Danny Diekroeger @dannydiekroeger

17 Jul 20 • 18 tweets • dannydiekroeger/status/1283928379201212416

Private Keys, Public Keys, and Digital Signatures

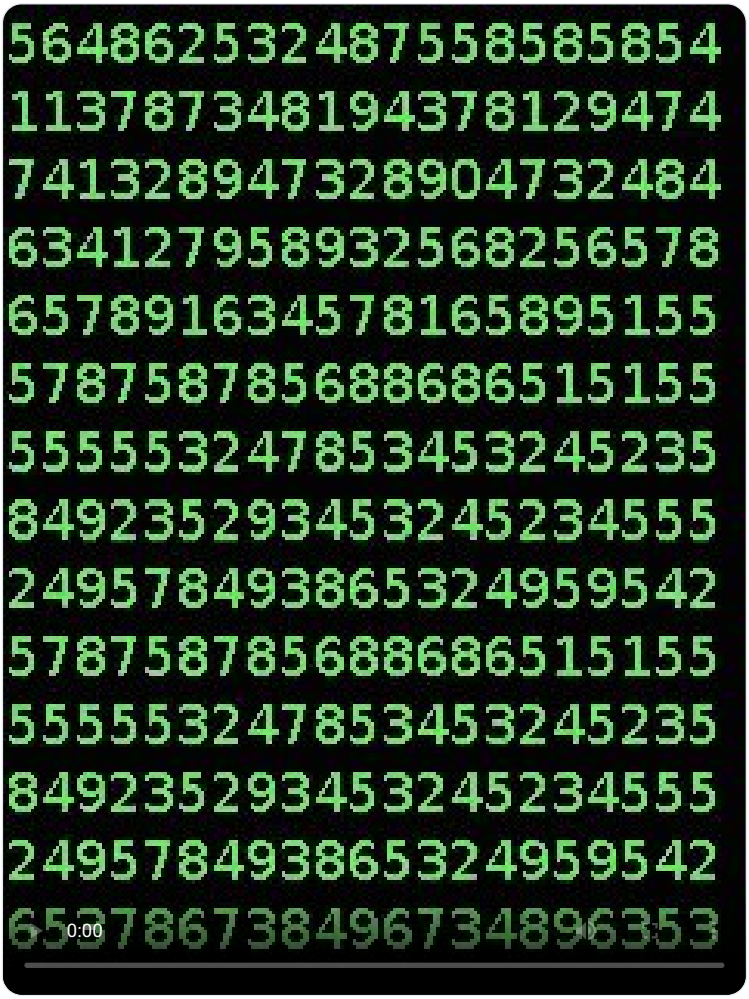
What do all these terms mean?

Here's a high level overview of the basics, and how they help us do cool things especially in bitcoin 👇

A Private Key is just secret number

Thats all

It's just a really large random number - so large that it can't be guessed by anyone



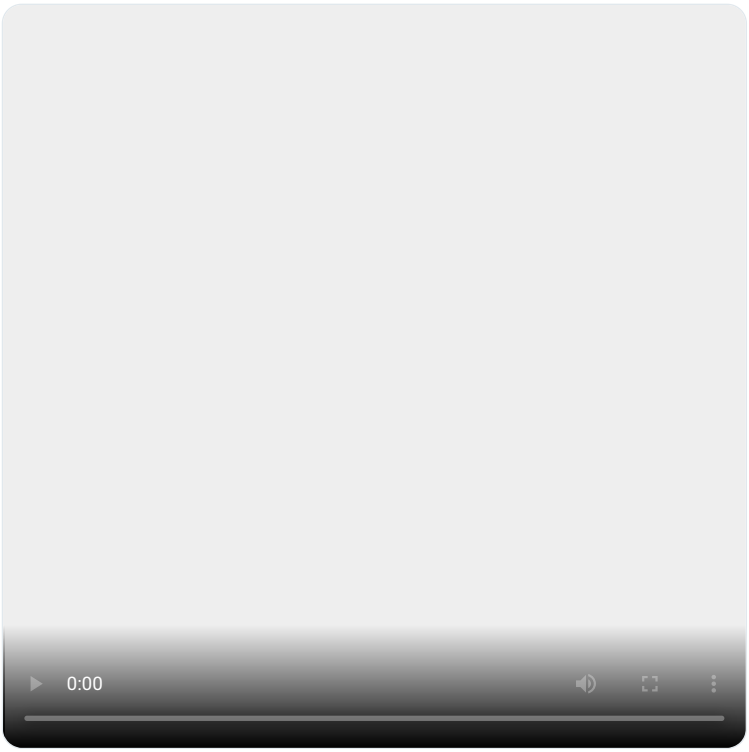
In bitcoin, private keys can be any number between 0 and 2^256

To get a sense of how many choices there are, 2^256 is roughly the number of atoms in the known universe

So if you use a good random number generator to pick a number between 0 and 2^256, it's basically impossible for anyone to guess what the number is

Once you have a Private Key, you can then calculate its Public Key

You do this by multiplying the Private Key by a set number that everyone has agreed upon (we call this set number G - the "Generator" point)



Now there are a couple important catches here..

This isn't regular multiplication...

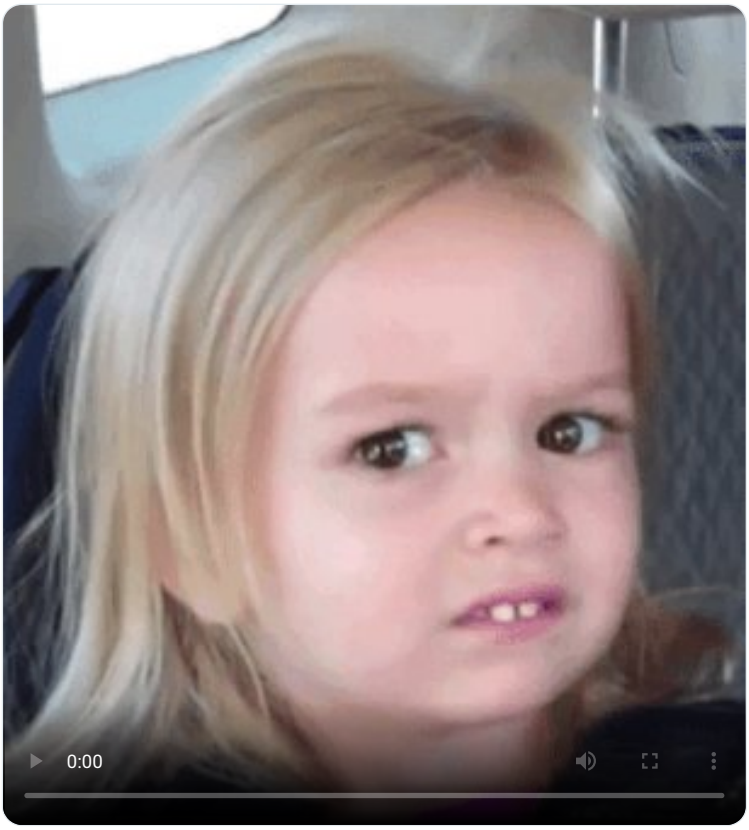
Its a fancy type of multiplication that uses a special number system (which I won't get into here)

In this number system, multiplication is easy, but DIVISION is IMPOSSIBLE

The important point is that if you have a just Public Key, there is no way to figure out the Private Key

You can't just divide it by G, because in this number system, division is impossible

(This number system is an Elliptic Curve over a Finite Field, aka "fancy math")



Let's not go too far into the math, but let's recap:

- Private key is a secret number

- Public key is also basically a number, and you get it by multiplying the private key by G

- Division is impossible, so you cannot figure out the Private Key if you only know the Public Key

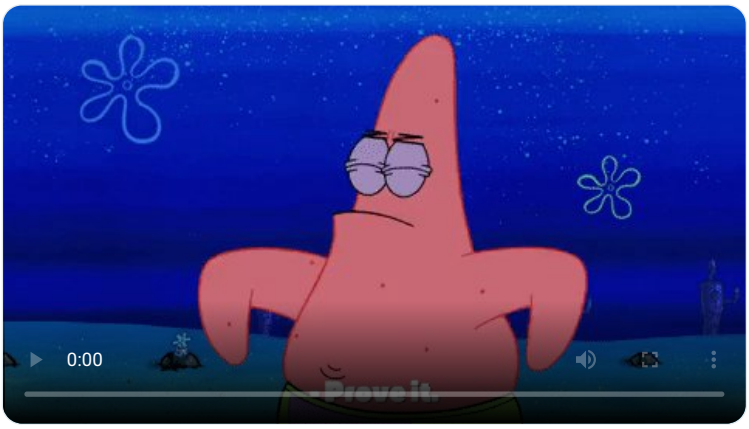
The nice thing about Public Keys is that you can safely share them with everyone

So they function kind of like your digital identity

So what can we do with this now?

Imagine I own 1 Bitcoin and I'd like to send it to my friend @SahilBloom

In order to send this coin, I need a way to "prove" to the network that I am the rightful owner of this coin and authorize it's transfer



This is where Digital Signatures come into play

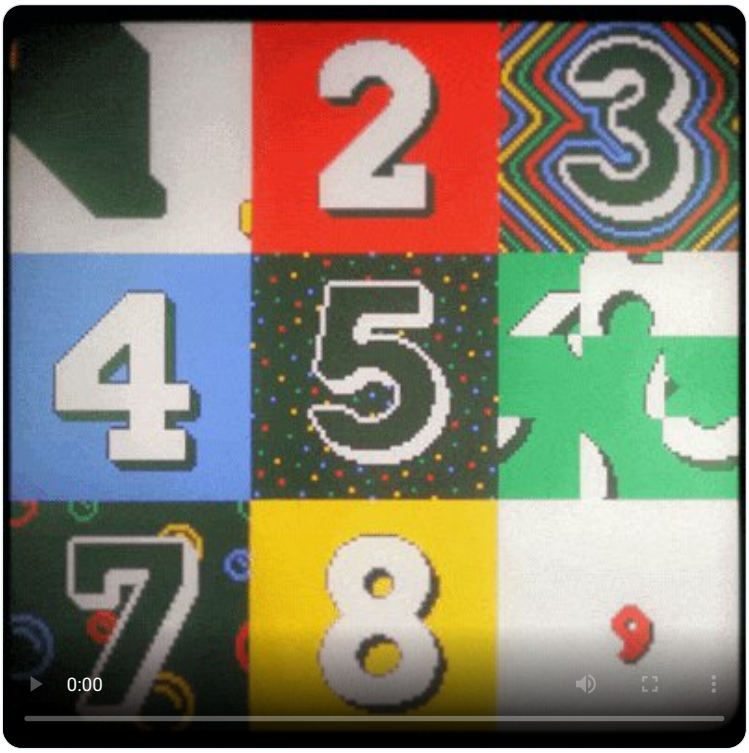
I first create a message (in this case its a bitcoin transaction) that says:

"I, the owner of Danny's Public Key, authorize the sending of this 1 Bitcoin to the owner of Sahil's Public Key"

Now I need to prove to everyone that I created this message

This proof is called a Digital Signature.

I basically just put my Private Key and the Message into an equation, and out pops another number - the Signature!



The cool thing about this number (Signature), is that anybody can look at the Signature, the Message, and the Public Key, plug them into another simple equation..

If the math checks out, they can be 100% sure that the owner of the private key is the one who created the signature

In other words, the Signature is mathematical proof that owner of the Private Key has authorized the Message!

Those are the basics of Private Keys, Public Keys, and Digital Signatures

These elements of cryptography are used everywhere in software and the internet (not just bitcoin), and are a great example of the powers the fancy math gives us

Unfortunately I've hand-waved over the wonderful math that makes this all possible...

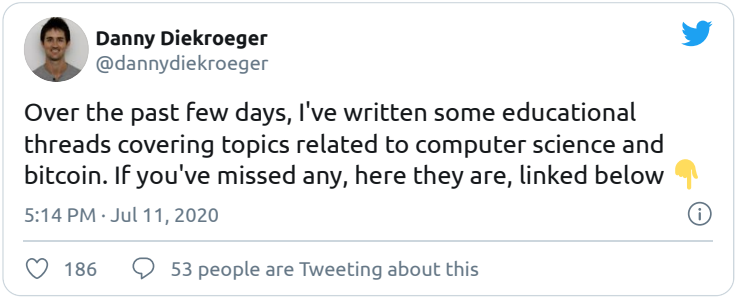
For more info on that, you can research "Elliptic Curves over Finite Fields"

The Math isn't too complicated, it's just very different from what they teach us in school

Hope that was helpful!

Let me know if I got anything wrong - I really appreciate all the feedback in the comments 😀

If you liked this thread, check out my others. I'm linking them all on this thread here:



• • •