Introduction to blockchain technology and smart-contract programming

Sylvain Conchon
University Paris-Saclay

Materials

All the materials for this course are available at the following address :

`https://usr.lmf.cnrs.fr/~conchon/blockchain/`

Contents

1. Introduction to Bitcoin and Ethereum (wallets, explorers, transactions, API, ...), blockchain architecture
2. Consensus algorithms used in Blockains (theory and practice)
3. Smart-contract programming (Ethereum/Solidity)

The Crypto market

Digital Currency

A form of money that exists exclusively in electronic form

Digital Currency

A form of money that exists exclusively in electronic form

Digital assets are managed, stored, and exchanged on computers or smartphones

Digital Currency

A form of money that exists exclusively in electronic form

Digital assets are managed, stored, and exchanged on computers or smartphones

Several types of digital currencies, including :

- Electronic money – PayPal
- Central Banks Digital Currency (CBDC) – Digital Euro
- Cryptocurrency – Bitcoin, Ethereum

Digital Currency

A form of money that exists exclusively in electronic form

Digital assets are managed, stored, and exchanged on computers or smartphones

Several types of digital currencies, including :

- Electronic money – PayPal
- Central Banks Digital Currency (CBDC) – Digital Euro
- Cryptocurrency – Bitcoin, Ethereum

$\hookrightarrow$ One of the key benefits of digital currencies is the ability to facilitate quick, worldwide transactions

Cryptocurrency

Cryptocurrencies are digital and decentralized currencies

$\hookrightarrow$ A crypto is not not controlled by any central authority
No central bank, no government, no company

Cryptocurrency implementations rely on cryptographic techniques for securing data and verifying transactions.

What is the Crypto Market ?

- **Global Marketplace**: A market for trading digital assets (cryptocurrencies, tokens) built on blockchain technology
- **Decentralization**: No central authority; transactions validated by a network of computers (nodes)
- **24/7 Operation**: Unlike traditional markets, the crypto market never closes.

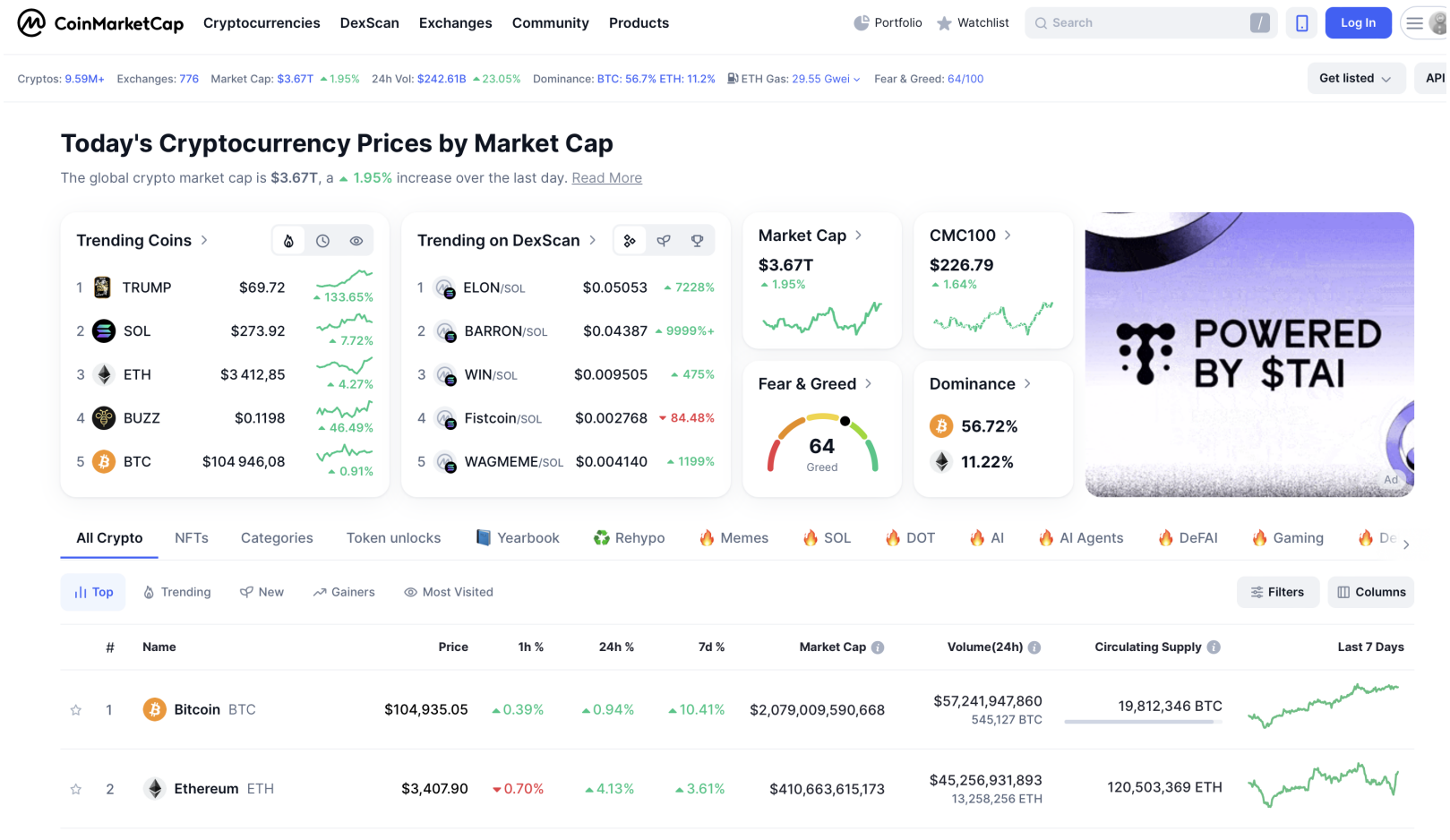
Innovations in the Crypto Market:

- DeFi (Decentralized Finance): Financial services such as lending, borrowing, and trading that operate without traditional intermediaries like banks.
- NFTs (Non-Fungible Tokens): Digital assets that represent ownership of unique items, such as artwork, music, or collectibles.

\begin{Practice}

Crypto market explorer

https://coinmarketcap.com



Practice

`https://coinmarketcap.com`

Analyze the top cryptocurrencies and understand key market metrics :

- Current price?
- Market capitalization?
- 24-hour volume?
- Circulating supply?
- Price change in the last 24 hours (percentage)?

\end{Practice}

Blockchains

Just like traditional currency, managing cryptocurrency involves using mechanisms to create accounts, process transactions between accounts, and more

The technology behind cryptocurrencies is called blockchain

Blockchains

Just like traditional currency, managing cryptocurrency involves using mechanisms to create accounts, process transactions between accounts, and more

The technology behind cryptocurrencies is called blockchain

Blockchains are based on two main components:

- Crypto wallets : Anyone can create accounts on a blockchain, without any authorization
- A distributed ledger : A database distributed accross a large network of computers that records and verifies transactions, without a central authority

Bitcoin

Bitcoin is the first blockchain created in 2009 by an unknown person or group using the pseudonym Satoshi Nakamoto

The concepts of this decentralized crypto currency are outlined in a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System"

Since its launch, there have been over 1 billion transactions on this blockchain

Today, the market cap (current price $\times$ circulating supply) of Bitcoin is equal to 1,800 billion dollars

Ethereum

Ethereum is the another blockchain, created in 2015 by Vitalik Buterin and a team of developers

The concepts behind this decentralized platform for smart contracts and decentralized applications (dApps) are outlined in the whitepaper titled "A Next-Generation Smart Contract and Decentralized Application Platform"

Since its launch, there have been millions of transactions and thousands of decentralized applications built on this blockchain.

Today, the market capitalization of Ethereum is around 370 billion dollars.

Main Components

Blockchains are based on two main components:

- Crypto wallets : Anyone can create accounts on a blockchain, without any authorization
- A distributed ledger : A database distributed accross a large network of computers that records and verifies transactions, without a central authority

Crypto wallets

Crypto Wallets

A crypto wallet is software or hardware that allows the storage, sending, and receiving of cryptocurrencies

It contains pairs of cryptographic keys:

- a public key : serves a similar purpose to a bank account number in traditional finance, both acting as addresses for receiving funds
- a private key is akin to the credentials used to access and control a bank account

Public Addresses

A public address is an alphanumeric string derived from the wallet's public key

> Public addresses are similar to bank account numbers in the cryptocurrency world, used to receive funds

Examples of bitcoin addresses :

bc1qhmptmhnrsuxtqfhydeh3teh9z9h2xgf6z5nyja
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo

Examples of Ethereum addresses :

0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8
0x00000000219ab540356cbb839cbe05303d7705fa
0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2

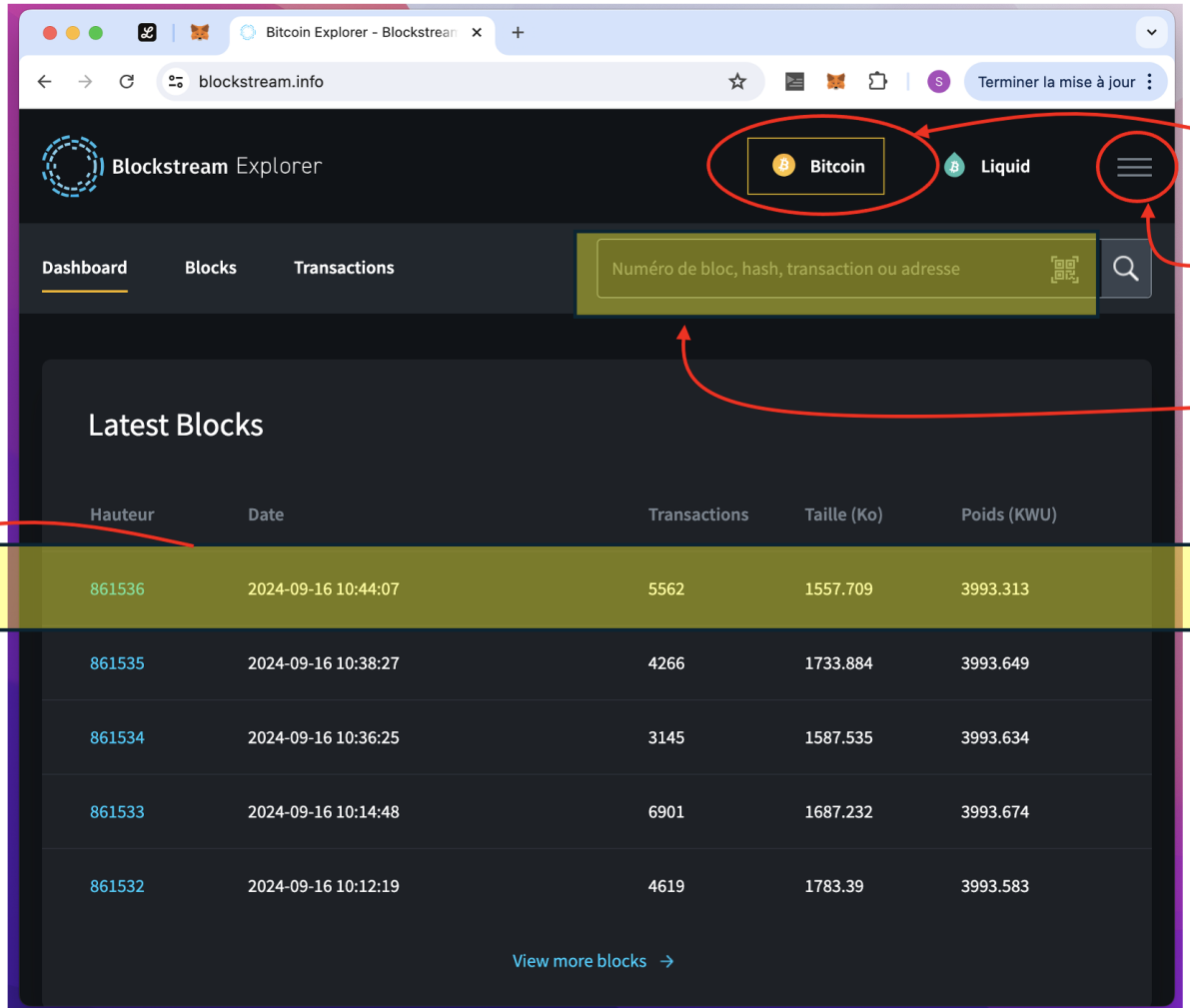
\begin{Practice}

Blockchain Explorers

Blockchain Explorer

A Blockchain Explorer is a tool that allows users to view and search the details of blockchain transactions, blocks, and addresses.

https://blockstream.info/



Practice

Use a block explorer to retrieve information about the Bitcoin addresses provided above

`https://blockstream.info`
`https://www.blockchain.com/explorer`
`https://bitcoinexplorer.org`
`https://etherscan.io/`

Practice

Use a block explorer to retrieve information about the Bitcoin addresses provided above

```
https://blockstream.info
https://www.blockchain.com/explorer
https://bitcoinexplorer.org
https://etherscan.io/
```

bc1qhmptmhnrsuxtqfhydeh3teh9z9h2xgf6z5nyja : Unkown user
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa : The genesis address of Satoshi Nakamoto
34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo : Binance

0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8 : Binance
0x00000000219ab540356cbb839cbe05303d7705fa : Beacon deposit
0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2 : WETH contract

\end{Practice}

Private Keys

A private key is a secret code that allows transactions to be signed and access to the funds in a wallet

> Private keys must be kept secure because anyone with access to this key can access the associated cryptocurrencies

Accounts

Unlike traditional financial systems with account numbers, cryptocurrencies don't use traditional accounts.

Crypto wallets do not store money/assets, they only contain public addresses (that represent destinations for transactions) and private keys

To use an account (and the assets it holds), you only need to :

- sign transactions with your private key to prove that you own those digital currencies associated with the account
- anyone can verify your identity using your public address

Wallet Features

In addition to storing cryptographic key pairs, a crypto wallet is a tool used to interact with blockchain networks

A crypto wallet allows the user to

- send cryptocurrency to other addresses by signing transactions with your private key
- receive cryptocurrency from others
- display a history of transactions (amount, fees, and confirmation status)
- show the current balance of the cryptocurrency held in the wallet

Wallets have also key management features : creation of new public/private key pairs, importing/exporting keys

\begin{Practice}

Wallets

Setting Up a Wallet

Downloading a Wallet

Electrum : a wallet for Bitcoin
MetaMask: a wallet for Ethereum

Testnets

For our exercices, we are using a testnet, a separate network that mimics the main blockchain (mainnet) but operates with test versions of cryptocurrencies that have no real-world value

Creating a Testnet Wallet: Set up a wallet specifically for the testnet.

For Bitcoin :

(Linux) `./run_electrum --testnet`

(Mac OS) `open -a Electrum.app --args --testnet`

For Ethereum : use sepolia testnet

Faucets

Obtaining Testnet BTC or ETH: Use a faucet to get free testnet Bitcoin. Faucets distribute small amounts of testnet coins for testing purposes.

For bitcoin :

https://coinfaucet.eu/en/btc-testnet/

https://faucet.testnet4.dev

https://bitcoinfaucet.uo1.net/

For Ethereum :

https://cloud.google.com/application/web3/faucet

https://faucets.chain.link

Seed Phrase

Private keys are extremely important and must be kept confidential. It is essential that you remember them.

Seed Phrase

Private keys are extremely important and must be kept confidential. It is essential that you remember them.

OK, but try remembering that !

5KCAskKGPWD4TaugT37og3wiNWBR8MdZkAnJQM86CzLkyAvoE9

Seed Phrase

Private keys are extremely important and must be kept confidential. It is essential that you remember them.

OK, but try remembering that !

5KCAskKGPWD4TaugT37og3wiNWBR8MdZkAnJQM86CzLkyAvoE9

Instead, you can use a seed phrase (or recovery phrase). It's a human-readable representation of the private key which takes the form of a sequence of 12, 18, or 24 words generated by a cryptocurrency wallet during setup

Seed Phrase

Private keys are extremely important and must be kept confidential. It is essential that you remember them.

OK, but try remembering that !

5KCAskKGPWD4TaugT37og3wiNWBR8MdZkAnJQM86CzLkyAvoE9

Instead, you can use a seed phrase (or recovery phrase). It's a human-readable representation of the private key which takes the form of a sequence of 12, 18, or 24 words generated by a cryptocurrency wallet during setup

The seed phrase is crucial for wallet recovery :

> If a wallet is lost, stolen, or the device is damaged, the user (or anyone else) can regain access to their cryptocurrency by entering the seed phrase into a new wallet

It’s Your Turn

1. Create an account using Electrum and MetaMask

Use block explorers to check the transactions in Bitcoin and Ethereum testnets.

It's Your Turn

1. Create an account using Electrum and MetaMask
2. Use a faucet to get some (testnet) coins

Use block explorers to check the transactions in Bitcoin and Ethereum testnets.

It's Your Turn

1. Create an account using Electrum and MetaMask
2. Use a faucet to get some (testnet) coins
3. Exchange your public addresses and get some BTC and ETH from your colleagues

Use block explorers to check the transactions in Bitcoin and Ethereum testnets.

It's Your Turn

1. Create an account using Electrum and MetaMask
2. Use a faucet to get some (testnet) coins
3. Exchange your public addresses and get some BTC and ETH from your colleagues
4. Check your translations using a block explorer

Use block explorers to check the transactions in Bitcoin and Ethereum testnets.

It's Your Turn

1. Create an account using Electrum and MetaMask
2. Use a faucet to get some (testnet) coins
3. Exchange your public addresses and get some BTC and ETH from your colleagues
4. Check your translations using a block explorer
5. Drain your colleagues' accounts by retrieving their seed phrase and transfer their coins to your account

Use block explorers to check the transactions in Bitcoin and Ethereum testnets.

```
\end{Practice}
```

Different Kinds of Wallets

We can distinguish two main categories of wallets

Custodial (or non-custodial) : refers to who controls the private keys

Hot (or Cold) wallets : refers to the wallet's connectivity to the internet

Custodial vs. Non-Custodial Wallets

Custodial Wallets :

- Managed by: Third-party service providers (e.g., exchanges)
- Private Keys: Held and controlled by the provider
- Features: User-friendly, offers recovery options, but requires trust in the provider.

  Examples: Wallets on exchanges like Coinbase or Binance.

Non-Custodial Wallets :

- Managed by: The user directly
- Private Keys: Held and controlled by the user
- Features: Greater control and security, but no recovery options if private keys are lost

  Examples: Hardware wallets like Ledger, software wallets like Electrum or MetaMask

Hot vs. Cold Wallets

Hot Wallets:

- Connectivity: Always online and connected to the internet
- Features: Easy access for frequent transactions, but more vulnerable to hacking
- Types: Can be custodial (e.g., exchange wallets) or non-custodial (e.g., software wallets)

  Examples: software wallets like Trust Wallet or MetaMask, Web-based wallets provided by exchanges

Cold Wallets:

- Connectivity: Offline and not connected to the internet
- Features: More secure for long-term storage, less accessible for frequent transactions
- Types: Typically non-custodial

  Examples: hardware wallets (Ledger Nano, Trezor), paper wallets (e.g., QR codes)