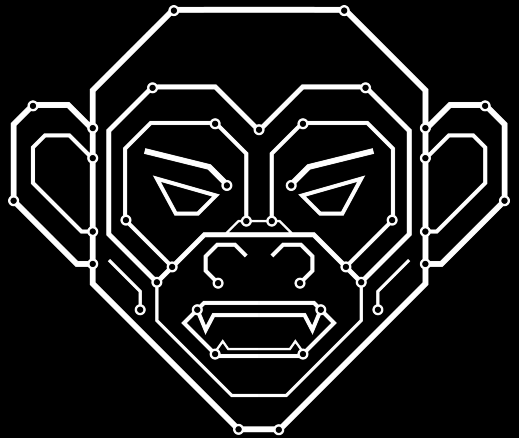
AFNOM Session 16

Blockchain



A·F·N·O·M

Society Recap

- We learn **hacking** skills and do **CTFs**
- No membership — just **turn up**!
- Come to the **pub** after sessions + occasional **events** (films / games)
- Ask **questions**!! We're all here to learn from each other :-)

AFNOM Values

- **Inclusive** — everyone is welcome, regardless of race, ethnicity, gender, gender identity, sexual orientation, age, class, physical ability, nationality, and text-editor preference.
- **Supportive** — we're not here to compete with each other; we've all got things to learn and teach.
- **Ambitious** — we all want to advance our cybersecurity skills.
- **Respectful** — let's be kind and humble.

Preface

- Some things we cover could be interpreted as or used immorally or illegally
- We are here to learn cool stuff and have fun!

“Don’t do crimes”
- Dr Ian Batten

- Good lecturer
- Sound advice
- We are the **ethical** hacking society

“Don’t be evil”
- Google

- Somewhat ironic
- They stopped using it in 2015
- But we are not multi conglomerate mega empire so we can reserve the right to morals

Disclaimer

What we will NOT be discussing

- Investment strategies
- Market volatility
- Liquidity
- Profit models
- Meme coins/NFTs
- Taxation and Legality
- Fraud or Crime

What we will be discussing

- Why Cryptocurrency exists
- How Blockchain works
- Consensus systems
- Transactions and Contracts
- Blockchain attack vectors
- Blockchain exploitation

Cryptocurrency Crash Course

(Semi-High level explanation)

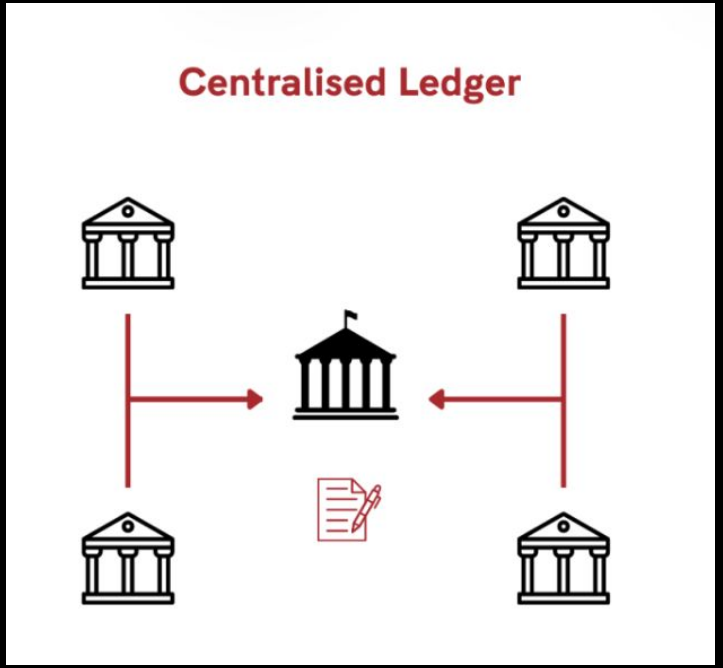
How banks work

Banks handle transactions using a centralised system where all balances and payments are stored and controlled in a single internal database.

This means the bank has full authority to:

- Approve transactions
- Block transactions
- Reverse transactions
- Modify transactions

Customers must also trust the bank to keep accurate records and protect their funds

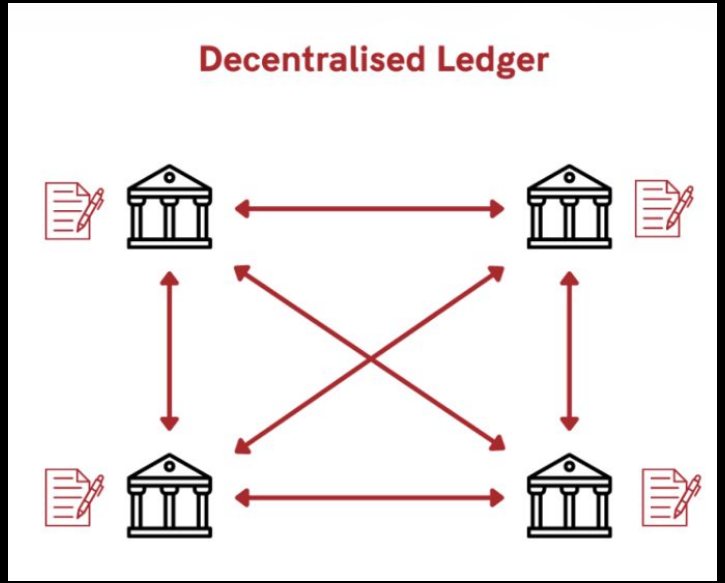


Why cryptocurrency

Cryptocurrency exists to remove the need for trusted central authorities by replacing them with cryptographically verified public immutable ledgers.

This makes cryptocurrency:

- Resistant to censorship (theoretically)
- Tampering becomes obvious
- No single centralised failure point



This also shifts responsibility to the user, since mistakes or lost keys cannot be undone.

But how do we replace the banks?

We replace the banks with a system using blockchain and smart contracts. Blockchain is a list of blocks, linked together in order, where each block contains data and a cryptographic link to the previous block.

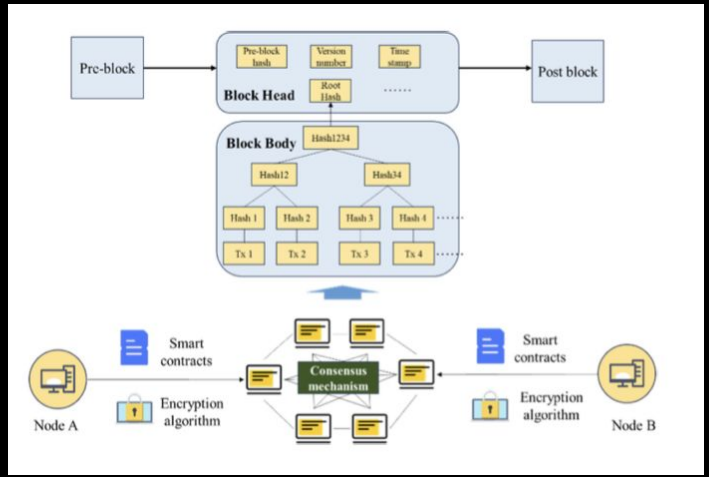
Put simply, it is a linked list where the links are hashes. Changing any block would change its hash and break the links to all following blocks, making tampering obvious.

Everyone has access to this list, which is known as a public ledger. Instead of trusting a single central authority, all participants independently verify and store a copy of the ledger.

Each blockchain or cryptocurrency uses a different system to determine

- What data goes into a block
- How blocks are created and added
- How the network agrees on the correct version of the chain
- What rules transactions and smart contracts must follow

Because the rules are enforced by cryptography and a consensus rather than a bank, the system can operate without a trusted intermediary.



But what is cryptocurrency?

Possible State Approaches to Cryptocurrencies

Jan Lansky
University of Finance and Administration in Prague
Czech Republic
zizelevak@gmail.com

DOI: 10.20470/jsi.v9i1.335

Abstract: *Cryptocurrencies are a type of digital currencies that are relying on cryptographic proofs for confirmation of transactions. Cryptocurrencies usually achieve a unique combination of three features: ensuring limited anonymity, independence from central authority and double spending attack protection. No other group of currencies, including fiat currencies, has this combination of features. We will define cryptocurrency ownership and account anonymity. We will define cryptocurrency ownership and account anonymity. We will introduce a classification of the types of approaches to regulation of cryptocurrencies by various individual countries. We will present the risks that the use of cryptocurrencies involves and the possibilities of prevention of those risks. We will present the possible use of cryptocurrencies for the benefit of the state. The conclusion addresses the implications of adoption of a cryptocurrency as a national currency.*

Key words: cryptocurrency, Bitcoin, anonymity, risk and prevention, state approaches

You control a blockchain address using a private-public key pair. The private key lets you authorize transactions, and the blockchain publicly records what that address holds.

Cryptocurrency is NOT to be confused with electronic money.

Cryptocurrency is NOT blockchain.

Blockchain is the fundamentals on which cryptocurrency is based.

Cryptocurrencies are decentralized digital currencies that follow a specific set of rules.

https://web.archive.org/web/20180212005102/http://si-journal.org/index.php/JSI/article/viewFile/335/325

Consensus systems

The blockchain is enforced by what is know as a consensus systems.

Consensus systems are a well known problem in computer science and there is no universally correct approach or solve.

This is again why blockchains differ so vastly as they will have different solutions.

Ways of having consensus include solutions such as Proof-of-Work (PoW), Proof-of-Stake (PoS), or Ripple Protocol Consensus Algorithm (RPCA).

(These are all permissionless consensus systems.)

Transactions and Contracts

A transaction is the basic action which records a transfer of information on the blockchain.

A smart contract is a program stored on the blockchain that automatically executes rules when certain conditions are met. They are immutable and hence must be secure as otherwise they will be exploited.

Smart contracts were supposedly based on the bitcoin protocol and now are mostly written the Solidity language (.sol) and Python.

https://docs.soliditylang.org/en/latest/introduction-to-smart-contracts.html#simple-smart-contract

Extra bits

Making transactions is NOT FREE.

Transactions cost an OPTIONAL fee. This fee is best represented as the cost it takes to write your transaction to the blockchain. Too little and your request may be ignored. Too much and you waste money.

Depending on your consensus system this will determining how your transaction fee is handled and how you can earn transaction fees (also known as mining).

Crypto “mining” refers to earning rewards, including transaction fees, by adding a block to the blockchain. Technically, only Proof of Work blocks are mined; in Proof of Stake and other consensus mechanisms, blocks are proposed and validated rather than mined.

Cryptocurrency Crash Course Complete!

Any Questions so far?

Blockchain Attack vectors

Because of how big and diverse blockchain is there is an enormous field of exploitation. Some examples are:

- Consensus & network-level attacks
- Transaction-level attacks
- Smart contract vulnerabilities
- Cryptography-related issues
- Wallet & user-level attacks
- Infrastructure & off-chain attacks
- Governance & economic attacks
- Cross-chain & Layer-2 attacks
- Privacy attacks

Almost all CTFs will focus on these two.

Transaction (Eth)

json

```
{
  "type": "0x2",                    // Transaction type (EIP-1559)
  "chainId": "0xaa36a7",                // Identifies which blockchain the transaction is for
  "nonce": "0x0",                    // Transaction count from sender

  // Gas fees (EIP-1559)
  "maxPriorityFeePerGas": "0x3b9aca00",    // 1 Gwei tip for miner  – Extra fee to encourage faster processing
  "maxFeePerGas": "0x59682f00",           // 1.5 Gwei max fee – Maximum total fee the sender is willing to pay
  "gas": "0x5208",                    // 21000 gas units – Maximum “work” units allowed for this transaction

  // Recipient and value
  "to": "0x90f79bf6eb2c4f870365e785982e1f101e93b906",  // Recipient address
  "value": "0x16345785d8a0000",           // 0.1 ETH in wei  –How much money is being sent

  // Optional fields
  "data": "0x",                     // Empty for ETH transfer –Extra instructions for smart contracts
  "accessList": []                    // No access list  –Lists resources the transaction will touch (optional)
}
```

Transaction (Eth)

```
{
  "type": "0x2",                  // Transaction type (EIP-1559)
  "chainId": "0xaa36a7",              // Identifies which blockchain the transaction is for.
  "nonce": "0x0",                 // Transaction count from sender

  // Gas fees (EIP-1559)
  "maxPriorityFeePerGas": "0x3b9aca00",    // 1 Gwei tip for miner  –Extra fee to encourage faster processing
  "maxFeePerGas": "0x59682f00",          // 1.5 Gwei max fee –Maximum total fee the sender is willing to pay
  "gas": "0x5208",                  // 21000 gas units –Maximum "work" units allowed for this transaction

  // Recipient and value
  "to": "0x90f79bf6eb2c4f870365e785982e1f101e93b906",  // Recipient address
  "value": "0x16345785d8a0000",          // 0.1 ETH in wei  –How much money is being sent

  // Optional fields
  "data": "0x",                   // Empty for ETH transfer –Extra instructions for smart contracts
  "accessList": []                  // No access list  –Lists resources the transaction will touch (optional)
}
```

RLP

0x02f872018504a817c800850773594000825208940 90f79bf6eb2c4f870365e785982e1f101e93b9016345785d8a000080c0

Type

ECSDA

0x02f8720185012a05f20082520894090f79bf6eb2c4f870365e785982e1f101e93b90601816345785d8a000080c001a0aa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa056bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
bbbbbbbbbbbbbbbbbbbbbbbbbbbbb

Transaction is serialized using Recursive Length Prefix (RLP).

The transaction is then cryptographically signed (ECDSA) to verify the sender's address.

Transaction (Eth)

0x02f8720185012a05f20082520894090f79bf6eb2c4f870365e785982e1f101e93b90601816345785d8a000080c001a0aa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa056bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
bbbbbbbbbbbbbbbbbbbbbbbbbbbbb

This transaction is then broadcast to the Ethereum network, where nodes validate it, and if everything is correct, it gets included in a block and eventually confirmed on the blockchain.

This final result is usually known as a tx

But how do we broadcast this to the network?

Transaction (Eth)

We use Remote Procedure Calls (RPC) to broadcast our transactions.

We choose the RPC method for our transaction

```
{
 "jsonrpc":"2.0",
 "method":"eth_sendRawTransaction",
 "params":["0x02f86b8085..."],  //  signed tx
 "id":1
}
```

Using curl we can interact with the chain

```
curl -X POST \
 -H "Content-Type: application/json" \
 --data "{"jsonrpc":"2.0","method":"eth_sendRawTransaction","params":["0x02f86b8085..."],  "id":1}" \
 https://mainnet.infura.io/v3/…….
```

Demo

Metavault

Local simulation of blockchain

Local contract deployment

Foundry basics showcase

Tools , Tools and more Tools

Languages

- Solidity
- Rust
- Go
- Javascript/Typescript
- Python
  - Cryptography
  - Sage-cell
  - Web3

Dev Toolkits

- Foundry
  - Forge
  - Cast
  - Anvil
- Hardhat
- Ether.js

Debugging and forensic

- Etherscan
- Anvil traces
- Tenderly

Misc

- Docker
- Vs Code
- Remix IDE

Wallets

- Anvil
- Metamask
- Rabby

Extra

- Echidna (Fuzzer)
- Ganache (Legacy local blockchain sim-nice GUI)

There are also blockchain specific IDEs!

You don't need every single tool but Foundry + Languages + Misc should enable you to do most challenges.

Links and resources

Getfoundry.sh

soliditylang.org

https://sessions.afnom.net

Github - Chainflag.org

Github - minaminao ctf blockchain challs

Web3 guides by Bitcoin and Ethereum

Right Now

sessions.afnom.net

- Hang around at 5pm for **pub social**! 🎉🎉
- Come back next week for **WiFi Hacking**!