Network Security

Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay

Week - 11
Lecture - 61
The Bitcoin Cryptocurrency: Part 1

Hello, we read about cryptocurrencies such as Bitcoin in the news all the time. So, in the last several years, there has been an explosion in the use of cryptocurrencies. In this lecture and the next few lectures, we'll discuss cryptocurrencies. We'll also discuss the basic concept on which cryptocurrencies are based, that is, blockchain. Our focus will be on one of the most popular cryptocurrencies, namely Bitcoin.

So, the motivation for cryptocurrencies and Bitcoin is the following. Bitcoin and other cryptocurrencies, such as Litecoin and Ethereum and so on, they are being extensively used by users around the world. Here is a useful statistic. It has been estimated that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, and most of them were using Bitcoin. So, a cryptocurrency wallet is a place where units of cryptocurrencies can be stored.

So, there were a large number of unique users using cryptocurrency wallets, as the statistic shows. What is a cryptocurrency? How is it different from usual currencies such as rupees and dollars? So, in a cryptocurrency, cryptographic techniques such as hash functions are used to regulate the generation of units and to implement transfers. So, whenever new units of a cryptocurrency such as Bitcoin are generated, that is done using a cryptographic hash function.

And cryptographic techniques such as public keys are also involved in the transfer of cryptocurrency units. These are not issued by a central authority such as a bank, unlike regular currencies such as rupees and dollars. Some example uses of cryptocurrencies are as follows. Cryptocurrencies can be used as an investment. For example, if someone invests in Bitcoin and the price of Bitcoin goes up, then they gain.

So, it can be used as an investment. Cryptocurrencies can be used to implement international monetary transfers. These transfers can be done fast and with low transaction

fees. Compared to alternative means such as using a bank for achieving international monetary transfers, cryptocurrencies can implement transfers faster and with lower transaction fees. Another example is as an alternative source of wealth that cannot be frozen by authorities such as governments.

For example, if a particular person is accused of a crime, then that person's assets, such as bank accounts, properties, real estate, and so on, can be frozen by authorities such as governments, but cryptocurrencies cannot be similarly frozen. So, one example use of cryptocurrency is as an alternative source of wealth that cannot be frozen by authorities. Bitcoin is a decentralized system based on blockchain technology. By a decentralized system, we mean that there is no central authority, such as a bank, which regulates the generation and transfer of Bitcoin. Instead, it is implemented through a peer-to-peer network that is several different nodes in the internet.

They run Bitcoin software and are connected to each other. Bitcoin is a decentralized system which is implemented through the use of a large number of users who are at different locations. So, what is blockchain? Blockchain is a database of all past transactions, which includes the creation of new bitcoins and the transfers of bitcoins. So, as the name suggests, blockchain is a list of several blocks, and each block stores some past transactions; that is, it records whenever new Bitcoins are created and whenever Bitcoins are transferred from one party, say Alice, to another party, Bob.

These transactions are recorded in blocks of the blockchain. So, a blockchain is a list of several blocks. It is difficult to modify transactions stored in it. So, for example, if Bob pays Alice a certain number of bitcoins and that transaction is stored in the blockchain, and later on Bob wants to undo that transaction so that he can spend the same currency again, then that is difficult to do. So, it is difficult to modify transactions that are stored in the blockchain.

A copy of the blockchain is stored at multiple nodes connected to the internet. There are multiple nodes which are computers. They are connected to the internet and a copy of the blockchain is stored at multiple nodes. No one node can unilaterally modify the blockchain. If one node were to modify the blockchain, then that would be detected because a copy of the blockchain is also stored at many other nodes. We'll study Bitcoin in detail.

As we have already mentioned, there are several cryptocurrencies, including Litecoin and Ethereum, but Bitcoin is one of the more popular ones. So, we'll study Bitcoin in detail, and our study of Bitcoin will introduce us to the concept of blockchain and

cryptocurrencies. So, it will become easy to understand other cryptocurrencies such as Litecoin and Ethereum as well. So, recall that currency is a system for storing and transferring value. For example, when we have 10 rupees, then the value of 10 rupees is stored in that currency, and similarly, we can transfer value by transferring currency.

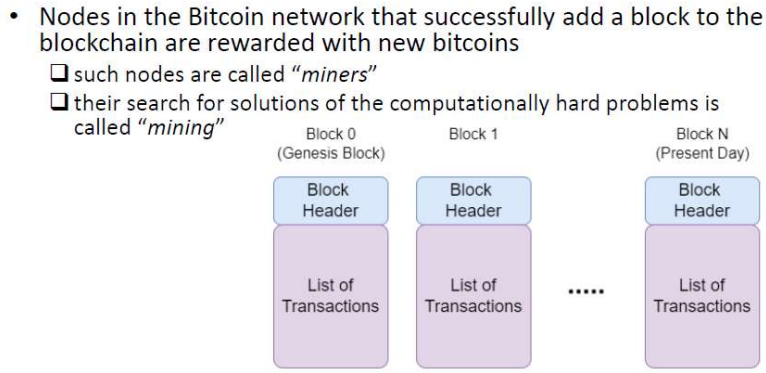
Bitcoin is a cryptocurrency. The notion of ownership of its units is established through cryptography. Also, cryptographic techniques are used to regulate the generation of units and implement their transfer. So, as we mentioned earlier cryptographic hash functions are used to regulate the generation of units and public keys are used to implement their transfer. The transfer of bitcoins between different people requires the sender to provide a digital signature proving the ownership of the bitcoins being transferred.

We discussed digital signatures earlier. So, for example, if Alice wants to transfer some Bitcoins to Bob, in that case, Alice has to provide a digital signature proving ownership of the Bitcoins that she's transferring to Bob. The Bitcoin system is decentralized; it is a peer-to-peer (P2P) network. This P2P network performs the creation of new Bitcoins and the recording of all Bitcoin transfers, called transactions. Anyone can join the Bitcoin network by running open-source software that is freely available on the internet.

So, Bitcoin with a capital 'B' is used to denote the cryptocurrency system, and bitcoin with a small 'b' is used to denote units of the cryptocurrency. So, for example, when we say '100 bitcoins,' then that is bitcoin with a small 'b.' When we refer to the cryptocurrency system, that is Bitcoin with a capital 'B.' So, what are the components of the Bitcoin cryptocurrency system? One component is a system for generating addresses where bitcoins can be received and stored. So, for example, if Alice wants to transfer some bitcoins to Bob, in that case Bob requires an address where those bitcoins can be received and subsequently stored. Another component is a method for ensuring that only the rightful owner of bitcoins stored in an address can move them to a new address.

For example, if Bob owns some bitcoins, then it should not be possible for an intruder like Trudy to move the bitcoins to another address. Another component of Bitcoin is a database of all past transactions, which is used to prevent double spending of the bitcoins stored in an address. Suppose Bob transfers some bitcoins to Alice; in that case, the transaction in which Bob transferred, say, one bitcoin to Alice, that transaction is stored in the database, in particular in the blockchain. So, later on, Bob cannot spend the same one bitcoin again. This database of all past transactions that helps in preventing double spending of Bitcoins.

This database is called the blockchain. What are the corresponding components of a traditional banking system? Corresponding to the first one, we have bank accounts. They are addresses where currency can be received and stored. Corresponding to the second one, we have different means, such as checks, which need to be signed, online banking transfers, for which we require a password (and sometimes an OTP), and debit cards, which require ownership of the card, and so on.



These correspond to methods for ensuring that only the rightful owner of the currency stored in an address can move it to a new address. So, this is the analog of the second component in the context of a traditional banking system. And for the third one, we have the following: each withdrawal, deposit, and transfer is recorded in the bank's database. So, this prevents someone from double spending some currency. Because each time a user spends some currency, then that transfer is recorded in the bank's database.

So, that prevents the user from double spending. So, this is the analog of the third component. However, it's much more challenging to implement these functions in the environment in which Bitcoin operates compared to a traditional banking system. The reason is that the Bitcoin infrastructure is provided by a peer-to-peer network. There are many entities at different locations, and they have to jointly perform these functions.

That is more challenging than in the case of a bank, where these functions are performed in a centralized manner. And another challenge in the case of Bitcoin is that some participants can be malicious. So, recall that anyone is free to join the Bitcoin network by using freely available software. So, some malicious participants can also join the network. So, that makes the implementation of these functions even more challenging.

So, we will now discuss the important concept of mining. We have mentioned that the blockchain consists of a linked list, or a chain of blocks, as the name suggests. So, the

blockchain is shown here. So, it is a linked list consisting of a large number of blocks, and the number of blocks keeps on growing every day. Each block consists of a block header and a list of transactions.

This list of transactions records all the transfers and generation of new Bitcoins that take place. For example, some Bitcoins were created by the miner Alice. In that case, this record about the generation of these new Bitcoins is included in this list of transactions. Then, Carol transferred some Bitcoins to David. In that case, that transaction is recorded in this block as well.

So, this is a list of such transactions, which record the generation of new Bitcoins and the transfer of Bitcoins. So, each block contains a set of transactions. Blocks are appended to the blockchain one at a time. At any time, a large number of nodes in the blockchain network try to create new blocks. That process is known as mining.

So, to add a block to the blockchain, a node needs to find the solution to a computationally hard search problem. Someone who wants to add a block to the blockchain cannot simply add it without any effort; the node needs to find a solution to a computationally hard search problem. When the node is successful in finding the solution, that node is allowed to add a new block to the blockchain. Nodes in the Bitcoin network that successfully add a block to the blockchain are rewarded with new Bitcoins. So, this reward of new Bitcoins is the incentive for the process of trying to solve this computationally hard problem and add a block.

Such nodes are called miners. And their search for solutions to the computationally hard problems is called mining. So, the blockchain is a database that contains a record of all Bitcoin transactions since Bitcoin came into existence in 2009. It's a linked list of blocks, as we mentioned earlier. So, that blockchain is shown here.

Each block is composed of a block header, which is this part, and a list of transactions. We'll discuss the structure of a block header as well as the structure of transactions later on. So, a transaction encodes the details of a transfer of Bitcoins from a source Bitcoin address to a destination Bitcoin address. For example, if Alice transfers one Bitcoin to Bob, then the source Bitcoin address, that is the address of Alice; the destination Bitcoin address, that is, the address of Bob;

and the quantity transferred; These are encoded in the transaction. So, here is some data about the blockchain. The first block in the blockchain is called the Genesis block or block zero. It was created in January 2009.

As of July 2017, the blockchain had around 478,000 blocks and occupied around 125 GB of space. A node that wants to be part of the Bitcoin network has to be ready to spend this much space, and this was the space that was required in July 2017. So, the amount of space required to store the blockchain keeps on increasing with time because new blocks get added to the blockchain all the time. So, we'll see that around, typically one block is added every 10 minutes or so. Until August 2017, the maximum size of a block was 1 MB.

In August 2017, a new feature called Segregated Witness (SegWit), was activated in the Bitcoin network. We omitted details of SegWit due to time constraints. So, because of this new feature, the maximum block size increased from 1 MB to 4 MB. Since one block is added every 10 minutes roughly, so, hence, the required space for storing the entire blockchain that keeps on increasing with time at this rate around 4 MB each time a block is added. We now discuss how the blockchain is updated and how rewards are allocated.

- As of July 2017, the blockchain:
  - had ≈ 478,000 blocks and
  - occupied ≈ 125 GB space
- Until Aug. 2017, the max. size of a block was 1MB
- In Aug. 2017, new feature called Segregated Witness (SegWit) (details omitted) was activated in the Bitcoin network:
  - this increased the max. block size to 4MB

So, the task of storing and updating the blockchain is performed collectively by nodes in the Bitcoin P2P network. Nodes called full nodes store a copy of the blockchain on their hard disks. There are different kinds of nodes. Some are full nodes, which store a copy of the entire blockchain, and others are nodes that store only the headers of blocks. When a full node connects to the Bitcoin network for the first time, it downloads a copy of the blockchain from existing full nodes.

As we mentioned earlier, to add a block to the blockchain, a node needs to find a solution to a computationally hard search problem. Later on, we'll see that this computationally hard search problem is the following. One needs to find a value whose hash function is less than a certain target. So, that is the computationally hard search problem. One needs to find a value whose cryptographic hash function value is less than a certain target.

So, that is the hard problem which a node needs to find a solution to in order to add a block to the blockchain. We'll discuss the details of that later. Nodes in the Bitcoin network that successfully add a block to the blockchain are called miners, and they are rewarded with newly created Bitcoins. So, this reward is called the block subsidy. So, whenever a new block is added, some new Bitcoins are generated and they are allocated to the miner who added that block to the blockchain, and this reward is called the block subsidy.

It currently equals 12.5 Bitcoins per block. In addition to the block subsidy, note that adds a new block also receives transaction fees in bitcoins, which are provided in the transactions in the block being added. So, we have mentioned that each block records a list of transactions which encode the transfer of certain bitcoins from a sender to a receiver. So, as an example, a sender may transfer x bitcoins, but the receiver may get y bitcoins, so this difference, x-y, is the transaction fee, which is allocated to the miner who successfully mined the block. So, for example, in this block, there may be a transaction which says that Alice transferred an amount to Bob.

So, Alice may have paid x bitcoins. Bob may have received y bitcoins. So, this difference, x-y, is positive, and that is the transaction fee that is allocated to the miner who mined the block in which this transaction is recorded. So, that is one of the incentives for the miner to add the block. So, each time a transaction is recorded in the block, some part of the amount goes to the miner who mines the block.

The sum of the block subsidy and the transaction fees is called the block reward. That is the total amount that the miner who mines the block gains. So, we now discuss the schedule for the generation of new Bitcoins. Mining is the only way that new Bitcoins are created in the Bitcoin system. The computational difficulty of mining a single block is adjusted by the Bitcoin network to ensure that a new block is added approximately every 10 minutes.

So, we have mentioned that to add a new block to the blockchain, one needs to solve a computationally hard problem. So, that problem is roughly to find a certain value x such that its hash value H(x) is less than some threshold. So, one needs to come up with some value x whose hash is less than a target T. So, the value of this threshold T is adjusted such that the computational difficulty of mining a single block is adjusted to ensure that a new block is added approximately every 10 minutes. This value T is adjusted so that every 10 minutes or so, someone will be successful in solving this problem and thereby will be able to add a new block to the blockchain. So, this schedule, along with the size of the block subsidy, controls the rate of new Bitcoin generation.

The block subsidy was 50 Bitcoins per block in Jan 2009 when Bitcoin came into existence. It is halved every 210,000 blocks. So, for example, it is halved every four years, assuming it takes 10 minutes to mine a new block. So, the block subsidy became 25 Bitcoins in November 2012, when block number 210,000 was mined. And then it was further halved to 12.5 Bitcoins in July 2016 when block 420,000 was mined, and so on and so forth.

- Mining is the only way new bitcoins are created in the Bitcoin system
- Computational difficulty of mining a single block adjusted by Bitcoin network to ensure that a new block is added approx. every 10 minutes
- This schedule along with size of block subsidy controls the rate of new bitcoin creation
- Block subsidy was 50 bitcoins per block in Jan. 2009 when Bitcoin came into existence
- It is halved every 210,000 blocks
  - about 4 years, assuming it takes 10 minutes to mine a new block
- Block subsidy became:
  - 25 bitcoins in Nov. 2012 when block 210,000 was mined
  - 12.5 bitcoins in July 2016 when block 420,000 was mined

So, we can see that every four years or so, the block subsidy becomes half of its previous value. The smallest indivisible unit of Bitcoin currency is called a Satoshi. One Bitcoin equals 100 million Satoshi. So, now this block subsidy keeps on halving every four years or so. So, as the block subsidy is progressively halved, it will eventually become less than one Satoshi.

So, at that time, it will be considered zero. The block subsidy will be considered zero. So, someone who mines a new block will not get any block subsidy from mining the block. But there will still be an incentive for mining new blocks, and that incentive will be the transaction fees of the transactions in the newly added block. So, the block subsidy will become zero when block number 6,930,000 is mined.

- Block subsidy will become zero when block 6,930,000 is mined
  - Expected to be around the year 2140
- Once block subsidy becomes zero, what incentive will miners have to mine new blocks?
  - transaction fees will be the only incentive for miners to continue mining new blocks
- As the rate of new bitcoin creation decreases geometrically, total number of bitcoins that will ever come into existence is:
  - ≈ 21 million

So, from the above schedule that we discussed for adjusting the block subsidy, it can be shown that the block subsidy will become zero when this particular block is mined. This is

expected to be around the year 2140, so that's a long way from now. Once the block subsidy becomes zero, what incentive will miners have to mine new blocks? So, recall that the block subsidy is only one part of the reward that a miner gets; the other part is the transaction fees. So, transaction fees will then be the only incentive for miners to continue mining new blocks.

As the rate of new Bitcoin creation reduces geometrically, the total number of Bitcoins that will ever come into existence is around 21 million. So, this can also be computed from the above schedule for generating new Bitcoins that we discussed earlier. So, what is the reason for choosing this particular schedule? So, we have discussed various aspects of the schedule. One is that the initial block subsidy was 50.

It could have been something else. For example, it could have been 100. It is halved every 210,000 blocks. This could have been some other value. For example, it could have been, say, 100,000.

So, why are these particular constants chosen? So, what's the reason for choosing this schedule? The motivation behind having a fixed limit on the total number of Bitcoins is to prevent inflation of the currency. So, if there is a lot of currency in existence, then that leads to inflation. Hence, that was motivation for limiting the total number of Bitcoins.

So, that is to prevent inflation of the currency. So, that is the overall motivation. But there is nothing special about the specific constants which are provided on the previous slide, chosen to represent the initial block subsidy and the halving schedule. So, they could have been some other constants, and in that case these numbers would have changed. 6,930,000—this would have been something else, and this 2140 would have been something else.

But this overall motivation would still have been met. So, in summary, we are discussing cryptocurrencies and blockchains. We introduced the Bitcoin cryptocurrency. We introduced the concept of mining, transactions, blocks in a blockchain, and we discussed the schedule for generating new Bitcoins. We'll continue our discussion of Bitcoin in the next lecture.

Thank you.