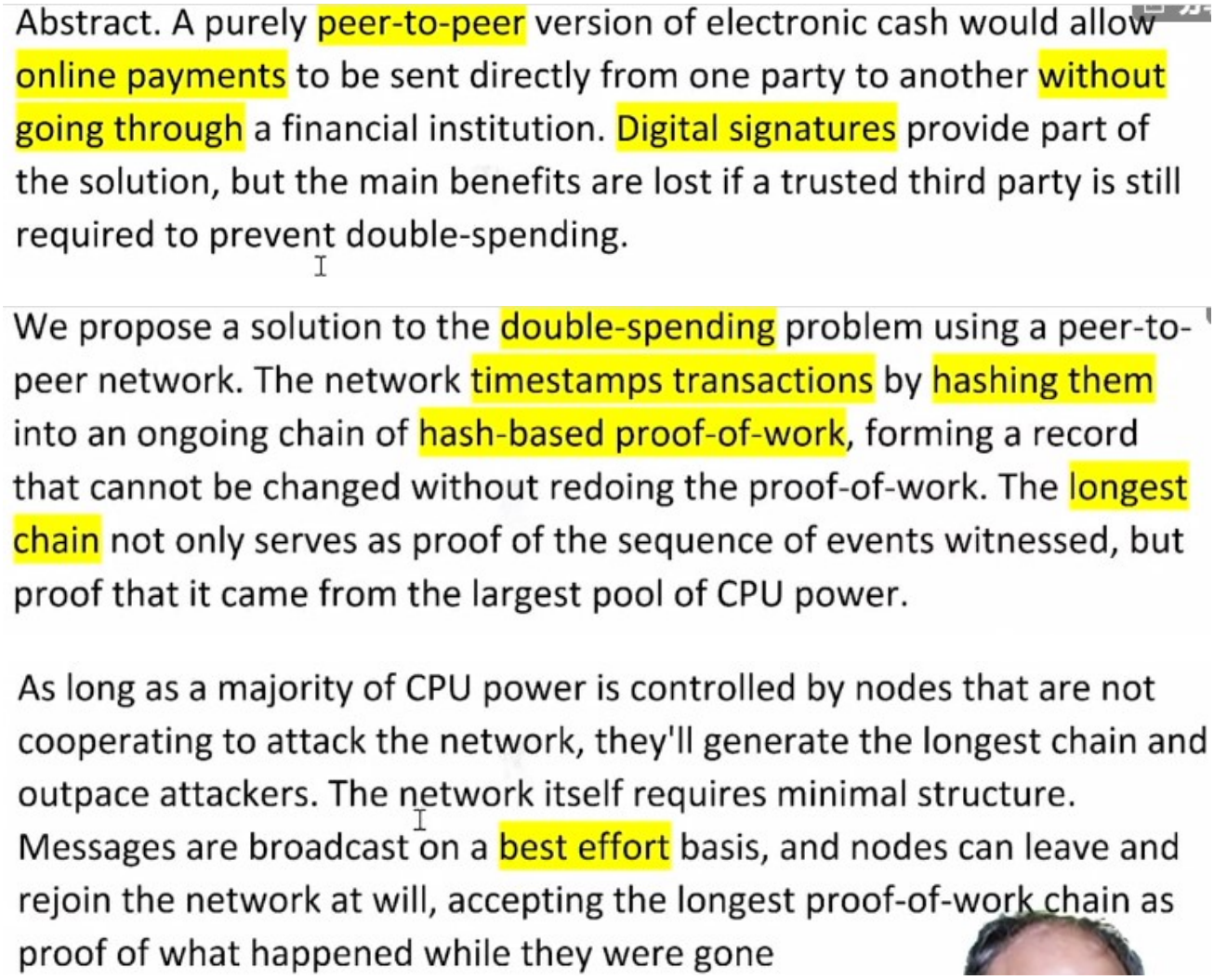
Computer Security -- Week 13

The Origins of Bitcoin

Abstract

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. 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. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack

the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.



Network and Transactions

Napster: people shared music files in a peer-to-peer network

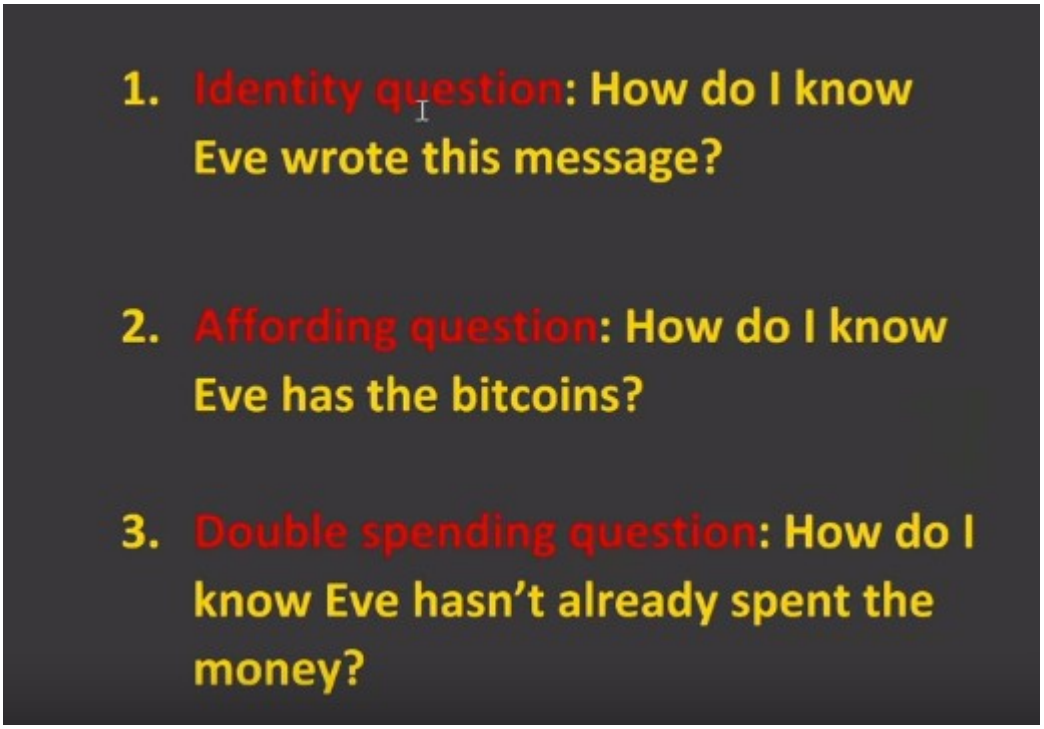
The Blockchain Will Do to the Financial System What the Internet Did to Media: *Harvard Business Review*

Main unit is a Transaction:

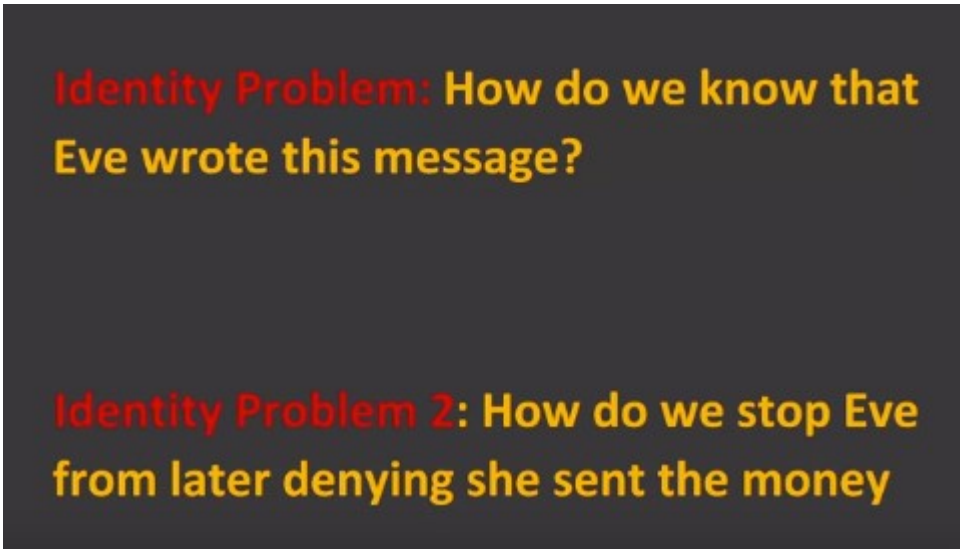
'I, Eve, give Dan 2.3 bitcoins'

These are not trusted people. So making this work raises three big questions:

1. Identity question: How do I know Eve wrote this message?



1. Identity Problem



- Answer:

Eve signs the whole transaction with her private key or secret key

Note that the private key is not part of the transaction

Digital Signatures

Eve has a public, *pk*, and a secret key, *sk*

We are not using the keys to hide the message

STEP 1:

Sig = sign(sk,mes)

returns a string

Note that this means the signature depends on the message as well as the secret key -- different signature for each message

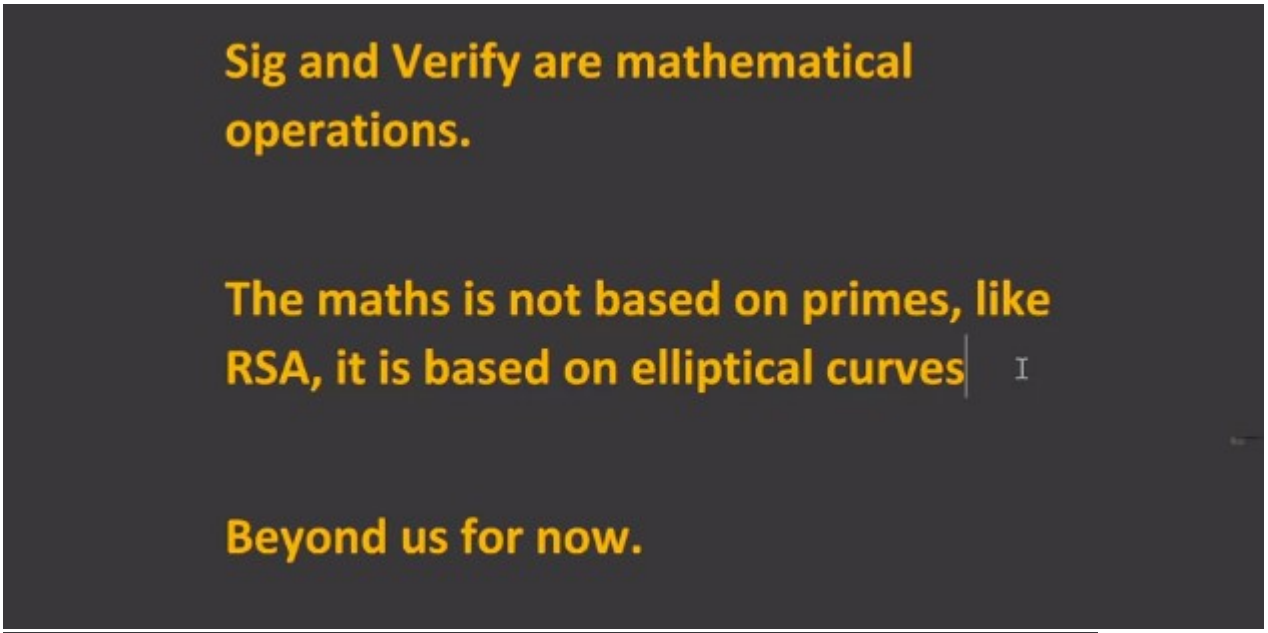
Step 2:

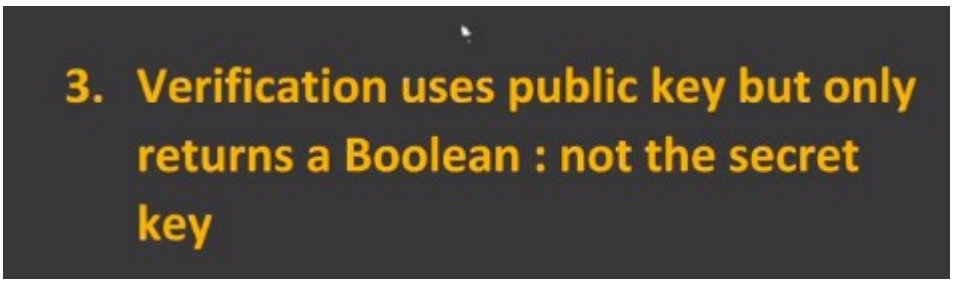
Verify (pk, mes, sig)

returns a Boolean

Verify returns TRUE if and only if the Signing function with inputs (1) the key that is the opposite of pk and (2) message mes would return the signature sig

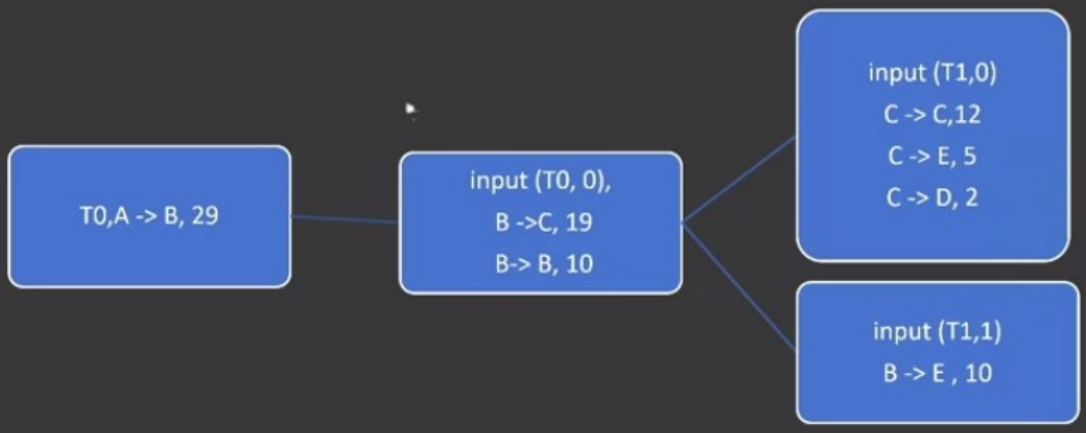
Note that this does not return the secret key. And it only works for this particular message





2. The solvency problem

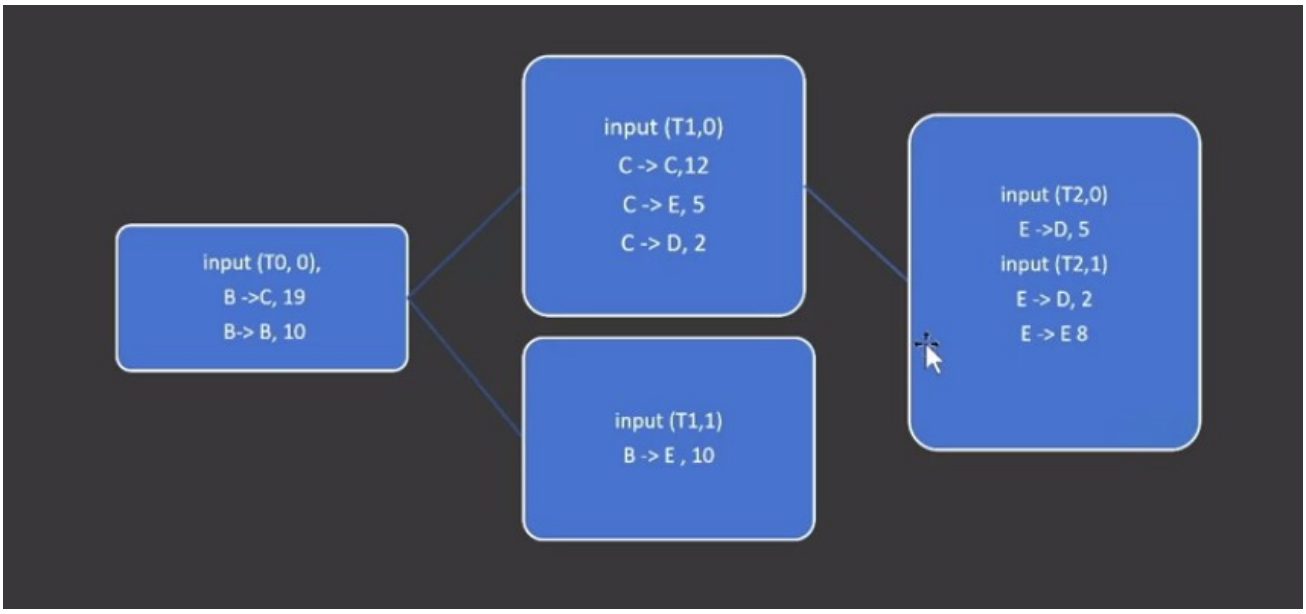
Every Transaction refers to the transactions in which the present owner got the money



When E wants to send 7 bitcoins to D, she puts into the transaction information that she got it from the second transaction from the top on the right.

Note: this is not the blockchain

A transaction can have more than one input.



In this bit B is giving 7 of the bitcoins received in the last transaction to E and keeping the rest

Need to be explicit to keep the chain going

Can be several outputs of a transaction.

An output is:

Address where the bitcoins are going paired with amount

Address?

Not a name

The Hash of the recipient's public key

Remember the Hash can be used as a proxy or signature for something.

This is not for security. It is to make all addresses the same length (160 bits).

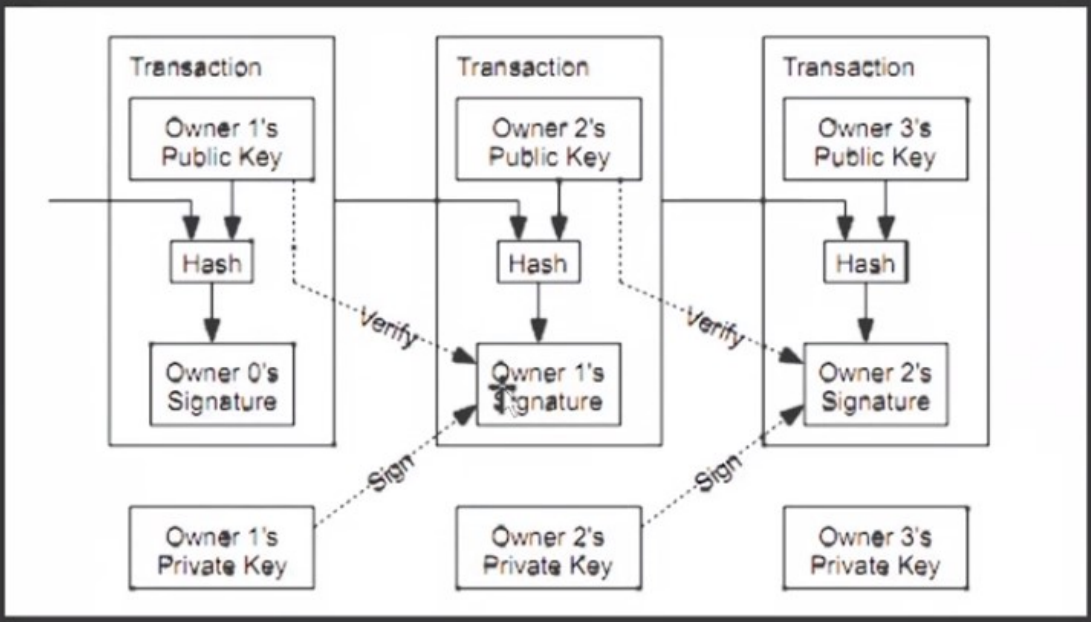
Can be several inputs of a transaction. An input is:

1. Amount
2. Signature of the account sending the money

3. Txid (the transaction id of the transaction) that the money is coming from: the hash of the transaction

4. The output of the last transaction you are using : this is called the index or vout 0,1,2…

White Paper description of a transaction:



We're now ready to start looking at the details of the way Bitcoin works. Using the abstract as a go ahead. The first thing we yellowed, was a peer to peer network so that's looking at the snipey. I mean I think that's one of the things you probably mostly know to do this quite quickly. Okay, so in this, in this lecture we're going to talk about peer to peer networks. And we're going to talk about transactions a little bit,okay,well, let's see what that means in a bit. So here's, it's a peer to peer network, these pictures taken from Wikipedia. And it's quite an old peer to peer network I'd say these are out of date blackberries and rather old looking up.

从 :1: 开始播放视频并学习脚本 1:00

Laptops and desktops but he is the point we've got all kinds of computational devices and they're talking to each other. There's no central, anything that in charge of it. It's just each talking to each other as it were without mediated by anything else. So they're just connected in various ways and the whole network will be connected. But not as you can see, not everybody is connected directly to everybody else. But everybody has got a connection somewhere from some place to another. And, of course the point is we've taking his banker and turn him out of our system, he's entirely gone.

从 :1:44 开始播放视频并学习脚本 1:44

So this picture, as it says, adapted from Wikipedia, though, a bit with the bank is not from Wikipedia. So we just have a bunch of computers and computation devices and mobile phones, like only blackberries. But you get the picture talking

to each other across this network, okay.

从 :2:7 开始播放视频并学习脚本 2:07

Now, one of the first ones I came across in my youth was Napster. I don't know how many you've heard of that, but at the time. What it was is that it was a big Destruction to the music industry. Because it was saying, okay, we've got digital copies of music, each of us. If we just share them in this peer to peer way, we don't need to pay Sony for them, or whomever, right. We could just share them among ourselves, we don't need to buy anything. We just share these because we own them so we have the right to share them with other people. They came a Cropper in the end with that model, but their model really did change the way. People thought that media it's changed in that it made us think we could just grab media, media is there for us. It's not a matter of us, some central repository that we have to buy things from. It's just changed, it's made media, made music feel like it should be. Something that's just like water streaming for us to take. And of course we've got that metaphor now, we didn't then, okay. So that's really what Napster did. And that's really what the internet did Napster and then kind of taken up Spotify, Apple, iTunes, etc. Be made commercial, a lot of the same ideas but not the peer to peer network but the whole feeling. And I really like this remark from the Harvard Business Review and, in fact it is the name of an article. The Blockchain will do to the financial system what the internet to media. This is part of what the internet did to media and made it feel like something you had control over. Something you can just get,yourself, not some big company that

you were dealing with. So that's one of the things that the internet has done for media. It brought it to people and I think that's what blockchains meant to do for financial system at least that's what this article suggest.

从 :4:24 开始播放视频并学习脚本 4:24

We haven't used the word blockchain yet but that's where we're getting. As I said, I think someplace earlier that the one of the lasting I think, effects of having Bitcoin started. Is the whole idea of blockchain and we will learn about that as we go.

从 :4:45 开始播放视频并学习脚本 4:45

Okay, so the idea is transferring financial services, financial tokens. Let's see if we were like using Spotify to get musical view. But we're not doing media files, we're doing transactions of bitcoins, that's the thing. So, it's quite a simple in that sense, it's a very simple thing. So we have transactions is the central issue here. It's not sharing media are transactions where say things like Eve give Dan 2.3 bitcoins.

从 :5:22 开始播放视频并学习脚本 5:22

Now I'm using Eve and Dan instead of our usual Alex and Bob. Because I want to underline here that we don't trust these people. Alex and Bob are really kind of trustworthy, Eve we know is not trustworthy. And a lot of what we're going to do In the Bitcoin protocol is be able to deal with Eve not being trustworthy. Which isn't even though you know we have this nice picture of people cooperating, cooperating etc. And that had a kind of hippyish feel to it, it's not that happening here at all, this isn't hippyish. This is serious financial system without trust built in.

从 :6:5 开始播放视频并学习脚本 6:05

We used to have a trusted banker, we've turned out to trusted banker, we don't trust anybody.

从 :6:14 开始播放视频并学习脚本 6:14

In cryptography we trust in in cryptographic users not so much. So that's what we're going to be doing, we're going to be making this system work even with not trusted players.

从 :6:31 开始播放视频并学习脚本 6:31

Okay, so that's really that's why I've got Eve here instead, we know not trust Eve. So with Eve not being that trusted, what are the questions to make this work that just stand out is what I've got these transactions. How do I know Eve wrote this message when it says, I Eve will get 10 1.5 or whatever it was? That's the identity question.

从 :6:59 开始播放视频并学习脚本 6:59

The affording question which I came up with a better name for later. I forgot what it is, so we'll come up in a later slide. How do I know Eve has the bitcoins? How do I know he can afford this, track this, to do this? So even if Eve is saying this, how do I know Eve can even as this money, I can't go to the bank, there is no bank. So, how do I know I have the dealers' money and then the double spending question. Which we which as I showed you, from the abstract is a really crucial element in this. So the simplest form of double spending the questions. When Eve tells me she's going to spend this money or give me this money. How do I know she's

hasn't already given it to somebody else? Even if I know she could afford it at some point, how do I know she hasn't given it to somebody else? That's double spending problem, that's what where the magic happens. That's where the magic of Bitcoin happens. That's where blockchains are invented. I'm getting ahead of myself, we will get there before the end of the topic.

从 :8:9 开始播放视频并学习脚本 8:09

But that's really the most exciting thing. To avoid double spending, Satoshi's invented blockchains. Hasn't used that word but he's invented what we now call blockchains, okay? But the first thing, before we get to the blockchains. Which is the answer to the third of these questions, we'll go to the identity question. How do I know Eve wrote this message? We'll get that in just a minute, for me here maybe. Anytime for you see you there.

We're now ready to tackle the second question, second problem, which I'm now calling the solvency problem, which I think I called the affording bomb before. How do we know that Eve has the money? The answer to that is, we don't have a bank account. We can just say show me your bank account or anything like that. All we've got is a list of transactions. We've talked about that already. We've got a list of transactions and so we need to get that information from the list of

transactions.

从 ::41 开始播放视频并学习脚本 0:41

Every transaction will have in it a reference to where the money came from for that transaction. Here, I've got a transaction that sends 29 Bitcoins from A-B. B's to send some of them to C but not all of them. It says in this transaction that I've got this money that I'm going to spend from this channel here which is the first output index zero from T0 and I've got two things that's happening with that money. There's 29 Bitcoins I'm going to send 19 of them to C, but I'm going to keep 10 of them myself. Now, I've got actually put that explicitly in. I've got to say that I'm going to send that to myself because I have to be able to chain through these transactions. I have to be able to say, I've got this 10 from giving to myself. Then how did I get that 10? Well, I got it from part of that. Then from here, I got two outputs. Some of it's carrying from C to various people, some's coming from B to various people and they're sending this to E if this getting 10 from here, and if it's getting 10 from here as it happens. Notice this all adds up to 19, and this all adds up to 10. The input to this is 19 and the input to that is 10 and so on.

从 :2:16 开始播放视频并学习脚本 2:16

When Eve wants to send money to D, she has to say where it come from. In fact, what I've now got is that E is going send. I've lost two, that should say here. I've lost the number here. Eve's actually sending seven to D is it happens. Let me change this for consistency. Eve is going to send seven Bitcoins to D. Suggested say where she's got the Bitcoins from.

从 :2:56 开始播放视频并学习脚本 2:56

Five of them she's got from here and two of them she's got from here. As to input into this transaction,

从 :3:7 开始播放视频并学习脚本 3:07

they can all get traced back. The seven can be traced back and Eve's going to keep paid from here. Well, actually she could have just sent seven from here, but she didn't. I hope that makes sense, but the important thing is, I can tell occurring chaining back where the all [inaudible] come from. I haven't told it all yet and I will do about where Bitcoins originate from. But for now, this is where we're just being to transact suggest. So just transfunds.

从 :3:47 开始播放视频并学习脚本 3:47

We need to be explicit, keep the chain going which even includes sending the residuals to yourself. The other thing I haven't mentioned is, you can put in a price or price you're paid for somebody to actually put this on the ledger, get back to that later.

从 :4:14 开始播放视频并学习脚本 4:14

The transactions could have several inputs, can have several outputs. What does the outputs look like? Well, that's sending address where Bitcoins are going and how much is going there and have a lot. What do I mean by an address? While it's not the name. The names were hidden, but what it is, it's the Hash of the recipient's Public Key as it turns out. That's what counts as address. Their Hash of he recipient's Public Key. It's just an address, we're saying where it's going and

how much money is. That's all the outputs or the inputs are more complicated. Remember that the hash can be used as a proxy. It can tell us because it's a cryptographic Hash. We can use the Hash as the name without having to say anything else about the word. We do that Hash though, not Hash for security reasons. We use that hashing just to make it more efficient. It used to be in the old days and if you look back to the white paper, in the first few years of Bitcoin, [inaudible] wasn't hashed. The output actually noted Hash of the Public Key, which is a public-key. However, there it's got too big. It ended up being unwieldy and it's more efficient to hash it first. Now, you can also have several outputs for a transaction. Whoops, this is supposed to be inputs, several input for its transaction. It's supposed to be inputs. We still have several inputs of a transaction and the inputs are more complicated. Obviously, you have to say the amount. We've already talked about the fact that you're going to have the signature from the person who's sending it. Remember, the signature relies on the whole transaction plus the secret key.

从 :6:22 开始播放视频并学习脚本 6:22

The signature is there and the transition ID of the transaction is Hash of the transaction. We've got that. We need that to say that where it comes from. It's a bit more than that because you have to say which of the outputs that it's more than one outputs and that's a loss bit at 012. Let me look a little bit at the whitepaper description of the transaction C, what it simply gets in sense of this now. I took this transaction in the middle. We've got going into this signature,

what have we got? We've got the private key, a secret key from the person who owns this. We've got the Public Key coming in for verification purposes. We've also got a Hash of the transaction before hand. This is what I am saying. This inputs include the Hash of what would happen before hand and the Public Key. Now, I'm saying we hash the public key. That's what's different about from this picture. We hash the Public Key as well, but the Public Key comes in for verification purposes. The signing happens. All of this goes and is ready for the next one. We've almost got this whole picture because we have got this whole picture. But we haven't got the blockchain yet.

从 :8:18 开始播放视频并学习脚本 8:18

I want to just pull up some websites. Here's something about blockcypher. This gives us a sense from recent transactions. You can see this is transactions that are actually happening on the Bitcoin. I'm getting ahead of myself. These are things that are happening in the Bitcoin world. Here, this one has one input and two outputs, so there is two outputs. Some Bitcoins, point one and Bitcoins being spread between two recipients. This one has one of a recipient and that's coming from two different places. You can see that these are not one-to-one, but they can be one-to-many, many-to-many. Here's one that actually makes 10 inputs, 10 outputs. This is going to 10 different places.