Danny Diekroeger @dannydiekroeger

19 Jul 20 • 26 tweets • dannydiekroeger/status/1284897057485053952

~ Bitcoin Addresses ~

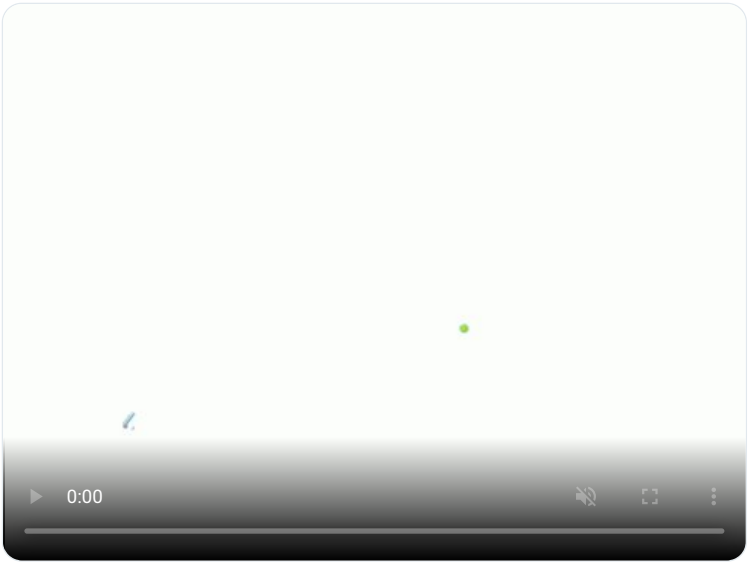
How do they work? Where do they come from? Why do some look different than others?

Thread 👇

When bitcoin gets sent, it always gets sent to an Address

You can think of an Address kind of like a Lock

When we say that an Address “has some bitcoin on it”, what we really mean is that a certain amount of bitcoin is locked to that Address



Like most Locks can only be opened by one key, bitcoin at most Addresses can only be unlocked by one person

But Locks can be more complex, and so can Addresses, sometimes requiring cooperation from multiple people or even knowledge of special secrets, in order to unlock them

Let’s dive into the most basic types of Address

Let’s pretend our friend Alice owns this Address:

1mEBFZ2iGmrDL6GXmrCAM8ZJdg7XVYdCM

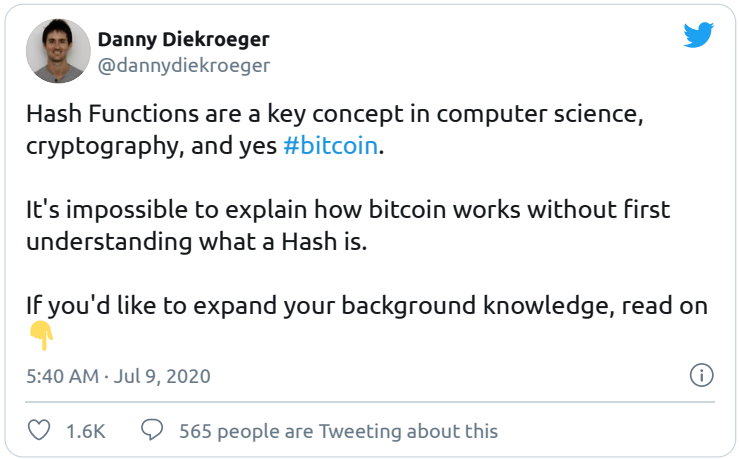
The “1” at the beginning tells us the “version” of the Address, or the “type of lock”

Addresses that start with a 1 are the most basic and are called "Pay to Public Key Hash" addresses, and require just one signature in order to unlock them

These are called “Pay to Public Key Hash” ("P2PKH") addresses because most of the rest of that data in the Address is a Hash of Alice’s Public Key

For some background on what Public Keys and Signatures are, I'd suggest checking out my previous thread:

For background on what a Hash is, check out this one:



You might be wondering why the address has the Hash of Alice's Public Key, and not just the actual Public Key

Good question

In fact, original bitcoin addresses were exactly that - "Pay to Public Key" (without the hash)

It wasn't until a little later that they realized hashing the public key provides some additional security benefits that make it more future-proof, so "P2PKH" became the standard

So we have this Address that has the Hash of Alice's Public Key in it

How does Alice spend from this Address?

To send a transaction, she needs to produce 2 things:

- Her actual Public Key

- A Signature of the spending transaction's data (signed by her Private Key)

When Alice produces this data, she will attach it to her Transaction

Then all the Nodes' software in the bitcoin network will check to make sure its valid

They will check:

- Does hashing the Public Key she provided equal the Hash thats in the Address?

- Is the Signature valid for that Public Key?

If these are both true, then Alice's transaction will be accepted

She will have successfully "unlocked" her Address and spent from it!

Great so we've covered the most basic type of Address version: "Pay to Public Key Hash", that starts with a "1"

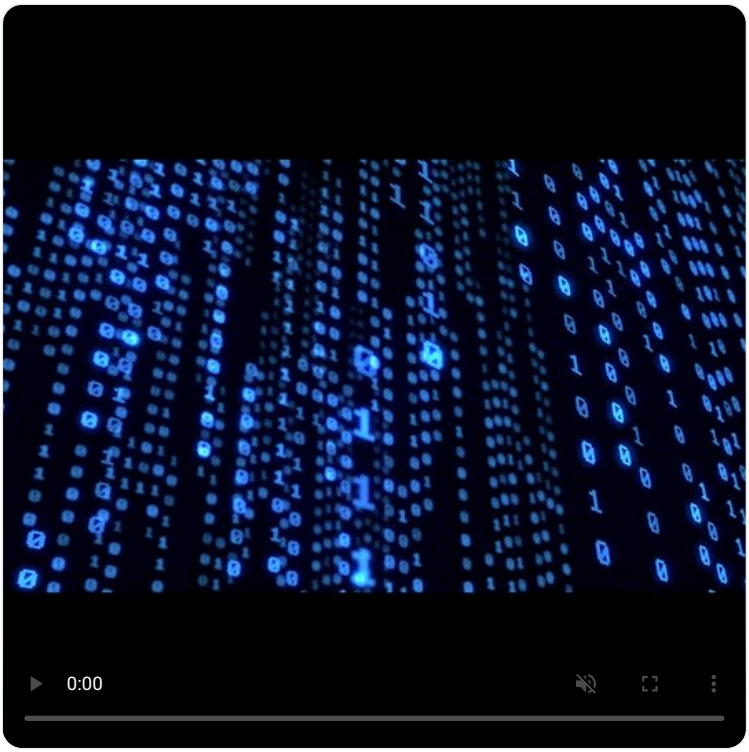
What about the other ones?

The next type are addresses that start with a "3", like this one:

32XsF8Ge2goSWiHKfwakMwQXTHawehzoFV

This is called a "Pay to Script Hash" address, and it allows for really awesome complex spending conditions

It gets it's name because the data encodes a Hash of a computer Script. Thats right - a miniature computer program!



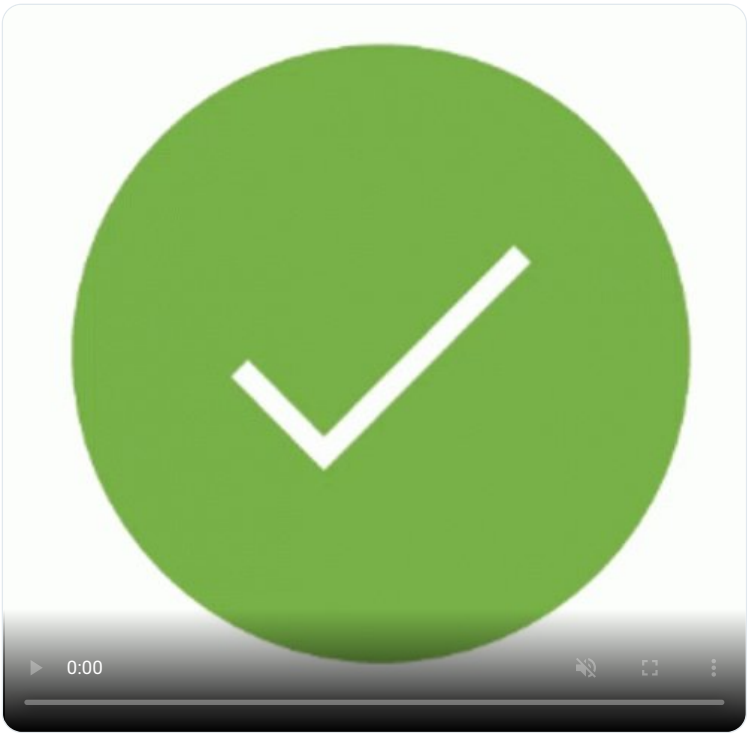
If Alice wants to spend from one of these Addresses, the following needs to happen:

- She must produce the actual Script that hashes to the data in the Address

- She must produce any signatures or other secret information that the Script requires

When a bitcoin Node gets this data along with the transaction, they will run the computer program Alice provides along with the Signatures / Secrets she includes

The program must evaluate to True in order for the transaction to be valid



That may sound a little bit vague, but it's because these types of Addresses can encode all types of fancy Scripts

The most common one is a "Multi-Signature" script, which requires Signatures from multiple different parties in order to Spend

Other types of Scripts can include Timelocks (Bitcoin locked for a certain amount of time) and many more possibilities, which I can cover in other threads

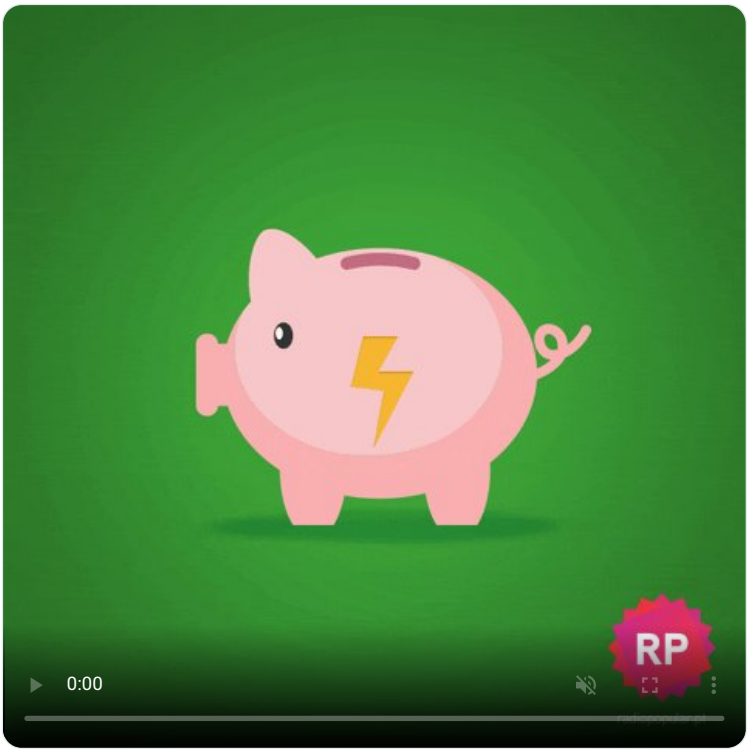
Finally, you may have also seen addresses that look like this:

bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7kytlcckxswvvzej

These, which start with "bc" are called “Segregated Witness” addresses, and they have similar functionality to the previous ones I described

The special thing about “Segwit” addresses is that they save money on Fees

When you spend from them, you don’t get charged for the Signature data (remember in bitcoin you pay for data!)



So to recap, we covered 3 types of addresses:

- Pay to Public Key Hash ("P2PKH") (1 key required)

- Pay to Script Hash ("P2SH") (Mini computer script required)

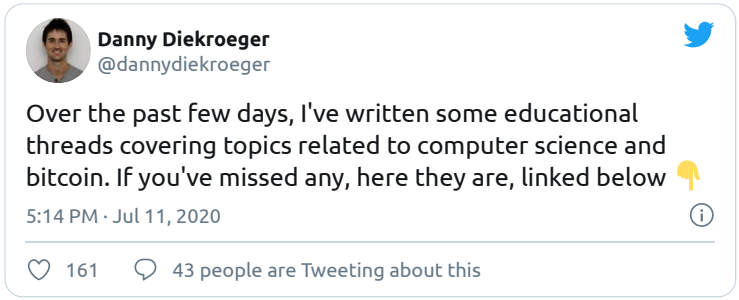
- Segregated Witness ("Segwit") (Same possibilities as above, but save money on fees)

Those are the basics of Bitcoin Addresses!

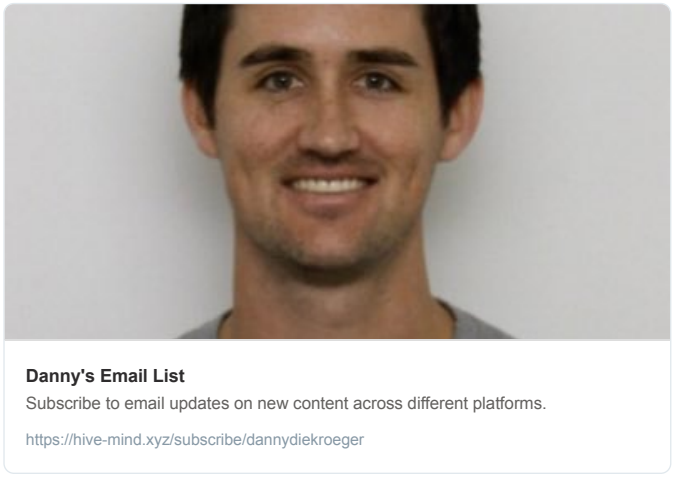
We can dive deeper in further threads, but I'll end it here

Let me know your questions in the comments!

All of my previous threads are linked here:



Also if you're interested, subscribe to my email list here:



@threadreaderapp unroll

• • •