An introduction to Blockchain technology

Mridul Gupta
2019PCP5037 MNIT Jaipur

October, 2019

Abstract

The aim of this paper is to provide an introduction and history of blockchain technology to people who consider venturing into the field of online transactions and security methods.

1 Introduction

Even though blockchain became popular in the recent years with the implementation as bitcoin[1] and other cryptocurrency mechanisms coming up, the ideas has been around for years.

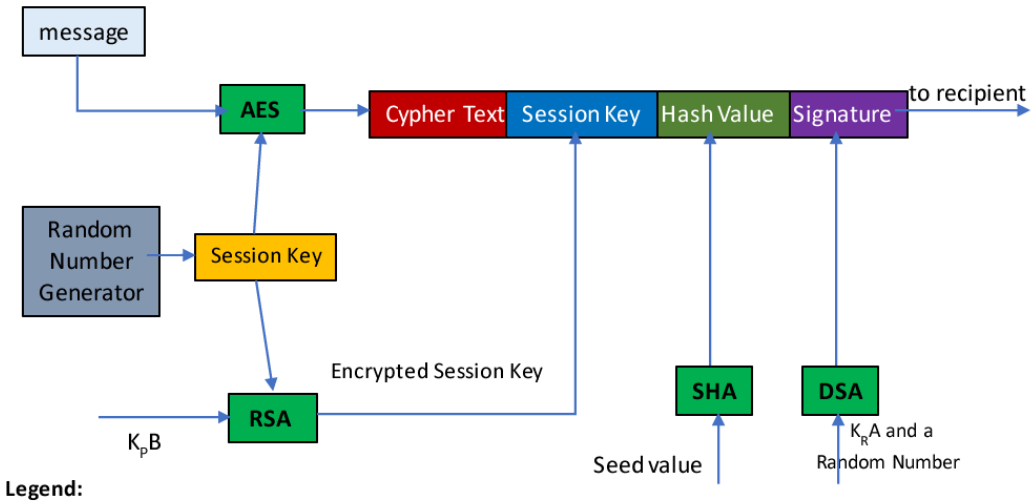
2 Parts of Blockchain

A blockchain is a type of distributed database, an atleast fifty years old idea, but the first mention of immutably chaning blocks of information using a cryptographic hash function appears in 1979 paper by Ralph Merkle[2].

Blockchain is a peer-to-peer distributed ledger that eliminates the need of a trusted third party in order to verify any piece of online data. The network itself acts as its own arbitrator to resolve any arbitration issues. As a result, blockchain makes complete non-reversible transactions possible[1].

Blockchain consists of cryptographically linked chain of blocks of data, each of which contains the cryptographic hash of the preceding block and the first block, usually called the genesis block, to create and immutable ledger.

Each node on the peer-to-peer network can append records to the ledger using transactions[4]. Blockchain protocol consists of *ac-*



Legend:

AES	Advanced Encryption Standard – a symmetric-key encryption algorithm
RSA	Rivest-Shamir-Adelman – an asymmetric-key encryption algorithm named after its designers
SHA	Secure Hash Algorithm – a standard hashing algorithm
DSA	Digital Standard Algorithm – a standard algorithm for digitally signing a block of information
K_PB	Public Key of recipient - (B)
K_RA	Private Key of sender - (A)

Figure 1: Blockchain components

cess policy to determine who may read the blocks. Blockchain also defines *control policy* to define who may participate in the evolution of blocks and *consensus policy* to determine which state of the blockchain is valid to resolve issues and conflicts[3][1].

3 History of blockchain

Any analysis of blockchain is incomplete without the understanding of the (at least) cryptographic concepts and papers listed in table 1, the discussion of which is beyond the scope here.

Blockchain borrows from various cryptographic ideas like public key cryptography, cryptographic hashing, digital signatures; and also from other computer science areas like database management systems, networking, peer-to-peer networks.

1974	Ralph Merkle, cryptographic puzzles
1976	Diffie Hellman, pioneering work on public-key cryptography
1977	Rivest, Shamir, Adleman, RSA cryptography created
1979	David Chaum, vaults and secret sharing (dissertation 1982)
2002	Adam Bach, Hashcash
2008	Satoshi Nakamoto, Bitcoin

Table 1: timeline of selected blockchain discoveries

Thus blockchain is a vast interdisciplinary that is difficult to understand.

4 Future of blockchain

Adaption of blockchains in e-Government, smart contracts, IoT, smart grids, smart cities, legal systems, public safety, public health, estate ownerships, property transactions, supply chain management, and many more is being considered rigorously. Many small start-ups are involved in studying applications of blockchain technology. The last decade has seen the growth of Bitcoin, and recently Bitcoin has gained enormous support from investors, thereby, raising its stock value. We believe the next decade will see the application of blockchain in other public and private sectors. This will have a significant enhancement in security and privacy of information.[4]

There are three areas that require attention to make blockchain a viable technology to be used in broader applications. Firstly, the time complexity of various algorithms providing utility services within blockchain schemes must be significantly reduced to allow time-critical transactions to occur; secondly, the implementation of blockchain technology in distributed as well as in centralized computing environments must be possible; and, thirdly, the provision of security and privacy when blockchain technology is employed in open/public networks must be continuously re-addressed.[4]

We believe practical and reliable solutions to the above challenges will expedite the use of blockchain technology and create a new capability within information networks of the future.[4]

References

[1] Nakamoto Satoshi, "Bitcoin: A peer-to-peer electronic cash system", 2008, https://bitcoin.org/bitcoin.pdf

[2] Merkle R.C., "Secrecy, authentication, and public-key systems", PhD Thesis, Stanford University, 1979

[3] Sherman Alan, Farid Javani, Haibin Zhang, Enis Golaszewski, "On the origin and variations of Blockchain Technologies", 2018

[4] "Blockchain: A Technical Overview - IEEE Internet Initiative", https://internetinitiative.ieee.org/newsletter/march-2018/blockchain-a-technical-review