

Role of blockchain and smart contracts in realising Web 3.0

Introduction

Web 3.0 is the next generation of the internet. Its core features include decentralisation, blockchain and tokens[1]. This is crucial to allow the internet to empower users by giving them greater control over their own data, giving users transparency, high security standards, and allowing for seamless collaboration.

Section 1: What are blockchain and smart contracts

A blockchain is a decentralised ledger distributed over many computers that records transactions securely and transparently. It consists of a chain of blocks each with verified transactions. The key components are as follows.

Blocks: Blocks have a header and a body. The header part contains metadata like timestamps and a reference to the previous block's hash. The body part contains a list of the transactions.

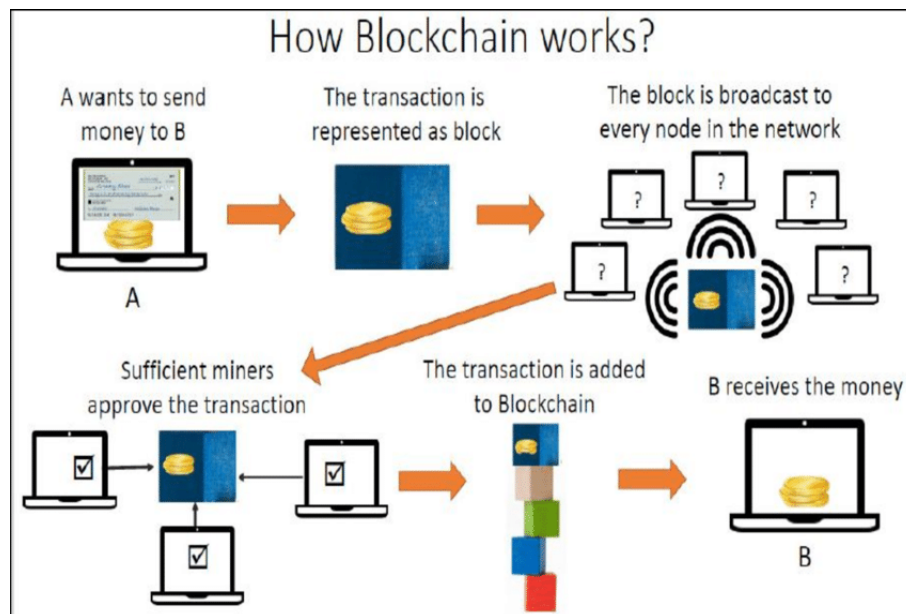
Hash functions : the cryptographic hash functions take data and make an output called a hash that is unique to that data. In most blockchains SHA 256 bit is used. No character in a hash function may be changed.

Consensus algorithms: These are rules used by the network to allow the nodes to agree on things in the blockchain. Examples include proof of work used by bitcoin or proof of stake.

Here is the python code for setting up a very simple blockchain.

```
import hashlib
class B:
    # set up the class constructor and initialise.
    def __init__(self, data, priorhash):
    # the data
        self.data = data
    # previous hash
        self.priorhash = priorhash
        self.hash = self.c_hash()
    def c_hash(self):
    # uses sha 256 bit which is most common in blockchain
        return hashlib.sha256( (self.data + self.priorhash).encode()).hexdigest()
    # make the genesis block
    Gblock = B("genblock ", "0")
    # make the new block with the hash of the previous block
    nblock = B("data of new block ", Gblock.hash)
    # Print the hashes
```

```
print("hash of the genesis block :", Gblock.hash)
print("hash of new block:", nblock.hash)
```



Smart contracts are blockchain based programs that automatically run when certain conditions are met. This automates contracts between parties without the need for middlemen and ensures that contracts are traceable, safe and irreversible.

python code for a simple smart contract.

```
class contract:
```

```
    def __init__(self, x , y =0): self.owner, self.balance = x,y
```

```
    def deposit(self, z): self. balance = self.balance + max(0, z)
```

```
    def withdraw(self , u, z): self.balance = self. balance - z if u == self.owner and z<=
self.balance else 0
```

```
c = contract("Ali")
```

```
# deposit 100 in the account
```

```
c.deposit(100)
```

```
# withdraw 50 from the account
```

```
c.withdraw("Alice", 50)
```

Section 1 references

1. Wikipedia, "web3" <https://en.wikipedia.org/wiki/Web3> accessed Mar.17, 2023
2. Gartner digital markets team, what is web 3.0, Gartner, May 27.
<https://www.gartner.com/en/marketing/insights/daily-insights/what-is-web-3-0-and-how-does-it-impact-digital-marketers> (accessed Mar. 17, 2023)

3. J.Chen and S.Gaurav, “blockchain facts: what is it, how it works and how it can be used, <https://www.investopedia.com/terms/b/blockchain.asp> (accessed Mar 17, 2023)

Section 2: How blockchain and Smart contracts play into Web 3.0

Decentralisation in Web 3.0 allows the power distribution to shift from platform owners to users which allows for greater security, trust and reduced censorship[1]. Blockchain facilitates this decentralisation through a secure and decentralised ledger that records transactions without a middle-man or third party[2]. This is achieved through a number of techniques including storing new blocks chronologically, cryptography and consensus among the participants in the network.

Blockchain and smart contracts enhance security and privacy in Web 3.0 through data verification, encryption, autonomous contracts and protection of user identity[5]. This allows for many Web 3.0 applications that require this heightened security like supply chain management, securities trading and secure data sharing.

New business models and applications are possible in Web 3.0 because of blockchain and smart contracts. These include Decentralised autonomous organisations, decentralised finance and non fungible tokens.

Section 2 References

1. MAQE, “web 3.0- what is decentralisation and where is the web going? MAQE. <https://www.maqe.com/insight/web-3-0-what-is-decentralization-where-is-the-web-going/> (accessed on Mar 17, 2023)
2. Curious owl “What is web 3.0 decentralisation” <https://curiousowl.co/web-3-0-decentralization/> (accessed on Mar 17, 2023) .
3. Addweb solution, “A beginners guide to web 3.0”, Addweb solution. <https://www.addwebsolution.com/blog/web-3-decentralized-internet> (accessed on Mar 17, 2023)
4. freeCodeCamp, "What is web 3 the decentralised internet of the future explained" freeCodeCamp. <https://www.freecodecamp.org/news/what-is-web3/> (accessed on Mar 17, 2023)
5. SANS, “Blockchain and smart contract security, SANS SEC554” <https://www.sans.org/cyber-security-courses/blockchain-smart-contract-security/> (accessed on Mar 17, 2023)

Section 3: Challenges and Future prospects

Blockchain and smart contracts are both technologies with good future prospects but they face challenges and limitations. These include issues like throughput, latency times, energy consumption, confidentiality and legal issues due to how recent these technologies have developed[4]. The legal issues that surround blockchain are very complex and include issues such as data privacy and issues in certain jurisdictions regarding the legality of smart contracts[5]. These issues are being worked on by developers who are working on data privacy solutions and also by lawmakers who are providing guidelines about legality and responsible use of this technology[5]. The future outlook of this technology has good prospects. Blockchain and smart contracts shape the future of Web 3.0 and usage is being accelerated by AI integration, the rapid adoption of smart contracts in various applications and the innovation of new standards for Web 3.0. As these technologies develop they have the potential to make data ownership more distributed, create a more open web and allow for new business models that use smart contracts.

References for section 3

1. IEEE Computer Society, "Welcoming Web 3.0 and Its Role in Development," <https://www.computer.org/publications/tech-news/trends/welcoming-web-3-and-its-role-in-development/> (accessed on Mar 17, 2023)
2. Z. Zheng et al. "An overview of smart contracts : architecture applications and future trends " IEEE Access , vol. 6, pp. 38062-38074 , 2018
3. A. Kaur et al, "web 3.0, the decentralised web blockchain networks and protocol innovation" in ICACCE, Dehradun, India, 2018
4. S.N. Khan et al , "Blockchain smart contracts: Application, challenges and future trends Peer to peer networking and applications" , vol. 14, no. 5, pp. 2901–2925, 2021.
5. Forbes "Smart contracts and law, what you need to know. " <https://www.forbes.com/sites/forbesbusinesscouncil/2022/03/17/smart-contracts-and-the-law-what-you-need-to-know/> (accessed on Mar 17, 2023)

Conclusion of analysis

The internet has gone through 3 stages historically. Web 1.0, 2.0 and now 3.0 which allows for better user control and security. Web 3.0 allows for data experiences and contracts that are not controlled by a single entity or person and is made possible by technologies like blockchain and smart contracts. Web 3.0 also makes the internet harder to censor due to no central authority having the final say on censorship. It allows people to interact without middlemen while maintaining high standards of accuracy of information and security which allows for applications like secure distributed online payments. New technologies like NFTs and cryptocurrency have been made possible by this distributed system of ownership which does not rely on any particular company or server. For these reasons I believe that web 3.0 will change the internet and allow for a more open ,secure ,distributed and fair internet going forward.