Part 1
Blockchain Technology

1
Introduction to Blockchain

DOI: 10.1201/9781003337393-2

Blockchain Technology is one of the four hot technologies shaping the future of the tech world in the coming decades, these four technologies (IBAC) are: **I**nternet of Things (IoT), **B**lockchain, **A** rtificial Intelligence (AI), and **C**ybersecurity (Figure 1.1). All four technologies are interconnected and impact each other in many ways. As Figure 1.2 shows that you can explain each technology with an analogy to human acts: IoT: Feels, Blockchain: Remembers, AI: Thinks, and Cybersecurity: Protects.

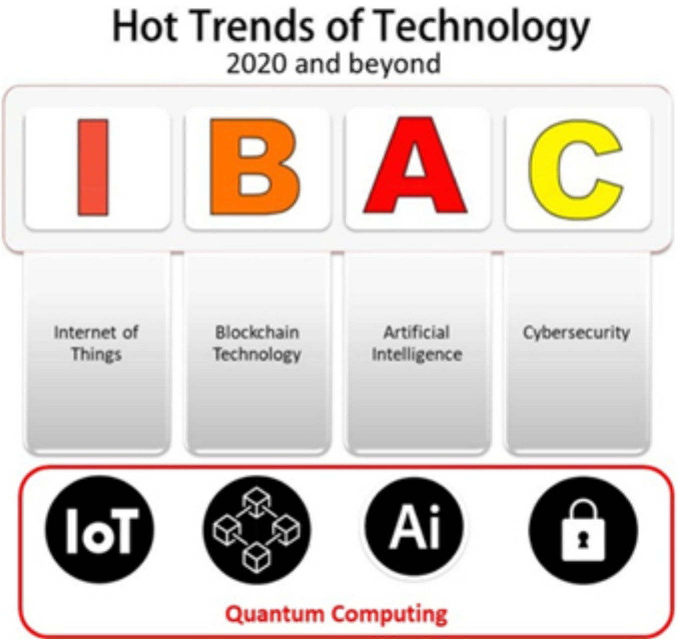


Figure 1.1: Simplified form of IBAC

Recently, “Quantum Computing” presented itself as a new player impacting IBAC in many ways, for example, Quantum Computing will make IoT faster in processing data and extracting insights, Quantum Computing will force Blockchain to invent new encryption techniques and will make processing data faster solving one of the main issues of Blockchain Technology, in the case of AI Quantum Computing will make analysis extremely faster which will, in turn, makes decisions done real-time in many cases not possible with current computing tools, in Cybersecurity, Quantum Computing will help in detection and prevention of cyber-attacks and open the doors for new Quantum Encryptions algorithms which will make it very hard for hackers to access systems and data.

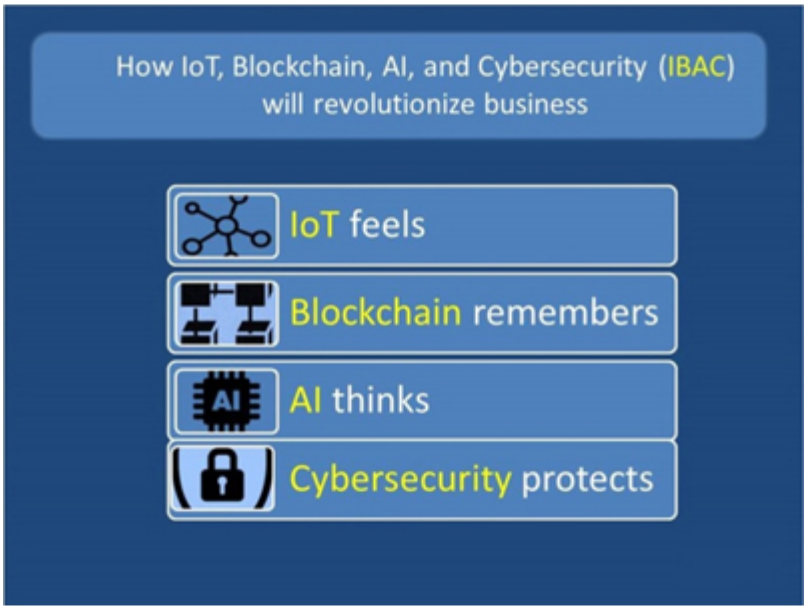

How IoT, Blockchain, AI, and Cybersecurity (IBAC) will revolutionize business
IoT feels
Blockchain remembers
AI thinks
Cybersecurity protects

Figure 1.2: Hot Trends of Technology in 2020 and Beyond

1.1 What is Blockchain?

Blockchain is simply a software to start with the classical definition of Blockchain is “a distributed database existing on multiple computers at the same time. It is constantly growing as new sets of recordings, or ‘blocks’, are added to it. Each block contains a timestamp and a link to the previous block, so they actually form a chain”, but the best definition of Blockchain according to MIT is: *Cryptography +Human Logic*.

If the internet is all about providing *connectivity*, Blockchain is all about enabling *trust*. For example, imagine there are 30 people in a classroom or an office building, with one main door and a security guard holding a list of authorized students/employees who can get into the building, you will show your card to him/her to check the list and if you are on the list you are in. This is the current centralized system. With the use of Blockchain, each one of the 30 people will have a list with pictures of people who are authorized to be in the room so if somebody came in, and that person was not on the list, they would start talking to each other, asking “Hey, can you please check if this person belongs here?” That is a synchronization and referred to as gossip protocol within the Blockchain. Human logic is the list you have, and the motion of everybody starting to talk to each other. On the top of the current system using encryption (user name and password), we added the human logic, consensus protocols and algorithms.

Figure 1.3: Best Definition of Blockchain

1.2 The Five Components of a Blockchain

1. Cryptography
2. P2P Network
3. Consensus Mechanism
4. Ledger
5. Validity Rules

All listed in Figure 1.4.

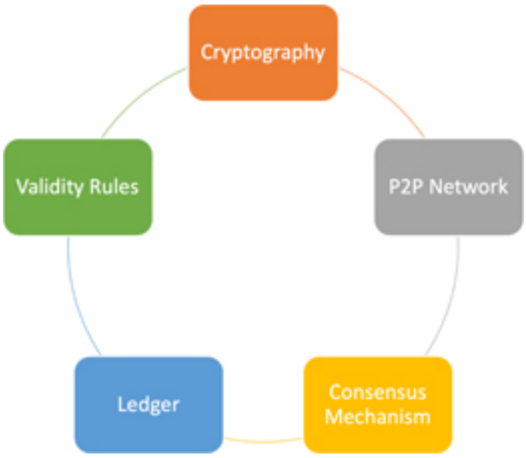


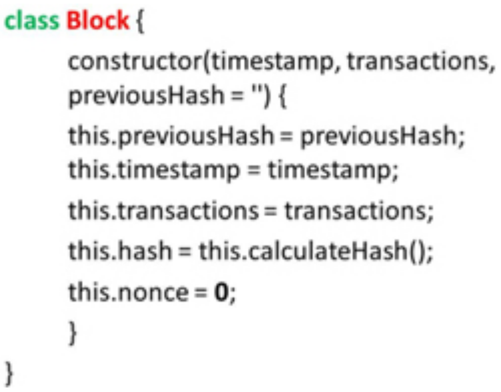
Figure 1.4: Five Components of a Blockchain

1.3 Blockchain Programming Languages

Any of the following programming languages can be used to create Blockchain platforms:

- C++ (Bitcoin)
- Python
- JavaScript
- Solidity (Smart Contract)
- Java
- Go

Figure 1.5 shows example of a “block” programming.



```
class Block {
        constructor(timestamp, transactions,
        previousHash = '') {
        this.previousHash = previousHash;
        this.timestamp = timestamp;
        this.transactions = transactions;
        this.hash = this.calculateHash();
        this.nonce = 0;
        }
}
```

Figure 1.5: Example of a “block’" programming

1.4 Mechanism of Blockchain Technology

First block called Genesis Block, created by the miner or validator based on consensuses protocol, each block have five elements (Index, Time-Stamp, Previous Hash, Hash, and Data), a Blockchain is initialized with the genesis block which is the foundation of the trading system and the prototype for the other blocks in the Blockchain. When you change any of these data’s you will change the whole block and the following blocks will see that something has changed, in addition to the other nodes with copies of the blocks and the altered node will be rejected, all nodes sync using a gossip protocol, Figure 1.6 shows this type of mechanism.

A gossip protocol is a procedure or process of computer peer-to-peer communication that is based on the way epidemics spread. Some distributed systems including Blockchain use peer-to-peer gossip to ensure that data is disseminated to all members of a group. Some ad-hoc networks have no central registry and the only way to spread common data is to rely on each member to pass it along to their neighbors. [1]

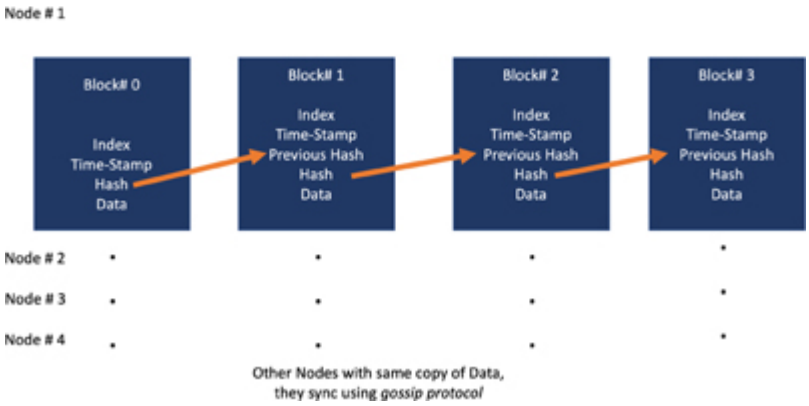


Figure 1.6: Example of Blocks of Blockchain in one node

1.5 Blockchain vs. Traditional Database

There are many differences between Blockchain and Traditional Database and Table 1.1 summarizes them:

Table 1.1: Blockchain vs. Traditional Database

Blockchain vs. Traditional Database		
Characteristics	**Blockchain**	**Database**
Authority	Decentralized	Centralized and controlled by the admin
Architecture	Distributed	Client-server
Data Handling	Read and Write	CRUD (Create, Read, Update, Delete)
Integrity	High	Can be altered by hackers
Transparency	High	Controlled by the admin
Cost	High	Low
Performance	Slow	Very fast

1.6 The Stack of Blockchain

Like any other technology, Blockchain can be defined by its stack, the following diagram explains it and it is worth mentioning to emphasize the importance of each layer as an opportunity for improvement and new business (startups), for example, UI/UX for different devices including smartphones, tablets, desktops, and laptops, in addition to the wide field of new consensus protocols for specific applications and industries, the introduction of smart contracts in the design process to avoid any surprises, and secure ways to connect the stack to the internet.

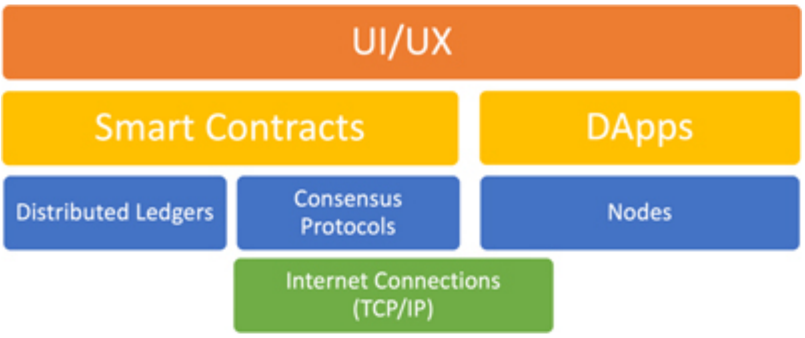


Figure 1.7: Blockchain Stack

1.7 Blockchain Tracks

To understand the future direction of Blockchain technology, we need to recognize the three tracks (Figure 1.8) of Blockchain technology:

- *Pure R&D Track*: This track is focused on understanding what it means to develop a Blockchain-based system. Ideally, working on real use-cases, the ultimate goal is investigation and learning, and not necessarily delivery of a working system.

- *Immediate Business Benefit Track*: This track covers two bases: (1) learning how to work with this promising technology and (2) delivering an actual system that can be deployed in a real business context. Many of these projects are intra-company.
- *Long-Term Transformational Potential Track*: This is the track of the visionaries, who recognize that to realize the true value of Blockchain-based networks means reinventing entire processes and industries as well as how public-sector organizations function.

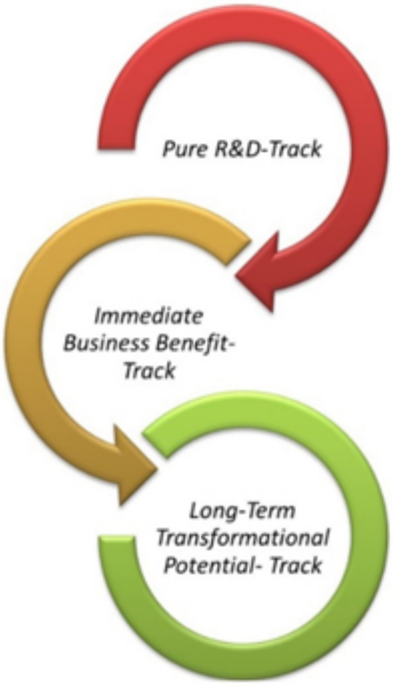

Pure R&D-Track
Immediate Business Benefit-Track
Long-Term Transformational Potential- Track

Figure 1.8: Tracks of Blockchain Technology

1.8 Challenges facing Blockchain Technology

Every new technology face challenge and Blockchain is not an exception, the following is a list of both technical and non-technical challenges (Figure 1.9):

Technical Challenges

- Scalability
- Processing Time
- Processing Power
- 51% Attack
- Double Spending
- Bad Smart Contracts
- Storage
- First Mile and Last Mile problem (Data before and after going through the Blockchain)

Non-Technical Challenges

- Regulations
- Public perception (Blockchain is Bitcoin)
- Lack of skilled staff

1.9 Types of Blockchain Networks

There are three types of Blockchain Networks (Figure 1.10):

- **Public:** a public Blockchain is the one where everyone can see all the transactions, anyone can expect their transaction to appeal¯ on the ledger and finally anyone can participate in the consensus process.

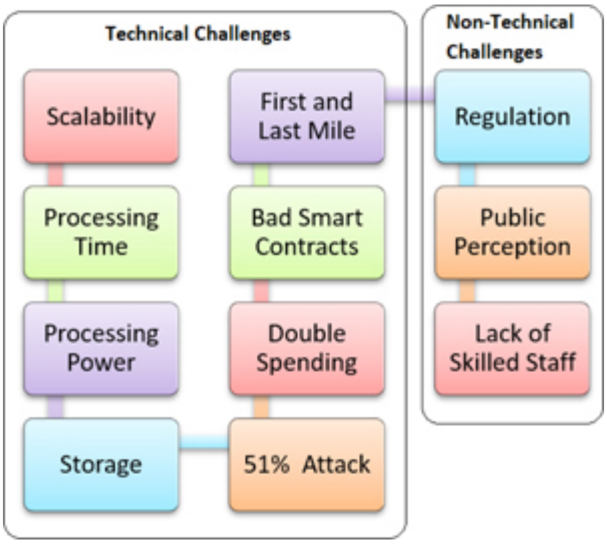


Figure 1.9: Challenges Facing Blockchain

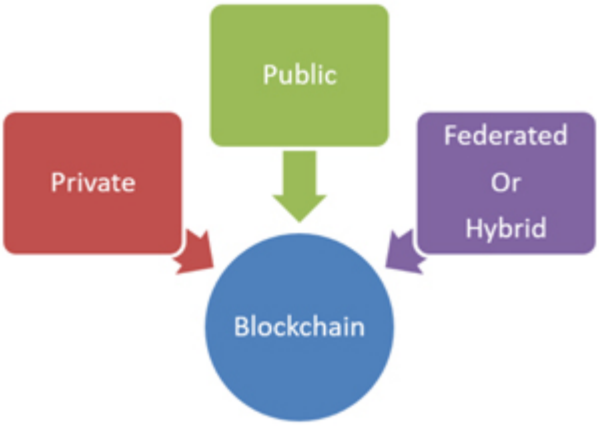


Figure 1.10: Types of Blockchain Networks

- **Federated/Hybrid:** federated/hybrid Blockchain does not allow everyone to participate in the consensus process. Indeed, only a limited number of nodes are given permission to do so. For instance, in a group of 20 pharmaceutical companies, we could imagine that for a block to be valid, 15 of them have to agree. The access to the Blockchain, however, can be public or restricted to the participants.

- **Private:** private Blockchains are generally used inside a company. Only specific members are allowed to access it and carry out transactions.