)

UNIVERSITY OF WESTMINSTER

Mechanics of Bitcoin

Mechanics of Bitcoin

Bitcoin Transactions



Create 25 coins and credit to Alice$_{\text{ASSERTED BY MINERS}}$
Transfer 17 coins from Alice to Bob$_{\text{SIGNED(Alice)}}$
Transfer 8 coins from Bob to Carol$_{\text{SIGNED(Bob)}}$
Transfer 5 coins from Carol to Alice$_{\text{SIGNED(Carol)}}$
Transfer 15 coins from Alice to David$_{\text{SIGNED(Alice)}}$

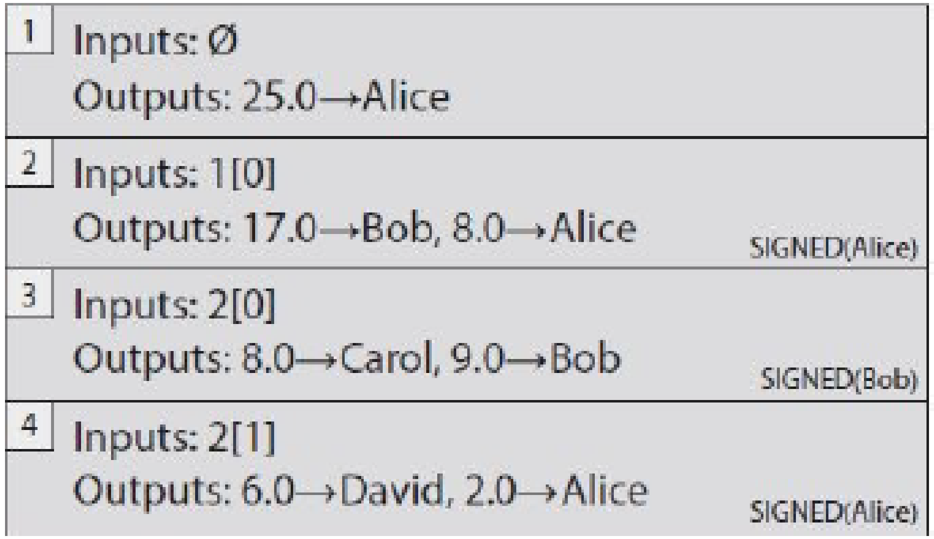
An account-based ledger.

A transaction would be something like “move 17 coins from Alice to Bob,” and it would be signed by Alice. That’s all the information in the ledger about the transaction. In Figure, after Alice receives 25 coins in the first transaction and then transfers 17 coins to Bob in the second, she’d have 8 bitcoins left in her account.

Does Alice have the 15 coins that she’s trying to transfer to David?

To figure this out, you’d have to track every transaction affecting Alice back in time to determine whether her net balance when she tries to transfer 15 coins to David is greater than 15 coins.

Let’s now work our way through Figure below.



1	Inputs: Ø Outputs: 25.0→Alice	
2	Inputs: 1[0] Outputs: 17.0→Bob, 8.0→Alice	SIGNED(Alice)
3	Inputs: 2[0] Outputs: 8.0→Carol, 9.0→Bob	SIGNED(Bob)
4	Inputs: 2[1] Outputs: 6.0→David, 2.0→Alice	SIGNED(Alice)

A transaction-based ledger. This is the type of ledger

Bitcoin

Mechanics of Bitcoin

The Bitcoin Network

Bitcoin network is a peer-to-peer network inheriting many ideas from other peer-to-peer networks that have been proposed for all sorts of other purposes. In the Bitcoin network, all nodes are equal. There is no hierarchy - no special nodes or master nodes. It runs over TCP and has a random topology, where each node peers with other random nodes. New nodes can join at any time. In fact, you can download a Bitcoin client today, spin up your computer as a node, and it will have rights and capabilities equal to those of every other node on the Bitcoin network.

What is the network good for? To maintain the block chain, of course. So to publish a transaction, we want the entire network to hear about it. This happens through a simple *flooding* algorithm, sometimes called a *gossip protocol*.

When nodes hear about a new transaction, how do they decide whether they should propagate it? There are four checks.

1. The first and most important check is transaction validation—the transaction must be valid with the current block chain. Nodes run the script for each previous output being redeemed and ensure that the scripts return true.
2. Second, they check that the outputs being redeemed haven't already been spent.
3. Third, they won't relay an already-seen transaction, as mentioned earlier.
4. Fourth, by default, nodes only accept and relay standard scripts based on a small whitelist of scripts.

The Bitcoin Network - Double Spend

Since the network has latency, it's possible that nodes will end up with different versions of the pending transaction pool. This becomes particularly interesting and important when a double spend is attempted. Suppose Alice attempts to pay the same bitcoin to both Bob and Charlie, and she sends out two transactions at roughly the same time. Some nodes will hear about the Alice → Bob transaction first, while others will hear about the Alice → Charlie transaction first. When a node hears about either transaction, it adds the transaction to its transaction pool. If it hears about the other one later, the node will detect a double spend. The node then drops the latter transaction and won't relay or add it to its transaction pool. As a result, the nodes will temporarily disagree on which transactions should be put in the next block. This is called a "race condition."

The good news is that this situation is easily handled. Whoever mines the next block will essentially break the tie and decide which of those two pending transactions should be put permanently into a block. **Let's say the Alice → Charlie transaction makes it into the block.** When nodes with the Alice → Bob transaction hear about this block, they'll drop the transaction from their memory pools, because it is a double spend. When nodes with the Alice → Charlie transaction hear about this block, they'll drop that transaction from their memory pools, because it's already in the block chain. So there will be no more disagreement once this block propagates through the network.

Since the default behaviour is for nodes to retain whatever they hear first, network position matters.

Limitations and Improvements

Storage Requirements

Fully validating nodes must stay permanently connected so as to hear about all Bitcoin transactions. The longer a node is offline, the more catching up it will have to do when it rejoins the network. Such nodes also have to store the entire block chain and need a good network connection to be able to hear every new transaction and forward it to peers. The storage requirement is currently in the tens of gigabytes (@2014. NOW, We need more than 500G.), well (still) within the abilities of a single commodity desktop machine.

Changing the Protocol

How can we go about introducing new features into the Bitcoin protocol? In reality, though, it is quite complicated. In practice, it's impossible to assume that every node would upgrade. Some nodes in the network would fail to get the new software or fail to get it in time. The implications of having most nodes upgrade while some nodes are running the old version depends very much on the nature of the changes in the software.

HARD FORKS: One type of change that we can make introduces new features that were previously considered invalid. (BCH, BSV)

SOFT FORKS: A second type of change that we can make to Bitcoin is to add features that make validation rules stricter.

How to Store and Use Bitcoins

How to Store and Use Bitcoins

Simple Local Storage

Storing bitcoins is all about storing and managing Bitcoin secret keys.

When figuring out how to store and manage keys, three goals should be kept in mind.

1. The first is availability: being able to actually spend your coins when you want to.
2. The second is security: making sure that nobody else can spend your coins. If someone gets the power to spend your coins, they could send your coins to themselves, and then you no longer have the coins.
3. The third goal is convenience: managing your keys should be relatively easy. As you can imagine, achieving all three simultaneously can be a challenge.

Different approaches to key management offer different trade-offs between availability, security, and convenience.

The simplest key management method is to store them in a file on your own local device: your computer, phone, or some other kind of gadget that you carry, own, or control.

In other words, storing your private keys on a local device, especially a mobile device, is a lot like carrying around money in your wallet or in your purse. It’s useful to have some spending money, but you don’t want to carry around your life savings, because you might lose it, or somebody might steal it. So what you typically do is store a little bit of information—a little bit of money—in your wallet and keep most of your money somewhere else.

Encoding Keys

Base 58

To encode an address as a text string, we take the bits of the key and convert them from a binary number to a base-58 number. Then we use a set of 58 characters to encode each digit as a character; this is called “base-58 notation.” Why 58? Because that’s the total number of available uppercase letters, lowercase letters, and digits that can be used as characters (minus a few that might be confusing or look like another character).

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

The address that received the very first Bitcoin block reward in the genesis block, base-58 encoded.

QR code

A simple kind of two-dimensional barcode. The advantage of a QR code is that you can take a picture of it with a smartphone, and wallet software can automatically turn the barcode into a sequence of bits that represents the corresponding Bitcoin address.

How to Store and Use Bitcoins

Hot and Cold Storage

As just mentioned, storing bitcoins on your computer is like carrying money around in your wallet or your purse. This is called hot storage. It’s convenient but also somewhat risky. In contrast, cold storage is offline. It’s locked away somewhere, it’s not connected to the Internet, and it’s archival. So cold storage is safer and more secure, but of course not as convenient as hot storage.

To have separate hot and cold storage, obviously you need to have separate secret keys for each—otherwise, the coins in cold storage would be vulnerable if the hot storage is compromised. You’ll want to move coins back and forth between the hot side and the cold side, so each side will need to know the other’s addresses, or public keys.

Cold storage is not online, and so the hot storage and the cold storage won’t be able to connect to each other across any network. But the good news is that cold storage doesn’t have to be online to receive coins—since the hot storage knows the cold storage addresses, it can send coins to cold storage at any time. At any time if the amount of money in your hot wallet becomes uncomfortably large, you can transfer a chunk of it to cold storage, without putting your cold storage at risk by connecting to the network. Next time the cold storage connects, it will be able to receive from the block chain information about those transfers to it, and then the cold storage will be able to manipulate those coins.

Hierarchical Deterministic Wallets/ Brain Wallet/ Paper Wallet

Splitting And Sharing Keys: Multisignatures

Instead of taking a single key and splitting it, Bitcoin script directly allows you to stipulate that control over an address be split among different keys. These keys can then be stored in different locations, and the signatures produced separately. Of course, the completed, signed transaction will be constructed on some device, but even if the adversary controls this device, all she can do is to prevent it from being broadcast to the network. She can't produce valid multisignatures of some other transaction without the involvement of the other devices.

As an example, suppose that Andrew, Arvind, Ed, Joseph, and Steven, the authors of this book, are cofounders of a company, and the company has a lot of bitcoins. We might use multisignatures to protect our large store of bitcoins.

Each of the five of us will generate a key pair, and we'll protect our cold storage using 3-out-of-5 multisignatures, which means that three of us must sign to create a valid transaction.

As a result, we know that we're relatively secure if the five of us keep our keys separately and secure them differently. An adversary would have to compromise three out of the five keys. If one or even two of us go rogue, they can't steal the company's coins, because you need at least three keys to do that. At the same time, if one of us loses our key or gets run over by a bus and our brain wallet is lost, the others can still get the coins back and transfer them to a new address and resecure the keys. In other words, multisignatures help you to manage large amounts of cold-stored coins in a way that's relatively secure and requires action by multiple people before anything drastic happens.

How to Store and Use Bitcoins

Online Wallets and Exchanges

Online Wallets

An online wallet is like a local wallet that you manage yourself, except the information is stored in the cloud, and you access it using a web interface on a computer or an app on a smartphone.

Bitcoin Exchanges

Bitcoin exchanges are businesses that—at least from the user interface standpoint—function in a similar way to banks. They accept deposits of bitcoins and will, just like a bank, promise to give them back on demand later.

Three Types of Risks

1. The first risk is the risk of a bank run. A run occurs when many people show up at the same time and demand their money back.
2. The second risk is that the owners of the banks might just be crooks running a Ponzi scheme.
3. The third risk is that of a hack: the risk that someone—perhaps even an employee of the exchange—will manage to penetrate the security of the exchange.

Example: Mt. Gox

How to Store and Use Bitcoins

Transaction Fees

When a transaction is put into the Bitcoin block chain, that transaction might include a transaction fee. Recall that **a transaction fee is** just defined to be the **difference** between **the total value of coins that go into a transaction minus the total value of coins that come out**. So, there is a cost—both to the peer-to-peer network and to the miners—of incorporating your transaction. The idea of a transaction fee is to compensate miners for those costs they incur to process your transaction. Nodes don’t receive monetary compensation in the current system, although running a node is of course far less expensive than being a miner. Generally you’re free to set the transaction fee to whatever you want it to be. You can pay no fee, or you can set the fee quite high. In general, if you pay a higher transaction fee, your transaction will be relayed and recorded more quickly and reliably.

The default transaction fees are as follows. No fee is charged if a transaction meets all three of these conditions:

1. the transaction is less than 1000 bytes in size,
2. all outputs are 0.01 BTC or larger, and
3. the priority is high enough.

Priority is defined as (sum of [input age · input value])/(transaction size). In other words, consider all inputs to the transaction, and for each one, compute the product of that input’s age and its value in bitcoins, and add up all those products. If you meet these three requirements, then your transaction will be relayed and recorded in the block chain without a fee. Otherwise a fee is charged. That fee is about 0.0001 BTC (around $2.5 now) per 1,000 bytes.

Bitcoin II

References to read

[1] Rauchs, M. and Hileman, G., 2017. Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance Reports.

[2] Rauchs, M., Blandin, A., Bear, K. and McKeon, S.B., 2019. 2nd Global Enterprise blockchain benchmarking study.

[3] Blandin, A., Pieters, G.C., Wu, Y., Dek, A., Eisermann, T., Njoki, D. and Taylor, S., 2020. 3rd Global Cryptoasset Benchmarking Study.