Blockchain Introduction

JEAN YVES ZIE

jeanyves.ziediali01@em-normandie.fr

jean.zie_diali@insa-cvl.fr

Slides:

http://cryptonuage.com/slides.pdf

Exercises:

https://cryptonuage.com/exercises.pdf

More Blockchain ressources:

ressources

Program of the course

Cryptography

- classical cryptography
- Digital signature
- hashing functions

Blockchains

- Consensus problems
- Merkle Tree
- POW
- Gossip protocols
- Bitcoin Blockchain

Blockchains

- Blockchain Bitcoin
- Security & Incentives
- Energy
- POS
- Ethereum
- Smart contracts

Research questions

- scalability
- L2
- Zero Knowledge

Use cases

- ICO
- DAO
- NFT
- Atomic swaps

DeFi

- lending
- flashloans
- stablecoins
- DEX
- MEV

Cryptography

history of cryptography

permutations

substitution

modern cryptography

digital signature

hashing functions

Classical cryptography

References

Histoire des codes secrets, Simon Singh

Definitions

- steganography: hide the message itself
- cryptography: hide the content of the message
- cryptanalysis: break the encryption of the message
- cryptology = cryptanalysis + cryptography

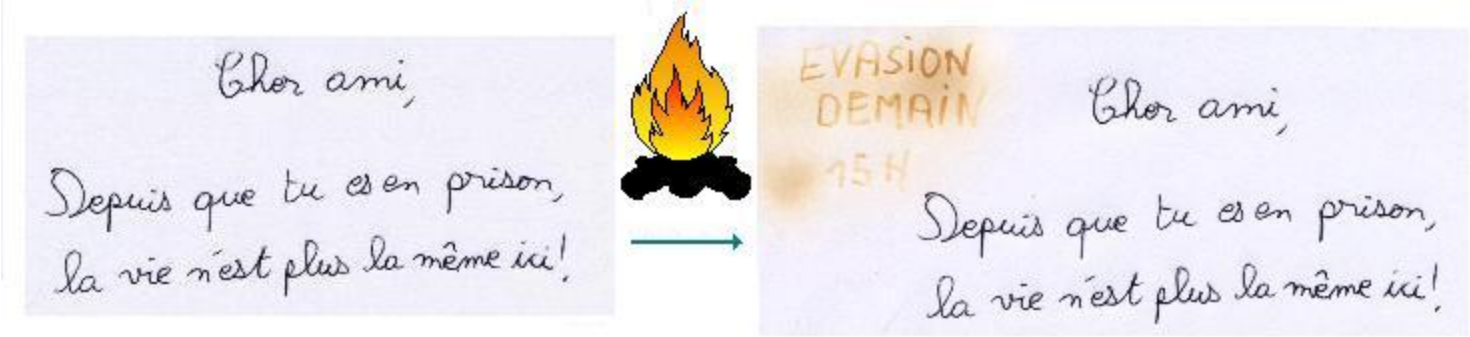
Vocabulary

- chiffrer(*encrypt*) = rendre le contenu du message incompréhensible sans une clef
- déchiffrer(*decrypt*) = rendre le contenu du message compréhensible grâce à une clef
- décrypter(*decrypt*) = casser le chiffrement sans avoir la clef
- 🚨~~crypter~~ : à ne pas utiliser

steganography

steganography

- message under the hair
- invisible ink: lemon juice



- message in MP3

In litterature

Musset >>>> George Sand :

Quand je jure à vos pieds un éternel hommage
Voulez-vous qu'inconscient je change de langage
Vous avez su captiver les sentiments d'un coeur
Que pour adorer forma le Créateur.
Je vous aime et ma plume en délire.
Couche sur le papier ce que je n'ose dire.
Avec soin, de mes lignes, lisez les premiers mots
Vous saurez quel remède apporter à mes maux.

Musset <<<< George Sand :

Cette indigne faveur que votre esprit réclame
Nuit à mes sentiments et répugne à mon âme

In litterature

Musset >>>> George Sand :

Quand je jure à vos pieds un éternel hommage
Voulez-vous qu'inconscient je change de langage
Vous avez su captiver les sentiments d'un coeur
Que pour adorer forma le Créateur.
Je vous aime et ma plume en délire.
Couche sur le papier ce que je n'ose dire.
Avec soin, de mes lignes, lisez les premiers mots
Vous saurez quel remède apporter à mes maux.

Musset <<<< George Sand :

Cette indigne faveur que votre esprit réclame
Nuit à mes sentiments et répugne à mon âme

Cryptography

Source: letterlocking

historical cryptography

Alice and Bob want to communicate. They need to agree on the method & the key(s)

- permutation/transposition: rearrange letters
- substitution: replace a letter by another one

Permutation

Tom marvolo riddle/ Tom elvis jedusor

scytale

PERMUTATION: example

bonjour à tous

BONJOUR A TOUS

B	O	N	J
O	U	R	A
T	O	U	S

BOTO UONR UJAS

substitution: Chiffre de César

Caesar Cipher: letter + 3

rot13: letter + 13

Easy to break since you only have 26 trials => bruteforce

clever attack: frequency analysis

substitution: Chiffre de Vigenère

It is like a ceasar cipher on each letter

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

plain text: MINCE ALORS

cipher key:HAHAH AHAHA

ciphertext:T**** *****

how do you break it?

crypto

With cryptography, we try to achieve 3 goals:

- Confidentiality: no one needs to know what you are buying on the website
- Integrity: your order should not be modified
- Authenticity: you want to be sure it is the right website

some examples:

- hieroglyphe script and rosetta stone
- enigma
- Navajo indians in second world war

Bad example: how to lose your head

Mary, Queen of Scots also known as Mary Stuart

modern cryptography

Kerchoffs' principles

modern cryptography (symmetric encryption)

Binary alphabet: 0 1

One time pad

DES: data encryption standard

AES: Advanced Encryption standard (animation)

To go further

- stream cipher vs block cipher
- encryption/decryption mode

bruteforce

How long des it take to bruteforce a 128 bit key (so 2^{128} possibility), knowing that your PC has a clock rate of 2GHZ?

Problem: key distribution

Say we have n users in our system.

How many keys do they need such that each couple has a unique symmetric keys ?

Problem: key distribution

For n users, the number of (unique) keys is:

$$\frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$$

=> roughly n^2

This means you would need to share a key before you go on Amazon.

For instance Enigma had a schedule book that you needed to distribute.

asymmetrical cryptography

principle: mailbox address

usage:

- encryption
- key exchange
- signature

Digital Signature

In real life: same signature all the time

In digital life: signature depdends on the the message

It consists of 3 algo:

- Key generation $Gen(seed) = (sk, pk)$
- Signature $Sign(msg, sk) = sig$
- Verification $Verif(msg, pk, sig) =$ 👍/👎

Cryptographic Hashing functions

principe: make a digest (fingerprint/dna) of data

problem: from pigeonhole principe(*VF: principe des tiroirs et chaussettes*) explains that you will get a collision

properties:

- collision resistance: hard to find file1 and file2 such that H(file1)=H(file2)
- non inversible
- fast to compute

Hashing and Birthday paradox

How many students do you need in a room to have 50% chance that two of them have the same birthday?

Hashing and Birthday paradox

How many students do you need in a room to have 50% chance that two of them have the same birthday?

Compute the inverse proba: "arrangement" formula

Hashing and Birthday paradox

How many students do you need in a room to have 50% chance that two of them have the same birthday?

Compute the inverse proba: "arrangement" formula

Application to hashing functions

If our hash have n bits, how many trials do we need to have a collision?

authentication (*authentification*)

- something you know: passphrase, pin code
- something you are: fingerprints,
- something you have: smartphone, access cards

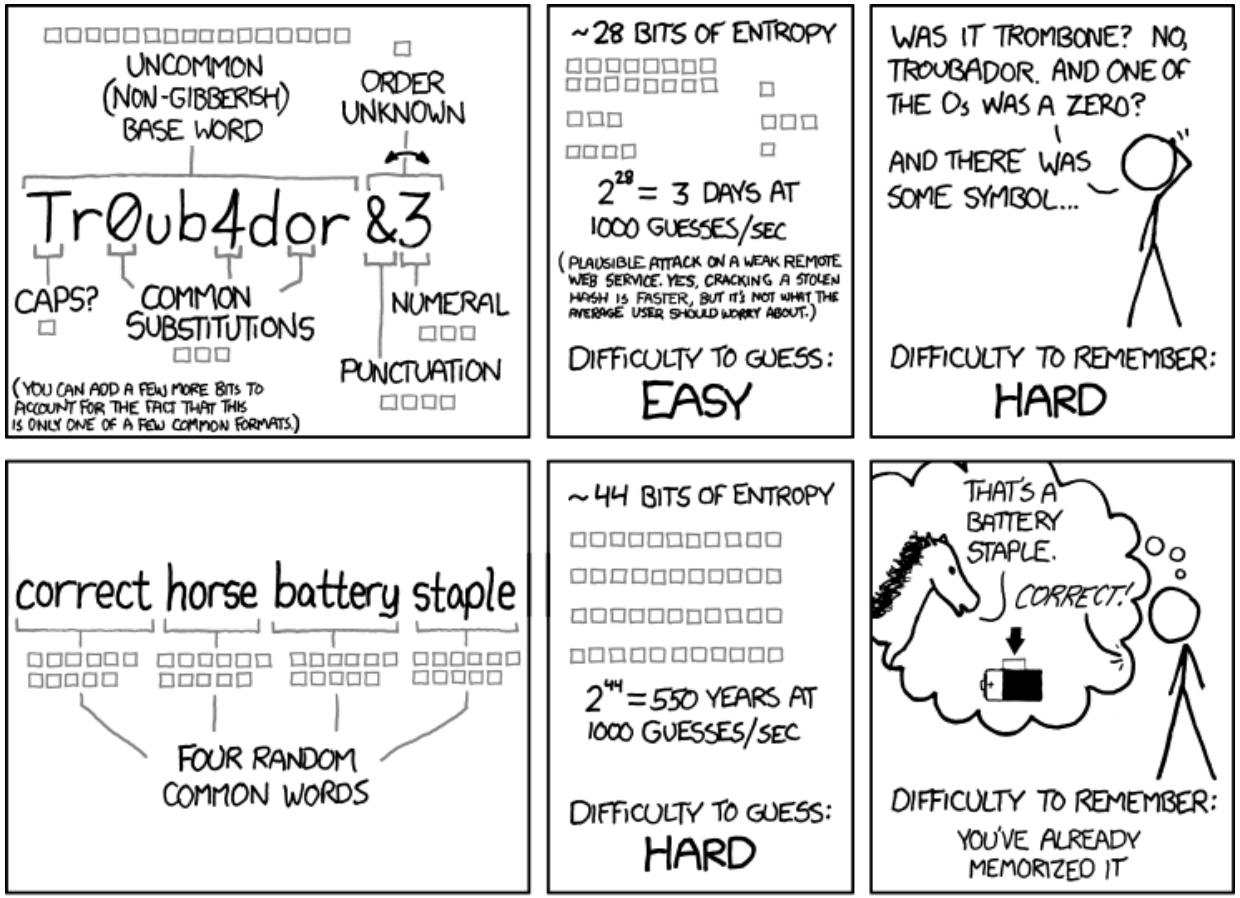
Secured login or nah

```
123456
bonjour
ji32k7au4a83
supercalifragilisticexpialidocious
correct horse battery staple
Tr0ub4dor&3
```

Worst passwords

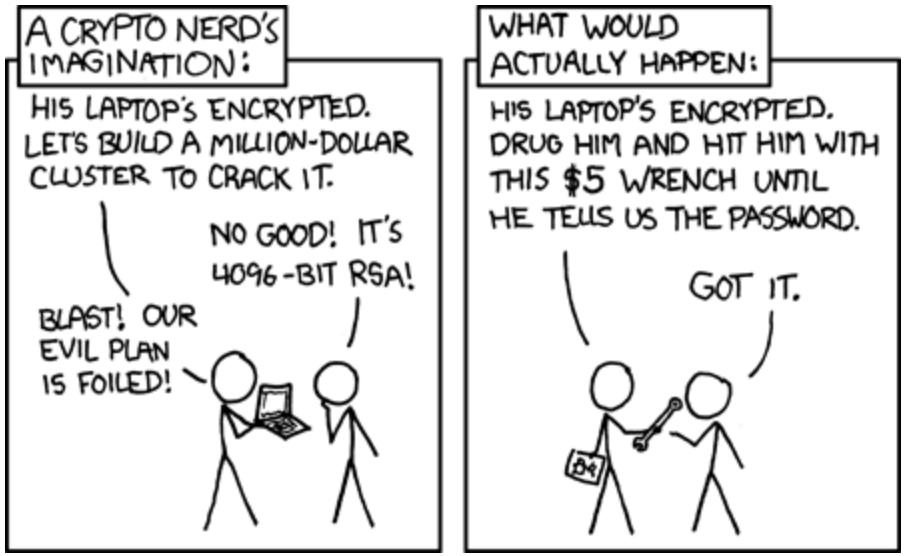
```
123456
password
123456789
12345678
12345
111111
1234567
sunshine
qwerty
iloveyou
princess
admin
welcome
666666
abc123
football
123123
monkey
654321
!@#$%^&amp;*
charlie
donald
password1
qwerty123
```

Choose your ~~password~~ passphrase



source

Security in summary



source

Consensus

What is consensus?

> "Never go to sea with two chronometers; take one or three."

Key properties:

- Liveness: transactions are eventually added to the history
- Safety/Consistency: everyone sees the same history

Consensus can have:

- asynchrony/synchrony/partial synchrony
- permissioned/permissionless access

✨Consensus is magic ✨

A bed time story of the blockchain (ELI5:

https://cryptonuage.com/posts/blockchain-bed-time-story/

Imagine you have a book:

> Anyone could get a copy of this book; they only had to ask.
> When a new line was added to one copy, it would appear on all other copies.
> No sentence, no word, no letter, not a single drop of ink could be removed.

Example: distributed Monopoly

Monopoly

`Centralized` vs `Decentralized`:

You can't be censored.

But how can you trust the tx?

the history?

Monopoly

`Centralized`:

There is a Trusted Third Party.

But you can be censored!

`Decentralized`:

You can't be censored.

But how can you trust the tx?

the history?

Exercise 10 :commit and reveal

Merkle Tree

Those are useful data structure using the properties of cryptographic hash functions.

Blocks, Transactions, Hash

How do we make a chain of blocks?

POW

Gossip protocols

Bitcoin Blockchain

Security & Incentives

Bitcoin: P2P Money

Created by Satoshi Nakamoto

Livre blanc(whitepaper) 2008

Genesis block janvier 2009

Block time: 10 minutes

21 millions

consensus: POW

Crypto + currencies

What's a currency?

Crypto + currencies

What's a currency?

1. Unit of account
2. Medium of exchange
3. Store of Value

Bitcoin Mining:

At first it was on Computer: `one-CPU-one-vote`

But then CPU ⏩⏩ GPU ⏩⏩ FPGA ⏩⏩⏩ASICS

Bitcoin Energy consumption: https://digiconomist.net/bitcoin-energy-consumption

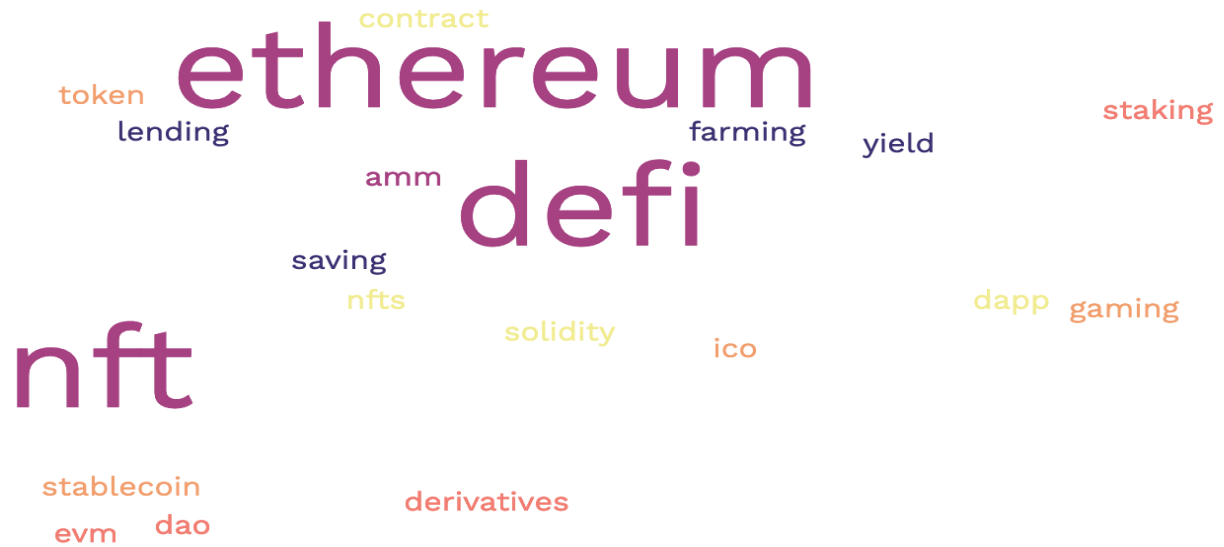
POS: Proof of Stake

The goal here is to replace POW mining by votes weighted by your stake.

> No Mining, just Signing

Ethereum & Smart contract

If the **blockchain** is a computer, a Smart contract, or **Dapp**(decentralized application) is equivalent to a software.



Blockchains

- Blockchain Bitcoin
- Security & Incentives
- Energy
- POS
- Ethereum
- Smart contracts & DAPP

Research questions

- scalability
- L2
- Zero Knowledge

Use cases

- ICO
- ERC20
- DAO
- NFT
- ERC721
- Atomic swaps

DeFi

- Oracles
- lending
- flashloans
- stablecoins
- DEX