

Blockchain Technologies and Decentralized Environments

Day 2

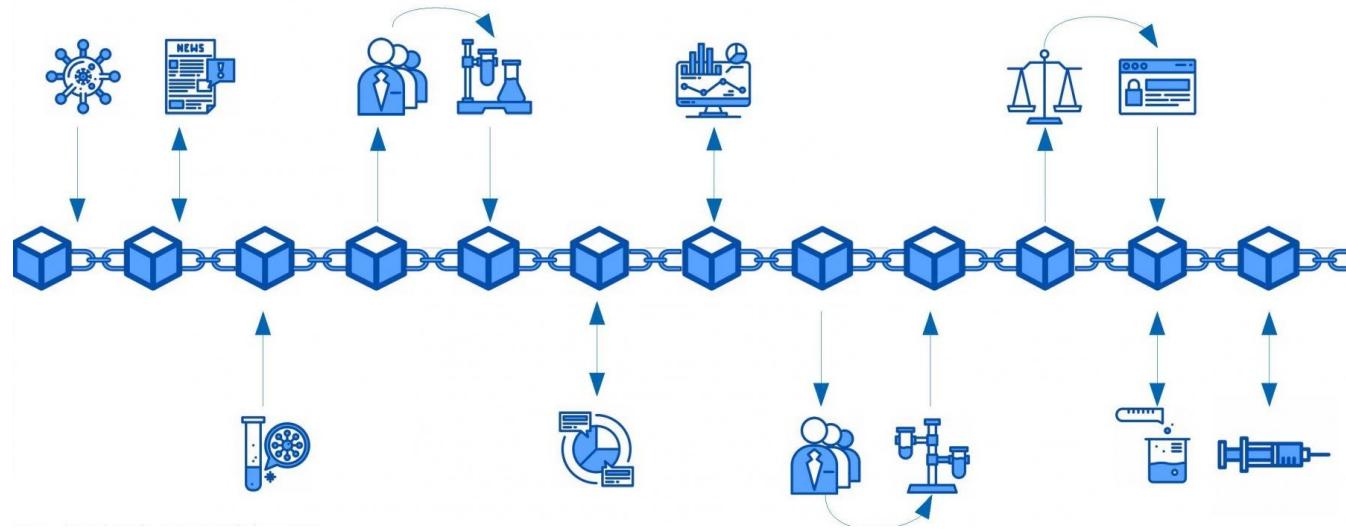
Davide Patti
davide.patti@dieei.unict.it

Outline Day 2

- **Asymmetric Cryptography**
- Transactions on Chain
- Short History of Bitcoin
- Blockchain as a Platform: Proof-of-Existence, NTF, Smart Contracts
- Scalability: the Blockchain Trilemma
- Bitcoin Layer 2: the Lightning Network

Impossible Mission?

- 1) We must guarantee the order of events
- 2) Ensure that sender and receiver are the correct ones
- 3) Entities not trusting each other agree on some “digital reality”



Transactions at Bitcoin Layer 1

Bob wants to send X bitcoins to Alice

- 1) How do we ensure that only Alice can receive the value?
- 2) How can Alice be sure that it is Bob that wrote the transaction?
- 3) How do we ensure that Bob has x bitcoins to give?

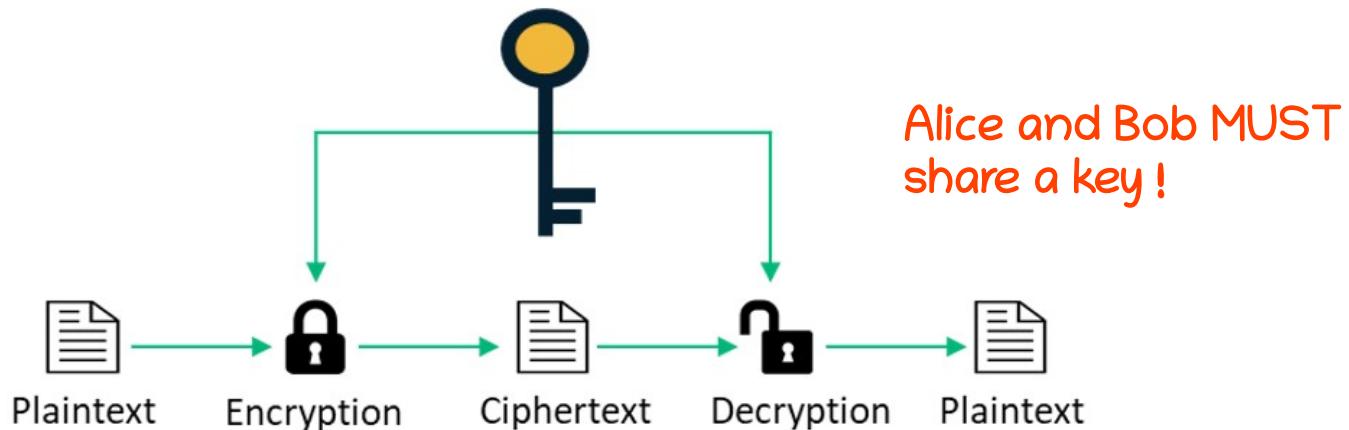
Notice: Human-like names are used only for clarity. They could also be non-human, smart objects, Artificial Intelligence entities etc...



Symmetric Encryption

Each pair of people wanting to exchange messages, must share a secret key
Alice and Bob encrypt messages using the same key

- **PROBLEM 1:** If Alice choose a key, must communicate it to Bob (possible leak)
- **PROBLEM 2:** If Alice wants to send messages to other people, must create a key **for each new person**, in theory, everyone in the world!



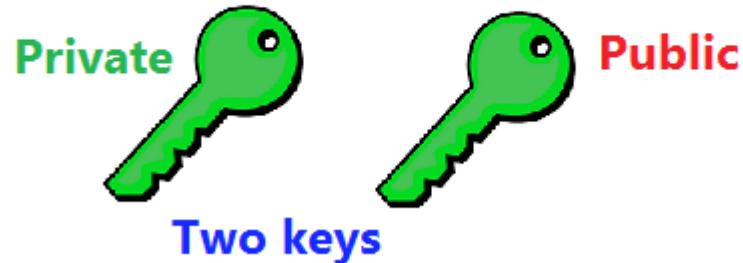
Asymmetric Encryption

- THERE IS NOT a new key for each couple of people communicating
- Each user has two keys:
 - A **public key**, given to everybody. Everyone knows the public key of all other people.
 - A **private key**, kept secret, never shared, never transmitted.

Symmetric Encryption



Asymmetric Encryption



Asymmetric Cryptography

- Imagine a box with two locks:
 - One for the private key
 - One for the public key
- ...and a particular mechanism:

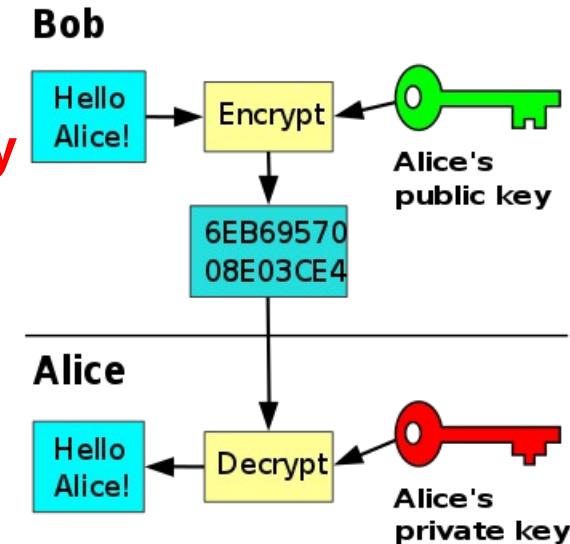
If you lock with one key, you will able to open the box only using the other key
- Anyone can get the **public key** of a given user, only the **private key** is **NEVER** shared



Q1: How do we ensure that only Alice will read the transaction from Bob?

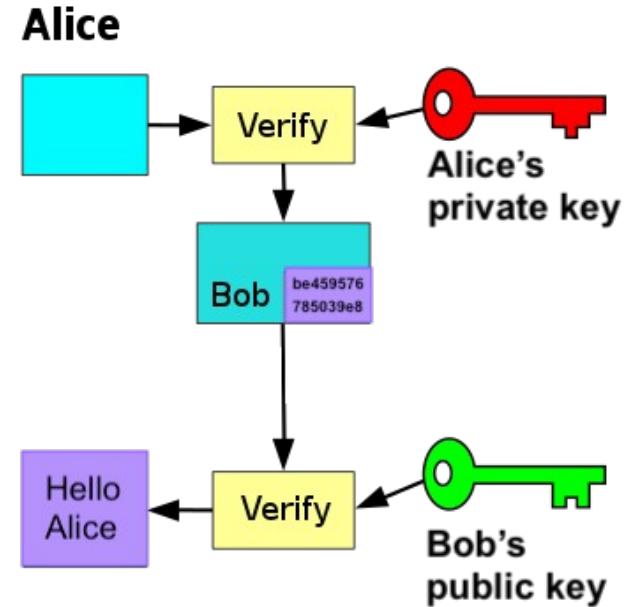
- Bob puts the transaction data inside the box, and closes it with the **Alice's public key**
- Now, it can only be opened with **Alices's private key**
- Only Alice has the **private key** to open that box.
- **Question 1 has been answered: Bob created a message that only Alice can read**

Notice: This still not ensure that it was Bob to send it



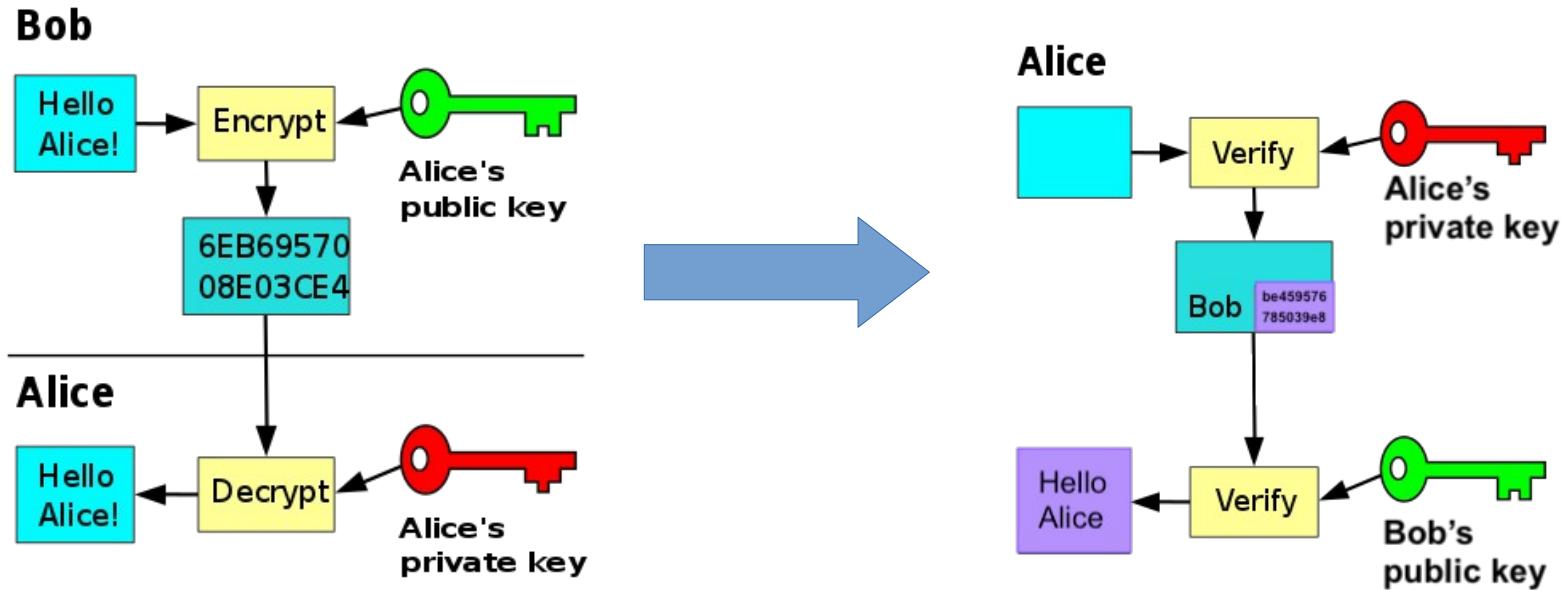
Q2: How can Alice be sure that it was really Bob that wrote that transaction?

- When Alice opens the box with her **Alice private key**, she finds **another box** inside
- But Alice, **like everyone**, has the **Bob's public key**, so he try to open the box she just found.
- If it opens, it means that it was really Bob that sent it, since **only Bob could use the Bob private key to close it**.



Mission Accomplished: Bob sent a message that only Alice can read, without sharing any secret

The **external ALICE BOX** could be opened only by Alice with her private key, and the **internal BOB BOX** could have been closed only by Bob with his private key



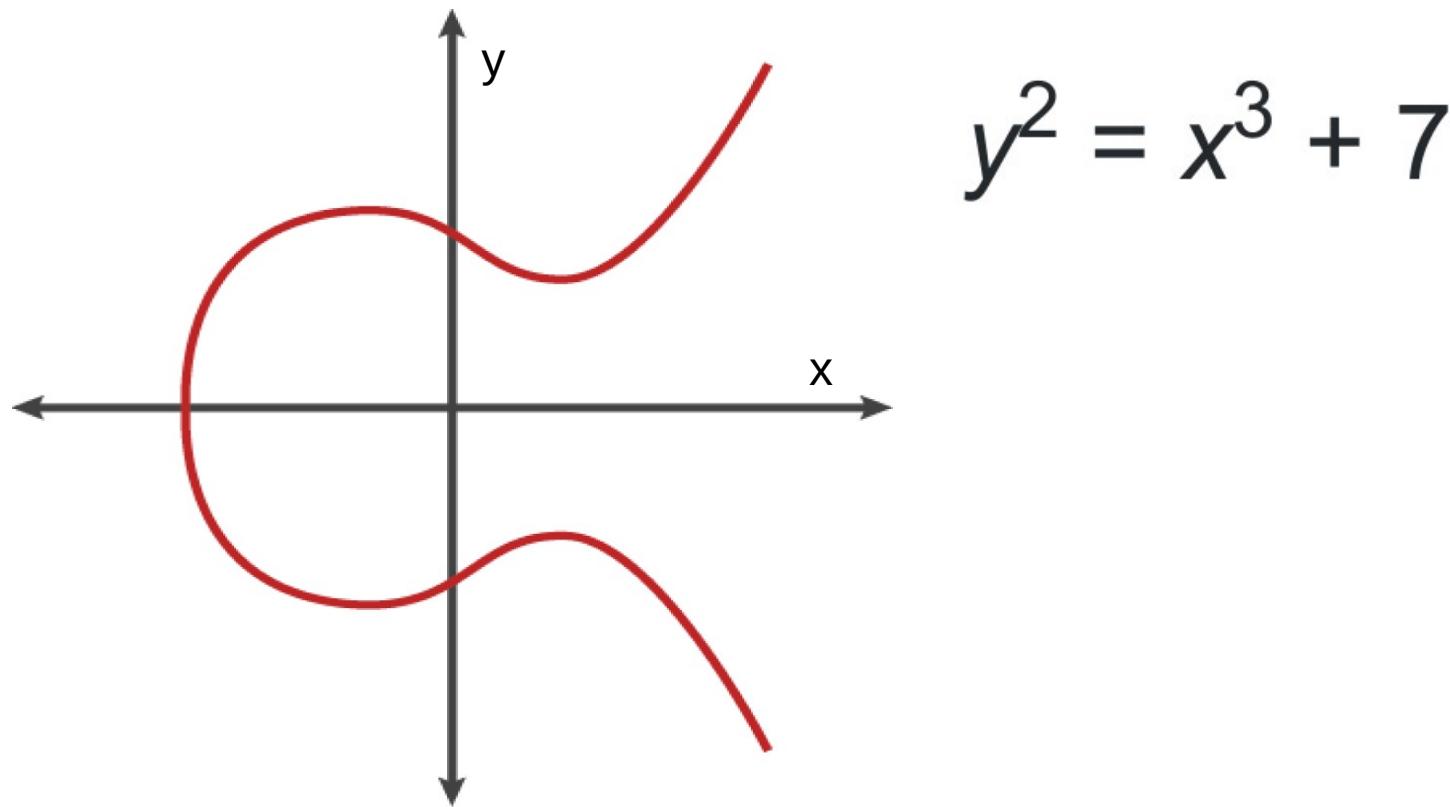
How are those Magic Boxes implemented digitally?

- How can **public key** and **private key** be related without being both revealed?
- In other words: how can I demonstrate to have the **private key** that unlocks was has been sent to my **public key**?
- **But most important:** what are those keys?

It's Time for Fun Math

- Let's consider a number: **e**
- Let's consider a constant number **G** which is the same for everyone and known by everyone
- In traditional math, if I have “**e**” and **G**, it's easy to compute:
 - $P = e * G$
- Also in the opposite direction:
 - if I give you the result **P**, and ask you to guess which is “**e**”, it's very easy: $e = P/G$
- Thus, in traditional math, the equation $P = e * G$ is reversible

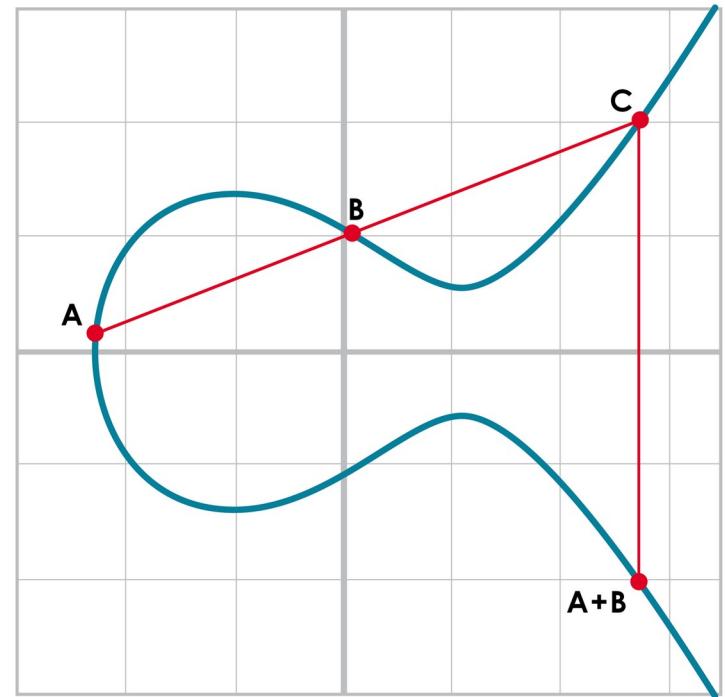
Elliptic Curve Math (secp256k1)



Let's define a new type of Addition

Define an addition operation like this:

- Given two points A and B, trace a line passing by A and B
- The result is the symmetric of the intersection C on the other side of the plane

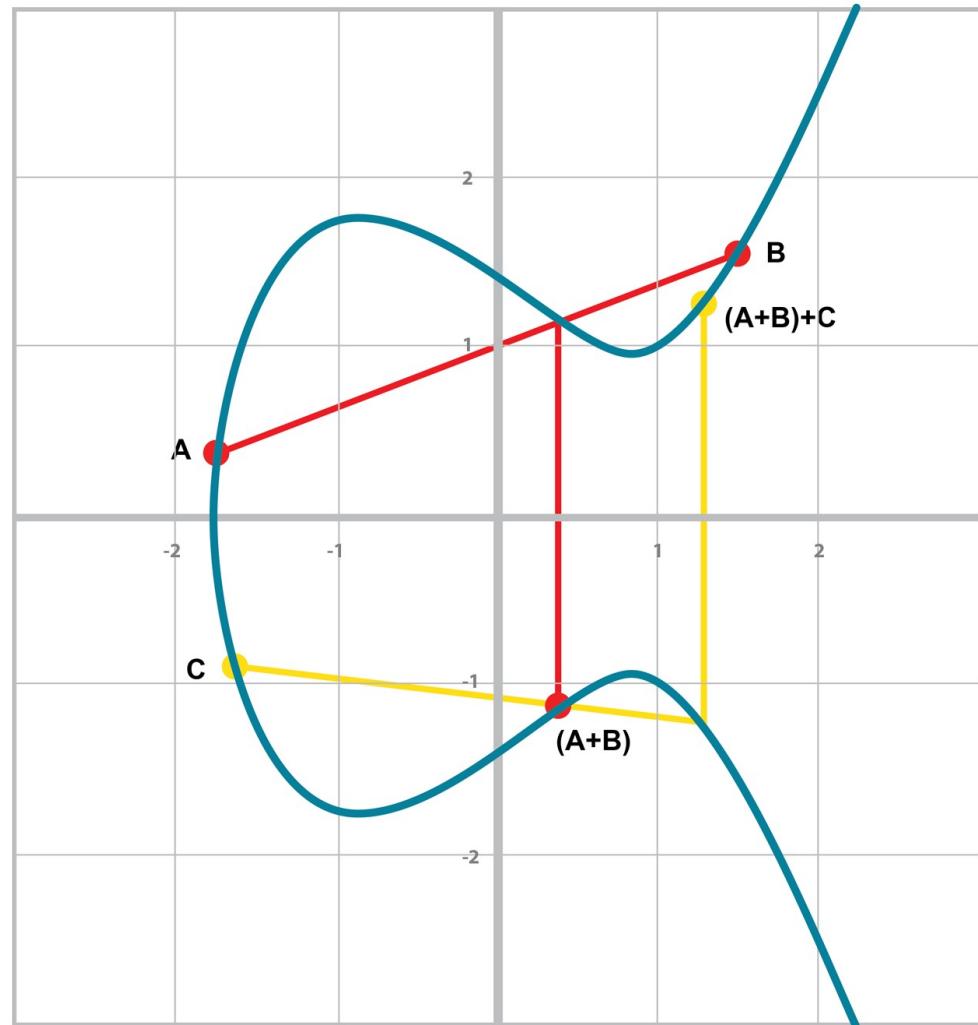


Fun fact: in a so defined addition,
all the traditional known properties
still remain!
(commutative, associative, etc...)

Try by yourself:

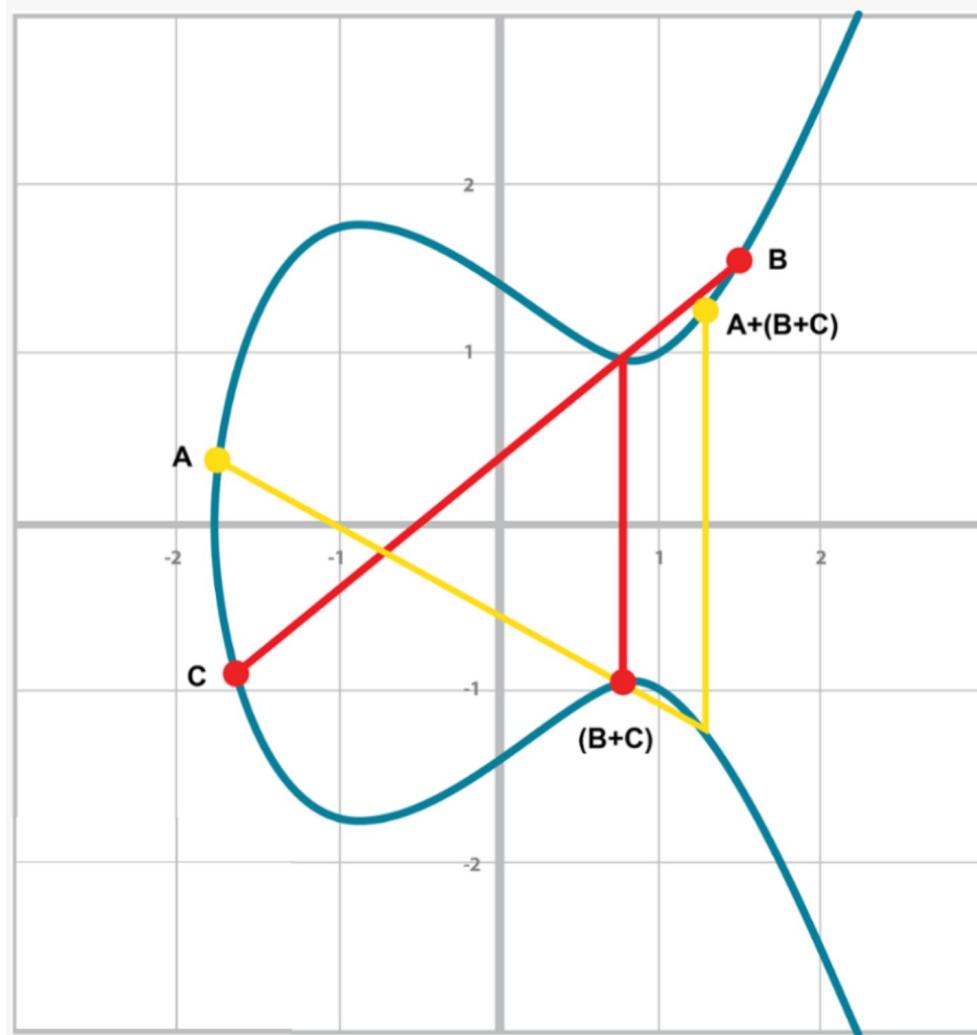
$$(A+B) + C = A + (B+C) ?$$

Start with $(A+B)$ then add C



...now do $A + (B+C)$

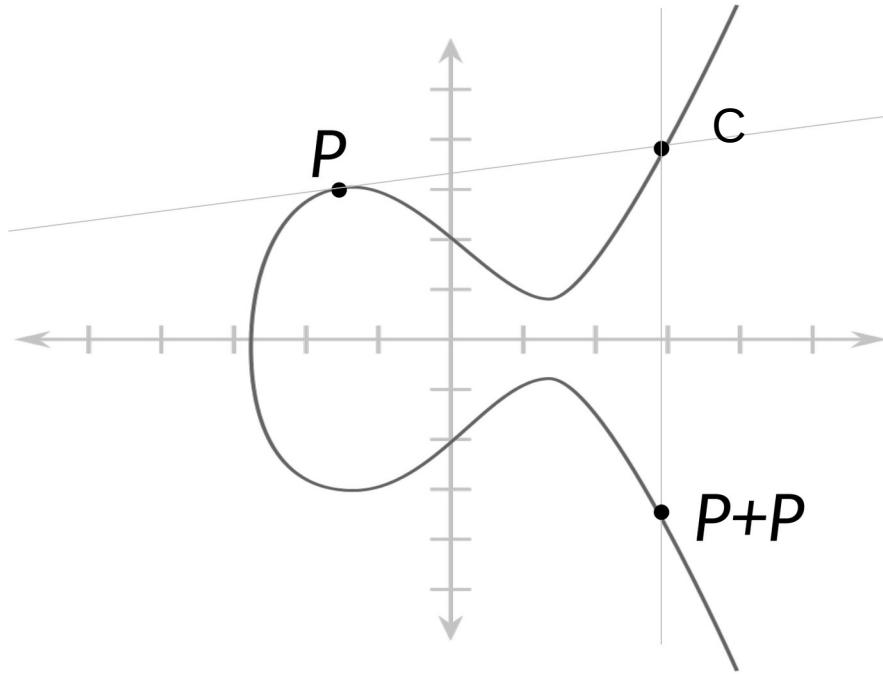
it's the same point as in
the previous slide!



Adding a Point to itself

A is the same as B, they are both in the “P” position, so it’s like:

- plotting the tangent to the curve passing by P
- going to the symmetric point of the intersection C, as usual

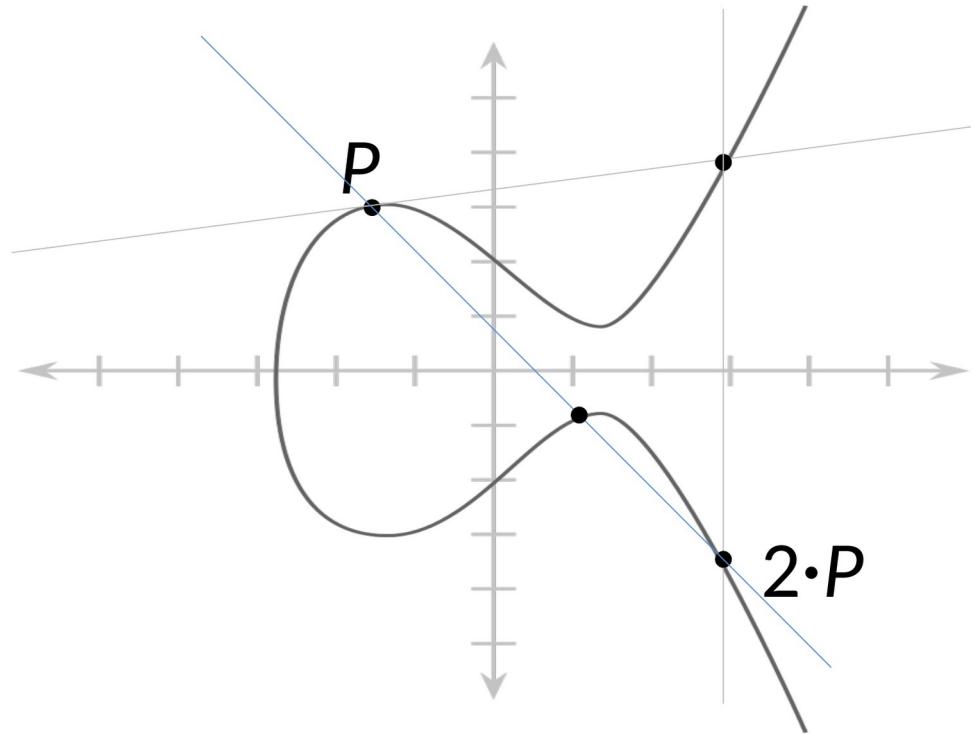


Scalar Multiplication

**What does it mean to start
from a point P and multiply it
by n ?**

For example, with $n = 6$:

$$6 \cdot P = P + P + P + P + P + P$$

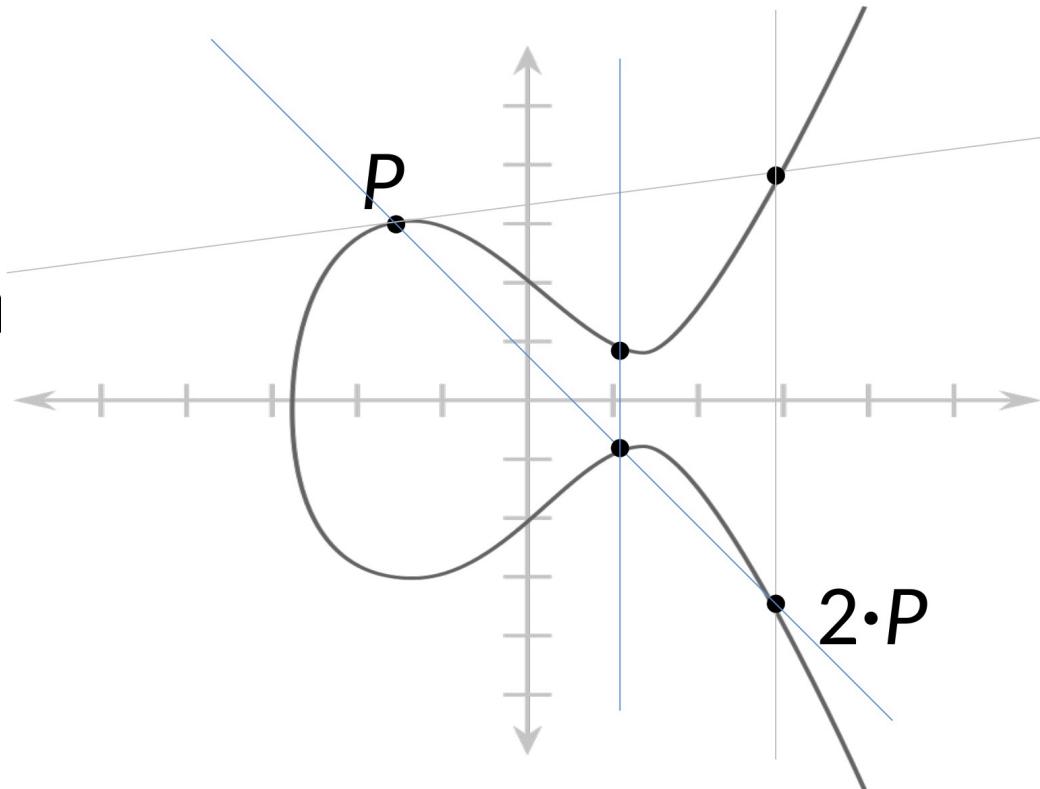


Scalar Multiplication

What does it mean to start from a point P and multiply it by n ?

For example, with $n = 6$:

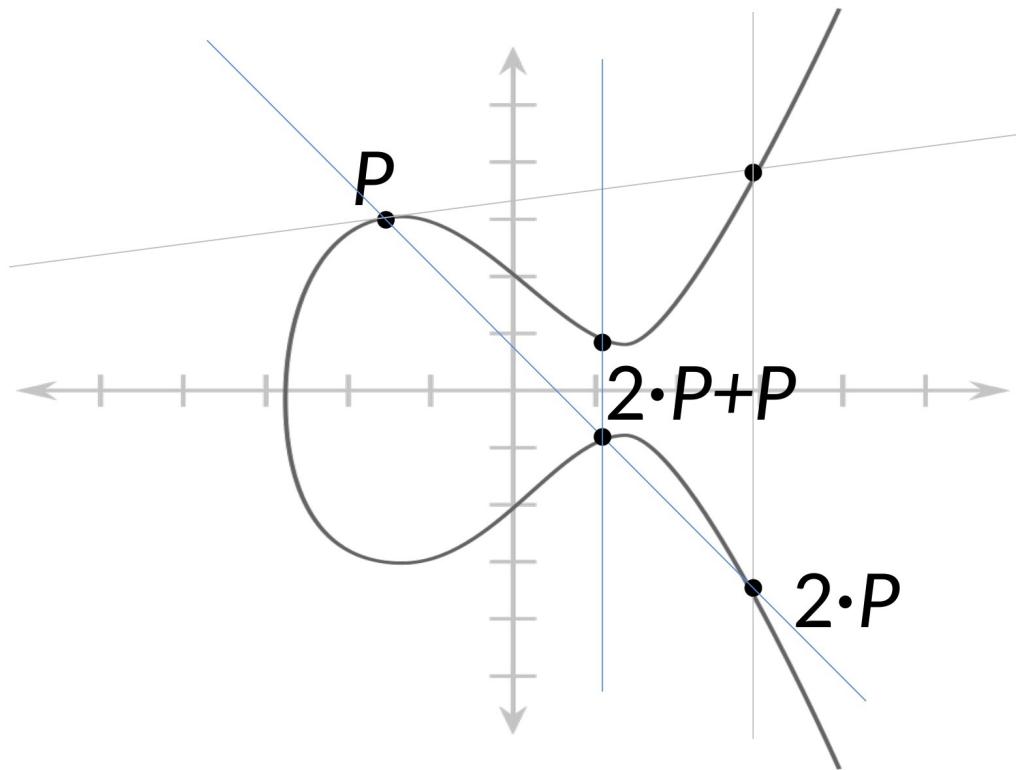
$$6 \cdot P = P + P + P + P + P + P$$



Scalar Multiplication

What does it mean to start
from a point P and multiply
by n ?

For example, with $n = 6$:
 $6 \cdot P = P + P + P + P + P + P$



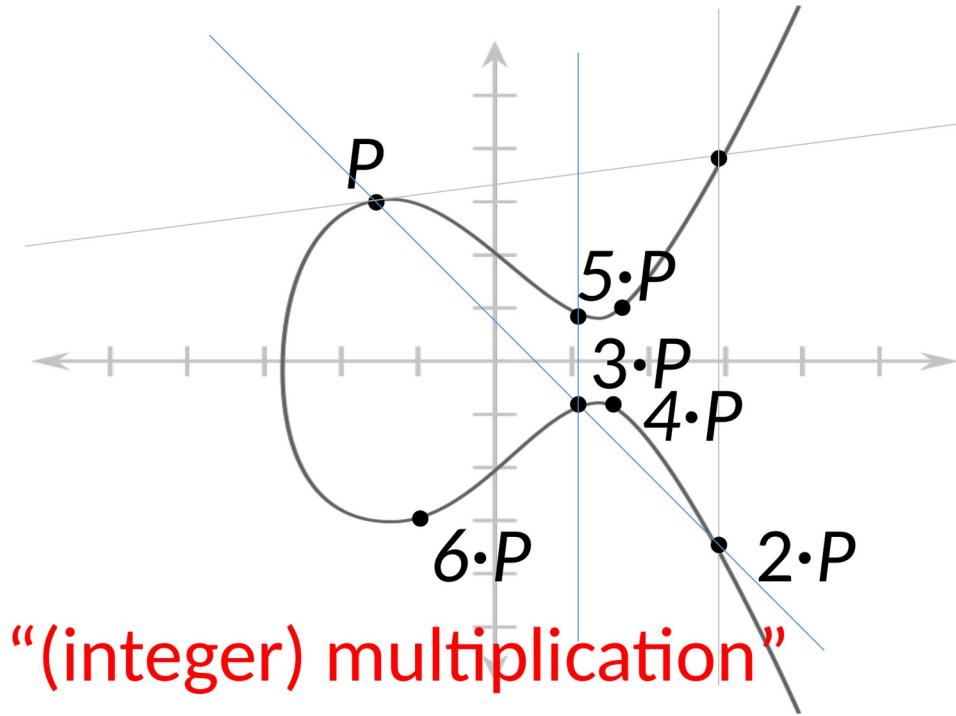
Scalar Multiplication

What does it mean to start from point P and multiply it by n?

For example, with $n = 6$:

$$6 \cdot P = P + P + P + P + P + P$$

Notice: every step it's easy, but it seems to follow strange path, like a bouncing ball...



Scalar Multiplications shortcuts

Scalar multiplication can be exponentially reduced by using the geometric properties of Elliptic Curve Math (eg, doubling using the tangent)

To go from a point P to $100 \cdot P$:

$$P \rightarrow 2 \cdot P$$

$$2 \cdot P \rightarrow 3 \cdot P$$

$$3 \cdot P \rightarrow 6 \cdot P$$

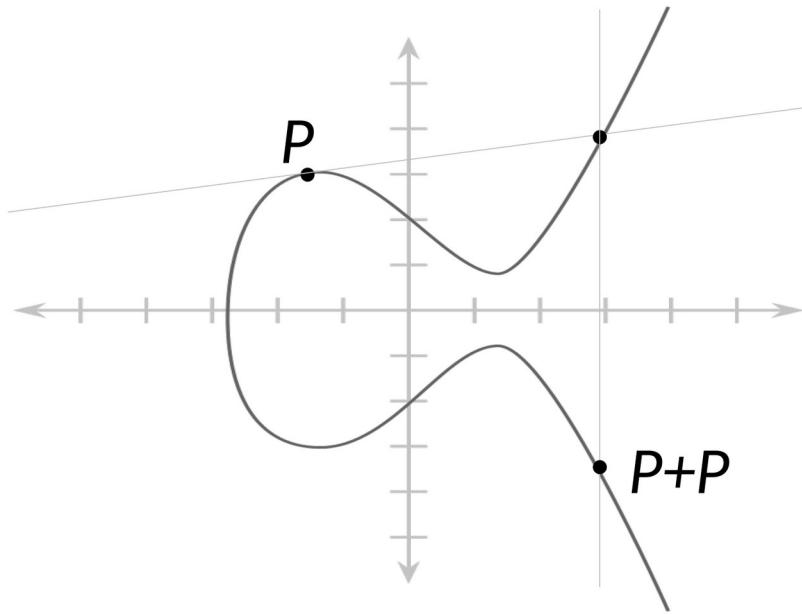
$$6 \cdot P \rightarrow 12 \cdot P$$

$$12 \cdot P \rightarrow 24 \cdot P$$

$$24 \cdot P \rightarrow 25 \cdot P$$

$$25 \cdot P \rightarrow 50 \cdot P$$

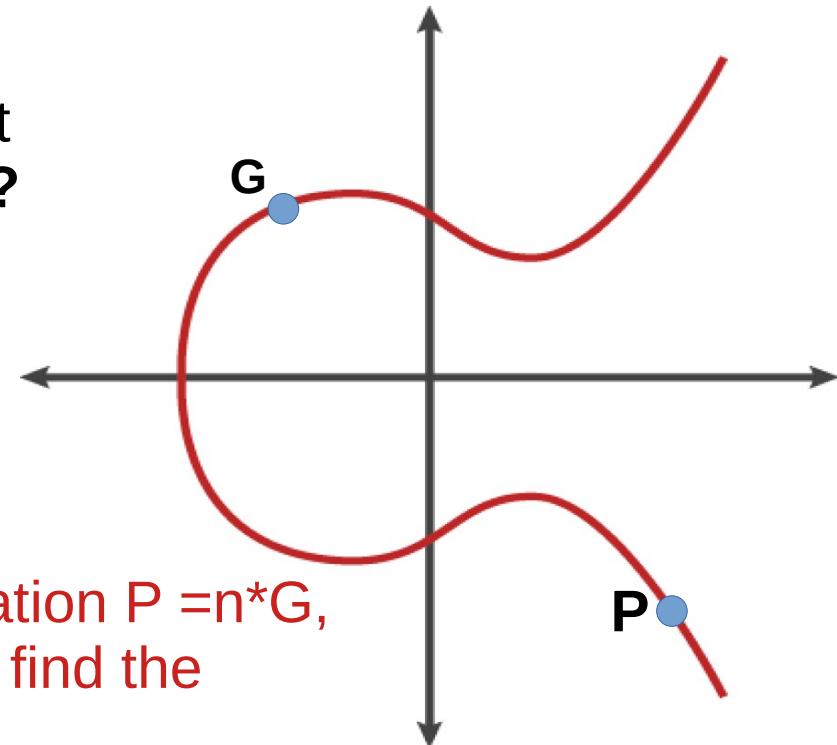
$$50 \cdot P \rightarrow 100 \cdot P$$



Inverting of Scalar Multiplication

Given a final point P and a starting point
Can you guess “n” such that $P=n \cdot G$?

the only way to find the number n is to
try P , $2 \cdot P$, $3 \cdot P$, etc.



There is no way to reverse the multiplication $P = n \cdot G$,
except testing every number until you find the
correct n

Private/Public Key Generation

- Starting from a BIG random number “**e**”, I compute $\textcolor{green}{P} = \textcolor{red}{e} * \textcolor{green}{G}$
- **G** is a prefixed point of the elliptic curve, known as “**generator point**”
- The coordinates of the resulting point **P** will be my **Public Key**
- I’m the only one who knows the “**e**” number, this will be my **Private Key**. Thus, **I’m the only one able to decompose P as $e * G$**
- All the numbers are 256 bits, so for the other people it is impossible to test every potential “**e**” to check if $\textcolor{red}{e} * \textcolor{green}{G} = \textcolor{green}{P}$

How Big is 2^{256} ?

To give you an idea, here are some relative scales: **2^{256} is about 10^{77}**

- Number of atoms in the universe $\sim 10^{80}$
- A trillion (10^{12}) computers doing a trillion computations every trillionth ($10^{(-12)}$) of a second for a trillion years is still less than 10^{56} computations.
- Think of finding a private key this way: **there are as many possible private keys in Bitcoin as there are atoms in a billion galaxies.**



Compact visualization of 256 bits

- 256 bits sized number are huge
- we can represent each group of 4 bits with a single hex digit
- The resulting string will be 64 digits long

DECIMAL	HEX	BINARY
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Secp256k1 Generation Point

Gx =

0x79be667ef9dcbbac55a06295ce870b07029bfedb2dce28d959f2815b16f81798

Gy =

0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8

Elliptic Curve Digital Signature Algorithm (ECDSA)

- Alice sends something to Bob, using Bob's **public key P**
- Bob is the only one owning the **private key e**, that is, the number so that **$e^*G = P$**
- **How can Bob demonstrate that he knows “e”, without revealing “e”?**
- *(notice: this is the mathematical equivalent of “unlocking with the other key” seen before in the two locks box)*

Bob chooses a random number \mathbf{k} , computes a random point $\mathbf{R} = \mathbf{k} * \mathbf{G}$ and shows that he knows two numbers \mathbf{u} and \mathbf{v} so that:

$$\mathbf{u} * \mathbf{G} + \mathbf{v} * \mathbf{P} = \mathbf{R} \quad (\text{equation 1})$$

Since Bob can replace \mathbf{P} with $\mathbf{e} * \mathbf{G}$ and \mathbf{R} with $\mathbf{k} * \mathbf{G}$

$$\mathbf{u} * \mathbf{G} + \mathbf{v} * \mathbf{e} * \mathbf{G} = \mathbf{k} * \mathbf{G}, \text{ then simplify } \rightarrow \mathbf{u} + \mathbf{v} * \mathbf{e} = \mathbf{k} \rightarrow \mathbf{e} = (\mathbf{k} - \mathbf{u}) / \mathbf{v}$$

Bob knows \mathbf{e} and \mathbf{k} , it's easy to find a couple of numbers \mathbf{u}, \mathbf{v} that work for equation 1

As consequence, someone able to find \mathbf{u} and \mathbf{v} that solve the above equation (even for some other \mathbf{k}), could simply derive “ \mathbf{e} ”

→ **Being able to find \mathbf{u}, \mathbf{v} that solve (eq 1) is logically equivalent of knowing the secret “ \mathbf{e} ”**

No Way to Cheat

- Please notice that Bob **only shows u and v** that solve:
 $u^*G + v^*P = R$...but he never reveals which k used!
- Otherwise, anyone could simply derive $e = (k-u)/v$
- **Only u and v have been revealed**, so using $e = (k-u)/v$ is not useful, since there are infinite e and k that solves it

For example: If you set k to some value and solve $e = (k-u)/v$ you will get only one of the infinite (e,k) couples that solves the equation, not the one so that $P = e^*G$

What Does it Means “Owning”?

- **Forget it:** There is nothing as “*having bitcoins in some place*”
- **There is no account, no storage point, no registration**
- “owning” x amount of bitcoin means only 2 things:
 - 1) Some other entity, in some previous transaction, used her/his/its own private key to write in some block that x bitcoin are sent to your **public key P**
 - 2) You know some **private key “e”** and **only you can demonstrate** that **$e^*G = P$** , unlocking them in the future

Since a destination **public key P** is always known, and the **G** point is fixed to a constant...

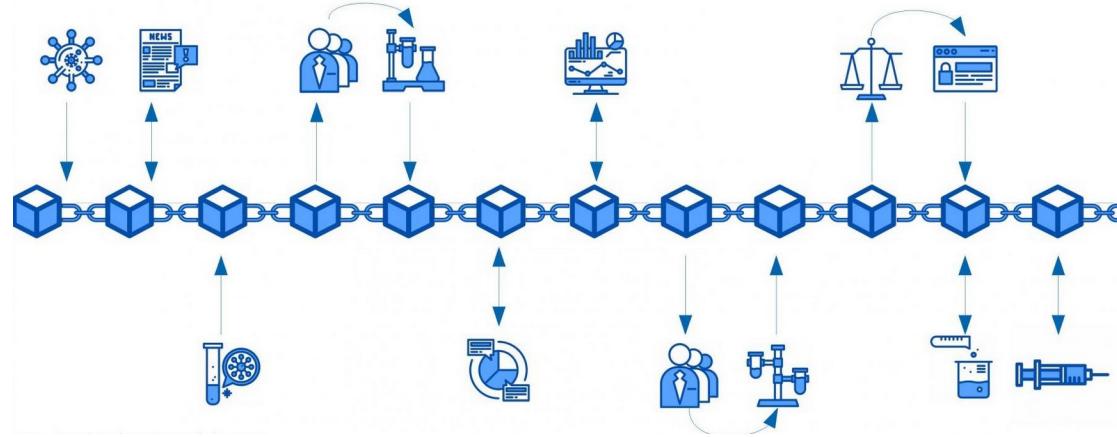
=>

...owning bitcoin means being in possession of a number e of 256 bits so that $P=e \cdot G$, where P is your public key

YOU NEVER TRANSMIT e ANYWHERE, you just prove that you know it!

Answering Question 3 is Trivial

- Does Alice have those x amount of bitcoins that she wants to send?
- **Blockchains allows everyone to agree with the history of transactions → the balance of each entity is known!**



FUD Moment...

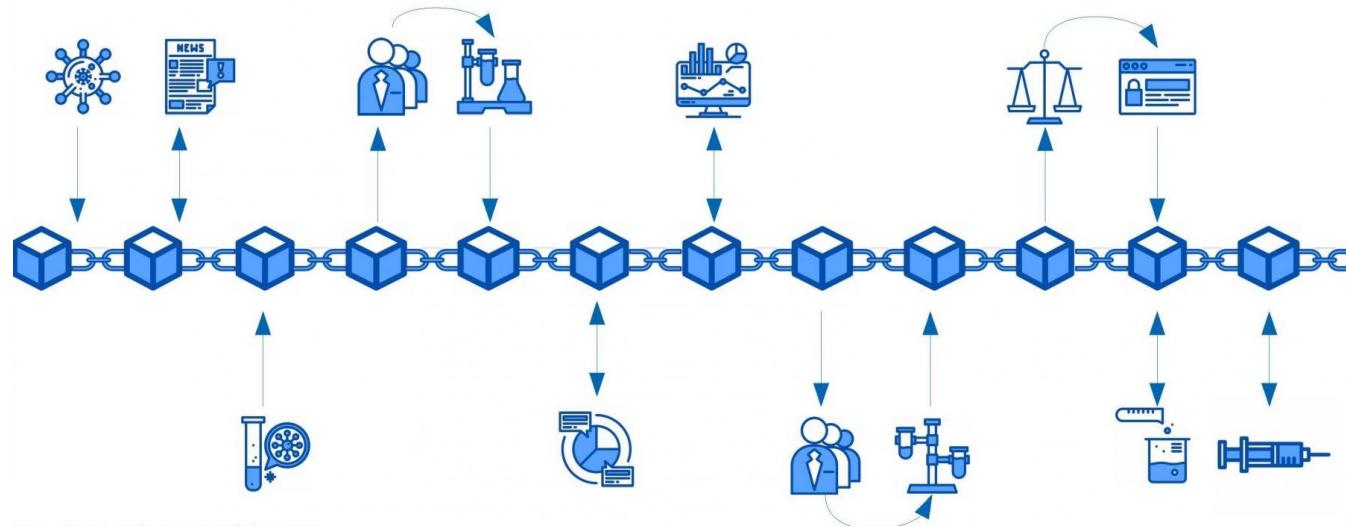


"They will ban you owning BTC"

*Think about it: is it possible to “ban” the possession
of... a number?*

Impossible Mission?

- 1) We must guarantee the order of events
- 2) Ensure that sender and receiver are the correct ones
- 3) Entities not trusting each other agree on some “digital reality”

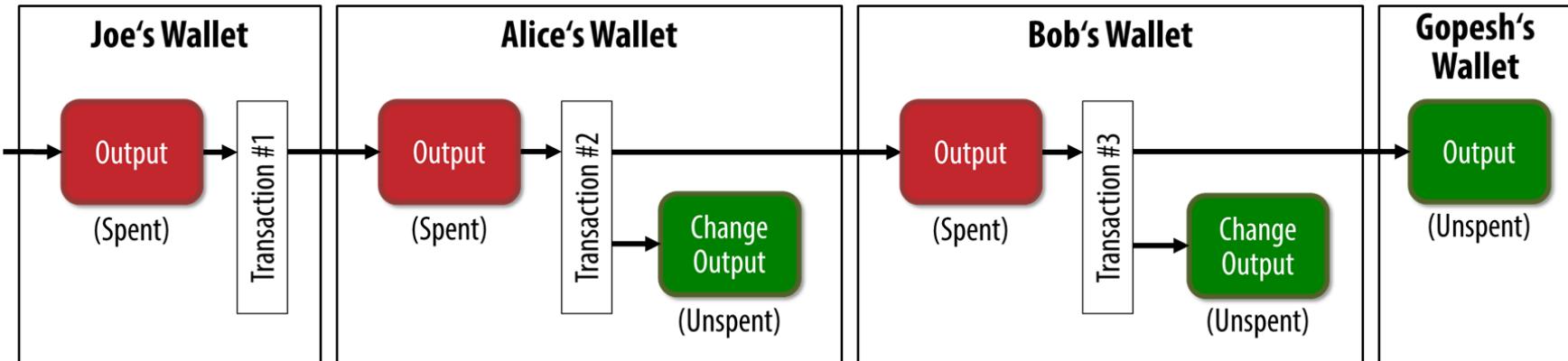


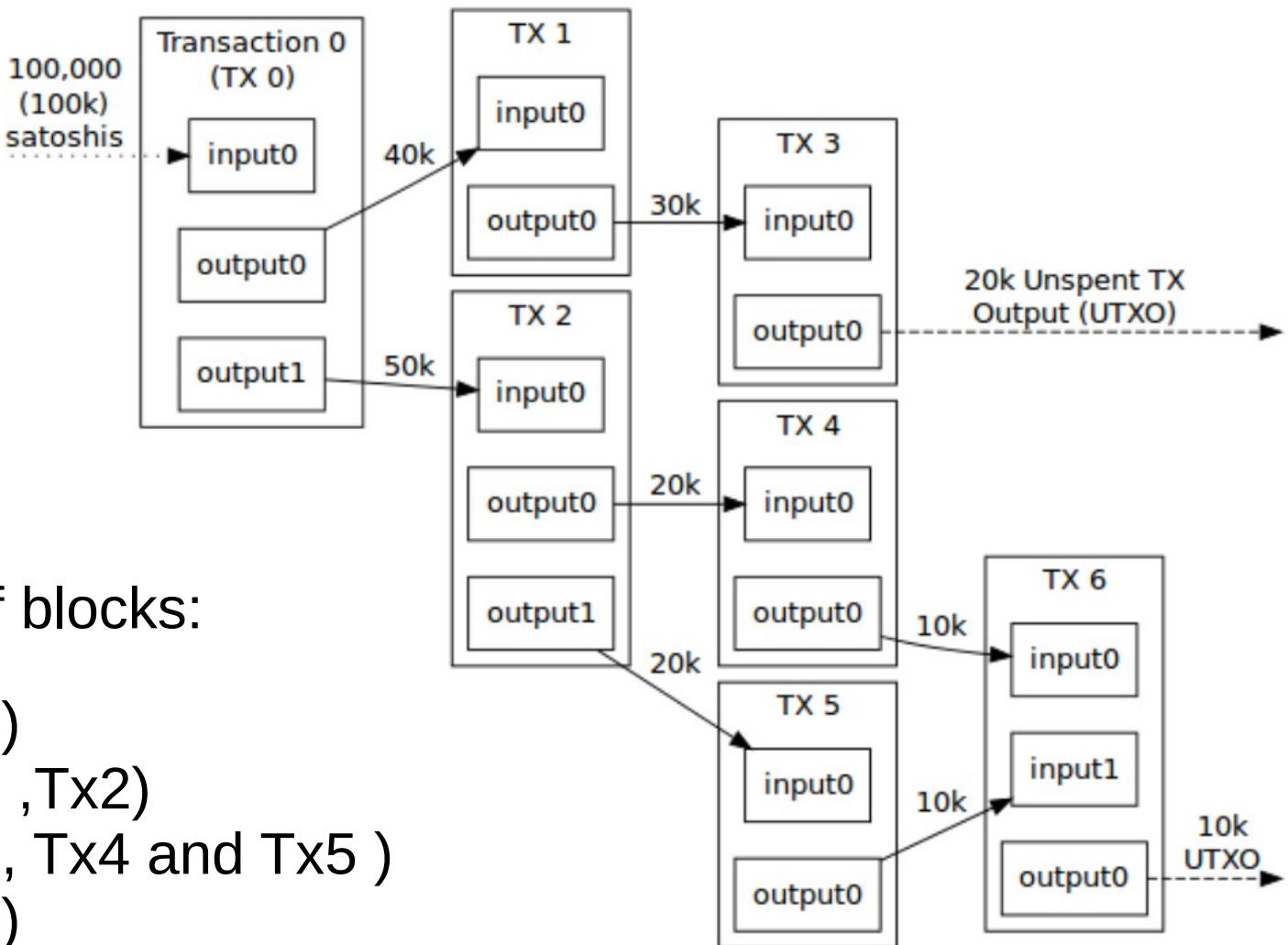
Outline Day 2

- Asymmetric Cryptography
- **Transactions on Chain**
- Short History of Bitcoin
- Blockchain as a Platform: Proof-of-Existence, NTF, Smart Contracts
- Scalability: the Blockchain Trilemma
- Bitcoin Layer 2: the Lightning Network

Transactions on Chain

- Each transaction consists in spending previous received bitcoin (outputs) using them as inputs
 - Only the private key owners can spend them, to create new outputs using public keys of destinations





Sequence of blocks:

Block 1(Tx 0)

Block 2 (Tx1 ,Tx2)

Block 3 (Tx3, Tx4 and Tx5)

Block 4 (Tx6)

DEMO: blockstream

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2

1Cd1d9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)



1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA
- (Unspent) 0.015 BTC
1Cd1d9KFAaatwczBwBttQcwXYCpvK8h7FK -
(Unspent) 0.0845 BTC

97 Confirmations

0.0995 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

FUD Moment...



"...so you can follow the history of each public key address... Wait a moment...."

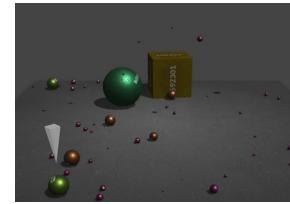
...wasn't it the perfect tool for hidden Illegal activity?!?

Transaction Visualization Tools

<https://blocks.wizb.it/#>



<https://privacypros.io/tools/bitbonkers/>



<https://bitnodes.io/nodes/live-map/>



<http://www.bitlisten.com/>

Brain Wallets

- **IDEA:** Choose some words you think you will always remember calculate the SHA256 hash, use the resulting 256 bits number as **private key e**
- The public key will be easy to calculate, since $P=e^*G$
- Everybody will use **P** to send you bitcoin, but nobody will be able to know “e” to unlock them
- **You will not need to remember the long number “e”, since you can recreate it by hashing your secret phrase**

Brain Wallets are a BAD Idea

- Human brain is not good a good source of entropy :)
- An attacker focused on you could try millions of words combinations related to you, e.g.:
“I love <WIFE/HUSBAND/CAT_NAME>”
- It's not required to attack a specific person: quotes like beginning of books, songs, etc are very easily checked in any moment

- Four of the sweeps occurred after 22 blocks
- The first one took a few seconds
- All the funds were swept away within a day

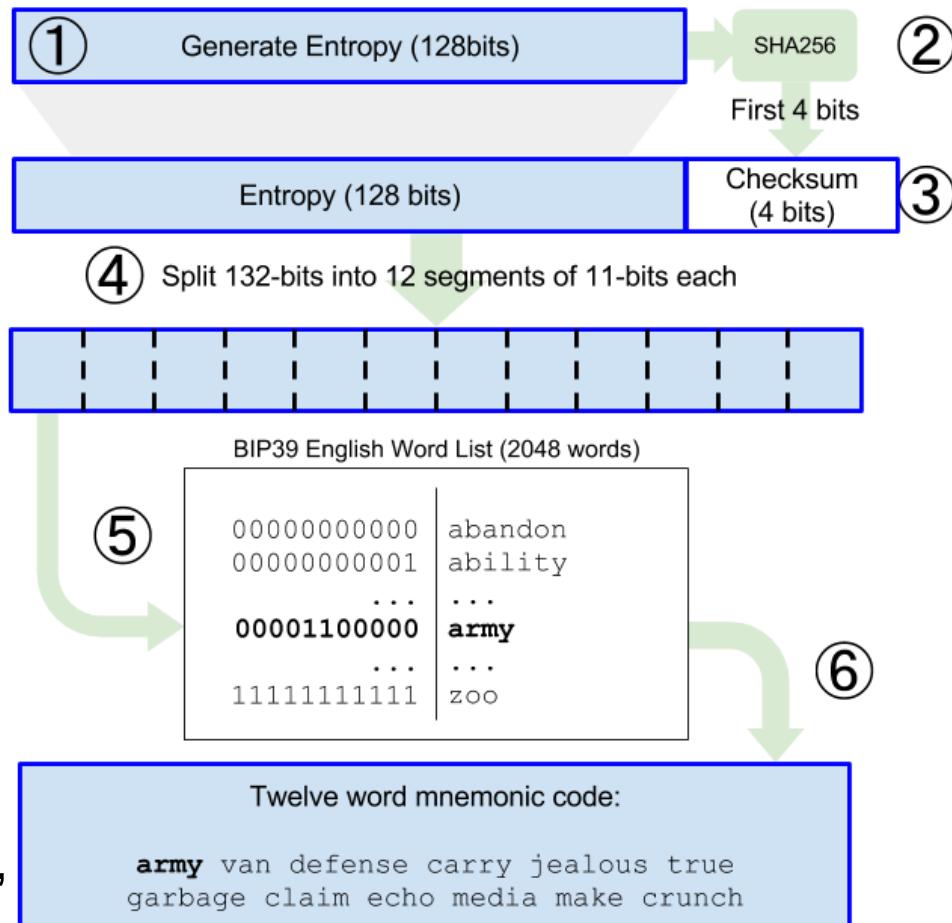
<https://blog.bitmex.com/call-me-ishmael/>

Passphrase	Source	Sha256
<i>Call me Ishmael</i>	"Moby-Dick" by Herman Melville	a88910233e176ef4489b 52d686f326d7ff9ccff6 86065a44cbd366538450 8ad6
<i>It is a truth universally acknowledged, that a single man in possession of a good fortune, must be in want of a wife</i>	"Pride and Prejudice" by Jane Austen	be09c4df6444afa6adff 8098c0cf273c3e9fef04 a1a8e20de8218eca0bec 383d
<i>It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair</i>	"A Tale of Two Cities" by Charles Dickens	e051a4337000945d99a4 6ac1b56244106f732535 c11c22c229c6d620ab47 199f
<i>In the beginning God created the heaven and the earth</i>	The King James version of the Bible	f153b22c61d6013bf2d7 aa5a3fe7532718763613 1e9022dab1304333751a 7301
The answer, my friend, is blowin' in the wind	"Blowin' in the Wind" by Bob Dylan	aeac73098d2b9a29ba47 c4893c2d0b6fbba487d 21b1b3a57a55ee11c7a6 a476

- The speed of the redemption of the funds clearly indicates that people have **servers up online 24/7 scanning the blockchain**
- These servers are likely to have **pre-generated many hundreds of thousands of Bitcoin addresses**, using text from thousands of published works, music, books, academic papers, magazines, blogs, tweets and other media and then stored these in a database.

Seedphrase

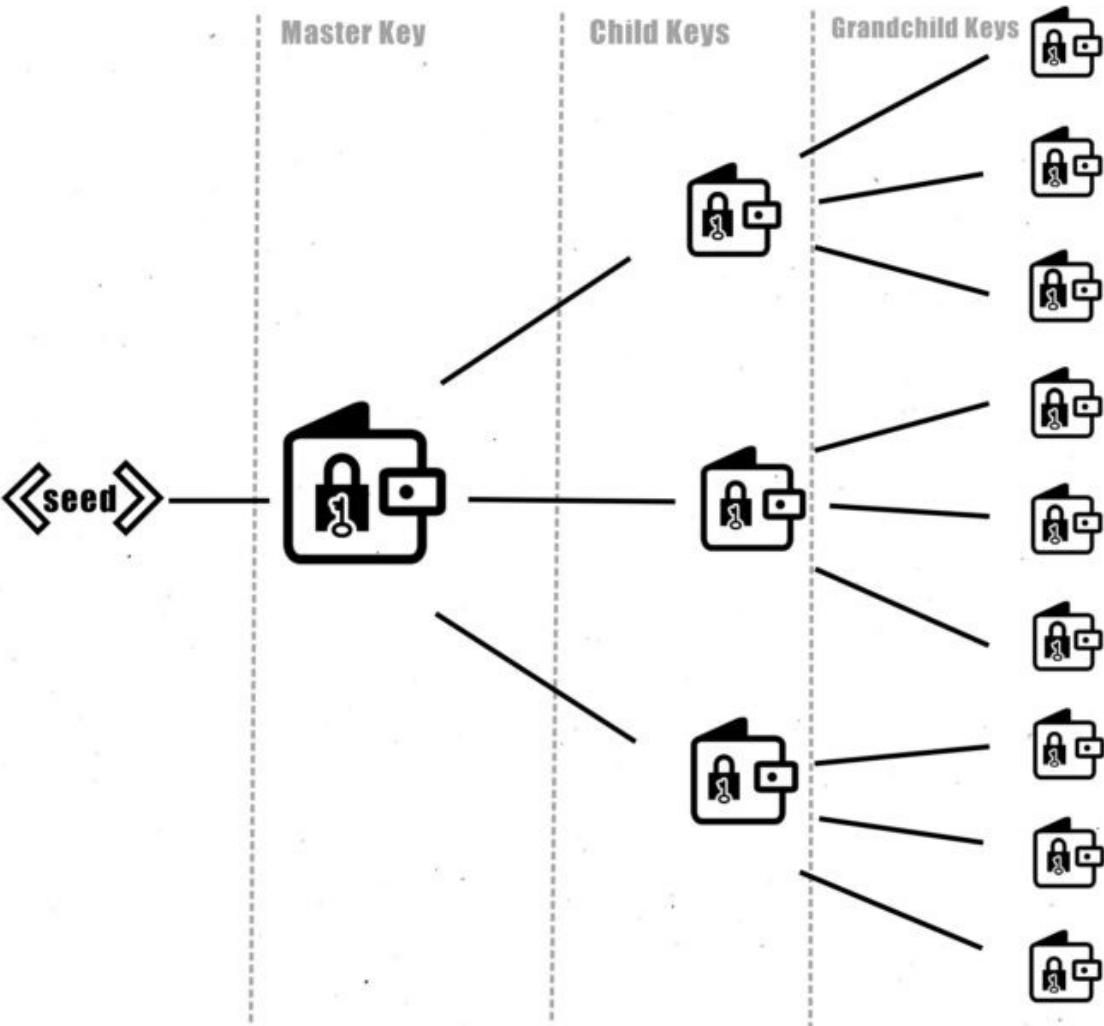
- NOT generate **private key** from a set of words (brainwallet), but the opposite!
- BIP39 is the most common standard used for seed phrases.
- Vocabulary of 2048 words, so each word can be associated to the combination of 11 bits
- These words are specifically chosen so that cannot be confused, even if handwritten



DEMO: Try BIP39

<https://learnmeabitcoin.com/technical/mnemonic>

- Until a few years ago, you still need a different Seephase of each of your private keys
- **Hierarchical Deterministic Wallet** allows you to generate a new private key every time you new.
- All your possible private keys numbers are deterministically derived from you master private key



“Not your Keys, Not your Coins”

Good news:

- you need only to keep safe a single seedphrase of 12 words
- **No accounts, no data backup, nothing, it's not a password:**
it's only a number that origins of all your possible private keys

Bad news:

- Such freedom comes with responsibility
- If you lose the seedphrase and don't have a copy of it, you lose access to your private keys → you will not be able to use your bitcoins

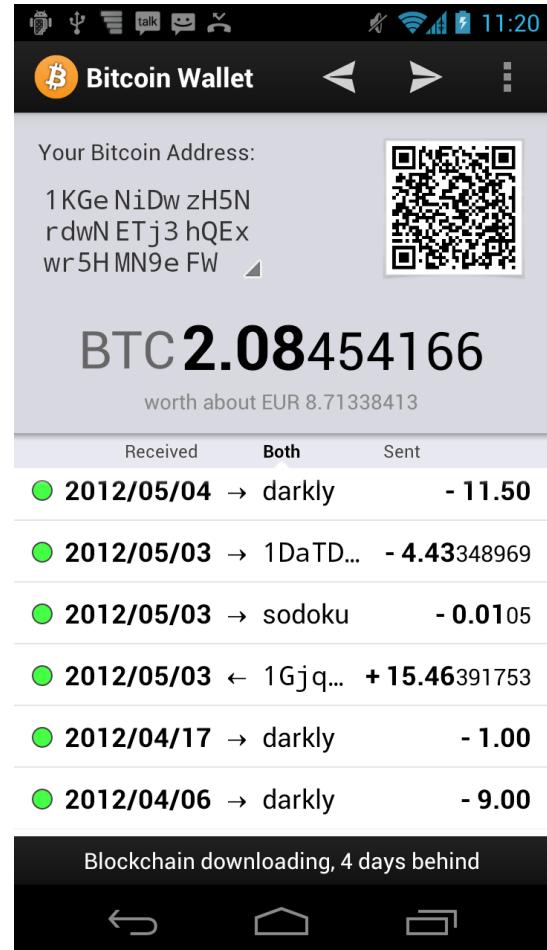
Some Common Sense Suggestions

- Just copy the words in 2 or 3 pieces of paper and put in different locations
- Never type the words in web sites
- Typing is required only when restoring your keys (formatting hard drive, moving to a new device etc...)

If you think this is too serious, you should look at this:
<https://jlopp.github.io/metal-bitcoin-storage-reviews/>

What are Wallets?

- An user could have multiple private/public keys in possession
- Thus, from the perspective of the user, the “balance” is the sum of all his/her unspent outputs
- A Wallet is a software that collects all private/public keys for a given user
- A Wallet is only meant to improve the user-experience: blockchain knows nothing about “wallets”, there only transactions



DEMO: Using a Wallet on Testnet

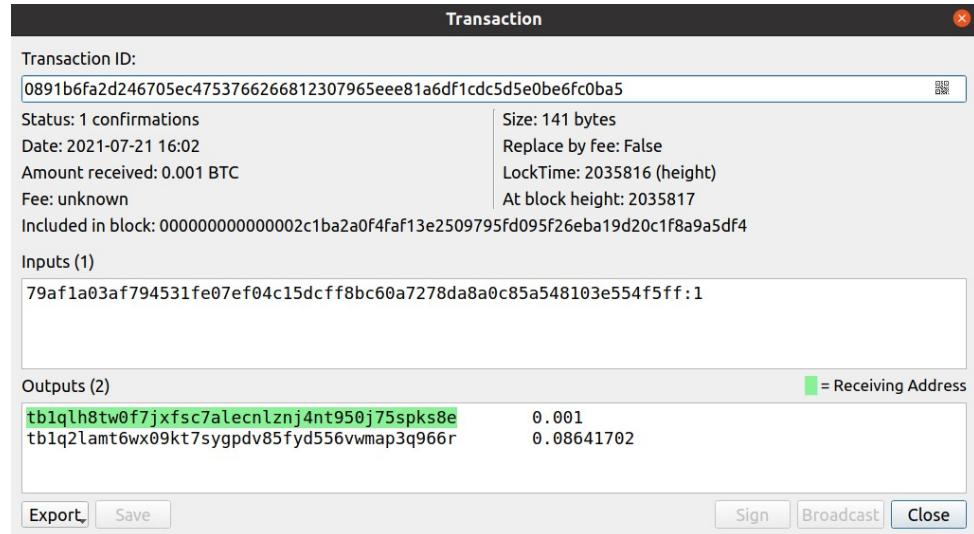
Electrum wallet (or another): <https://electrum.org/#download>

Run normally at least once, then try the testnet:

- On MacOS terminal:
 - open -n /Applications/Electrum.app --args --testnet
- On Windows terminal:
 - electrum-4.0.4-portable --testnet
 - or equivalent, depending on your executable name
- On Ubuntu/Linux:
 - python3 Electrum-4.1.5/run_electrum --testnet

DEMO: Testnet Faucets

- Get free testnet bitcoins from a faucet (see <https://en.bitcoin.it/wiki/testnet>)
- <https://testnet-faucet.mempool.co/>



Outline Day 2

- Asymmetric Cryptography
- Transactions on Chain
- **Short History of Bitcoin**
- Blockchain as a Platform: Proof-of-Existence, NTF, Smart Contracts
- Scalability: the Blockchain Trilemma
- Bitcoin Layer 2: the Lightning Network

How all this started...

On October 2008, in a mailing list named “cypherpunks” dedicated to cryptography, an anonymous person using the name “Satoshi Nakamoto” announced that (he/she/they?) has solved a problem in Computer Science

Bitcoin P2P e-cash paper

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Fri Oct 31 14:10:00 EDT 2008

- Previous message: [Fw: SHA-3 lounge](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:

<http://www.bitcoin.org/bitcoin.pdf>

The main properties:

Double-spending is prevented with a peer-to-peer network.

No mint or other trusted parties.

Participants can be anonymous.

New coins are made from Hashcash style proof-of-work.

The proof-of-work for new coin generation also powers the network to prevent double-spending.

Satoshi's White Paper

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

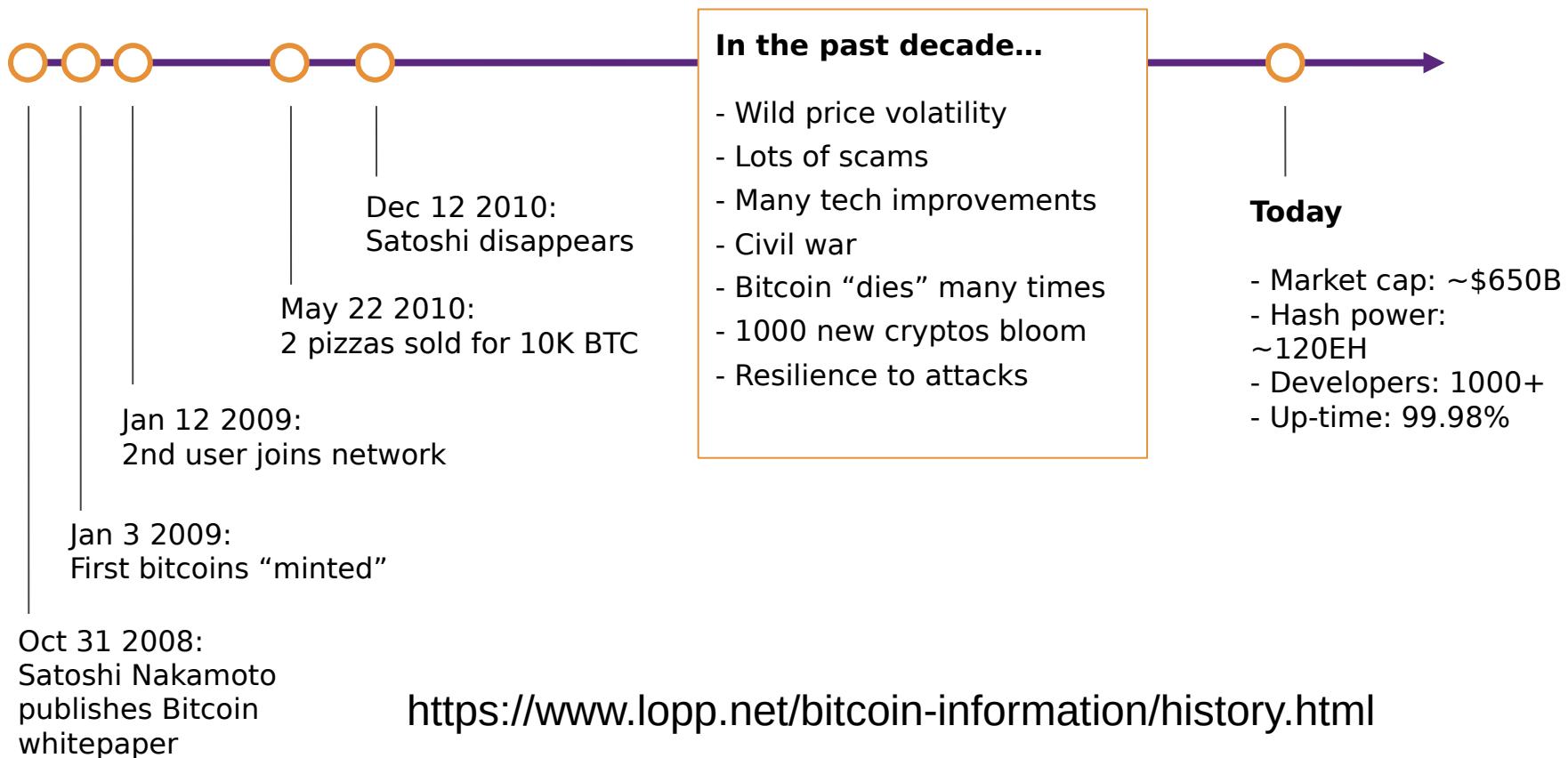
The Mystery of Satoshi

- Who is Satoshi Nakamoto? He? She? *They*? No one knows.
- Has remained anonymous despite worldwide attention.
- **Lack of a leader is a huge benefit to Bitcoin.**
- Satoshi's coins have never moved
- Many impostors: beware!



<https://satoshi.nakamotoinstitute.org/>

Short history of Bitcoin



Bitcoin Genesis Block

Raw Hex Version

00000000	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020	00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E	7A 7B 12 B2 7A C7 2C 3E;fíýz{.²zC,>
00000030	67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA	88 8A 51 32 3A 9F B8 AA	gv.a.È.À^SQ2:Ý,a
00000040	4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iÿÿ...¬+
00000050	01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070	00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D	FF FF 4D 04 FF FF 00 1DÿÿÿM.ÿ..
00000080	01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F	69 6D 65 73 20 30 33 2F	..EThe Times 03/
00000090	4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C	20 43 68 61 6E 63 65 6C	Jan/2009 Chancel
000000A0	6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20	72 69 6E 6B 20 6F 66 20	lor on brink of
000000B0	73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66	61 69 6C 6F 75 74 20 66	second bailout f
000000C0	6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05	FF FF FF FF 01 00 F2 05	or banksÿÿÿ..ð.
000000D0	2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27	67 8A FD B0 FE 55 48 27	*....CA.gSý°þUH'
000000E0	19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6	5C D6 A8 28 E0 39 09 A6	.gñ q0..\\Ö"(à9.
000000F0	79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4	49 F6 BC 3F 4C EF 38 C4	ybaë.ap"!Ök?Li8Ä
00000100	F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57	5C 38 4D F7 BA 0B 8D 57	öU.å.Á.p\8M+º..W
00000110	8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00	AC 00 00 00 00	ŠLp+kñ._¬....



First Usage Ever Documented

Author Topic: Pizza for bitcoins? (Read 774759 times)

Laszlo
Full Member
 #1

Activity: 199
Merit: 149



Pizza for bitcoins?
May 18, 2010, 12:35:20 AM
Merited by alani123 (12), OgNasty (10), d5000 (5), EFS (1), vapourminer (1), iluvbitcoins (1), jacktheking (1), LoyceV (1), coolcoinz (1), Kda2018 (1), TheQuin (1), Toxic2040 (1), Toughtit (1), nullius (1), alia_armelle (1)

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

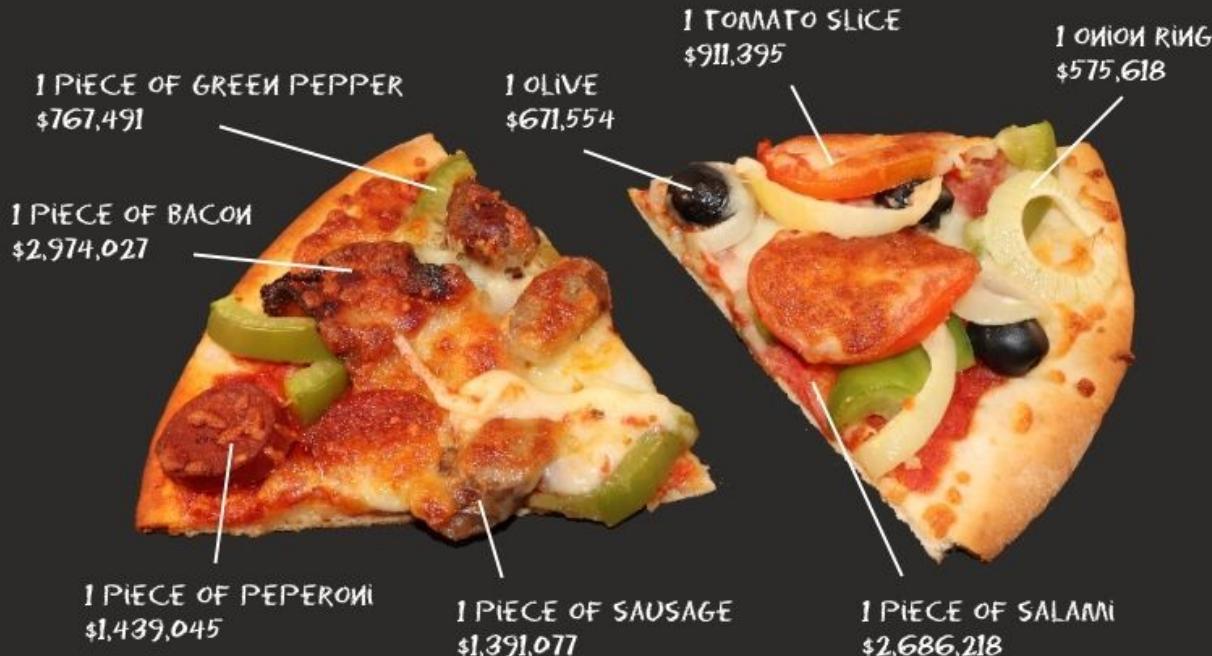
Thanks,
Laszlo

BC: 157fRrqAKrDyGHR1Bx3yDxeMv8Rh45aUet

2 PIZZAS: \$314,671,231

1 PIZZA: \$157,335,616

1 SLICE: \$19,666,952



July 16 2021, [BitcoinPizzaIndex.net](https://bitcoinpizzaindex.net)

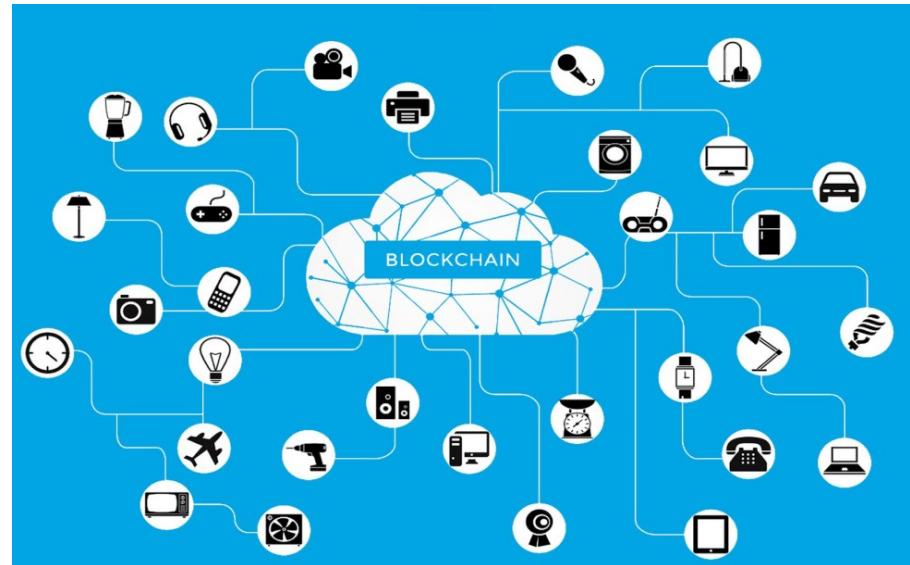
<https://bitcoinpizzaindex.net/>

Outline Day 2

- Asymmetric Cryptography
- Transactions on Chain
- Short History of Bitcoin
- **Blockchain as a Platform: Proof-of-Existence, NTF, Smart Contracts**
- Scalability: the Blockchain Trilemma
- Bitcoin Layer 2: the Lightning Network

Blockchain as a Platform

- What is revolutionary about Bitcoin and Blockchain **it's not strictly limited to the idea money**
- A blockchain is a layer that represents **an immutable sequence of events** on which different actors must agree, not by trusting each other, but trusting in in the laws of math.



Layer 1 Native Asset: BTC (bitcoin)

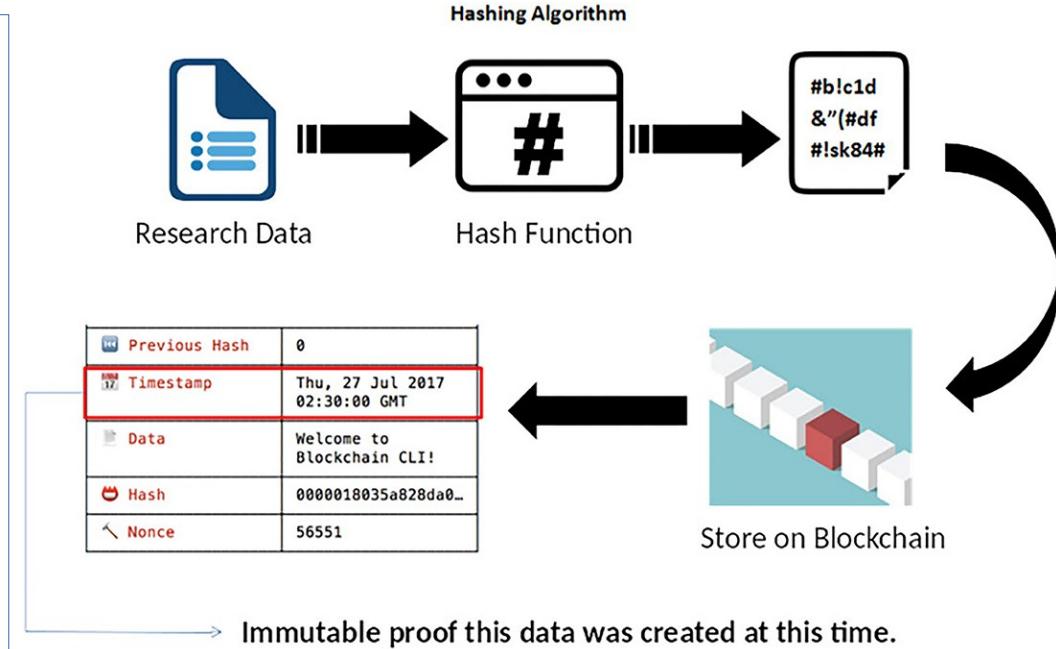
- The simplest kind of transaction that can be imagined is a transfer of value
- 21 Millions of BTC will be asymptotically reached around the year 2140
- The basic unit is the **satoshi**, which is 0.00000001 BTC, that is, 100M sat = 1 BTC
- At layer 1, the Bitcoin protocol implements the first form ever seen of “digital scarcity”

(From Workshop Day1) What makes good money? Bad money?

- **Durable**: doesn't perish
- **Portable**: easy to transport
- **Fungible**: one is interchangeable with another
- **Verifiable**: easy to check authenticity
- **Divisible**: support exchange of small amounts
- **Scarce**: can't be abundant or easy to produce (iron is an useful metal...but..)

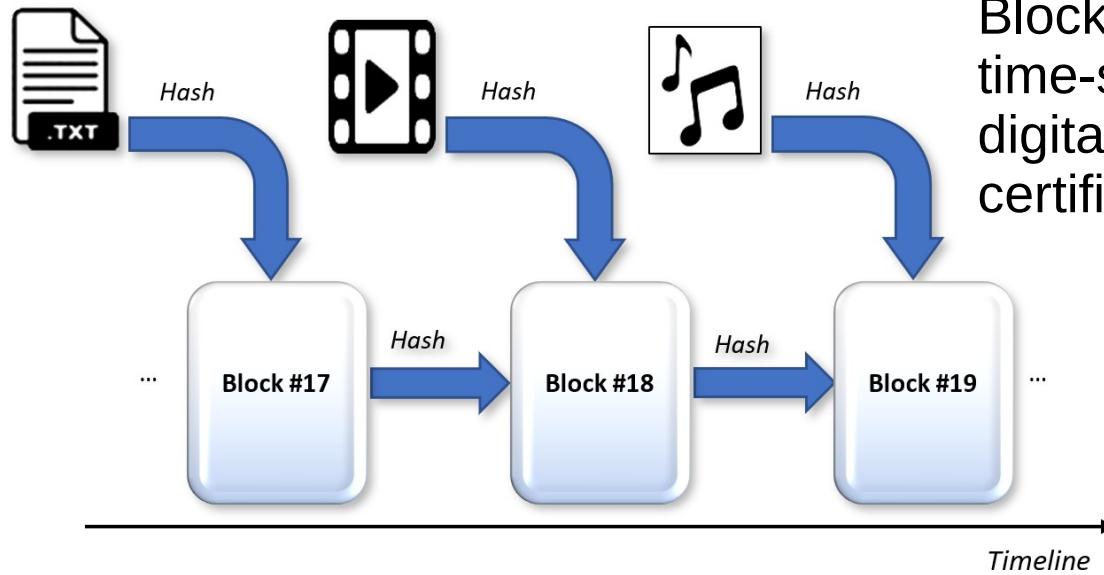
Proof-of-Existence using Unspendable Outputs

- In place of the public key of the destination, **the hash value of some data** could be used
- Of course, **no one holds the corresponding private key e** , since it hasn't been generated
 $P=e^*G$
- By sending a few satoshis, you stored forever the proof-of-existence of that data at the transaction date.



Proof-of-Existence

The Blockchain doesn't know if the 256 bits of a destination are a public key of the SHA256 hash output of some file.



Blockchain as distributed and time-stamped ledger system for digital notary services, stock certificates, smart contracts, etc.

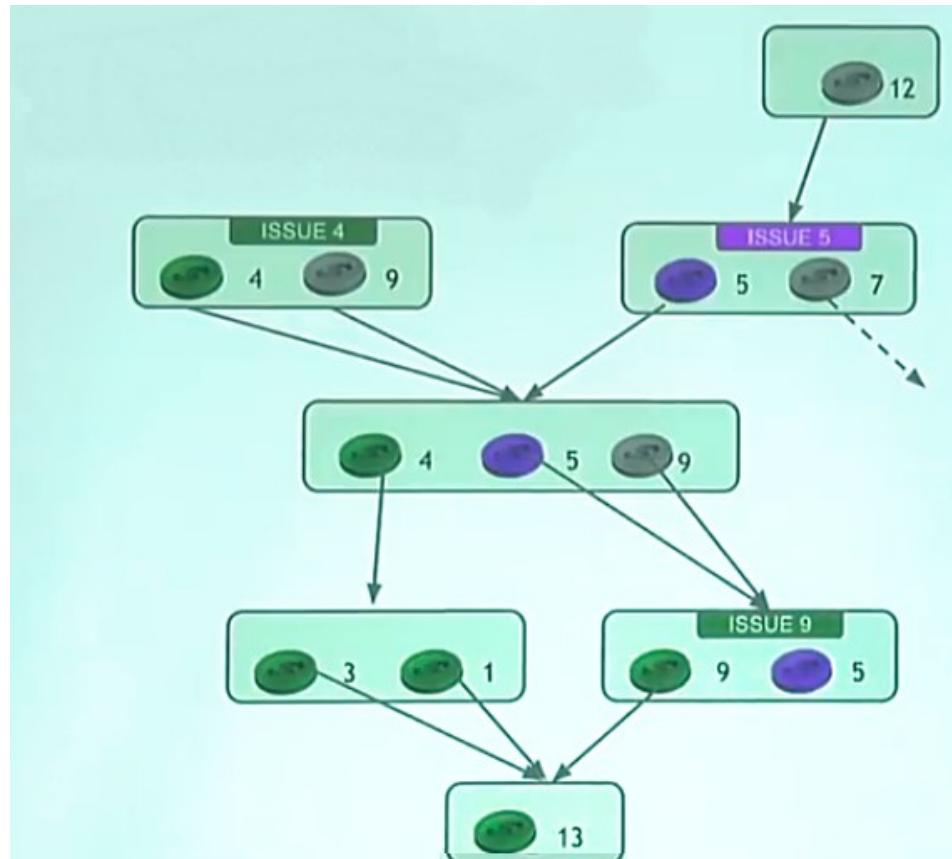
Hash pointers, not entire data

- A key point to understand, is that every node participating to the blockchain is required to put a transaction with only the hash of the data produced, NOT the whole data content
- **When/If required, everyone will check that the data provided matches that hash that was previously posted**

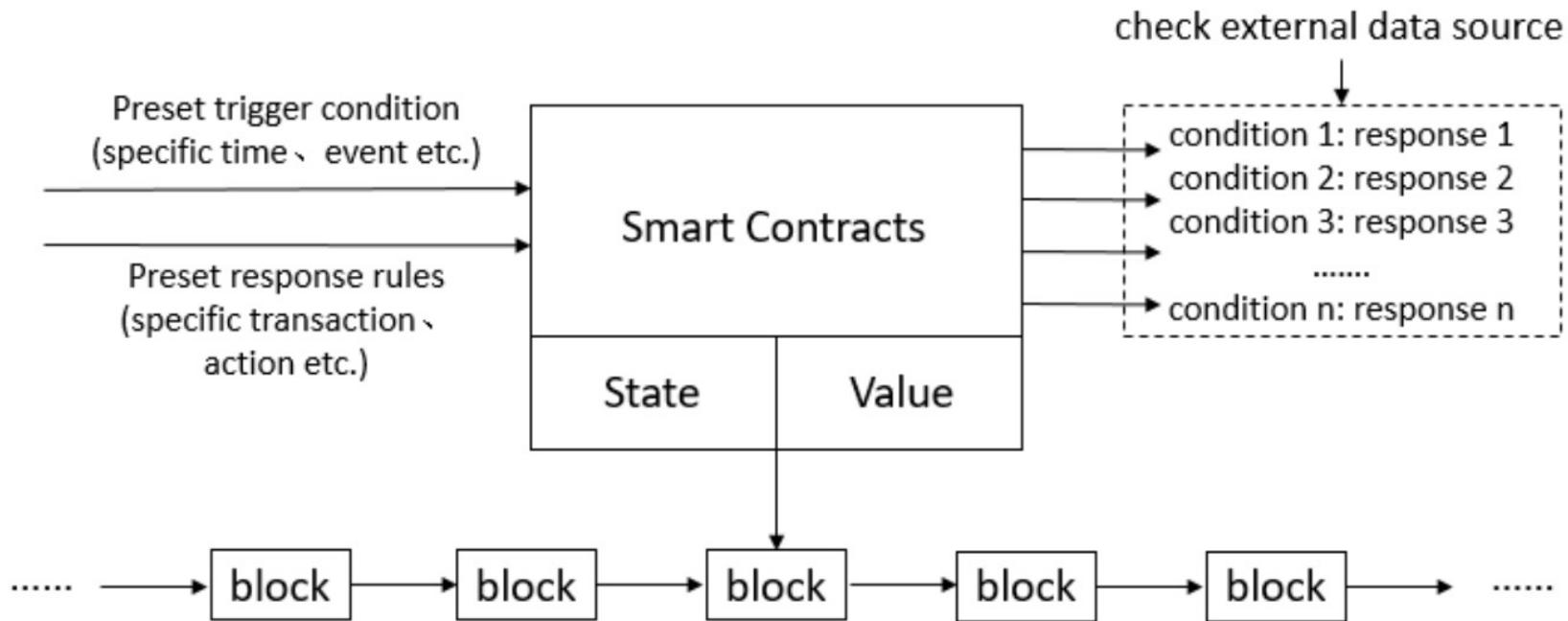
Industry	Use Case	IoT Data
Logistics	<ul style="list-style-type: none"> • Track, monitor, and report on container status and location. • Optimize packing and transfer of shipments through shipping lanes. 	<ul style="list-style-type: none"> • Location • Temperature • Handling • Carrier
Electronics	<p>Track, monitor, report on</p> <ul style="list-style-type: none"> • Automated meter readings • Building management systems • Water heater management 	<ul style="list-style-type: none"> • Electricity usage • Building state • Water heater usage
Finance	Enable pay-per-use models where connected devices contribute sensor reading to indicate/log usage that triggers payment	<ul style="list-style-type: none"> • Items consumed • Location visited • Usage of device
Manufacturing	Communicate and agree on shared information across vendors in manufacturing equipment and supply according to Digital Business Ecosystem (DBE) Core data model	<ul style="list-style-type: none"> • DBE Core documents • Device state • Location
Electronics	<p>Edge computing in devices</p> <p>Agreements for peer-to-peer appliance, home, vehicle interactions and decisions driven by contracts on a shared ledger</p>	<ul style="list-style-type: none"> • Location • Temperature • Inventory • Appliance state
Automotive	Warranty and service logging for vehicles, proof of service work performed, and logging of parts installed into vehicles	<ul style="list-style-type: none"> • Parts inventory • Service performed

Non-Fungible Tokens (NFT)

- Recall “**fungibility**: every coin is interchangeable with the another
 - Applications can be build at layer 2, so that some BTC represent **some a different assets other than bitcoin**
 - It’s like virtually “coloring” some coins so that you can follow them.
 - For example: a theater could sell 100 colored satoshis, where each satoshi represent a ticket.
- Other: voting rights, stocks, collectibles



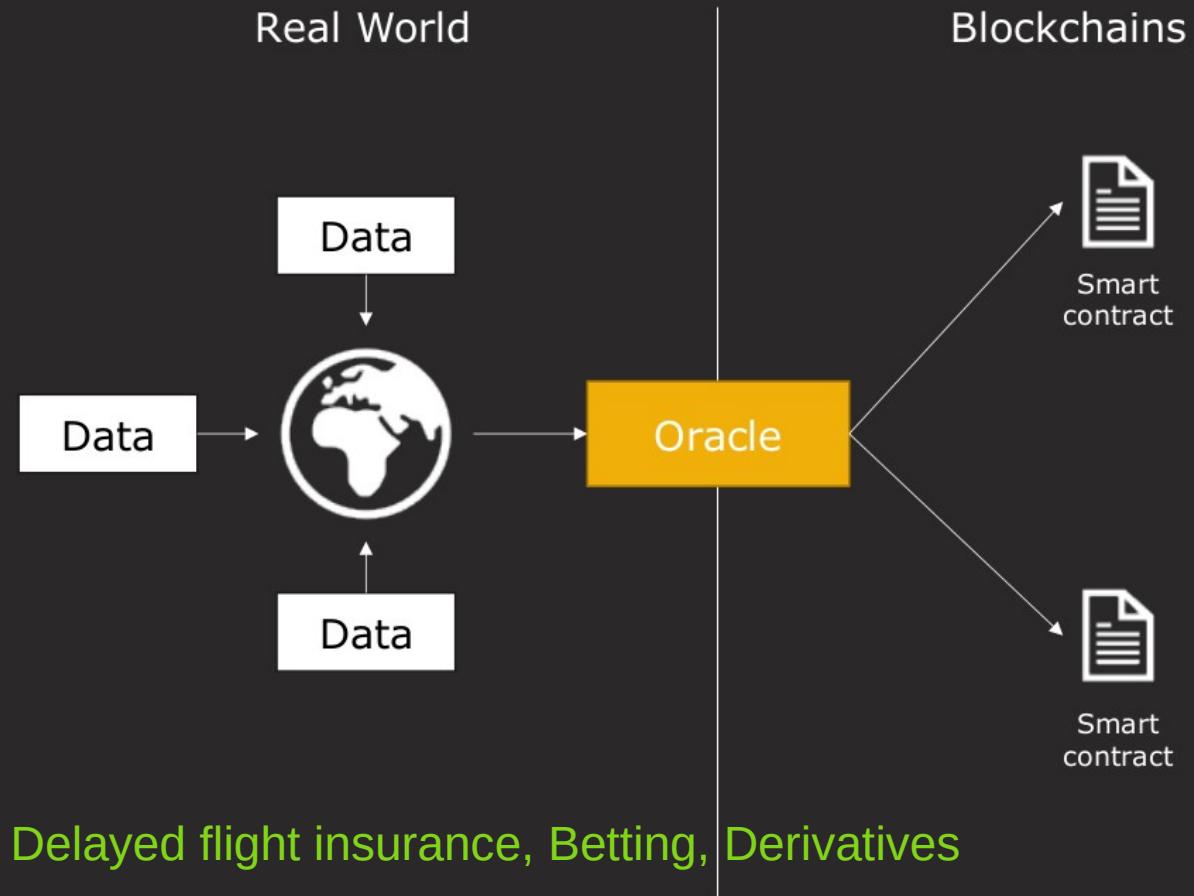
Smart Contracts



Bitcoin: Turing-incomplete (by purpose)
Ethereum: Turing Complete

Oracles

- Smart Contracts live like in a walled garden, they cannot fetch external data on their own
- An Oracle acts as a data carrier, a reliable connection between Web APIs and smart contracts
- The good behavior is enforced by cryptographic proofs

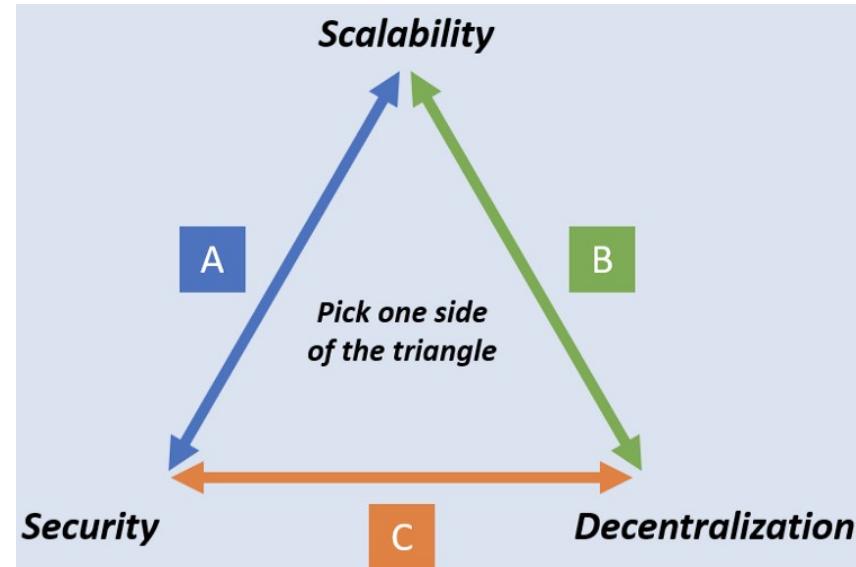


Outline Day 2

- Asymmetric Cryptography
- Transactions on Chain
- Short History of Bitcoin
- Blockchain as a Platform: Proof-of-Existence, NTF, Smart Contracts
- **Scalability: the Blockchain Trilemma**
- Bitcoin Layer 2: the Lightning Network

Blockchain Trilemma

- **Bigger Blocks** → more hw resources to verify blocks → less nodes → (less decentralisation)
- **Reduce block time** → less difficulty → (compromise on the security)
- As a result, you will have a trade-off between **Security** and **Decentralisation**



Community: The Two (di)Visions

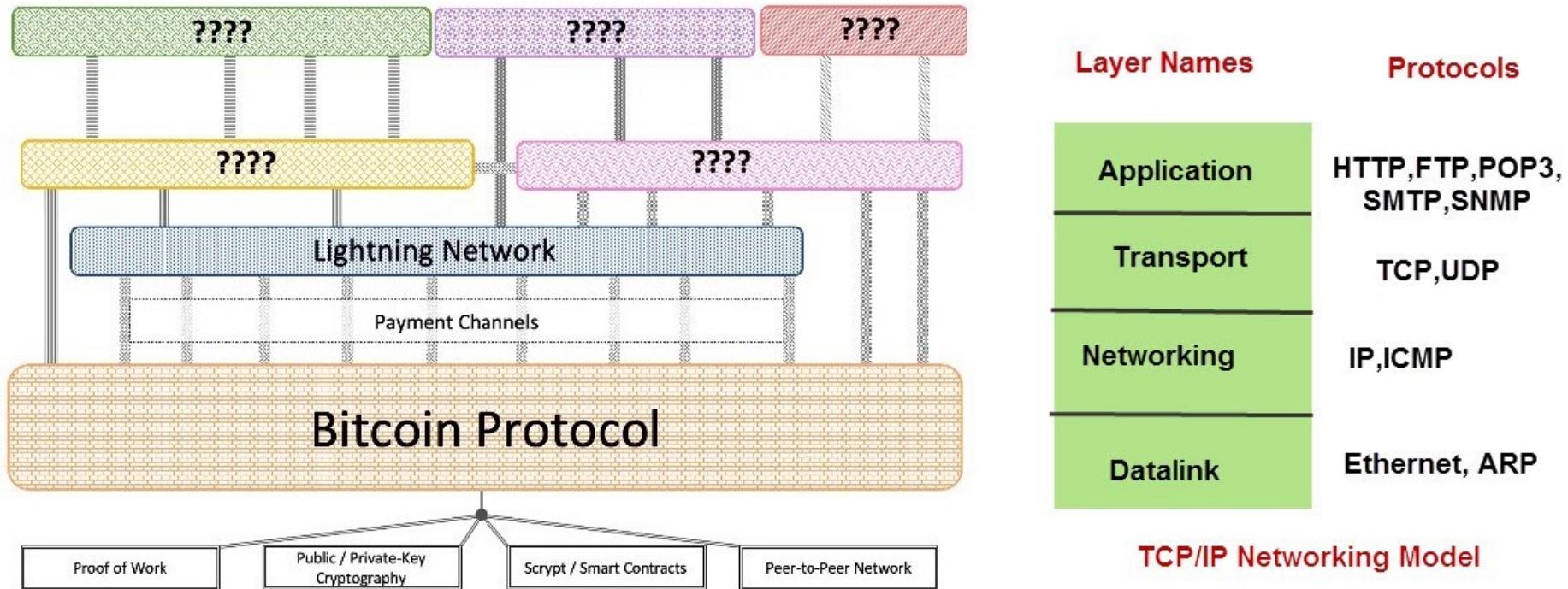
- **The decentralised nature of the Bitcoin protocol is the most important thing** → we should scale building on top of this solid layer
- **No, we can re-create a new blockchain from scratch** → we will add new features and put everything we need directly there

Bitcoin vs altcoins

- This happened in 2013, and since then many attempts have failed, other revealed to be scams
- In many cases, the problem was simple: the presence of a precise group of interest, a company, a leader etc...
- **Don't trust: do your own research**
 - Don't look at the price
 - Look at the github code repository activity
 - Look number of transactions
 - Look at the market capitalisation

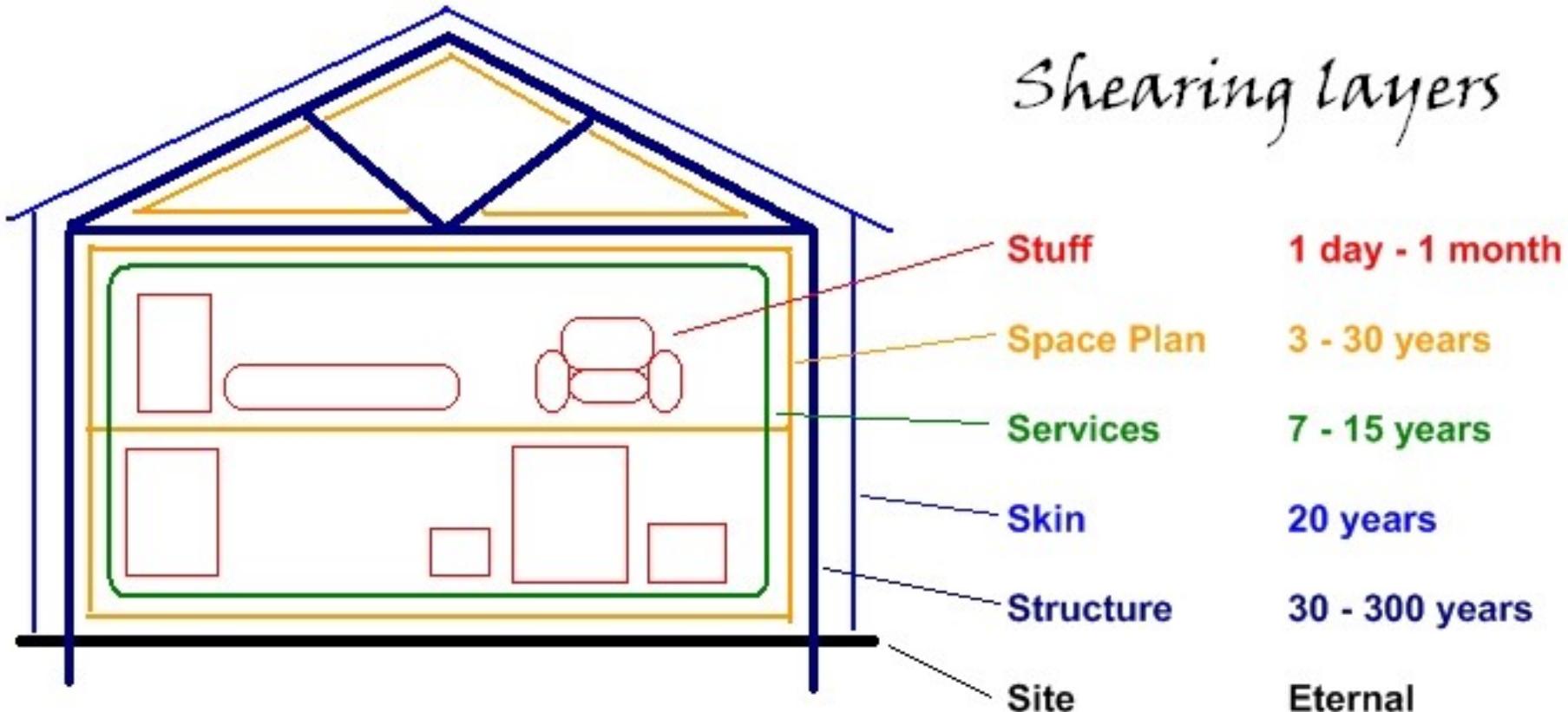
<https://coin360.com/>

Building on Bitcoin base layer



Lower levels change slowly, acting as a solid foundation

Shearing layers



Stewart Brand's 6 S's from *How Buildings Learn*

Lower levels change slowly, acting as a solid foundation

Outline Day 2

- Asymmetric Cryptography
- Transactions on Chain
- Short History of Bitcoin
- Blockchain as a Platform: Proof-of-Existence, NTF, Smart Contracts
- Scalability: the Blockchain Trilemma
- **Bitcoin Layer 2: the Lightning Network**

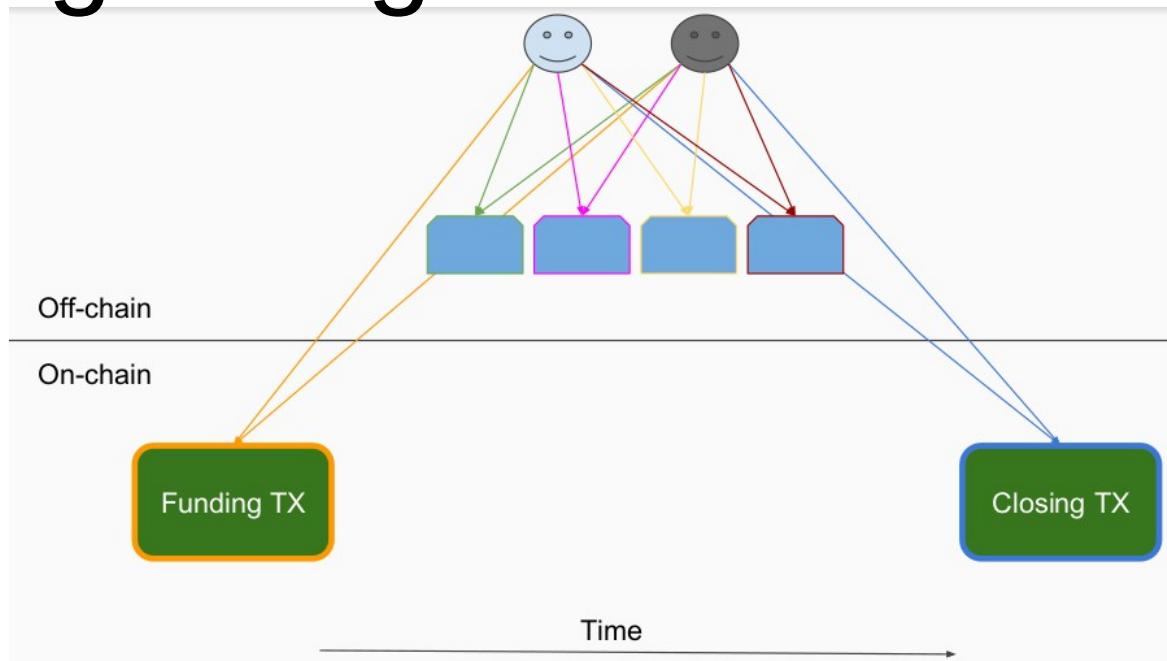
Addressing Scalability at Layer 2

Addressing scalability at layer1 ?!?

7 billion people doing 2 blockchain transactions per day

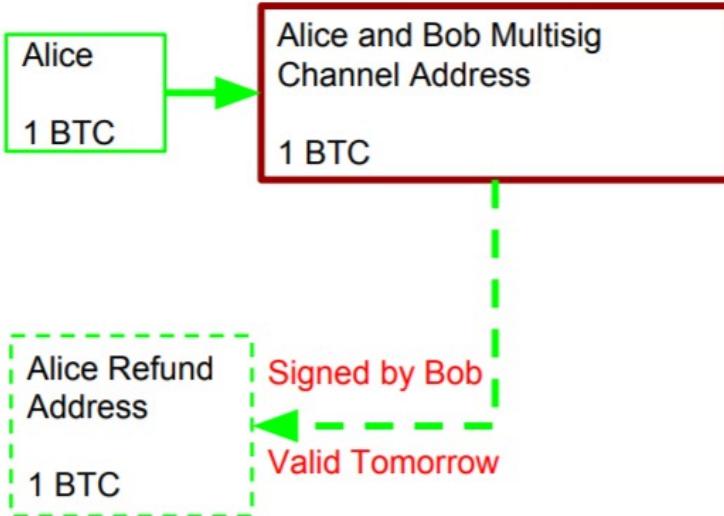
- 24 GB blocks
- 3.5 TB/day
- 1.27 PB/year
- **Bigger blocks = Centralization**
 - Very few full nodes
 - Very few miners
 - De facto inability to validate blockchain

Lightning Network Channel



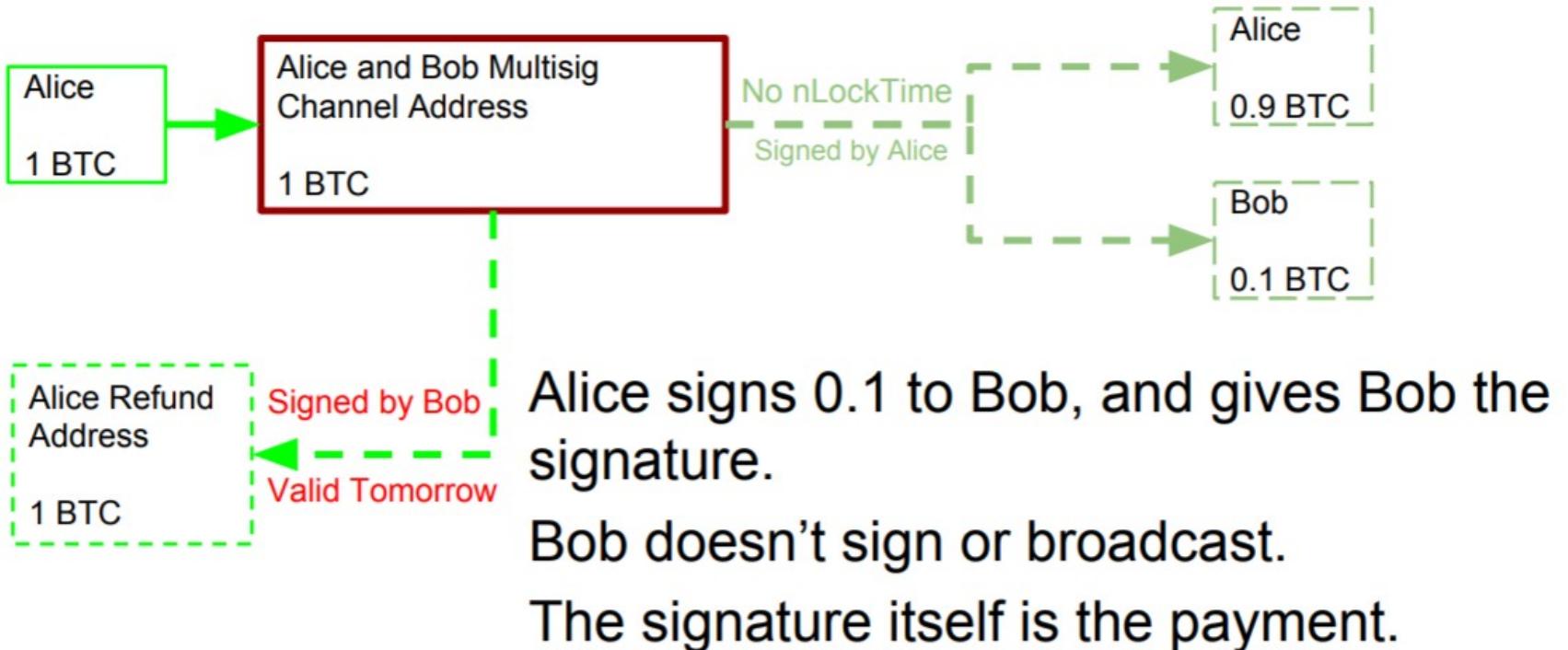
Since the transactions inside payment channels are between two parties, the transaction doesn't need to be broadcasted to the public blockchain network until the parties decide to close the channel.

Opening a Channel



First Alice gets a refund signed by Bob, then sends to the multisig address.

Even if Bob disappears, she can get the coins back tomorrow.



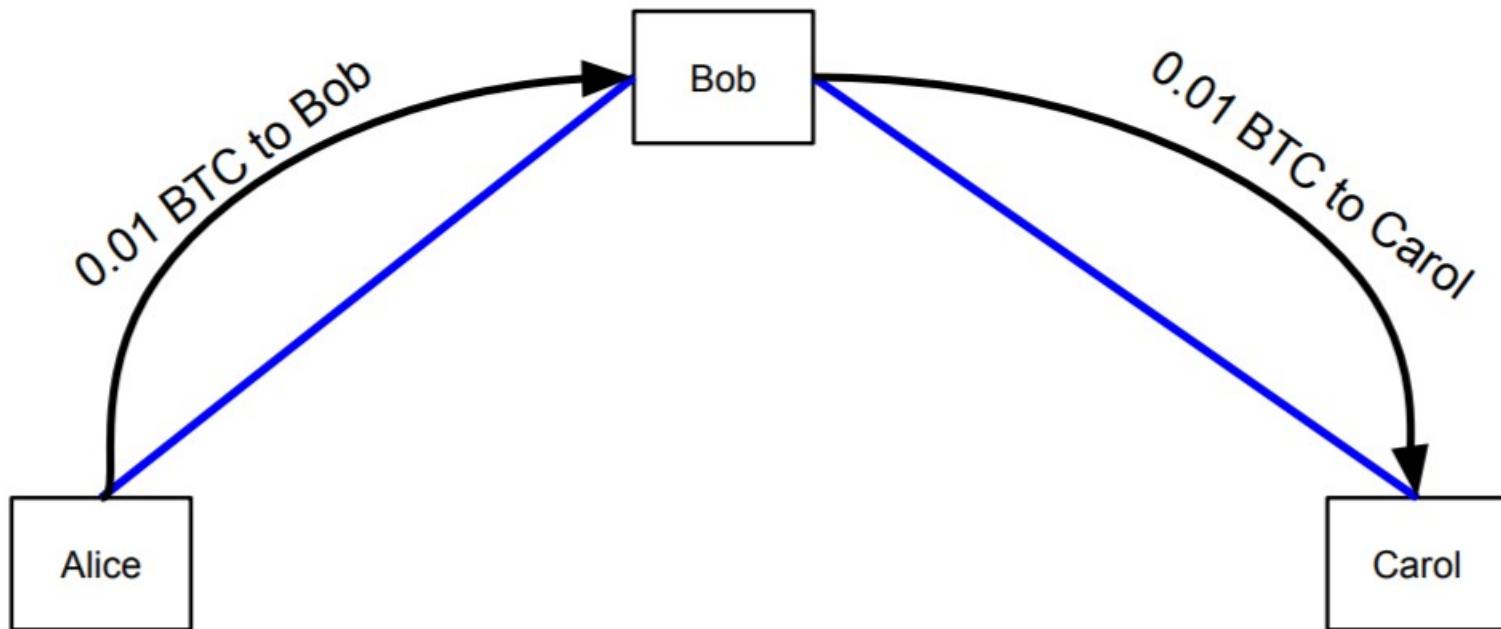
It's like Bob has in his hands a transaction that he could spend with his private key, but there is no reason to do that, since other updates may arrive

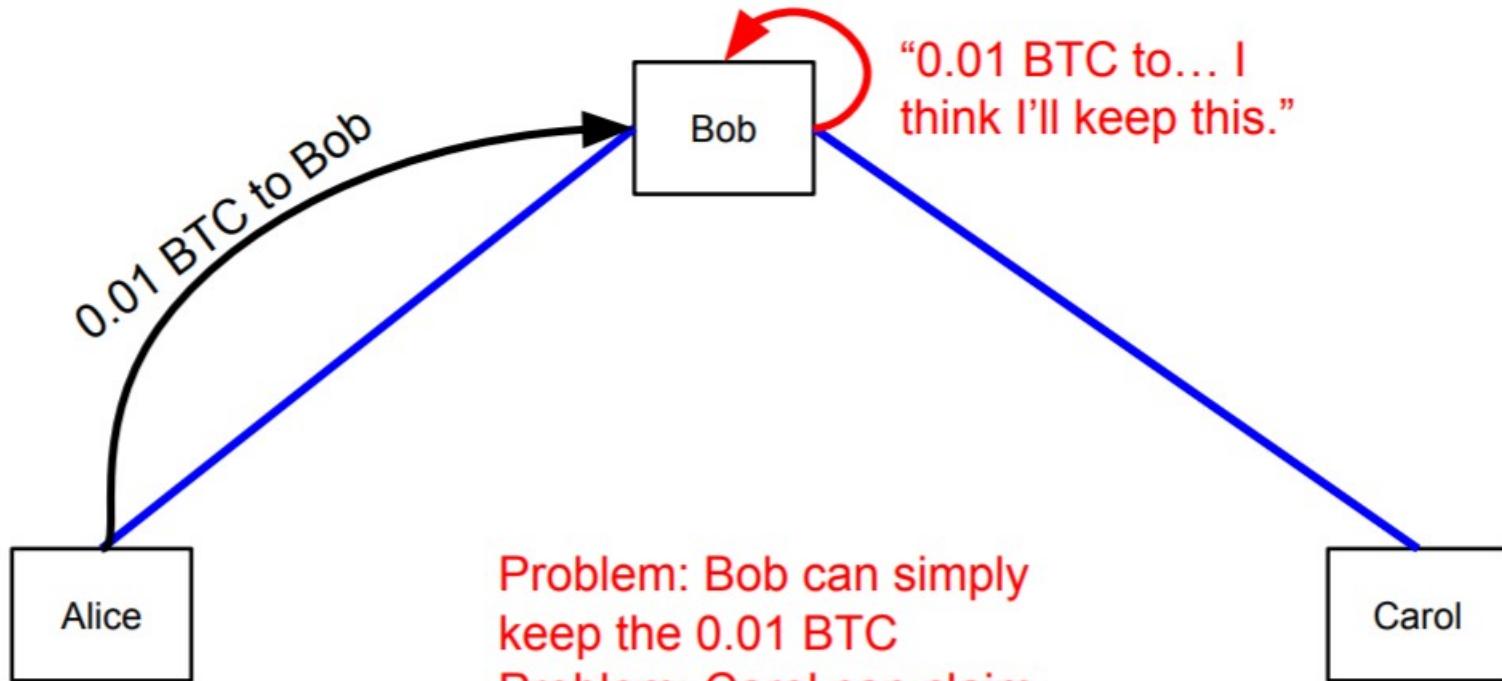


Alice signs 0.2 to Bob, overwriting the previous spend.
 Alice can increment many times without transaction fees.

- This can go on forever (the funding transaction could be delayed)
- If they agree to close the channel, Bob will write the latest transaction on chain
- Bob can close the channel, but cannot cheat using previous transactions, because they have lower sequence number (in this case makes no sense)
- If Bob disappears for long time, the refunding transaction lock time will become valid

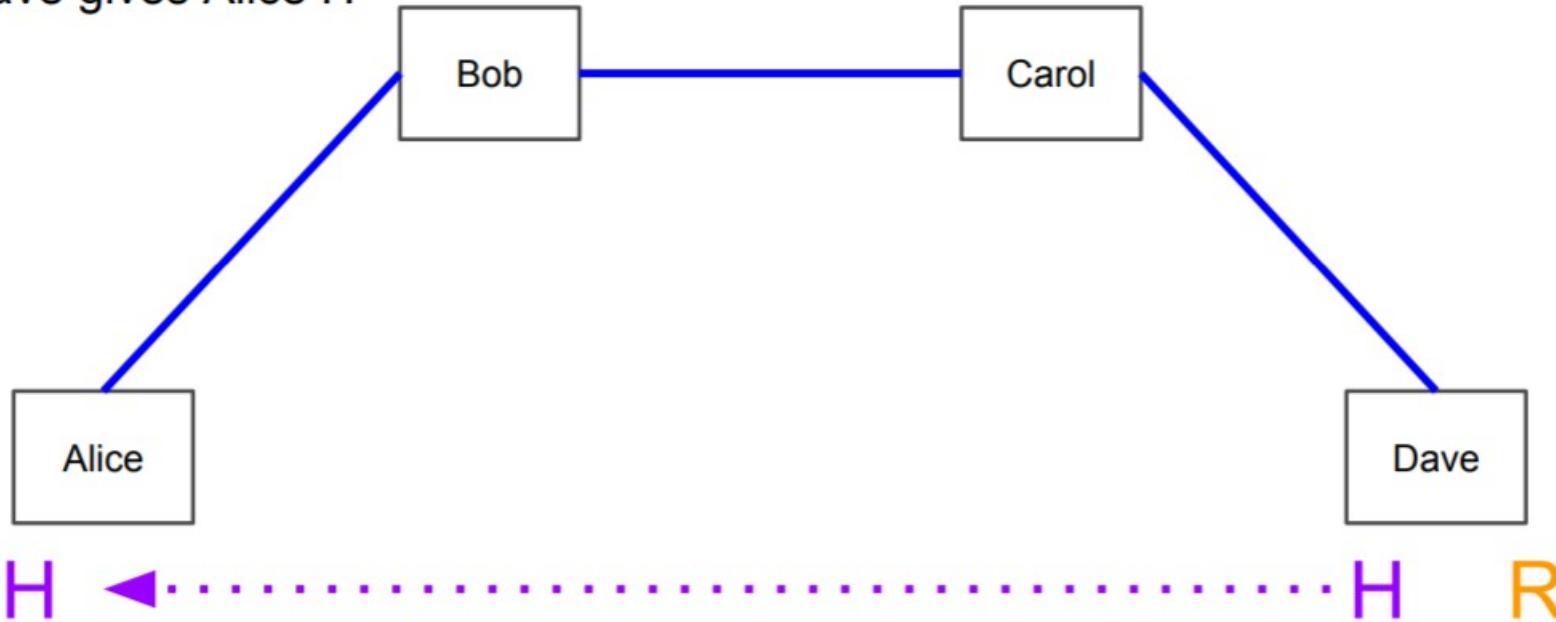
You don't a channel for every destination, just a path that connection to such destination
Example: Alice must give 0.1 to Carol

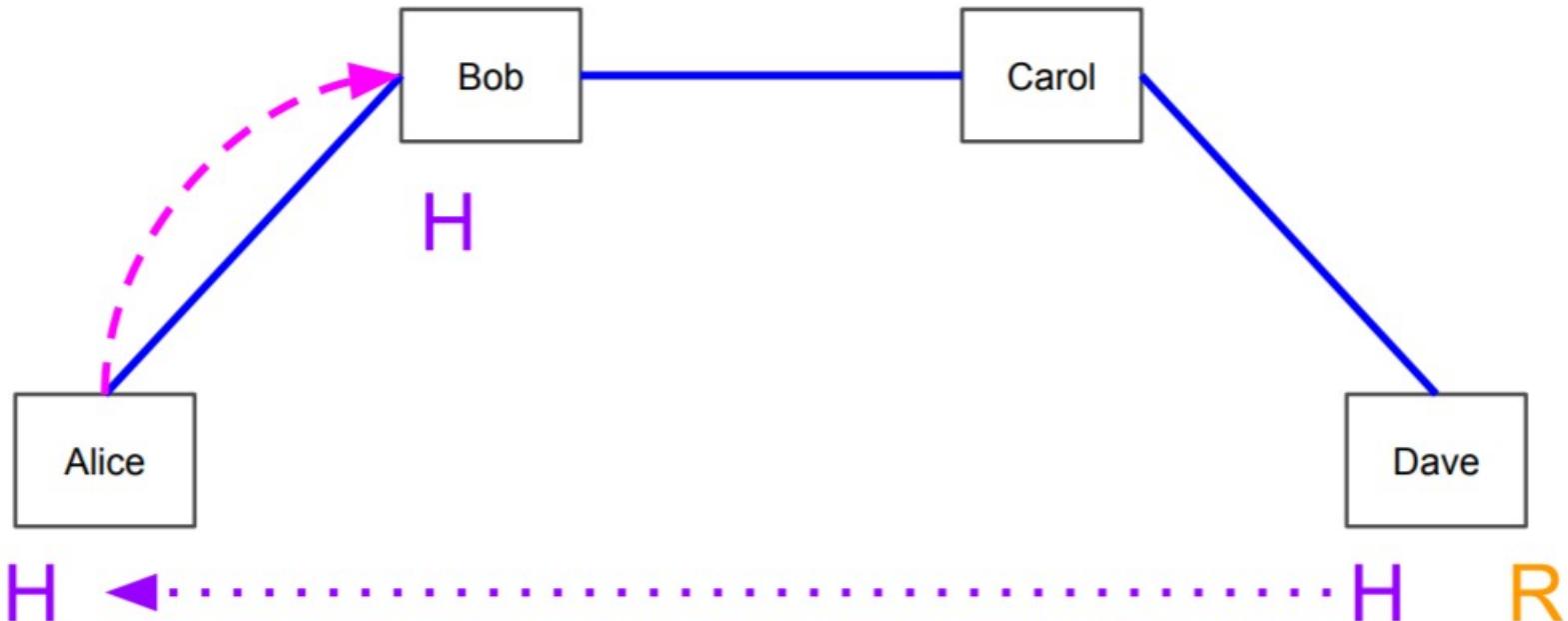




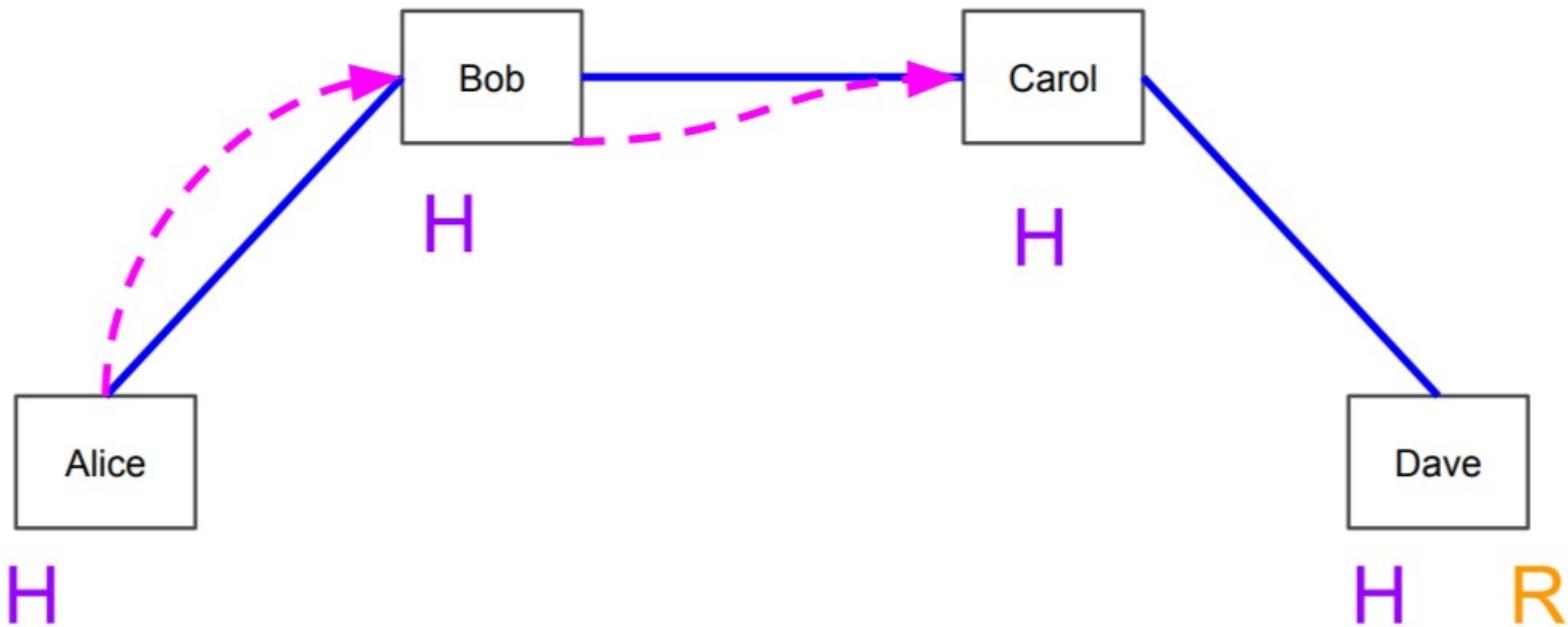
Dave makes a random number R and hashes it to H.

Dave gives Alice H

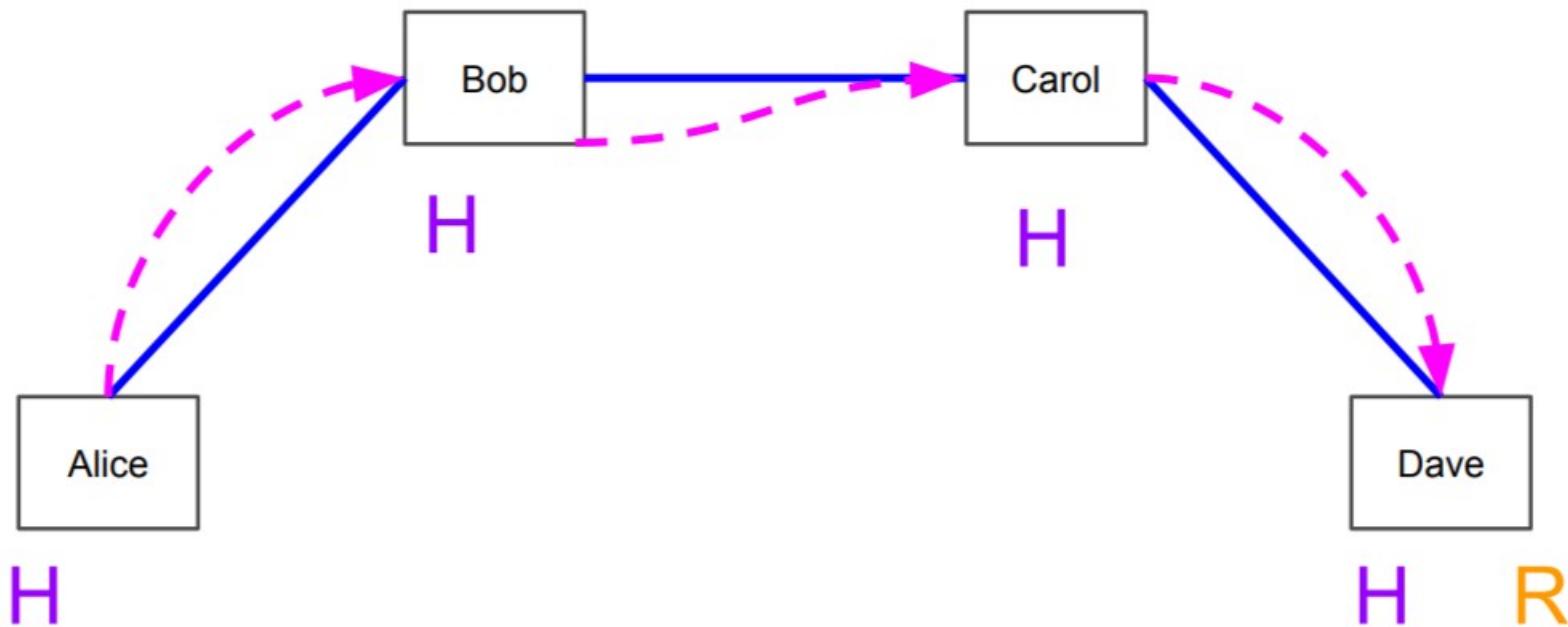




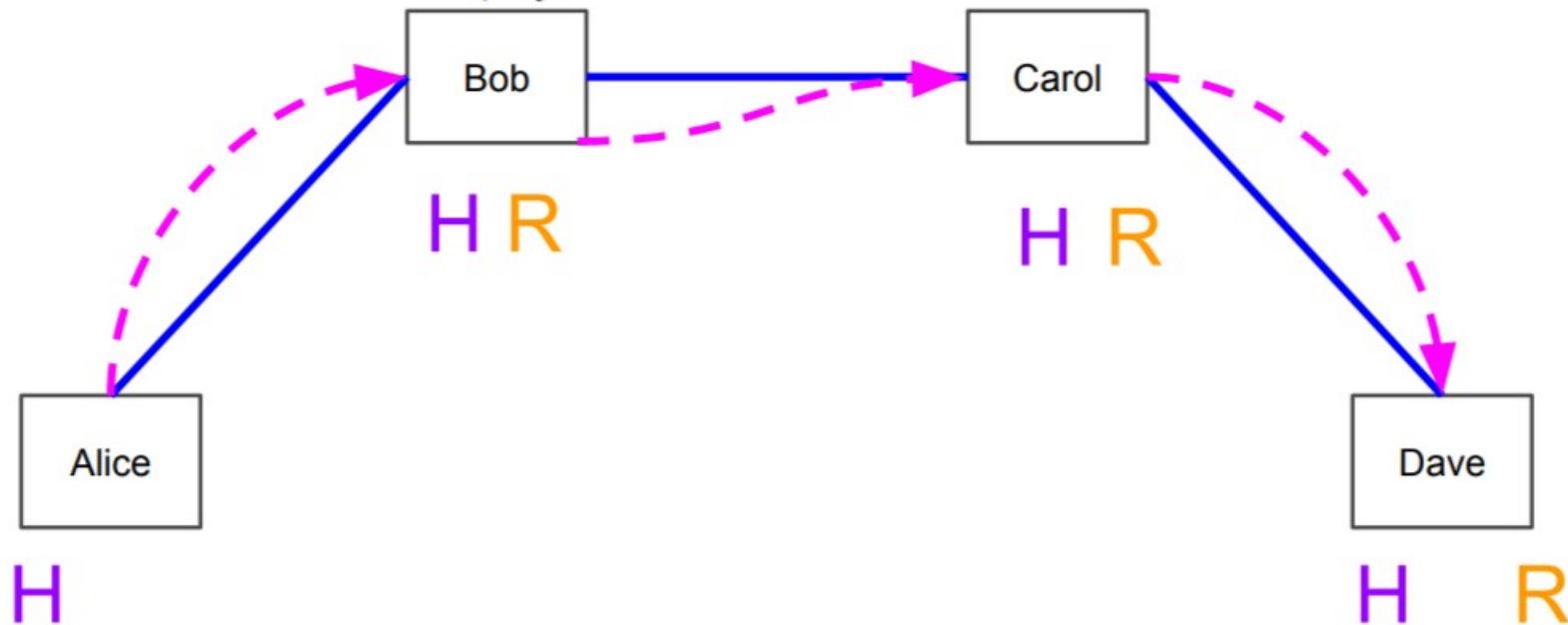
Bob pays Carol, but only if she knows R, the pre-image of H



Carol pays Dave, but only if he knows R... and he does!



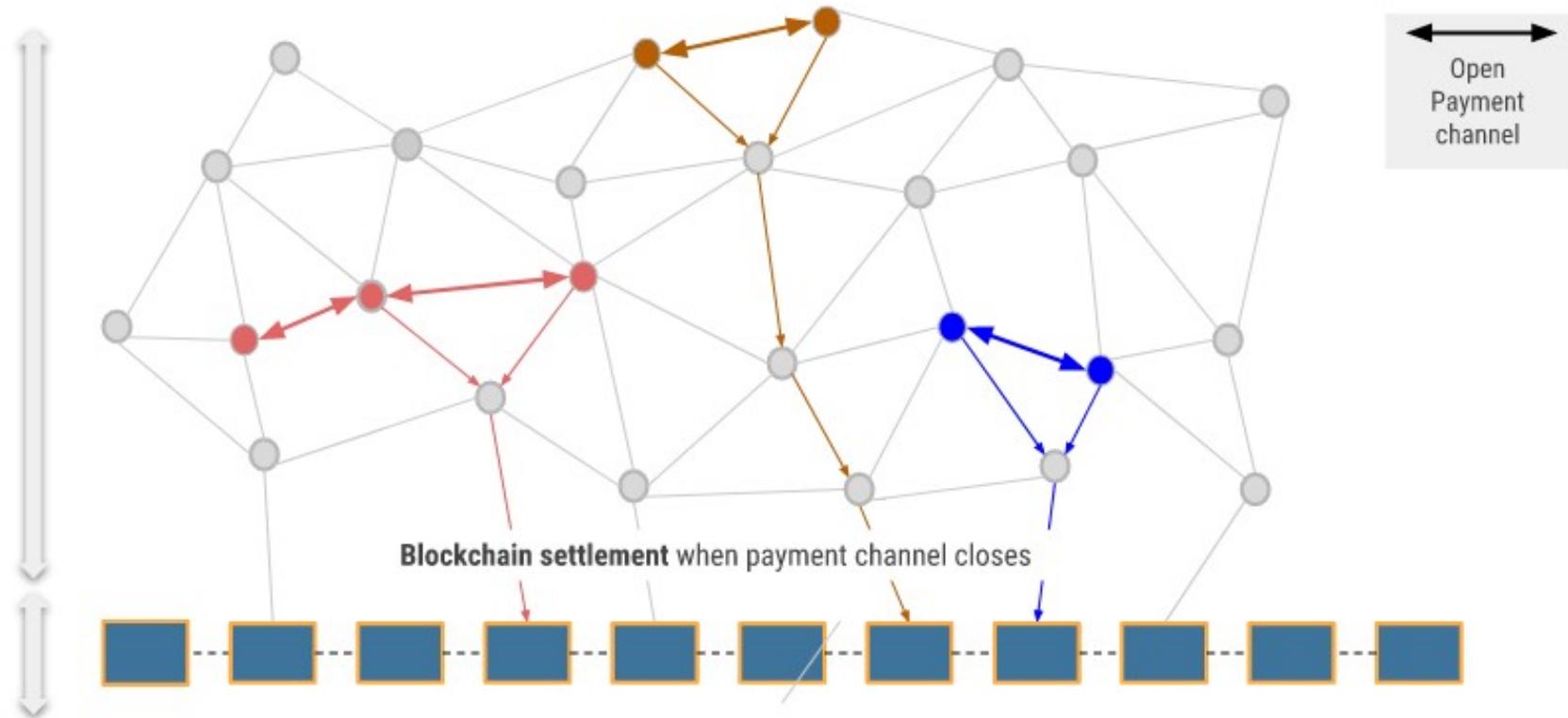
When Dave receives the payment, he must reveal R. Revealing R allows Carol and Bob to receive their payments.



Streaming satoshis

- Each Bitcoin or BTC can be split into 100,000,000 pieces. A Satoshi is one-hundred millionth of a Bitcoin (0.00000001).
- The LN allows sats to be further subdivided into millisatoshis. This allows users to make payments as small as \$0.0000001 or one hundred thousandth of a dollar cent per transaction.
- This design feature will make it possible for satoshis to be streamed on a per second base.

Lightning Network



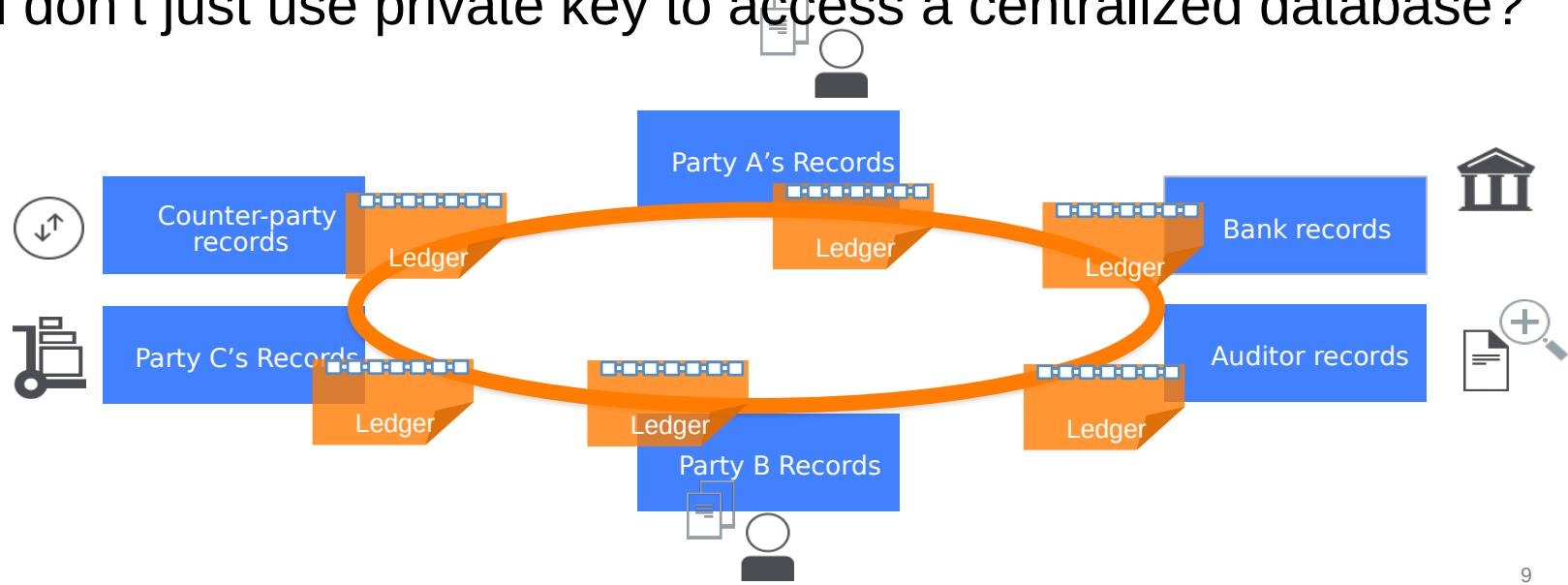
The Lightning Network



<https://explorer.acinq.co/>

Distribubuted Ledgers (DLT) are NOT blockchains

- A consortium that just share a database
- Still need to trust each other, 6 of them could reverse a 12 participants blockchain history
- They need and want control over the permission in partecipation
- Why they should write transaction in a sequence of chained blocks and don't just use private key to access a centralized database?



“A private blockchain is an LAN, and a public blockchain is the internet. The world was changed by the internet, not a bunch of Local Area Networks.

Brian Forde, MIT, former senior adviser for mobile and data innovation at the White House

<https://bitcoinmagazine.com/articles/mit-s-brian-forde-companies-will-be-disrupted-the-most-by-public-blockchains-1466028606>

“it's not about some silly ‘sequential data structure’ . It's about stateful decentralized applications [...] giving [...] networks global persistent memory”

(Vitalik Buterin, the creator of Ethereum)

*“If you can replace the word “**blockchain**” with “**database**” and the meaning doesn’t change... that’s not a blockchain”*

Andreas M. Antonopoulos

https://www.youtube.com/watch?v=SMEOKDVXIUo&t=0s&ab_channel=aantonop

Blockchain Checklist

- ✓ **Open:** anyone can participate, no permission, no requirement (not even being human)
- ✓ **Censorship-resistant:** nobody can't prevent you from doing a transaction
- ✓ **Public:** everyone can verify the entire transaction history
- ✓ **Immutable:** no one can modify the transaction history

All the above properties are enabled by a math
→ No one can control Math Laws

(Think about all the above next time you will hear:
“Our company propose Our new blockchain for...”)

References

https://bitcoinwallets.com/bitcoin_white_paper.pdf

https://www.youtube.com/watch?v=UIKZ83REIkA&ab_channel=aantonop

Technical:

<https://github.com/Xel/Blockchain-stuff>

<https://github.com/igorbarinov/awesome-bitcoin>

<https://www.lopp.net/bitcoin-information/technical-resources.html>

<https://www.lopp.net/bitcoin-information/other-resources.html>

<https://nakamotoinstitute.org/>

<https://www.sfbtcoindevs.org/>