

# Blockchain and cryptocurrencies

1. Preliminary concepts at the basis of Blockchain [\[2\]](#),[\[3\]](#)
  - 1.1. Introduction to the cryptography concepts used in Blockchain [\[3\]](#)
    - Cryptography services (confidentiality, authentication, integrity, non-repudiation)
    - Public and private key cryptography
    - Elliptic curve cryptography
    - Hash functions
    - Elliptic curve digital signature algorithm (ECDSA)
  - 1.2. Distributed systems and decentralization
  - 1.3. Consensus & Byzantine generals problem
2. Introduction to Blockchain [\[2\]](#),[\[3\]](#)
  - 2.1. What is a Blockchain
  - 2.2. Blockchain features
  - 2.3. Types of Blockchain (public, consortium, private)
  - 2.4. Blockchain history (why it was invented)
  - 2.5. Overview of today Blockchain applications
3. Bitcoin [\[7\]](#),[\[1\]](#)
  - 3.1. Bitcoin protocol specification
    - Overview of Bitcoin data types (transaction, scripts, addresses, blocks)
    - Transactions
    - Bitcoin network architecture
    - Bitcoin blockchain (blocks structure, Merkle trees, mining, proof of work)

### 3.2. Bitcoin wallets

## 4. Bitcoin privacy

- Considerations on user anonymity in Bitcoin
- Possible attacks
- How to enhance privacy in Bitcoin (explanation of mixing services + reference [6])

## 5. Bitcoin blockchain scalability

- Considerations on the scalability of the Bitcoin blockchain and possible solutions [7],[5]

## 6. Alternatives to Bitcoin

- Bitcoin limitations
- Alternatives to proof of work [4]
- Namecoin
- Litecoin
- ZCash

## 7. Smart contracts

- History
- What smart contracts are
- Security

## 8. Ethereum

- History
- Ethereum components (Keys, addresses, accounts)
- Ethereum blockchain
- Ethereum network
- Ethereum transactions
- Ethereum virtual machine

## 9. (Possibly) Practical example of blockchain application: development of a distributed application through Ethereum Solidity (Something similar to the application development shown in reference [2])

## References

- [1] A.M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, 2017. ISBN: 9781491954362. Available at: <https://books.google.it/books?id=MpwnDwAAQBAJ>.
- [2] J.J. Bambara et al. *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*. McGraw-Hill Education, 2018. ISBN: 9781260115864. Available at: <https://books.google.it/books?id=z5hIDwAAQBAJ>.
- [3] I. Bashir. *Mastering Blockchain*. Packt Publishing, 2017. ISBN: 9781787125445. Available at: <https://books.google.it/books?id=dMJbMQAACAAJ>.
- [4] Iddo Bentov, Ariel Gabizon, and Alex Mizrahi. “Cryptocurrencies Without Proof of Work”. In: *Financial Cryptography and Data Security*. Ed. by Jeremy Clark et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 142–157. ISBN: 978-3-662-53357-4.
- [5] Kyle Croman et al. “On Scaling Decentralized Blockchains”. In: *Financial Cryptography and Data Security*. Ed. by Jeremy Clark et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 106–125. ISBN: 978-3-662-53357-4.
- [6] Ethan Heilman, Foteini Baldimtsi, and Sharon Goldberg. “Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions”. In: *Financial Cryptography and Data Security*. Ed. by Jeremy Clark et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 43–60. ISBN: 978-3-662-53357-4.
- [7] G. Karame and E. Androulaki. *Bitcoin and Blockchain Security*. Artech House information security and privacy series. Artech House, 2016. ISBN: 9781630810139. Available at: [https://books.google.it/books?id=b%5C\\_nwjwEACAAJ](https://books.google.it/books?id=b%5C_nwjwEACAAJ).