Blockchain-Based Cyber Security

Snehlata Barde

Abstract The term cyber security is referred to as security of information technology. Major goal of cyber security is to provide the protection of computers, networks, programs, and data and keep safe from unauthorized person and does not allow them to access or change the data and information. Cybercrime can be classified into three categories like cybercrime against individual, crime against property, and cybercrime against organization. Application development is a process that reduces human effort in doing the things manually such as ticket booking and banking. It is a new technology known as a next-generation solution to a wide variety of transactional blockchain. It is a collection of records which are called blocks, which are linked and secured using cryptography. Blockchain technology increasingly receives attention and recordkeeping problems. The core ideas behind blockchain technology emerged in the late 1980s and early 1990s by STUART HABER and W. SCOTT STORNETTA. Blockchain can be defined into four categories such as data structure, immutable, validated by distributed network and cryptography for security. There are two types of blockchain available public and private. In this chapter, we have described the problem with current system and their solution with the help of distributed system, block identifiers and different terms that is supported by blockchain technology such as smart contracts.

1 Introduction

Today we cannot imagine the world scenario without the computer and communication devices, network between devices increases every time and every day, Internet provide the facilities where every person can access any type of information from the net within a small part of time. It is huge storage of information and supports communications technology in order to the human race. World growth increases remarkable day to day by the use of Internet. Where the Internet is helpful in human progress, the Internet has also given rise to heinous crime like cybercrime [1].

S. Barde (✉)
MSIT, MATS University Raipur (CG), Raipur, India
e-mail: v.snehabarde@gmail.com

R. Agrawal and N. Gupta (eds.), *Transforming Cybersecurity Solutions Using Blockchain*,
Blockchain Technologies, https://doi.org/10.1007/978-981-33-6858-3_4

This type of crime is technology based and done by the technocrats. That required the need for strong computer security also becomes increasingly necessary and important. The boost in the computer network system has exposed many networks to various kinds of Internet threats, and with this exposure, one can see that the need of improved network security is vital and important in every term [8].

Cyber word related to all electronic equipments such as computer and mobile and security means protection from unauthorization. Cyber security means not only to protect data and information but also to protect all electronic and network devices from attacker. We define in other way cyber security as information security and network security technology [2].

Cybercrime perpetrators are very intellectual; their purpose is to commit crime in customer as well as in public and private organization. Cybercrime is caused by the lack of some innovation of cyber security, its responsible computers, and people who operate computers. We can provide the security at different level such as [3].

(a) **Network Security**

Network security is dealt with the problems of network and computers inside network. The network security problem can be of any size dealing with external issues, problems from users inside the network, etc. [9]. Network security problems arise in issues of client server models.

(b) **Internet Security**

Internet security deals with malware and hackers. Internet is an open zone where anyone can occupy web space by creating their own Web site and put malware to place in your computer or in server.

(c) **Port scanning**

Port scanning is the technique ports on your computer or server are accessed by hackers. They keep on trying, once locate the open port, they can read access and manipulate data from computer.

(d) **Accidental Data Losses**

Accidental data loss part is applicable to networks, computers nodes in networks and standalone nodes whether connected or not with Internet [10]. A sudden crash of hard disk and network failure during transmission creates problem of data loss.

(e) **Computer Security in standalone system**

Standalone computers refer to computers that are not connected to any network (but may be connected to Internet) [11]. For standalone computers, major types of computer security are factors affecting on data. The major threat is stealthy techniques.

2 Classification of Cybercrime

There are different types of cyber attacks these terms used in several of contexts and it can be divided into following categories as shown in Fig. 1 [4].

A. **Cybercrime against Individual:**

- E-mail spoofing: A spoofed e-mail means duplicate e-mail its look like at original masses and person thinks that it has been coming from actual source but it is not true because it has been sent from false source [12]. It is also called as e-mail forging. The main goal of attacker is to interrupt the service of the e-mail sender for which he sends e-mails repeatedly as shown in Fig. 2.
- Phishing: Phishing is a type of forgery where a cyber criminal creates same webpage to fool people through the Internet in which people enter with their user id and password and fill the personal information for accessing the account [13]. Cyber criminal uses this secrete personal information and

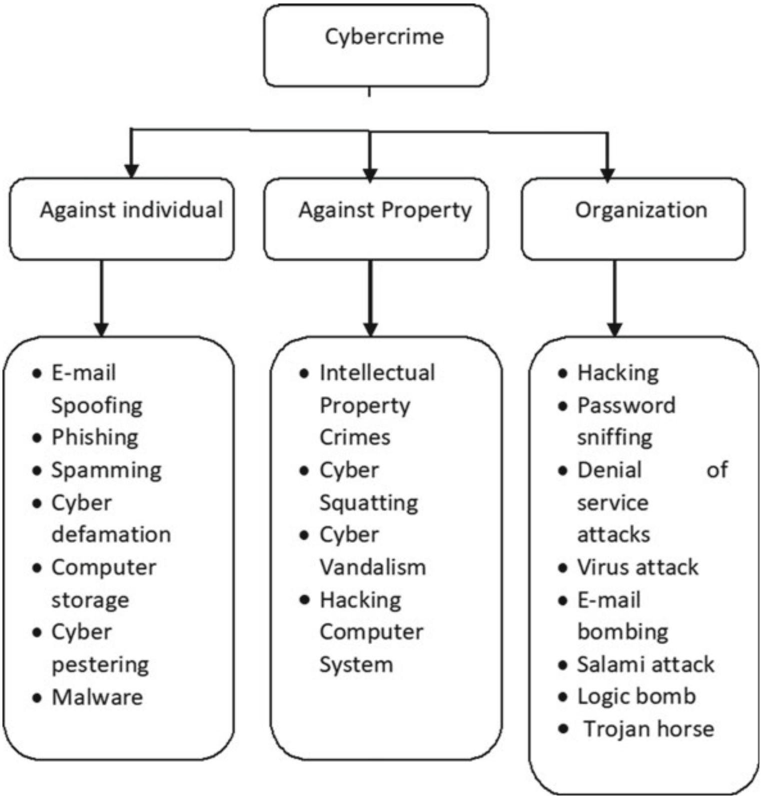


Fig. 1 Classification of cybercrime

•

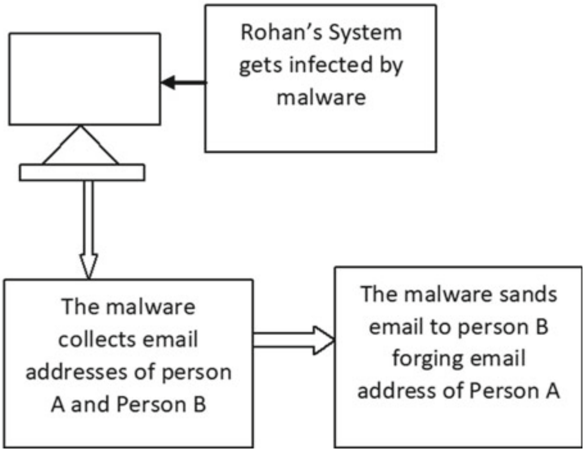

Rohan's System gets infected by malware
The malware collects email addresses of person A and Person B
The malware sands email to person B forging email address of Person A

Fig. 2 E-mail spoofing

financial information of person in illegal way and gets the profit from them; without knowledge of customer, criminal does the forgery from his account.

- pamming: Spamming is the sending of multiple unsolicited e-mails or text messages, usually for marketing purposes, commercial advertising, or for any prohibited purpose(especially for the fraudulent purpose of phishing).
- Cyber defamation: The purpose of this crime is to damage the image of well-known person by using his mail and send the vulgar message from their account that degrade the dignity of person in society [14].
- Cyber pestering: Cyber pestering means harass the other person or organization through the Internet This type of crime generally could be sexual in nature.
- Computer sabotage: Computer sabotage means disturbing the normal process of system by the harmful viruses and worms through the use of Internet.
- Malware: Malware is software whose purpose is to infect network system. It damages not only client side activities but also server side without client and server knowledge. Malware takeover all the controls of any individual system and spreads the bug from that to other system. Malware remotely controls all the network services which is used to send the viruses and spam [4].

B. **Crime against property**

- Intellectual property crimes: Any unlawful act by which the owner is deprived completely or partially of his rights is a crime. The most common type of crimes are software piracy, infringement of copyright, trademark, theft of computer source code, etc.

- Cyber squatting: It involves two persons claiming for the same domain name either by claiming that they had registered the name first. For example two similar names, i.e., www.yahoo.com and www.yahhoo.com.
- Cyber vandalism: Vandalism means damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted.
- Hacking computer system: Hacking in simple terms means an|| illegal intrusion into a computer system and/or network. Hacking attacks include famous social networking sites such as Facebook, Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company [15].

C. **Cybercrime against Organization**

- Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs.
- Password sniffing: Password sniffers are programs that monitor and record the name and password of network users as they login, at site.
- Denial-of-service attacks: DoS is an attack to shutdown a machine or to make inaccessible for intended users or imposing it for crash. DoS attacks often target web servers. Flooding and crashing are two most common DoS attacks [5]. Flood attacks when server needs too much load for buffering, causing their performance slow down and stop. Most common flood attacks are buffer overflow attacks, ICMP flood, and SYN flood. Crashing is done by bugs in the target that crashes or severely destabilizes the system from user access or by being used.
- Virus attack: A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected."
- E-mail bombing/mail bomb: E-mail bomb refers to sending a large no. of e-mails to the victim to crash victim's e-mail account or server crash.
- Salami attack: These attacks are used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed, e.g., a bank employee inserts a program into bank's servers that deducts a small amount from the account of every customer.
- Logic bomb: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are available. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company.

- Trojan horse: Trojan horse is another type of e-mail virus it creates duplicity itself; the purpose of this virus is to damage the system and get the information from the system, or harm the computer system [6]. “Trojan,” enters into system disguised as a normal, harmless file or program to trick users into downloading and installing malware. As soon as install a Trojan, it is giving cyber criminals access to the system. This allows the cyber criminal to steal data install more malware, modify files, monitor user activity, destroy data, and steal financial information.

3 Types of Security Attacks

There are many high-risk web application vulnerabilities such as:

(a) SQL injection: SQL injection is a procedure of susceptibility where the attackers have right to change backend and it is possible through the SQL statements that are manipulated by the user input [7]. It occurs when the user input accepted by the web applications is directly placed into a SQL statement and does not properly clean out unsafe characters.

(b) Cross-site scripting(XSS): Cross-site scripting (also called as XSS) is a vulnerability which allows an attacker to upload, post, or send malevolent contents such as comments, images, and messages (usually in the form of JavaScript) [6]. Since a browser cannot know whether the script should be trusted or not, it will execute the script in the user context allowing the attacker to perform unusual action like phishing, running a set of commands, or even stealing login session cookies.

(c) Sensitive data exposure: This type of errors occurs when the application lacks the protection of the sensitive data means an application does not effectively protect sensitive data. These data can be unencrypted passwords, credit card details, database backup, etc.

(d) Malicious file upload: It is referred to an opportunity where an attacker is uploading a file from narrow or remote resources and execute arbitrary script code in it with the privileges of the web server.

(e) Security misconfigurations: Directory listing or directory traversal is a vulnerability that allows an attacker to access confidential directories and perform commands from outside of the web server’s root directory [8].

4 Blockchain

Any application development is the process which reduces human effort in doing the things manually such as ticket booking and banking. According to Satoshi Nakamoto “A blockchain is a collection of records which is continuously growing; these records are called blocks, that are linked together and used cryptography for

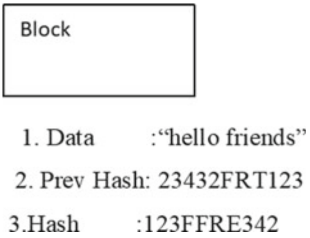


Fig. 3 A Block

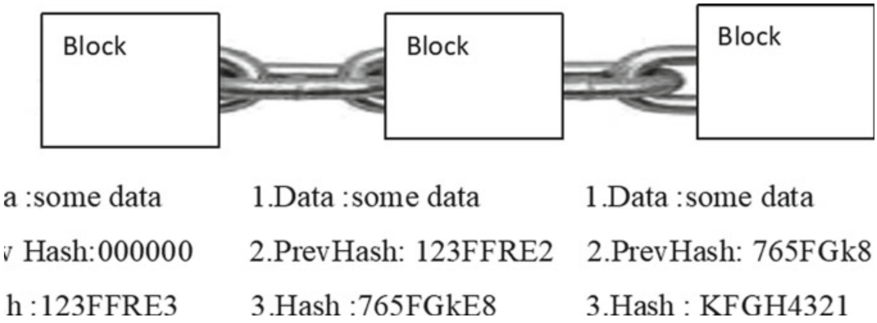


Fig. 4 Blockchain

security purpose.” Blockchain technologies offer a solution of huge variety of transaction in future and manage the problem of record storage for a next generation. The basic dream behind to develop a blockchain technology between 1980s and 1990s by the STUART HABER and W. SCOTT STORNETTA. Blockchain has collection of blocks; Fig. 3 shows the block that has three values data, pre-hash value and hash value and Fig. 4 shows the diagram of blockchain [8].

4.1 Hash Function

A cryptographic hash function takes an input (or message) and returns a fixed size string of bytes. The string is called hash value or checksum.

$$F_{\text{hash}}(\text{Message}) = \text{Output}_{\text{fixed length}}$$

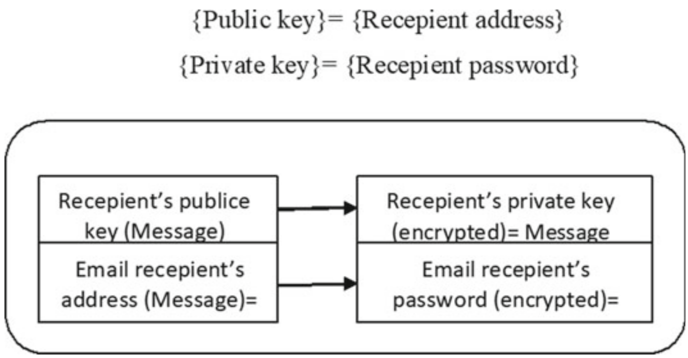

{Public key}= {Recepient address}
{Private key}= {Recepient password}
Recepient's publice key (Message)
Recepient's private key (encrypted)= Message
Email recepient's address (Message)=
Email recepient's password (encrypted)=

Fig. 5 Message transmission

4.2 *Ledger*

A ledger is a record-keeping book that stores all the transactions of an organization. Once the transaction is verified it is stored in a shared ledger across the network unconfirmed transaction will be store in main pool area and from there miner will pick and create the block in blockchain for the transaction.

4.3 *Cryptography*

In cryptography, original message before being transformed is called plain text keys used in cryptography are private and public key in asymmetric-key cryptography work on two keys one public and second private. They have a special relationship to each other public key is used for encryption, it is shared on the network and derived from private key while private key is used for decryption, it is not shared on network and not derived from public key shown in Fig. 5.

4.4 *Digital Signature*

Sender must require authenticity before sending his information means message. Sender's address plays a role of public key and private key is sender's password defined in Fig. 6.

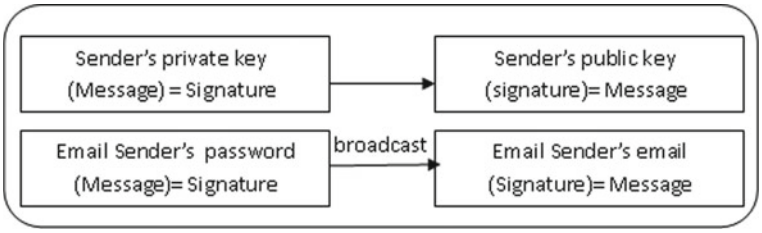

Sender's private key (Message) = Signature
Sender's public key (signature)= Message
Email Sender's password (Message)= Signature
broadcast
Email Sender's email (Signature)= Message

Fig. 6 Authenticity of transmission (digital signature)

5 Block Structure

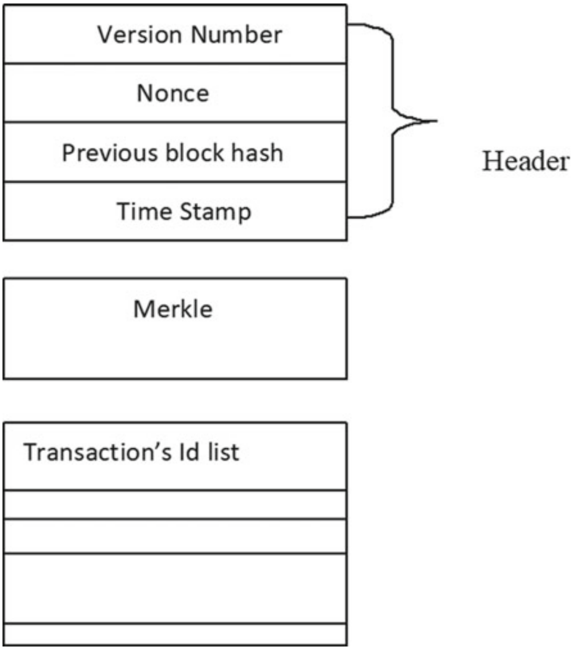
Blockchain blocks are shown in Fig. 7 which is divided into three parts.

Header: Contains version info, nonce, previous block id, and time stamp

Merkle: A hash built from a block's transaction identifiers.

List of record's: Identification hashes that were included into the block's Merkle tree

Fig. 7 Block structure



5.1 Characteristics of Blockchain

Blockchain is a new word we are listing nowadays everywhere frequently, many people correlate the term bitcoin and blockchain vice versa. But bitcoin is a digital currency which is used in blockchain technology [7]. Blockchain has data structure, immutable, validated by distributed network and cryptography for security characteristics.

- Data structure: Fundamental unit is a block consist of a header, transaction, and market root structure for every block is consistent each block maintains the reference to the parent block
- Immutable: Data once written to the blockchain cannot be changed. If wrong data has been written to the chain, it will exist on chain and another transaction is needed to correct the state maintaining audit trail of wrong data.
- Validated by distributed network: The nodes in the distributed network individually validate the data. The data is only written to blockchain once the network reaches an agreement or consensus.
- Cryptography for security: Hashing is used to ensure data is not tempered with asymmetric public key infrastructure is used to ensure transaction authenticity and validity.

5.2 Types of Blockchain

There are three types of blockchain public, private, and consortium and Table 1 indicates feature differences of public and private blockchain [5].

- Public: Public blockchains are a collection of ledgers which is able to be seen by everyone that is available on the Internet and provide the facilities to anyone that can add a number of block into the blockchain for transactions and verify the block. Bitcoin, Ethereum, and Factom are an example of public blockchain [6].
- Private: All permissions are kept centralized to an organization private blockchain allow only specific people in the organization to verify and add transaction blocks but everyone on the Internet is generally allowed to view.

Table 1 Difference between public blockchain and private blockchain

Features	Public	Private
Access	Open read/write access to database	Permission read and/or write access to database
Speed	Slower	Faster
Security	Proof of work/proof of stake	Pre-approved participants
Identity	Anonymous/pseudonymous	Known identities
Asset	Native assets	Any asset

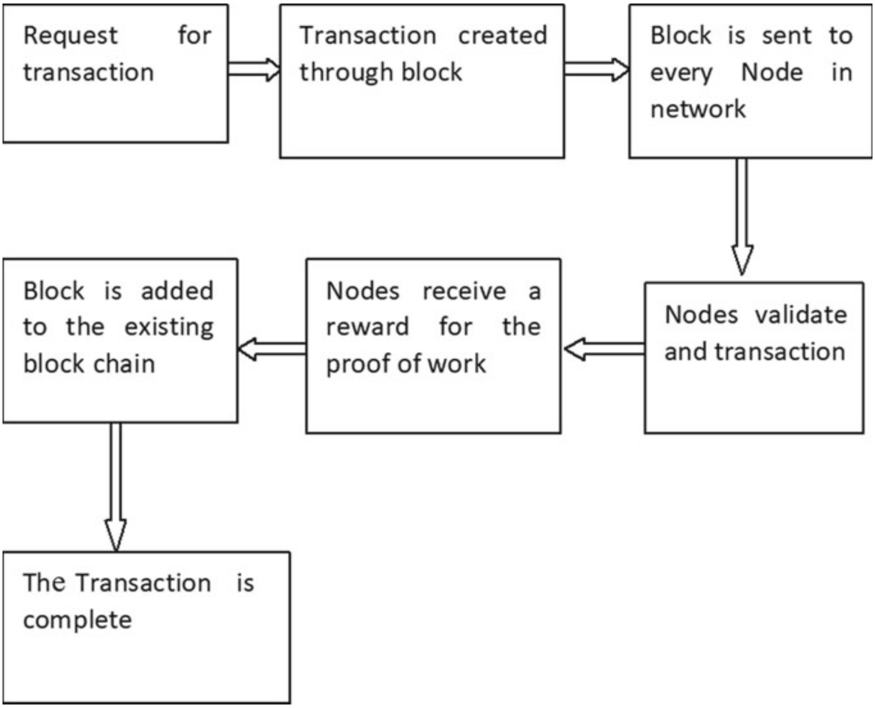

Request for transaction
Transaction created through block
Block is sent to every Node in network
Nodes validate and transaction
Nodes receive a reward for the proof of work
Block is added to the existing block chain
The Transaction is complete

Fig. 8 Work process of blockchain

- Consortium: A collection of nodes that is used to write the data or block which is controlled by the members of consortium. Example: Ripple, R3, and hyperledger1.0.

5.3 Process of Blockchain

Blockchain completes their work in the following steps shown in Fig. 8.

5.4 Problems with the Current System

- Customer has to pay fees when he want to transfer a money from the banks and other parties;
- The transaction costs is increased by the mediator;
- Transaction is limited for the minimum size;
- Financial process of exchange is very slow. It takes few days to complete the services due to low cost wire;

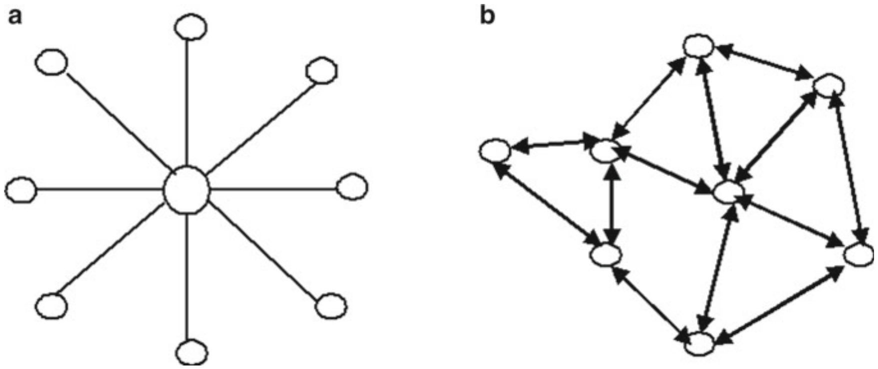


Fig. 9 **a** Centralized network, **b** distributed network

- System does not provide the fairness and transparency.
- Central authority over use the power and control to create money as per their own choice.

5.5 Distributed System

Distributed system provides the facility where computers create a network between them and arrange the large amount of date as a record of book keeping through the Internet. It is an open system not hold the command of single party but available in one ledger that is distributed transversely the network and give the solution of problems with current system. [5]

A collection of two or more than two nodes in a system achieves the target of same output by the coordination of between them. A role of node as an identity processing entity is defined in a distributed system. All nodes have a capability to send and receive the messages from each other. The sender and receiver see the distributed system in terms of a single logical model; Fig. 9 shows centralized network and distributed network.

5.6 Block Identifiers

There are two identifiers block header hash and block height shown in Table 2.

Table 2 Block identifiers

Block header hash	Block height
The primary identifier of a block is its cryptographic hash	It is the position of the block in the blockchain
A digital fingerprint made by hashing the block header twice resulting 32-byte hash	The first ever block created is at block height zero
The block hash identifies a block uniquely	Each block added on the top has one position higher in the blockchain
The block hash not included inside the block's data structure	It is also not a part of the block's data structure

5.7 Blockchain Technologies

(a) **Smart contracts**

An agreement or bound between two people or organization is known as contract shown in Fig. 10. Smart contract is a small computer program given by Nick Szabo in 1994. Smart contract program developed using solidity which is a programming language the syntax of solidity language is similar to the JavaScript [6].

Smart contract executed the terms of contract and behave like transaction protocol roll of smart contract in blockchain as a self operating program that execute automatically when all specific conditions are met.

An option contract in a blockchain is written in the form of code between parties where they are involved individually and public ledger is used to write the contract. Date of termination and smack of price is treated as triggering event hit and the contract automatically executed itself when the code is generated [3]. Regulators can the blockchain to understand the activity in the market while maintaining the privacy of individual actor's position.

(b) **Ether**

The value token of the Ethereum blockchain is termed as Ether. It is remarked as crypto means secure currency and used in ETH, the Ethereum get charges on the exchange services when computational and transaction services would be performed. A contract is executed every time and GAS is used as a token in Ethereum.

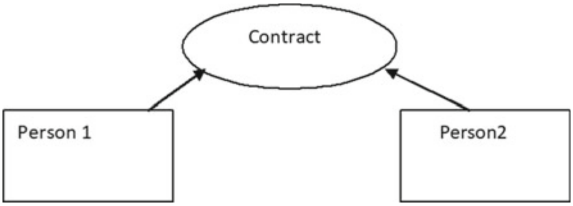


Fig. 10 Contract between two people

- **GAS**: The requirement of GAS in an Ethereum blockchain to be compensated for performance of any operation. A few amount of Ether has been charging as a fee of transaction and is directly deducted from the account of originator who had the transaction, and miners include fee that is paid for transaction. The more about fee, the miners pick up this transaction detail in future in the block [8]. Providing too little gas may result in the transaction failure.
- **Ethereum Virtual Machine**: Ethereum virtual machine is the engine in which transaction code gets executed, it enables the development of thousands of different applications at one platform. Contracts are written in a smart contract-specific programming languages which are later compiled into "bytecode," which could be read and executed by EVM. All the nodes execute this contract using their EVMs [7].
- **Solidity**: The solidity source code is passed to the solidity compiler and the compile returns the EVM bytecode which is deployed to the Ethereum blockchain and to the contract Abstract Binary Interface (ABI). There are many solidity compilers available such as: remix browser-based compiler, command line solc compiler.

ABI is list of contract's function and arguments and it is in JSON format. It known at compile time generated from source code through compilation. If we do not have the source code we cannot generate the contract ABI than only from the bytecode using reverse engineering. Anyone that wants to interact with the contract must have access to the contract ABI.

ABI is defined as the procedure of calling a functions within the contract and publicly access data in a bytecode from the contract. It is saved on the blockchain and cannot be encrypted because it must be run by every Ethereum node;

Opcodes are the human readable instructions of the program. It can be easily obtained from bytecode. There are tools like porosity that can reverse engineer the bytecode to source code. Contract source code does not have to be public.

Solidity is a high-level, statically-typed smart contract programming language and is similar to JavaScript, solc is the solidity command line compiler. Solidity is case-sensitive every line must end with a semicolon it uses curly braces {} for delimiting the blocks of code most of the control structures are available: if, else, while, for, break, continue, return [9].

References

1. Sarmah A (2017) A brief study on cyber crime and cyber law's of India. Int Res J Eng Technol (IRJET) 4(6):1633–1641
2. Dashora K (2011) Cyber crime in the society: problems and preventions. J Altern Perspect Soc Sci 3(1):240–259
3. Barde S, Tikariha N (2020) Cyber crime problems and prevention effect on society. J Inf Comput Sci 13(1):29–36
4. Barde S, Tikariha N (2020) Study on Cyber Laws of India. Int J Res Appl Sci Eng Technol 8(6):385–389

5. Melanie S (2015) Blockchain: blueprint for a new economy. 'O'Reilly Media, Inc
6. Marco J, Lakhani K (2017) The truth about blockchain. Harvard Bus Rev 95(1):118–127
7. Michael C et al (2016) Blockchain technology: Beyond bitcoin. Applied. Innovation 2:6–19
8. Aste T, Tasca P, Di Matteo T (2017) Blockchain technologies: the foreseeable impact on society and industry. Computer 50(9):18–28
9. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (bigdata congress), pp 557–564
10. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Www.Bitcoin.Org, (Online). Available: https://bitcoin.org/bitcoin.pdf
11. Wood G (2014) Ethereum: a secure decentralized generalized transaction ledger yellow paper. Ethereum Project Yellow Pap 1–32
12. Buterin V (2014) A next-generation smart contract and decentralized application platform. Etherum, (Online). Available: http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf
13. Androulaki E et al (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth eurosys conference, pp 30:1–30:15
14. Kan L, Wei Y, Muhammad AH, Siyuan W, Linchao G, Kai H (2018) A multiple blockchains architecture on inter-blockchain communication. In: 2018 IEEE international conference on software quality, reliability and security companion (QRS-C), pp 139–145
15. Miller D (2018) Blockchain and the internet of things in the industrial sector. IT Prof 20(3):15–18