PPT - 22 Sep 2024

By Shubham Hudda

What is Blockchain?

it is some sort of a chain made of
Blocks. Blockchain stores data in blocks that
are linked together via cryptography. "distributed,"
"peer-to-peer," "decentralized," "secure," "open,"
"immutable," "ledger," etc.

Some definitions

"Blockchain is a shared, immutable ledger for recording transactions, tracking assets and building trust." - IBM

"Cryptocurrencies like Bitcoin and Ethereum are powered by a technology called the blockchain. At its most basic, a blockchain is a list of transactions that anyone can view and verify." - Coinbase

"Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network. A blockchain database stores data in blocks that are linked together in a chain. The data is chronologically consistent because you cannot delete or modify the chain without consensus from the network. As a result, you can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts, and other transactions. The system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of these transactions." - Amazon AWS

Types of Blockchains

They can be public, private, permissioned or built by a consortium.

Public blockchain networks
A public blockchain is one that anyone can join and participate in, such as Bitcoin, Ethereum or Polkadot.

Private blockchain networks
A private blockchain network, similar to a public blockchain network, is a decentralized peer-to-peer network. However, one organization governs the network, controlling who is allowed to participate, execute a consensus protocol and maintain the blockchain. A private blockchain can be run behind a corporate firewall and even be hosted on premises.

Permissioned blockchain networks
Businesses who set up a private blockchain will generally set up a permissioned blockchain network. It is important to note that public blockchain networks can also be permissioned. This places restrictions on who is allowed to participate in the network and in what transactions.

Consortium blockchains
Multiple organizations can share the responsibilities of maintaining a blockchain. These pre-selected organizations determine who may submit transactions or access the data. A consortium blockchain is ideal for business when all participants need to be permissioned and have a shared responsibility for the blockchain.

Centralisation vs Decentralisation

Always a trade off between two, example :

1. Apple vs Android
2. Mainframe computers vs Individual Computers
3. Roman vs Greek Empire

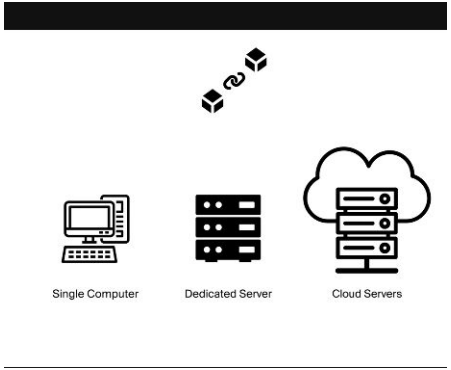
Benefits of Blockchain Technology

Greater trust
With blockchain, you can trust the network protocol and need not trust the network participants. The blockchain protocols are modeled for adversarial environments.

Greater security
Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.

More efficiency
With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated. And to speed transactions, a set of rules — called a smart contract — can be stored on the blockchain and executed automatically.

Where do blockchains live?



On any computer running a blockchain node.
Can be a single computer - can be multiple.

The blockchain network listens to all transactions and events happening on the network and faithfully packs them into blocks.

One can open up this process of block production and let anyone who runs the nodes to add blocks to the blockchain by listening to the transactions happening on the network. Different blockchains try to address these challenges in different ways.

How many nodes Bitcoin has?

https://bitnodes.io/

https://ethernodes.org/countries

Build your own blockchain

Substrate is a Blockchain building framework that provides a flexible, open, and extensible development environment that allows you to design and build fully-customized blockchain nodes to suit your application or business model needs.

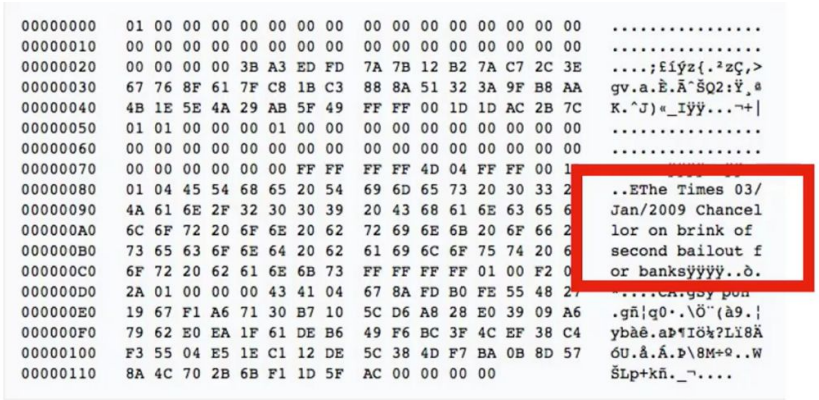
If you are interested, you can run a Blockchain on your machine.

Here are the instructions to install Substrate on your computer
https://docs.substrate.io/install/

Here is the tutorial to build and run a local blockchain
https://docs.substrate.io/tutorials/get-started/build-local-blockchain/

History of Money & Trust

Money is central to human history, but we are not aware how it is created. Why is it important for our course?



Genesis Block - The first block of Bitcoin Blockchain

History of Money & Trust

Debt is an integral part of individual lives and institutions. Almost every country in the world has a national debt which only keeps growing each year.

- Who do they owe that money to?
- How did that money come into existence?
- Can banks legally loan more money than what they have in reserve?
- What causes hyperinflation and devaluation of currency?

History of Money & Trust

We all place immense trust in centralized institutions and hope that they act in our best interest, but history shows us that such trust can be taken advantage of.

How is Money Created?

Fiat - The concept of Money that we take granted today is relatively very new and has started to started to predominate during the 20th century.

Fiat money is an alternative to commodity money, which is a currency that has intrinsic value because it contains, for example, a precious metal such as gold or silver which is embedded in the coin. Fiat also differs from representative money, which is money that has intrinsic value because it is backed by and can be converted into a precious metal or another commodity. Fiat money can look similar to representative money (such as paper bills), but the former has no backing, while the latter represents a claim on a commodity (which can be redeemed to a greater or lesser extent).

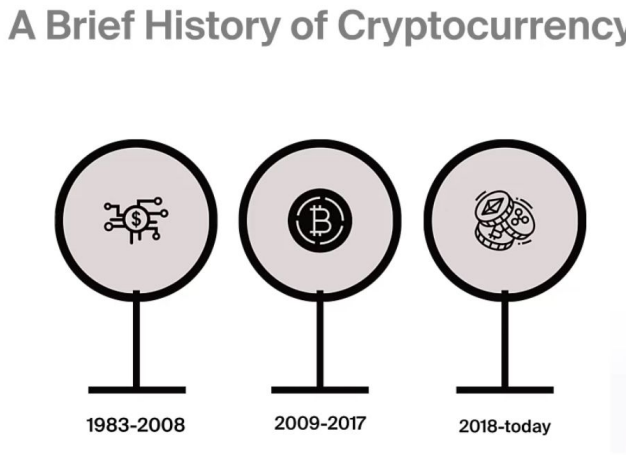
The concept of Money has evolved over the millennia and there is still scope for improvement!

Properties of Money

1. Durability
2. Portability
3. Divisibility
4. Uniformity
5. Limited Supply
6. Acceptability

eCash

Introduced by cryptographer David Chaum.
Idea - blind signatures.



Brief History of Blockchain

1991 A cryptographically secured chain of blocks is described for the first time in "How to Time-Stamp a Digital Document" by Stuart Haber and W Scott Stornetta.
1998 Computer scientist Nick Szabo works on ‘bit gold’, a decentralised digital currency.
2000 Stefan Konst publishes his theory of cryptographic secured chains, plus ideas for implementation.
2008 Developer(s) working under the pseudonym Satoshi Nakamoto release a white paper establishing the model for a blockchain.
2009 Nakamoto implements the first blockchain as the public ledger for transactions made using bitcoin. Solved Double Spend Issue in a decentralized way!
2014 The Ethereum blockchain system introduces computer programs into the blocks known as smart contracts.
2024 Web3 is an idea for a new iteration of the World Wide Web which incorporates concepts such as decentralization, blockchain technologies, and token-based economics.

Introduction to Bitcoin

Bitcoin is a decentralized digital currency that can be exchanged between users on a peer-to-peer network.

It operates free of any central control or the oversight of banks or governments.

Instead it relies on software run on several machines and a bit of cryptography.

Bitcoin is open-source and its design along with its code is public.

It cannot be shut down or banned.

Scarcity

- Fifth property of money - it must be of limited supply - you must work to get it
- Computers to do computational work
- Can we use computation as backing for our currency?
- We can't find physical objects that are rare in the computational world, in the digital world because it's trivial to copy things
- This is how hashcash came into life

Proof of Work

The idea to require a user to compute a moderately hard, but not intractable function was proposed by Cynthia Dwork and Moni Naor in their 1992 paper "Pricing via Processing or Combatting Junk Mail." In short, the user has to prove that they have done some work to send an email, or in other words they have to show **Proof-of-Work (PoW)**.

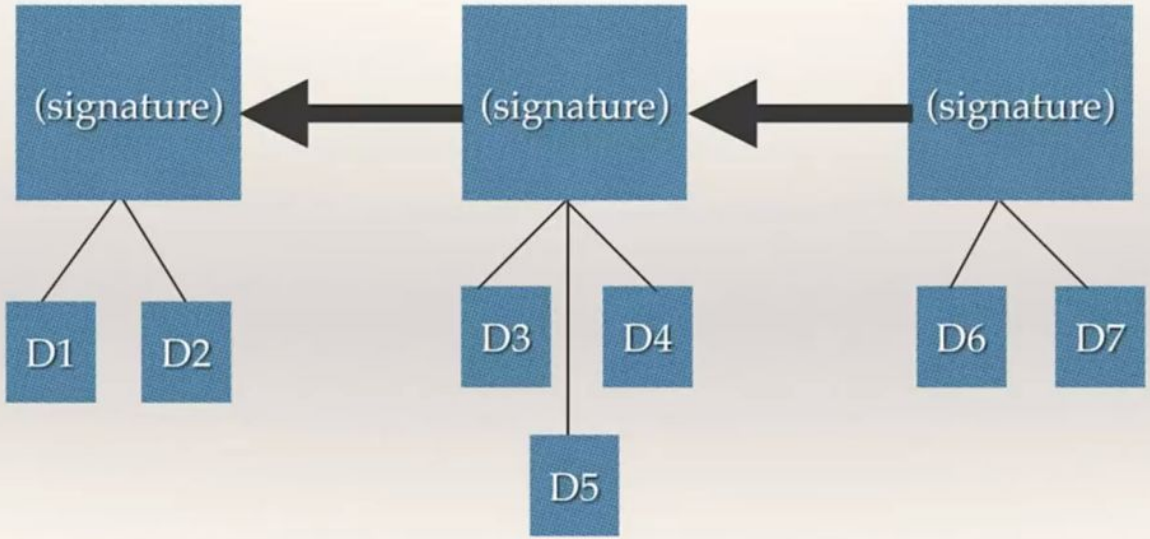
Linked Timestamping

- Ordering the events without a common clock is tricky
- But we can provide a signature that shows what the last document was. We can make a cryptographic signature of each of the documents and have them point to the previous document.
- So much granularity not needed, we can bunch some pieces together - put them in a block and then link to previous block

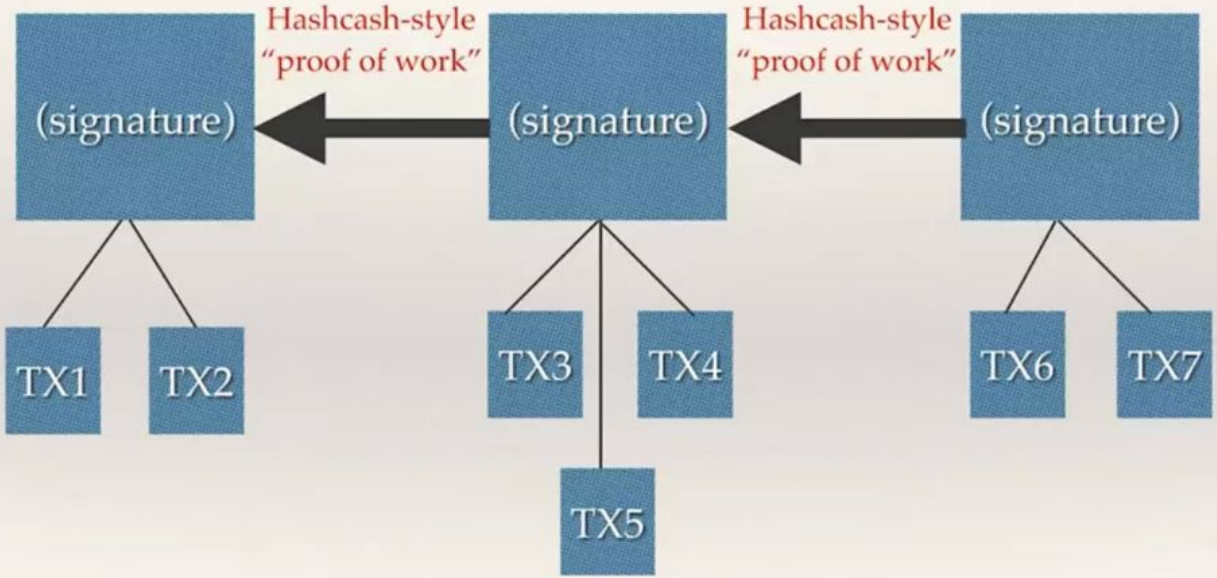
Bitcoin style blockchain

If we then make sure that these links are very difficult computationally to make and thus they're going to be very difficult for someone else to create a fake version of.

A "Block Chain"



Bitcoin-style "Blockchain"



Bitcoin

- The first modern cryptocurrency
- Decentralized - no central arbiter and no easy way to censor transactions
- Transactions signed cryptographically
- Blocks added to a blockchain with proof of work, and those who add them are rewarded with bitcoins

Resolving the double-spending problem

→ With Bitcoin, creating the link to a previous block (and generating a new one via a complex computational challenge) creates money

→ In case of conflict, chain with most work behind it wins (originally it was the longest chain, this has since been modified)

→ This is what miners are doing and what they are rewarded for

→ Key modification that allowed Bitcoin to solve previous digital money problems

Satoshi Nakamato!

→ Bitcoin was created by the pseudonymous "Satoshi Nakomoto"

→ Note that Satoshi is a male Japanese name, but there is no evidence that they are a male, female, or possibly a collective

→ Satoshi interacted with people online for several years, then went dark entirely

→ Many theories on his true identity

→ Writings collected in "The Book of Satoshi", edited by Phil Champagne

Bitcoin Issuance

Bitcoins are created at a decreasing and predictable rate. The number of new bitcoins created each year is automatically halved over time until bitcoin issuance halts completely with a total of 21 million Bitcoins in existence. Bitcoin is divisible into 100 million satoshis, meaning that one satoshi is 0.00000001 bitcoin or 100 million satoshis equals 1 Bitcoin.

Is it possible to break Bitcoin?

Since Bitcoin launched in 2009, Proof-of-Work has been the mainstream method of securing decentralized cryptocurrencies against double-spend attacks. Proof-of-Work is intended to make it prohibitively expensive for an attacker to rewrite the blockchain and reverse transactions that are considered settled. An attacker could double-spend through a "51% attack" in which the attacker amasses a majority of the hashrate on the target cryptocurrency. Satoshi Nakamoto assumed in the Bitcoin whitepaper that acquiring 51% of Bitcoin's hashrate would be impossible and thus did not consider the economic incentives behind a 51% attack.

What is Ethereum?

Ethereum is the community-run technology powering the cryptocurrency Ether and thousands of decentralized applications.

https://ethereum.foundation/

Ethereum and most of its apps are transparent and open source. You can fork the code and reuse functionality others have already built on.

Ethereum utilizes blockchain technology to not only store transactions like Bitcoin, but also store and execute code that can power tamper-proof decentralized smart contracts and applications.

What is Ethereum? In it’s cofounder’s words

It is an idea of a computer in the middle of the planet, a sort of computer at the center of the world, or the world computer. So it's like a single computer that everybody can use. Now that's very compelling if everyone can use it, it means there's a single machine that has rules but that everyone can use to interoperate. So you can kind of set your own rules up and anyone else can come in and operate, play in your playground operating your rules. Everyone can check the computer has indeed operated correctly. Now the problem with having a single computer shared by everybody is that, well, sometimes you might all want to use it at the same time, and it becomes a very scarce resource. There's only one of them. So, the idea is that as the desire to use this computer increases and increases and increases and the volume of transactions increases accordingly, we need to spread them out between different chains. So different kinds of computers mostly just be isolated, yeah, and kind of get on with their own thing. And then now and again come together and swap messages, you know, tell each other what's been going on, but also making it possible for these much more sophisticated applications to exist in their own context on their own chain in a way that's designed specifically for them and not in a generalized fashion for everybody.

What are smart contracts?

Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met. In the context of Ethereum, Smart contracts are simply computer programs living on the Ethereum blockchain. They only execute when triggered by a transaction from a user (or another contract). They make Ethereum very flexible in what it can do and distinguish it from other cryptocurrencies. These programs are what we now call decentralized apps, or dapps.

Once a smart contract is published to Ethereum, it will be online and operational for as long as Ethereum exists. Not even the author can take it down. Since smart contracts are automated, they do not discriminate against any user and are always ready to use. Popular examples of smart contracts are lending apps, decentralized trading exchanges, insurance, crowdfunding apps - basically anything that can be written as a computer program.

Difference between Ethereum and Bitcoin

Ethereum builds on Bitcoin's innovation, with some big differences. Both let you use digital money without payment providers or banks. But Ethereum is programmable, so you can also build and deploy decentralized applications on its network. Ethereum being programmable means that you can build apps that use the blockchain to store data or control what your app can do. This results in a general purpose blockchain that can be programmed to do anything. As there is no limit to what Ethereum can do, it allows for great innovation to happen on the Ethereum network. While Bitcoin is only a payment network, Ethereum is more like a marketplace of financial services, games, social networks and other apps that respect your privacy and cannot censor you.

ETH is the native token of Ethereum. Unlike Bitcoin, Ethereum has no limits on its total amount of ETH issuance.

Transactions on Ethereum

Because every Ethereum transaction consumes computational resources, transactions come with a cost. Gas is the fee needed to conduct an Ethereum transaction. So in essence, an eth gas fee is a transaction fee on the Ethereum platform. Sending ETH from one Ethereum wallet to another also requires fees. Moreover, the Ethereum network charges fees to run applications on using its blockchain technology, giving an ETH transaction fee an added type of utility. ETH gas prices are denominated in a unit known as “gwei.” And one gwei equals 0.000000001 ETH (1 ETH equals a billion gwei).

CRYPTOGRAPHY

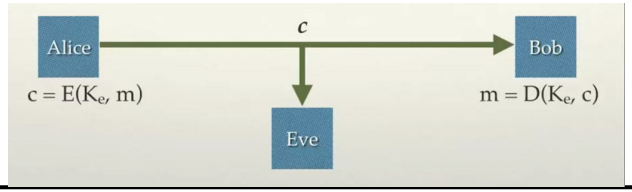
A brief explanation

Encryption

- The oldest use for cryptography is in communication
- Alice wants to send a message, m, to Bob, but Eve can read everything that is sent over the communication channel between them.
- How can Alice send m to Bob without Eve understanding the message?

Symmetric Key Encryption

- The oldest form of encryption
- Assume Alice and Bob share the same secret key, K.
- Alice can encrypt text using encryption function c = E(K, m) then send ciphertext c over the unencrypted channel
- Bob can decrypt using function m = D(K, c)
- Eve only ever sees c, not m, which is useless to her without K, even if she knows the decryption algorithm D



Example of Symmetric Key Encryption

Using Caesar Cypher : Converting a letter to a number, then given a Key (K), adding K to the number to get a new letter.

Kerckhoff's Principle

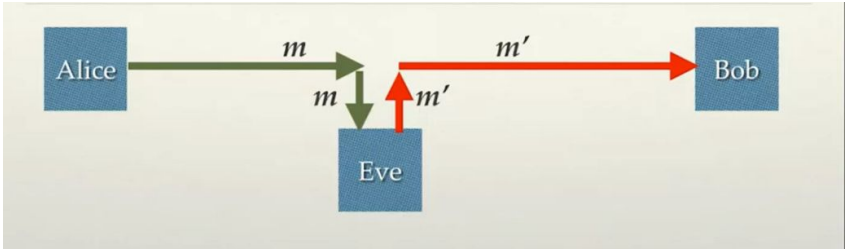
- The security of a system must depend only on the secrecy of the key, and not the secrecy of the algorithm." Security through obscurity is not a valid defense!
- How could you break our Caesar cipher, even if you don't know K?

Breaking Caesar

- Frequency Analysis
- Known Plaintext Attack
- Brute Force (there are only 25 real possibilities for Ke)

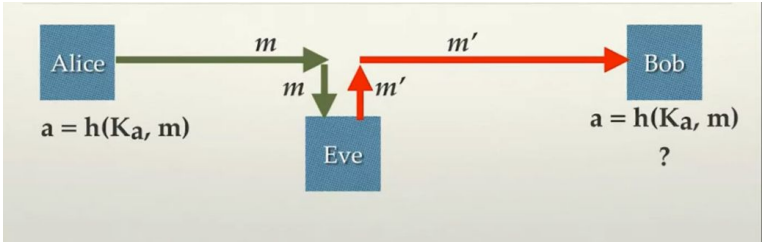
Authentication via Encryption

- Let us assume that Eve has gained the ability to modify traffic in-transit, or send a different message entirely
- How can Bob verify that Alice sent the received message (i.e., that it is message m from Alice and not m' from Eve)?



Authentication via Symmetric-Key Cryptography

- Assume Alice and Bob share another secret key, Ka, and know an authentication function h(Ka, m)
- Alice sends the message m which includes a message authentication code (MAC), a
- When Bob receives m, if h(Ka, m) does not return a, he will know that it was not "signed" with key Ka



Symmetric-Key Encryption Weakness

- How do Alice and Bob share keys Ke or Ka? They will need a separate, secure channel.
- But if they have a separate, secure channel, why use an insecure one? (Note: there are actual reasons!)

Asymmetric Key (aka Public-Key) Encryption

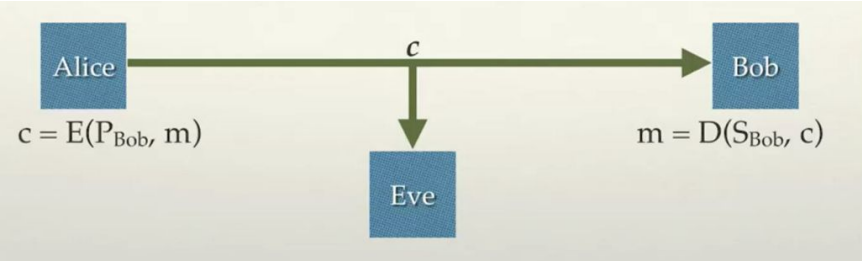
→ Two different keys: one to encrypt, P, a separate one to decrypt, S

→ P is your public key - anyone can encrypt a message to you with it

→ S is your secret (or private) key - you can use it along with P to decrypt a message (as its name implies, you should keep it private!)

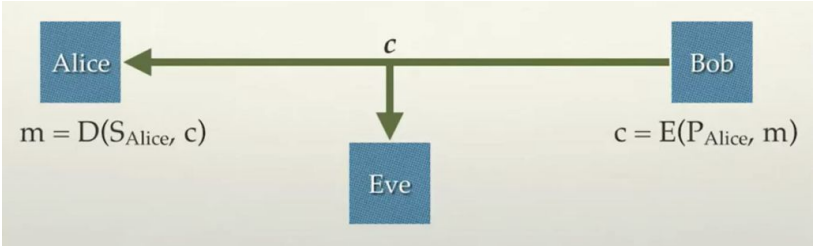
Public-Key Encryption Fundamentals

- Bob tells the world about PBob but keeps SBob secret
- If Alice wants to communicate with Bob, she can encrypt a message m to ciphertext c with function E(PBob, m)
- The only way to DECRYPT the message is with function D(SBob, c) which requires knowledge of SBob



Secure Communication Without Secure Channels

- Bob can also communicate with Alice by using Alice's public key, PAlice
- Alice and Bob can communicate over an insecure channel, even if all communication is over that channel
- Eve will only ever see ciphertext c



Efficiency

- Turns out asymmetric encryption itself is extremely inefficient compared to symmetric encryption
- Most modern systems use a hybrid approach
- Step 1: Establish a secure communications channel using asymmetric encryption
- Step 2: Share a symmetric encryption key
- Step 3: Use symmetric encryption for further communication

Public Key Infrastructure (PKI)

- How do I know that PBob is actually Bob's key and not Eve's? Very important for websites/users - make sure you are on amazon.com and not amazoon.com!
- Various approaches: certificate authorities, web of trust, SPKI, even some blockchain-based approaches
- With most cryptocurrencies, no built-in PKI - if you have the key, you "own" the coins associated with that account
- "Not your keys, not your coins"

FIN

Telegram : @shubhamhudda

Linkedin: linkedin/in/imhudda

Twitter: twitter.com/imhudda