Blockchain & Smart contracts

Introduction

In 1982, Cryptographer David Chaum proposed a protocol like the blockchain his dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups."

In 1991, Stuart Haber and W. Scott Stornetta introduced the concept of a cryptographically secured chain of blocks

In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees into the design, which improved its efficiency by allowing several document certificates to be collected into one block

The first decentralized blockchain emerged in 2008 with the Paper “Bitcoin: A peer-to-peer electronic cash system” by Satoshi Nakamoto

Blockchain technology got its first adoption with the use of cryptocurrencies in the financial industry.

With that initial adoption of the technology, we got decentralized applications that functioned without the use of a trusted third party with the appearance of smart contracts.

Explaining Blockchain technology

It's a type of distributed ledger technology (DLT) that consists of growing list of blocks, that are securely linked together using cryptography

Blockchain technology has been used as a distributed database that records all transactions that happened in a peer-to-peer network. It is regarded as a distributed computing paradigm that successfully overcomes the issue related to the trust of a centralized party (need of trusted third party, for example, a banking institution when two companies want to exchange a product for money). Or, as stated by Naheed Khan, Loukil, Ghedira-Guegan, Benkhelifa, and Bani-Hani, a blockchain network is composed of “several nodes collaborate among them to secure and maintain a set of shared transaction records in a distributed way without relying on any trusted party”.

This security and consistency in accesses is only possible because each node collectively adheres to a consensus algorithm protocol to add and validate new transaction blocks

Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data

Timestamp: proves that the transaction data existed when the block was created;

Cryptographic hash: a way to secure the message block and is used to connect the blocks in a chain

Transaction data (generally represented as a Merkle tree): data nodes are represented by leaves

Signing and Verifying Nodes in the Blockchain

Signing the message with private key: To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash — along with other information, such as the hashing algorithm — is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

Verifying the message with public key: This would involve two steps, generate hash of the message and signature decryption. By using the signer's public key, the hash could be de-crypted. If this de-crypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (authentication).

Decentralization

Being a decentralized solution, it means that the data is stored in a peer-to-peer network. A peer-to-peer network is an architecture that shares tasks, work and data between those peers. Those peers are together in the network and have the same privileges and inside the network, all of these peers are called Nodes.
The Blockchain consists in a series of computers and servers where which one of them acts as a Node in the network. As soon as a new message enters the network, the info in this message is shared across all Nodes in the Peer-to-Peer network. This info is encrypted and private, without being able to trace the identity, every participant just trusts the validation provided by the system.

With this, we remove the need of a third-party organization or with a central administrator that needs to know every participant information and data and all decisions are made by its participants

By not relying in a third-party organization, both parties can avoid operational costs (such as a banking institution when it comes to the exchange of a product/service in exchange for currency).

Uses for the Blockchain technology

Cryptocurrencies

Most of cryptocurrencies (such as Bitcoin Ethereum) use the blockchain technology to record its transactions and in the last year, various entities have shown interest in having a crypto currency of their own.
Facebook announced its cryptocurrency Diem. China has developed a national digital currency in 2020 and to follow example, the EU and the US have initiated similar projects.

Financial services

Many banking institutions have shown interest in using distributed ledgers for banking and cooperating with other companies through the use of private blockchains.

The use of this technology has potential to speed up back-office settlement systems.

Smart Contracts

But what exactly are smart contracts? These can be defined as computer protocols designed to facilitate, verify, and automatically enforce the negotiation and agreement among multiple untrustworthy parties, without human interaction.

Smart Contracts can be defined as executable code that use the Blockchain that “facilitate, execute, and enforce an agreement between untrustworthy parties without the involvement of a trusted third-party” as stated by Naheed Khan S. This means that the need for a trusted third party becomes unnecessary.

The big difference between traditional written contracts is that (since Smart Contracts are technically pieces of code) agreements transactions are now automated and occur without the need of a central authority

Smart Contracts Platforms

Bitcoin: The Bitcoin Blockchain platform used for cryptocurrencies transactions, but has limited computing capabilities and limited ability when it comes to create smart contracts.

NXT is an open-source blockchain platform that relies entirely on a proof-of-stake consensus protocol. It includes a selection of smart contracts that are currently living. However, it is not Turing-complete, meaning only the existing templates can be used and no personalized smart contract can be deployed.

Ethereum is the first blockchain platform for developing smart contracts. It supports advanced and customized smart contracts with the help of a Turing-complete virtual machine, called the Ethereum virtual machine (EVM). EVM is the runtime environment for smart contracts, and every node in the Ethereum net-work runs an EVM implementation and executes the same instructions. Solidity, as a high-level programming language, is used to write smart contracts, and the contract code is compiled down to EVM bytecode and deployed on the blockchain for execution. Ethereum is currently the most popular development platform for smart contracts and can be used to design various kinds of decentralized applications (DApps) in several domains.

Hyperledger Fabric is permissioned with only a collection of business-related organizations can join in through a membership service provider, and its network is built up from the peers whose are owned and contributed by those organizations. Hyperledger Fabric is an open-source enterprise-grade distributed ledger technology platform, proposed by IBM and supports smart contracts. It offers modularity and versatility for a broad set of industry use cases. The modular architecture for Hyperledger Fabric accommodates the diversity of enterprise use cases through plug and play components.

Use Cases for the Blockchain Technology

Lygon – Banking

Taking a look at AZN Banking (The Australia and New Zealand Banking Group Limited, an Australian multinational banking and financial services company headquartered in Melbourne, Victoria and Australia's second largest bank) and the Banking Industry, a Bank Guarantee is a unconditional agreement/promise made by a Bank or an insurer to certify liabilities of a debtor will be met.

Looking at Australia and New Zealand, there are 11,500 retailers that use paper guarantees created using a manual workflow.

With physical paper system, the guarantee process becomes susceptible to fraud and forgery, and is additionally costly and hard to monitor (and landlords end up managing and storing said guarantees like in fireproof safes).

As said by Nigel Dobson, the Banking Services Lead of Australia New Zealand Banking Group Limited; and the Chairman of Lygon 1B Pvt Ltd, "To better serve our customers, we wanted to deliver a guarantee solution that was contemporary, digital and that could be used in a multi-bank setting.". Using a physical paper for bank guarantees just doesn't meet the security requirements for this day and age.

ANZ and IBM together concluded that the Blockchain would be a key component in implementing a solution that could transform the guarantee life cycle, including issuance, amendments, cancellations and any claims.

With this, ANZ and IBM were joined by other two Australian banks, Westpac Banking Corporation and Commonwealth Bank, and formed the consortium known as Lygon 1B Pty Ltd.

With the creation of Lygon, a tenant can request a guarantee online, a landlord can set the terms and then the tenant and bank can review the guarantee. When all parties agree on the document, it will be stored in the DLT in a standardized, trackable way that is trusted by all parties with the data being shared using DLT (Distributed Ledger Technology) based on the Hyperledger Fabric from the Linux foundation.

The end result is a solution that benefits all parties, allowing everyone to have access to said documents in a digital, secure and private way and removes the needs for papers, which in turn allows bank guarantees to be issued in less than one day, where it previously took as many as 30 days.

References

Naheed Khan S, Loukil F, Ghedira-Guegan C, Benkhelifa E, Bani-Hani A. (2021). Blockchain smart contracts: Applications, challenges, and future
trends

https://en.wikipedia.org/wiki/Blockchain

https://ravikantagrawal.medium.com/digital-signature-from-blockchain-context-cedcd563eee5

Golosova J., Romanovs A. (2018). The Advantages and Disadvantages of the Blockchain Technology

https://www.ibm.com/case-studies/lygon/

https://institutional.anz.com/insight-and-research/Distributed-Ledger-Technology-and-Bank-Guarantees-for-Commercial-Property-Leasing

https://www.ibm.com/topics/hyperledger