# BLOCKCHAIN

**Chapter** · May 2020

DOI: 10.1002/9781119621201.ch1



**6 authors**, including:

Gururaj H L
Manipal Institute of Technology
**156** PUBLICATIONS **701** CITATIONS

SEE PROFILE

PART I

# CRYPTOCURRENCIES AND BLOCKCHAIN TECHNOLOGY

# CHAPTER 1

# BLOCKCHAIN: A NEW ERA OF TECHNOLOGY

Gururaj H L,* Manoj Athreya A, Ashwin A Kumar, Abhishek M Holla, Nagarajath S M, Ravi Kumar V

Vidyavardhaka College of Engineering, Mysuru, India

* Corresponding author: gururaj1711@vvce.ac.in

**Abstract**

As the whole world is moving towards digital payments, ethers and transaction methods with quick payment, information is stored in a blockchain in a distributed network. The distributed network is a network system through which data, software and computer programming are spread across more than one node (computers) and these nodes are dependent on each other. It is nothing but a peer-to-peer network which eliminates a single point of failure. The blockchain is a growing list of records called blocks that are linked using cryptography. It is a decentralized, distributed and immutable ledger to store digital transactions. Its databases are managed using a peer-to-peer network where all the nodes in a network are equal and are the major concern in the types of network architecture. The consensus protocol is used for transacting and communicating between the nodes. In this chapter, an approach for storing data in a blockchain is investigated and reported whereby the record is kept safe and secure, preventing it from being manipulated by others. With the help of the above blockchain technology we are able to achieve data that is secure from manipulators.

***Keywords***: Blockchain, inter-planetary file system, Ethereum, Web 3.0, consensus protocol, mining, distributed P2P network, Ethereum transaction, SHA-256 algorithm, decentralized application

Blockchain is one of the booming words in the field of computer technology, which has the power to change the lives of people as the Internet did in the past twenty years. Blockchain is ready to make a big impact on the lives of people if we adhere to this technology. It is a fundamental and parallel part to the Internet and not just a use case like emails, e-commerce, etc. When people hear the term blockchain many come to a conclusion that it deals mainly with cryptocurrency and Bitcoin but it is not all about that. The cryptocurrency and Bitcoin can be compared to email where the backbone technology behind it is the internet. As such, blockchain is a technology. Blockchain can be broadly described as a digital form of the ledger where you can store whatever data you want and then later access it through the hash value you received. It's just like the acknowledgment number you get when you produce some documents. Consider a scenario where some person $x$ needs to send money to person $y$ who lives in a different country; it takes at least 5-6 working days to transfer the money because we have middle parties like banks which require time to process it. When it comes to blockchain we have an immutable universal ledger where it stores transaction details of all the individuals in a block. When a transaction is made it adds a new block into the existing set of blocks in the system which is authenticated by everyone. When it comes to security it uses the best cryptographic algorithms and is difficult to hack. It uses the SHA-256 algorithm to keep the hash value secured. When a hacker tries to hack a blockchain system, first of all, he needs computation power of more than 50% of the supercomputer in the word and he also needs to change all the blocks because they are cryptographically linked to each other; moreover, the blocks reside in a distributed node and every time it checks with other nodes to see whether they possess the same details which are based on the consensus protocol. As it is a collection of chained blocks you can trace back to the transactions that have occurred by going back block by block. They also have originated smart contracts which are the logic built into most blockchains, where when an event happens it triggers another event. Finally, all the blocks are not owned by anyone like a bank or any trusted authority. The blockchain is owned by all of us and to maintain it we need resources, electricity, computing power, time, money, etc. So for the people who maintained all these resources, in 2008 Satoshi Nakamoto introduced the concept of Bitcoins to give them as incentives, and the persons who looked after the blockchain mined it and hence they were called miners. In this blockchain the word TRUST plays an important role. Consider an example of a party where ten people put in a thousand rupees each and draw one name from the box; this lucky person will get the entire amount. Here, it is the trust between all ten people which works like a blockchain and brings the trust from a centralized to decentralized platform. The blockchain works on the following four major features:

1. Consensus
2. Security
3. Provenance
4. Trust

The countries which use this technology are Japan, Canada, Dubai, Estonia and many more. Dubai is transforming itself as the world's first blockchain-powered government. Estonia is being called Ethereum Island. When it comes to India we have certain blockchain information such as:

1. State Bank of India partnered with BankChain and Intel to develop blockchain solutions.

2. West Bengal and Andhra Pradesh is transitioning to using blockchain software for solving land property issues.

3. The Centre for Development of Advanced Computing (C-DAC) Hyderabad is working on blockchain projects.

4. Blockchain patents are claimed by the Indians and many more.

Some of the recent blockchain technology being hyped in the current industry are as follows:

1. Google is bringing blockchain technology to its cloud services.

2. Facebook has plans for blockchain-based authentication.

3. Microsoft Azure allows the development, testing, and deployment of secure blockchain apps.

4. IBM is now delivering blockchain service around the world.

5. Walmart has partnered with IBM to create a blockchain for tracking food globally through its supply chain.

6. Mastercard has started to build their own blockchain-based payment gateways.

7. Huawei's blockchain technology offers mobile carriers superb opportunities to subscribers.

Figure 1.1 shows the different sectors in which blockchain technology is being used.

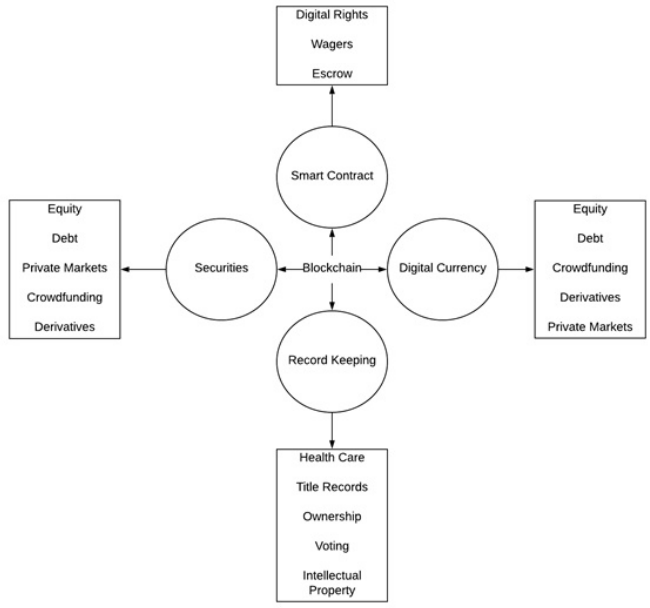


**Figure 1.1** Sectors of blockchain.

Blockchain is making its way into many sectors like agriculture, power production, education, banking, voting and many more. Consider the example of power production where if you have solar panels installed in your home and if you produce electricity, the excess can be sent to others and in turn you get money through Blockchain; and where we can have the IoT also being used with it. Basically, blockchain comes into the picture when you can prevent data hoaxes and establish trust in the distributed network. The internet has solved many more problems like information searches (Google, Yahoo), distribution (YouTube, Amazon Prime, Netflix) and communication (email, chat applications) but it has not solved two major problems, which are trust and intermediation. On the internet, we find fake news and fake profiles which are not to be trusted; and in intermediaries, the big companies like Google, Amazon, Facebook, etc., have acquired the market and are not open to all, which means there is a middleman between producer and consumer. But with the advent of Blockchain, we can solve all these problems and bring back a trusted environment.

## 1.1 Introduction to Web 3.0

With the web entering a new phase of evolution, Web 3.0 is lined up to be the next big thing marking a fundamental change in how developers create websites and how people interact with those websites. Internet experts claim that these changes will make the internet smarter, thereby making our lives easier [2].

### 1.1.1 Web 1.0

This is referred to as the first generation of the web, invented by Tim Berners-Lee. It is often referred to as the read-only web as few people created content for the rest of the customers. Commonly used technologies are HTTP, XHTML, HTML, CSS, etc. It supports both server-side scripting (like JSP, PHP, etc.) and client-side scripting (JavaScript, VBScript, etc.) [3].

Web 1.0 has a lot of vulnerabilities, some of them are:

1. It is extremely slow.
2. Each time new content is pushed onto the webpage, it needs to be refreshed.
3. It doesn't support two-way communication as it can be initiated only by the client (HTTP).

### 1.1.2 Web 2.0

This is also referred to as the read-write web as the users can interact with websites that have predetermined behaviors according to the inputs. With the emergence of blogs in the 20th century, widgets and other instant and universal authorizing tools and sites are always ready to accept the content. These have played a substantial role in the democratization of the web. Commonly used technologies are Ajax, DOM, REST, etc. [6].

Web 2.0 has a lot of vulnerabilities, some of them are:

1. SQL Injection
2. Information Leakage

3. Cross-Site Request Forgery
4. Authentication and Authorization Flaws
5. Cross-Site Scripting

### 1.1.3 Web 3.0

This term was coined by the reporter John Markoff of *The New York Times* in 2006. It allows online applications to receive information from the web and provide new information (results) to the users [4].

Web 3.0 is made up of these 4 basic properties:

- *Semantic Web*: This deals with the meaning or the emotion conveyed by the data.
- *3D graphics*: This is being used to provide a realistic feel to the websites.
- *Universal*: This will allow accessing the content/service on the web from anywhere.
- *Artificial intelligence*: This will allow websites to filter and present users the best data possible.

## 1.2 Blockchain

The concept of blockchain was first introduced by Stuart Haber and W. Scott Stornetta while they were trying to build a system in which document timestamps could not be modified.

This was later implemented in the year 2008 by Satoshi Nakamoto, whose real identity is still unknown.

Blockchain can be defined as a growing list of records called blocks, which are linked and stored using cryptography. The first block of the chain is referred to as the genesis block [11].

Each and every block will have the following details in it:

1. *Data*: String of characters stored.
2. *Nonce*: A unique number related to mining.
3. *Previous hash*: Hash value of a block that came before the current block. This field establishes the cryptographic link with the subsequent block.
4. *Hash*: Fingerprint of some amount of data stored in the block.

As shown in Figure 1.2, the hash value of a block is calculated using all of the other three fields, i.e., data, nonce and the previous hash field.

The concept of blockchain can be understood with the help of the following:

1. Hash Cryptography
2. Immutable Ledger
3. Distributed P2P Network
4. Mining
5. Consensus Protocol

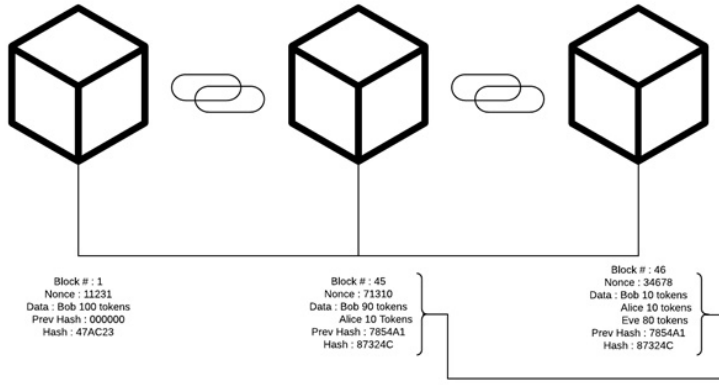


**Figure 1.2** Cryptographically linked blocks.

### 1.2.1 Hash Cryptography

Each and every human being in this world will have a unique fingerprint and there exists a very minimal chance, i.e., one in 60 million, for this to be the same. Similarly, the digital document like an operating system, video, etc., can be identified uniquely with the hash value calculated using the SHA-256 algorithm [5]. This was first developed by the National Security Agency (NSA) and the expansion is as follows:

- SHA stands for secure hash algorithm.
- 256 is the total number of bits consumed in the memory.

The requirements for any hash algorithm are as stated below:

1. *One-way*: Every digital document will have a hash value associated with it. This can be retrieved through the digital document but the reverse cannot be achieved.
2. *Deterministic*: Every digital document will have a unique hash value generated by a hashing algorithm which will remain the same until the file content is not changed.
3. *Fast computation*: The hash value generation should be instantaneous and must not be sluggish.
4. *Avalanche effect*: Any change in the input file causes a radical change in the hash value generated previously.
5. *Must withstand collisions*: If a hash function generates the same value for two digital documents, this is referred to as collisions. Data integrity makes it obligatory that such collisions are prevented.

Figure 1.3 shows the conversion of message to hash value using SHA-256 algorithm where for each character change it generates a different hash value. The important feature is that we cannot obtain the message from hash value.

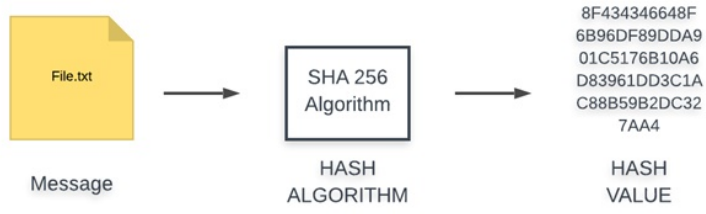


**Figure 1.3** Hash function.

### 1.2.2 Immutability

Immutability refers to anything and everything that cannot be changed once recorded. For example, a mail sent to a bunch of people cannot be reversed. An additional field called timestamp is stored inside the block when a transaction is approved and appended onto the blockchain. If anyone tries to alter the data in a block the cryptographic link is broken [7]. This helps us to recognize the precise section of the chain where the data is manipulated. Thus, one has to compute the previous hash value of the entire chain again to restore the link. It requires a lot of computational power in order to do so. Therefore, making sure that the data stored is resistant to any kind of alterations. This feature is not available in the earlier databases which only provide an option to delete or modify records. Moreover, blockchains sustain the entire history and data path of any application. This acts as a backbone for any auditing process. Preserving a full historical record is not only a blessing for auditing, but also provides new chances in the query, analytics, and overall business processes [9].

Figure 1.4 shows the immutability feature of blockchain.

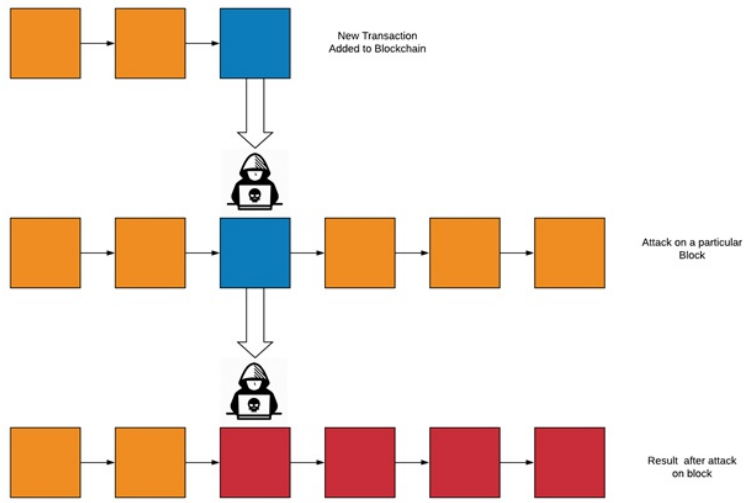


**Figure 1.4** Immutability of blockchain.

### 1.2.3 Distributed P2P Network

The backbone of blockchain methodology is formed by P2P network architecture. This policy authorizes us to remove the dependency on a central decision-making source called a server [12]. The user has to completely trust networks and hope they don't have a backdoor to quietly read or manipulate the reports. Also, one should hope that they don't go out of business and shut down their servers. The nodes comprising tablets, routers, etc., interact and share data directly with one another; thus, distributing all the data across all nodes in the grid rather than using a server. All the nodes in the network will have a copy of the blockchain, thereby making it completely impossible for anyone to modify any value in the chain [10]. Hypothetically, all these nodes are joined via a path. None of the nodes have precise knowledge about the network topology and merely reroute messages to the designated node. Members of the P2P network share the resources between other members, including bandwidth, disk storage, etc. This is accomplished with the help of minimum resource contribution threshold defined for all peers in the network. The peer-to-peer network enables us to solve all the obstacles faced in client-server architecture, i.e., single source of failure and scalability, efficiently [13]. Table 1.1 below shows the contrasting characteristics of both the architectures.

**Table 1.1** Difference between Client-Server and P2P.

| Client-Server Architecture | P2P Architecture |
|---|---|
| The Server acts as the master and client as a slave | Peers are treated as nodes with equal capability |
| Adopted in small and large companies | Normally adopted small companies |
| Easy to set up and manage | Hard to set up and manage |
| Software installation is done on the server and it is accessed by the clients | Software installation is done on all the nodes and accessed by the nodes itself |
| Ex: Instagram | Ex: BitTorrent |

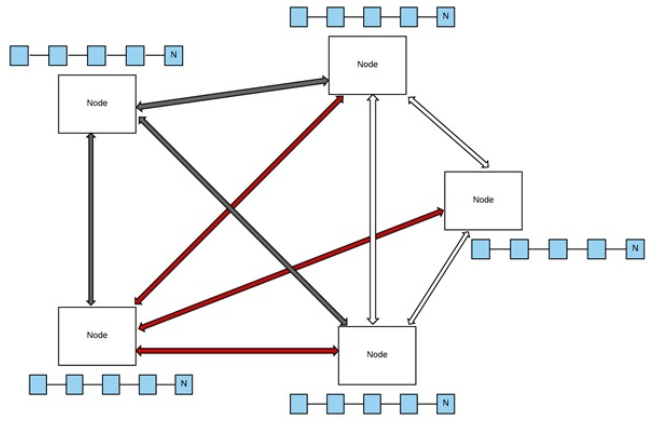


**Figure 1.5** P2P network of blockchain.

### 1.2.4 Mining

This term picked up steam due to the recent surge of Bitcoin. It can be defined as the process of adding new transactions to the distributed system by predicting the value of the nonce such that the hash value generated is less than the target range. Miners compete against each other to figure out a hash value by solving a mathematical problem and receive a reward in terms of tokens or transaction fees. One of the solutions or mining algorithm used is proof-of-work [15]. This acts like a testament that the miner spent a substantial bulk of time and resources to figure out the solution to the problem. The miner needs to wait a while before his transaction is confirmed and added to the block. Afterward, the reward is credited to the miner. Going by the trend, the amount associated with a block mined decreases by half every 210,000 blocks. The decrease in the amount credited is evened up by the increase in the transaction fees. Subsequently, no new coins are generated or issued.

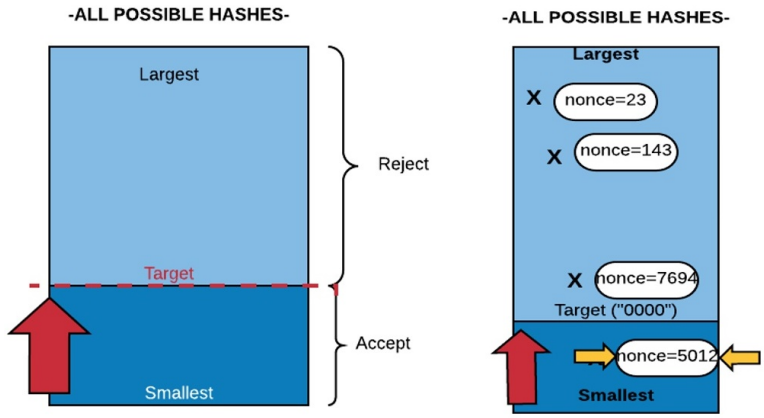


**Figure 1.6** Process of mining.

### 1.2.5 Consensus Protocol

Blockchain consensus protocol creates an indisputable system of understanding between various nodes across a distributed network. This permits us to keep all the nodes on the grid synchronized with one another [16]. As a result of a distributed system, it becomes mandatory to maintain the same state of blockchain across the network. This is being challenged by two main factors:

a) *Attackers*: This nature of attack is prevalent when an attacker wants to disrupt the distributed chain by brute-force method. There are two probable ways in which the attacker can do it:

   1. *Adding a new block between the chain*: Suppose the attacker adds a new block in between the blocks of the chain, then the entire cryptographic link will be broken. The chain on distribution will perceive that the chain that it contains is different from all the other copies in the network. Instantly, the node will recognize the same and replace the entire copy of the chain, thereby integrating the data across the grid.
   2. *Adding a new vicious block at the end of the chain*: Each and every node performs a series of checks on the newly mined blocks before confirming it to the miner.

During this process, if some node feels that the block is malicious, it will soon bring it to the notice of the network and necessary actions will be taken against it.

b) *Competing chains*: This problem arises when two nodes mine a block into the chain at approximately the same time. With a large number of nodes present in the distributed network, a conflict crops up with the development of two competing chains and it thereby becomes imperative to make a call [17]. The solution to this dilemma is achieved with the help of a simple notion, i.e., to accept the chain which will add the next block. Now, a lot depends on the hashing power of the nodes and whichever set of nodes has the higher power will have a greater possibility of mining the next block. The entire copy of the accepted chain among the competing chains is now relayed across the network to retrieve what is known as the orphan blocks. These are mostly blocks (enclosing the miner's reward) now no longer a part of the chain [18].

This forms the core of the blockchain technology to exist and function methodically.

## 1.3 Bitcoin

Bitcoin, launched under the name Satoshi Nakamoto in 2008, is a digital currency which overcomes the inefficiency and greed of banks. Bitcoin's nature is resilient to the encroachment of banks and governments. It uses P2P technology that operates under no central adversaries where transactions are approved mutually by the network participants [22]. Here, a private key protects the access to the money of an individual account, which is contradictory in the case of fiat currency. Additionally, the number of bitcoins minted is limited to 21 million, unlike traditional currency minted by authorized central banking agencies. Blockchain is the underlying technology that stores each transaction on Bitcoin network globally in a shared ledger which is verifiable, accessible and constantly updated by a global fleet of computers. Once a transaction is done, its details are globally recorded, which provides no means to reverse the transaction. At the same time, Bitcoin requires no identity of one's personal information for participating in a network, thus it cannot be traced back to an individual until and unless he/she wishes to reveal it.

## 1.4 Ethereum

Ethereum is a decentralized, open-source, dynamic service that works on the properties of the blockchain. It was first introduced in 2013 through a white paper by Vitalik Buterin. This was obtained from the Bitcoin project which is primarily a tool intended towards monitoring transactions among people. He himself was an enthusiast of the Bitcoin project but firmly felt that this technology can be applied to diverse varieties of transactions [20]. The core of Ethereum largely revolves around smart contracts. They are small blocks of code that reside in the blockchain meant for accomplishing a specific task. This system went online in July 2015 and continues to thrive even today. Its main aim is to develop a platform which runs on DApps in order to create a more global, free and more mature internet, Web 3.0. Their intention is to give users and creators more control in developing their apps rather than the conglomerate. It runs on the same protocol as that of Bitcoin, proof of work (PoW), but the disadvantages are a 51% danger of attack and the enormous energy consumption required for the security. Thus, proof of stake [19] came into existence which works akin to PoW. Instead of nodes approval in the network, it makes use of token

holders. *N%* of a block reward is received for *N%* of tokens (computing power in the case of PoW) for accounting on the network [21].

The concept of Ethereum can be understood with the help of the following:

1. Ethereum Network
2. Interfacing with Ethereum
3. Ethereum Account
4. Transaction

### 1.4.1 Ethereum Network

The infrastructure of a decentralized network is made up of an assortment of nodes interacting with each other. The Ethereum network is largely related to the transfer of money and storage of data, thus permitting us to build diverse exciting applications. This is achieved with the help of a cryptocurrency called ether. This is similar to bitcoin and is responsible for fueling the Ethereum ecosystem. There exist many Ethereum networks, some of which are:

1. *Main Network*: Production applications are deployed here so that they can be used by the user. It is in this network that ether coins have real value and can be turned into U.S. dollars.
2. *Rinkeby, Kovan, Ropsten Test Network*: These provide us with free ether coins to test code and contracts before deploying them to the main network.
3. *JSON RPC API*: This allows us to connect to the local Ethereum test network which runs at "localhost" on port 8445.

Figure 1.7 depicts the organization of the Ethereum network.

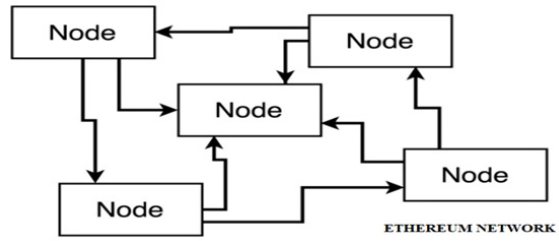


**Figure 1.7** Ethereum network.

### 1.4.2 Interfacing with Ethereum

Interfacing refers to the process of interacting with the network. This can be accomplished in two ways:

1. *Web3 library*: This is an API predominantly used by the developers to interact with the network. It enables the performance of numerous operations like creating smart contracts, sending ethers, etc. It communicates with the blockchain through JSON

RPC and ensures that it is communicating with only one node in the distributed P2P network.

2. *MetaMask*: This is a browser extension used by users to interface with the network. Normally, it is preferred by users who do not have previous knowledge of Ethereum.

Figure 1.8 depicts the interfacing with Ethereum.

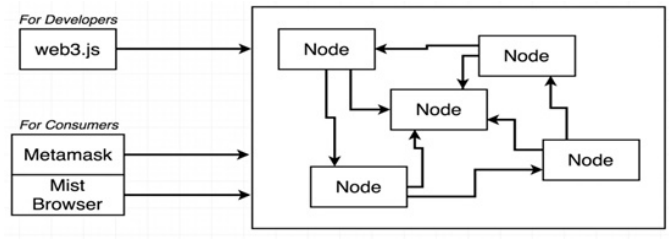


**Figure 1.8** Interfacing with Ethereum.

### 1.4.3 Ethereum Account

MetaMask creates two distinct sorts of accounts:

1. *Externally owned accounts*: These are generated and managed by private keys and will have the following:
   a) No associated code
   b) Ether balance
   c) Help in triggering contract code
   d) Ether transfer
2. *Contract accounts*: These are generated and regulated by code and will have the following:
   a) Associated code
   b) Ether balance
   c) Code implementation is triggered by transactions

Ignoring the kind of account created, the following four essential elements are:

1. *Balance*: The amount of Wei possessed by this address.
2. *Nonce*: In case of externally owned accounts, it depicts the number of transactions carried out from a specific account address; whereas, in a contract account, it illustrates the number of contracts generated by the account.
3. *CodeHash*: The hash of the EVM code of this account. These codes are stored in the database supporting the respective hash value for future retrieval.
4. *StorageRoot*: A 256-bit value representing the encoded version of the data stored in the chain.

### 1.4.4 Ethereum Network Transactions

Any sort of transaction in the Ethereum network should possess a MetaMask account and some ethers in it. If the user makes an order, they will automatically be redirected to a payment gateway to confirm and pay with ethers. Upon confirmation, their balance is checked in the back-end server to confirm whether it meets the appropriate requirements or not. If the requirements are met then the transaction of ethers will take place. When the user pushes the submit button, it sends the ethereum address to the back-end server for validation. Then the back-end server uses the web3 library to create a transaction object. For demo purposes, the researchers use the test networks while in the real world it is done in the main network. After a successful transaction, the back-end server pushes the success message onto the user screen. The user needs to wait for a few seconds as the transaction object generated needs to be added to the network. This will be approved by the miners by randomly generating a nonce value and is added as a new block in the network. The block will have a unique hash value assigned to it and thus data integrity is ensured.

Figure 1.9 below shows all the steps followed throughout this process in detail.

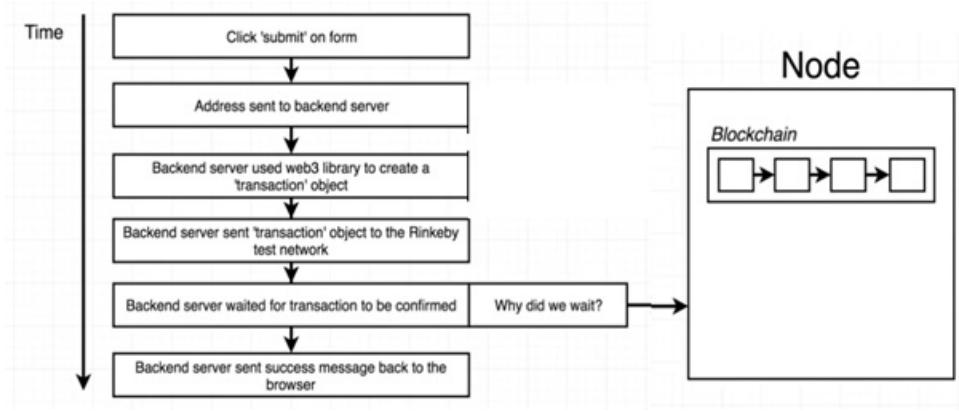


**Figure 1.9** Transaction in Ethereum network.

## 1.5 InterPlanetary File System (IPFS)

The HTTP fails to merge with the modern file distribution techniques recently invented. Without affecting the current network the upgrades are nearly impossible because of the large involvement of the present HTTP model and the web. To overcome these challenges, IPFS network works on distributed peer-to-peer network which has a similar file data structure called Merkle DAG. IPFS works in a manner similar to BitTorrent where bitswap protocol is used. Clients can set their own Bitswap strategies using Bitswap protocol. A Bitswap strategy tells a node how it should request and send blocks to/from its peers. Through the collective use of distributed technologies, IPFS enables a unique file and data sharing in a decentralized fashion. IPFS has its file-system or directories mounted globally and provides high performance and cluster persistence, which is enough to store and organize the world's information [23].

IPFS as the distributed web also offers features like:

1. *Content Addressing*: The addressing data in IPFS is performed by addressing the content of the file or document in the network rather than addressing location where the addressing is different, which is performed using IP addresses. The IPFS address resolves the IPFS objects, the entities present which contain a list of links and content data which is being addressed. When the large files are added to IPFS, the file is decomposed into much smaller representation of data and stored into an array of links that points to the broken pieces of the original data. This type of addressing ensures that a particular address will always result in querying the same file. Content addressing also has an advantage over the content hosted by a node where the content can be retrieved from the IPFS network as long as the file is hosted in the network. Thus, a single copy of a file is enough to retrieve a file from the network.

2. *Distributed Hash Table (DHT)*: The DHT is the database distributed over a network which can be used to store data in terms of key/value pairs in a peer-to-peer network consisting of nodes. The distributed hash table has the mechanism of fault tolerance triggered when key/value pairs are duplicated or not accessible in the network. To evenly share the information across the network, DHT uses the concept of hashing where a hash function that serves as a randomized function accepts keys. Since DHT nodes don't store all the data, routing layer has to perform the necessary function which enables a client to contact other peers in the network that stores the certain key which then can be used to retrieve the value and access the content. The two routing protocols that are significantly used in the routing layer in DHT are iterative lookup and recursive lookup, which are classified on the manner in which they process a complete request.

3. *Versioned File System*: IPFS allows a versioned file system that is made use of in Git versioning which enables maintaining different versions of the same file and can be easily traced to the original file using commit objects. The commit object in the versioned file system has links to name ID which points to last committed object, and also the link which contains the object which points to the globally mounted file directory which is started by that commit.

## 1.6 Decentralized Applications (DApps)

Decentralized applications are completely open-source applications that work entirely on the smart contract code run on the blockchain. They are a type of software program designed to exist in such a way that is not controlled by any single entity but instead controlled by blocks of code known as smart contracts. DApps uses decentralized storage to store data and code. Decentralized application is a blockchain-based app, where the smart contract is what allows it to connect to the blockchain [1].

The main difference between Satoshi Nakamoto's bitcoin and Vitalik Buterin's ethereum is given in Table 1.2.

**Table 1.2** Difference between bitcoin, ethereum, and hyperledger.

| Characteristics | Bitcoin | Ethereum | Hyperledger |
|---|---|---|---|
| Permission Restriction | Permission less | Permission less | Permissioned |
| Access restriction for data | Public | Public or Private | Private |
| Consensus | Proof-Of-Work | Proof-Of-Work | Practical Byzantine Fault Tolerance |
| Scalability | High Block scalability | High Block scalability | Low Block scalability |
| Governance | Low, decentralized decision making by miners | Medium, core developer group, but EIP process | Low, Open governance model based on Linux model |
| Anonymity | Pseudo-anonymity, no encryption of data | Pseudo-anonymity, no encryption of data | Pseudo-anonymity, encryption of data |
| Native Currency | Yes, bitcoin | Yes, ether | No |
| Scripting | Stack-based scripting | Turing complete virtual machine with support to high-level language | Turing complete scripting of chain code in go language |

## 1.7 Case Study: FIR

The first information report (FIR) is the written document maintained by the police department that has the information collected about any criminal offense. It is generally a complaint lodged with the police by the victim of a cognizable offense or by someone on his or her behalf, but anyone can make such a report either orally or in writing to the police, after which an investigation is started by the police. The person giving information has the right to see what is being mentioned and has to affix his signature to it, stating it's correct. The existing system is handwritten, time-consuming and less secure; and there is no way to track if events are being recorded properly. The FIR acts as sensitive data and provides clues for the investigation. Thus, the data stored must be secured and should not be tampered with or influenced by external pressure once the report is written. The FIR details are stored in a ledger where they can be manipulated. So, to mitigate this we can use blockchain technology once the data is stored in a block since it has its hash value and it is linked. Whenever anybody tries to change even a small character or even a space the hash value immediately changes due to the avalanche effect and hence indicates that data has been tampered with. This provides high security of data and eliminates the manipulation of information. The person who provided the information can keep track of it by using the hash value that is generated when the data block is added. The advantages of the FIR is that it reduces cost and time, eliminates manual errors, and online information can be seen by anybody. The FIR consists of information like place, time, date, and detailed descriptions, all of which are stored in a block of the blockchain and the hash value is given to the user to check whether the details are provided correctly and to make sure no information is misinterpreted. Thus, by using blockchain technology a major problem is solved and data integrity is ensured.

### 1.7.1 Project Description

The FIR dApp is a provable public crystal-clear platform based on decentralized and open source technologies that use blockchain to assure the authenticity of a report filed by the user. It aims to be the standard on decentralized projects communications. With this application, users can lodge a complaint and also protect their identity and publish what really matters to them. This application permits searching for the FIR based on the ID provided to them. This application is eternal and can't be stopped by anyone or anything. All data is securely encrypted before leaving your browser. Also, the code which runs the dApp is viewable by everyone and is free of politics and human error, thus making it secure, trustworthy, and accessible to anyone.

**Secure**: Ethereum blockchain is fully decentralized. Due to the immutability property of the blockchain, any record added via this application cannot be omitted. This system cannot be controlled by any single adversary or authority.

**Trustworthy**: All the documents are accumulated on Ethereum along with a timestamp. Neither the content nor the time of the document can be changed or mishandled in any way.

**Accessible to anyone**: Complaints lodged by the user can be viewed by anyone without incurring any transaction fees. All the vital data required to access the information regarding any application is publicly available.

This distributed application is able to :

- Save arbitrary documents on the InterPlanetary File System (IPFS).
- Receive a receipt for the submission.
- Prove time of submission (via block timestamp).

### 1.7.2 Tools Used

The tools cited below are needed for the development of the project.

#### *1.7.2.1 Node.js*

JavaScript runtime environment is built on Chrome's V8 JavaScript engine. The main strategy of Node.js is that it uses non-blocking and event-driven I/O which enables maintaining a lightweight state in the case of data-concentrated applications which are mainly run as real-time applications. Node.js comes with default package management and a tool called an NPM tool which is installed with every Node.js installation. Node.js can be installed through an installer available via an online repository, with version and dependency management.

#### *1.7.2.2 Truffle*

Truffle[1] is a smart contract development environment and framework used to deploy Ethereum DApps, which makes the smart contract development easy for ethereum developers. Since Truffle is a fully fledged framework with development and testing capabilities, it is also embedded with the Web3.0 library by default, which makes it more attractive to users with a Web 3.0 development background. Truffle is operated in the Terminal, using various commands at the different stages of developing a dApp. Contracts can be tested using popular testing frameworks like Mocha and Chai. Truffle supports the development of both web apps and console apps. It also has a feature of migration which helps in in-

[1] https://www.trufflesuite.com

stant rebuilding of assets during development. Contract compilation and deployment can be done using the RPC client.

#### 1.7.2.3 Ganache

Ganache[2] is a simulation of blockchain nodes that works to set up a local ethereum node where smart contracts are compiled and can be migrated with a development tool such as Truffle. By using Ganache there is no additional set up of a geth client and other dependencies. It provides a total of 10 virtual accounts, each account loaded with 100 ethers which can be used for the purpose of development where the virtual accounts are used to pay for gas when running transactions on the blockchain. Along with the virtual accounts their private keys are also given and through these keys the transaction is signed and written in the blockchain. Ganache has both the visual user interface and command line interface, which allows users to see the current status of all accounts, including their addresses, private keys, transactions, and balances. Apart from these features, Ganache also provides blockchain log output, which displays the log output of Ganache internal blockchain, including responses and other vital debugging information and advanced mining controls.

#### 1.7.2.4 Infura

Infura[3] provides a set of tools to connect the application to the Ethereum platform. These tools enable secure and reliable access to Ethereum APIs and the InterPlanetary File System. Through Infura one can host their application in the decentralized network of ethereum using the API key available through their platform. Infura also hosts IPFS nodes which connect to IPFS network and users can also connect to them using the URL provided. Infura has a scalable infrastructure with the ability to transfer 2.5 PB of data per month and handle over 10 billion user requests daily.

#### 1.7.2.5 MetaMask

MetaMask[4] is a browser extension that offers crypto wallet and an interface for signing transactions for DApps.Through MetaMask, the transaction can be signed onto the ethereum network without actually running a full ethereum node. MetaMask also enables users to store the wallet-related data like public addresses and private keys similar to any other Ethereum wallet, and users can also interact with websites running DApps and smart contracts. MetaMask includes a feature called secure identity vault, which provides a user interface to handle their identities on different sites and sign transactions onto the blockchain.

#### 1.7.2.6 Solidity

Solidity[5] is a contact-oriented, high-level language for writing smart contracts. Solidity code runs on Ethereum virtual machine (EVM), where once deployed cannot be changed or manipulated. It offers features like inheritance and libraries, and complex user-defined types are also supported. The programming style of Solidity is influenced through C++, JavaScript, and Python and is statically typed. Solidity also has development tools such as Solidity REPL, which is a Solidity interpreter with a command-line Solidity console and solgraph which is a visualization tool that visualizes control flow and highlights potential security vulnerabilities.

[2]https://github.com/trufflesuite/ganache
[3]https://infura.io
[4]https://metamask.io
[5]https://github.com/ethereum/solidity

### 1.7.3 Project Workings

1. *Lodge Complaint*: This facilitates the user to register a new accusation by specifying the required trivia. The information cannot be altered once submitted, thereby giving the end user the freedom of trusting the system and filing a case without bothering about the external influence.
2. *Fetch Complaint:* This element enables us to retrieve the details of a specific accusation using the unique ID number provided when it was first loaded onto the chain.
3. *Recent Complaints*: This element helps to retrieve all the recently added complaints, thereby making sure that the system is available publically.

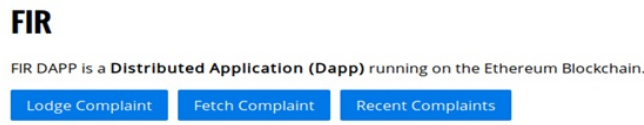


**Figure 1.10** Index page of the application.

Figure 1.10 depicts how a user can file a complaint on this distributed application by specifying the following mandatory details:

1. Police station name
2. Title
3. Detailed description of the complaint

All the aforementioned are considered as inputs for the transaction and are approved by the transfer of a nominal fee of 0.001 ETH.

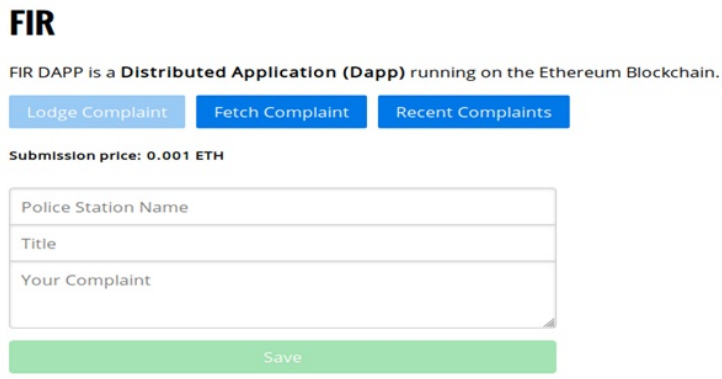


**Figure 1.11** Fields for a complaint.

Figure 1.12 demonstrates how MetaMask browser extension pops up when the save button is pushed. A total cost of 0.001 ETH will be debited from the account as a sign of validation and the transaction will be attached to the block upon mining. The user has the choice of either confirming or declining the transaction.

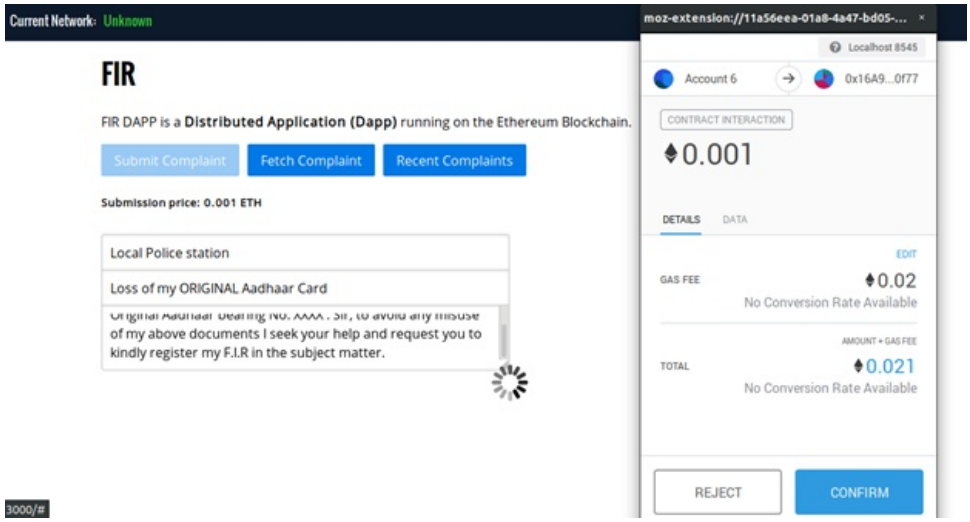


**Figure 1.12** Submitting the complaint.

Figure 1.13 illustrates how a user can fetch details concerning any complaint on the network by using the ID number. On fulfilling the requirements, the entire report filed along with the Ethereum hash and timestamp is retrieved. IPFS hash is also revealed which confirms the storage of the report in the network.

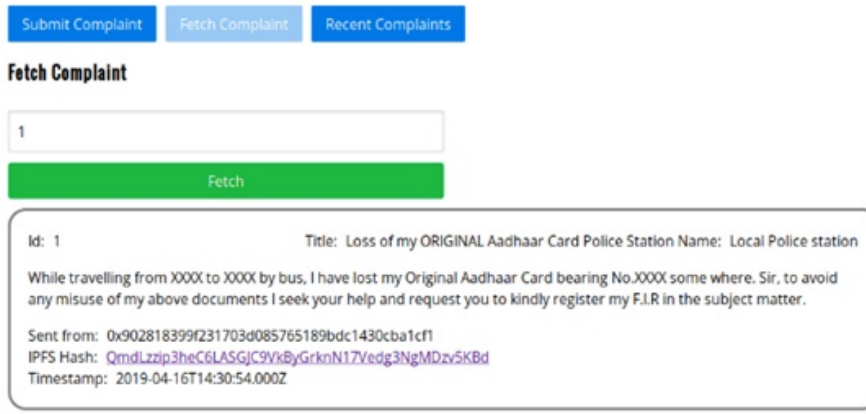


**Figure 1.13** Fetching complaint by ID.

This component of the system serves in establishing transparency with pseudo-anonymity. Any user can check for recent submissions of complaints under this option. This would give users a possibility to view the pending cases in the network.

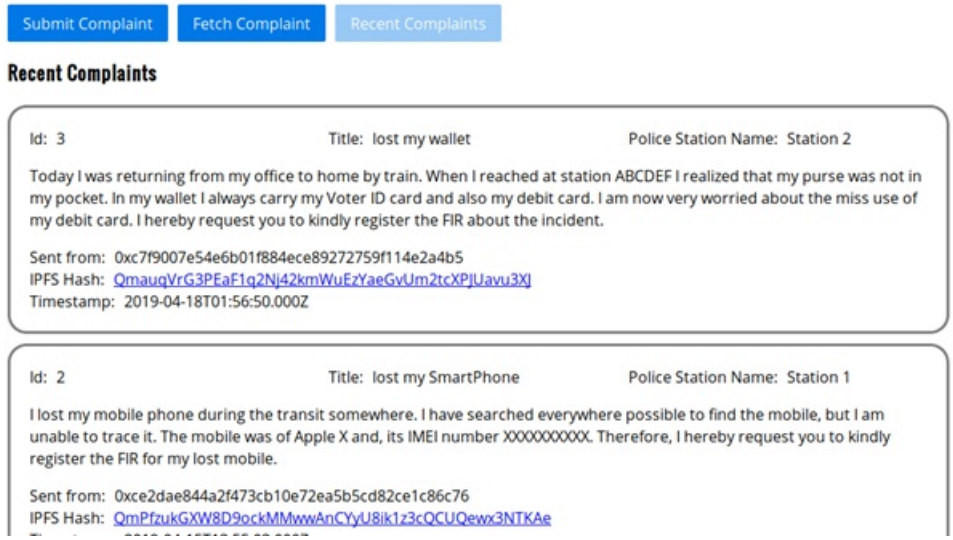


**Figure 1.14** Fetching recent complaint.

## 1.8 Conclusion

The advent of blockchain technology has changed the lives of people, giving it a new dimension. It has changed the perspective of viewing things on the web and has been more user-centric and user-friendly. With its wide range of technology, blockchain has provided more data security, as mentioned in the above topics about how it works, its hashing algorithms, its security parameters and so on. In addition, it has a wide diversity in controlling the cybercrimes occurring in the world and also solves the problem of data breach and money- and property-related issues. With this, sectors like digital advertising, cybersecurity, forecasting, supply chain management, IoT, and networking have a fantastic future. Blockchain also has a wide perspective of the new occupations emerging in industry. With this, we can transform the whole world into a much smaller place. In a client-server architecture, users experience a single point of failure, and even it is prone to attacks; therefore, to provide a better solution to prevent these attacks the use of distributed network improves the efficiency of the system and provides more security to the system. The transactional activities can be performed much faster and efficiently using blockchain. Blockchain technology is going to be used in many more sectors in the future, such as in government systems, as these systems are slow, dense, and likely to be affected by corruption. Implementing blockchain technology in government systems can make their operations much more secure and efficient. Even though storing data on a blockchain is a slow and expensive process, in certain cases its benefits outweigh the cost, and in the future the Ethereum network will be faster and cheaper. The blockchain technology provides a sustainable and efficient method to the existing service structures whereas some other methods underperform and have unreliable security. Blockchain is in its early phase

where experiments are performed on existing systems by developers working on reducing the cost and making user activities faster. Their support is limited in terms of computing power and the number of nodes within the network is small. Currently solutions are usually designed to address where solutions are made by the decentralized system. Coin offerings made by blockchain technology implemented using smart contract can deliver high proposition value to the solution over a decentralized network where each and every node will have equal importance and control over the decisions made by the system. In the future, real power is empowered by smart contract where advanced technologies will enable transactions at a faster rate. Satoshi Nakamoto's paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," was published in October 2008 and released in January 2009, which was a clear sign of the disruption of the financial and banking sectors to come. With an effective solution but limiting technology, it seemed too unlikely to have drawbacks to succeed and fully implement. With the exception of financial sectors, healthcare, supply chains and governments look forward to implementing game-changing results. Companies acting as a middleman to conduct business can be eliminated using this technology. Thus, they are looking forward to utilizing blockchain technology to remove central authority over the network. Blockchain technology enables transformative change but it will take time to solve existing challenges with user scalability and complexity in transaction processing systems. Thus, blockchain technology can be imagined as the ozone layer in the atmosphere whose presence can stop many malicious activities in the field of computer technology by acting as a protective shield to the users' data against the attackers.

## REFERENCES

1. Buterin, V. (2017), A next-generation smart contract and decentralized application platform, *Ethereum White Paper*.
2. Aung, Y. N., & Tantidham, T. (2017, November). Review of Ethereum: Smart home case study. In *2017 2nd International Conference on Information Technology (INCIT)* (pp. 1-4). IEEE. https://doi.org/10.1109/incit.2017.8257877
3. Yavuz, E., Koc, A. K., Cabuk, U. C., & Dalkilic, G. (2018, March). Towards secure e-voting using ethereum blockchain. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-7). IEEE. https://doi.org/10.1109/isdfs.2018.8355340
4. Dinh, T. N., & Thai, M. T. (2018). AI and blockchain: A disruptive integration. *Computer*, 51(9), 48-53. https://doi.org/10.1109/mc.2018.3620971
5. Ming, Z., Yang, S., Li, Q., Wang, D., Xu, M., Xu, K., & Cui, L. Blockcloud: A Blockchain-based Service-centric Network Stack.
6. Ehmke, C., Wessling, F., & Friedrich, C. M. (2018, May). Proof-of-property: a lightweight and scalable blockchain protocol. In *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain* (pp. 48-51). ACM.
7. Sambra, A., Guy, A., Capadisli, S., & Greco, N. (2016, April). Building decentralized applications for the social Web. In *Proceedings of the 25th International Conference Companion on World Wide Web* (pp. 1033-1034). International World Wide Web Conferences Steering Committee. http://dx.doi.org/10.1145/2872518.2891060
8. Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7), 1366-1385. https://doi.org/10.1109/tkde.2017.2781227

9. Bartoletti, M., Lande, S., Pompianu, L., & Bracciali, A. (2017, December). A general framework for blockchain analytics. In *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers* (p. 7). ACM. https://doi.org/10.1145/3152824.3152831
10. Wichtlhuber, M., Heise, P., Scheurich, B., & Hausheer, D. (2013, October). Reciprocity with virtual nodes: Supporting mobile peers in Peer-to-Peer content distribution. In *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)* (pp. 406-409). IEEE. https://doi.org/10.1109/cnsm.2013.6727866
11. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, http://bitcoin. org/bitcoin. pdf.
12. Dai, P., Mahi, N., Earls, J., & Norta, A. (2017). Smart-contract value-transfer protocols on a distributed mobile application platform. URL: https://qtum.org/uploads/files/cf6d69348ca50dd985b60425ccf282f3.pdf, 10.
13. Wright, C., & Serguieva, A. (2017, December). Sustainable blockchain-enabled services: Smart contracts. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 4255-4264). IEEE. https://doi.org/10.1109/bigdata.2017.8258452
14. Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)* (pp. 45-59).
15. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018). OmniLedger. A secure, scale-out,decentralized ledger via sharding. In *IEEE Symposium on Security and Privacy (SP)*, IEEE. https://doi.org/10.1109/sp.2018.000-5
16. Dang, H., Dinh, T. T. A., Loghin, D., Chang, E. C., Lin, Q., & Ooi, B. C. (2019, June). Towards scaling blockchain systems via sharding. In *Proceedings of the 2019 International Conference on Management of Data* (pp. 123-140). ACM. https://doi.org/10.1145/3299869.3319889
17. Poon, J., & Buterin, V. (2017). Plasma: Scalable autonomous smart contracts. White paper, 1-47. http://plasma.io/plasma.pdf.
18. Wu, K. (2019). An Empirical Study of Blockchain-based Decentralized Applications. arXiv preprint *arXiv:1902.04969*. https://doi.org/10.3390/computers8030057
19. Chang, J., Gao, B., Xiao, H., Sun, J., Cai, Y., & Yang, Z. (2019). sCompile: Critical Path Identification and Analysis for Smart Contracts. *Lecture Notes in Computer Science*, 286-304. https://doi.org/10.1007/978-3-030-32409-4_18
20. Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P., & Zhou, Y. (2018, April). Detecting Ponzi schemes on ethereum: Towards healthier blockchain technology. In *Proceedings of the 2018 World Wide Web Conference* (pp. 1409-1418). International World Wide Web Conferences Steering Committee. https://doi.org/10.1145/3178876.3186046
21. Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017, June). Blockchain based data integrity service framework for IoT data. In *2017 IEEE International Conference on Web Services (ICWS)* (pp. 468-475). IEEE. https://doi.org/10.1109/icws.2017.54
22. Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint *arXiv:1407.3561*.
23. Storj: A Decentralized Cloud Storage Network Framework (2018) v3.0 https://github.com/storj/whitepaper