University of London

MSc Data Science and Artificial Intelligence

DSM070 Blockchain Programming Coursework

Transactions and Verification in Blockchain

Program: 50% - Essay: 50%

Table of Contents

List of Tables

1. Bitcoin:

In the 1980s, cryptography started to gain widespread interest among researchers and started to be used to build various digital currencies (Antonopoulo, 2014). Digital currency is a form of currency that relies on transferring currency over the internet and gains value only upon exchanging. Digital currency started on a centralised based. In 2009 the first decentralised digital currency, called bitcoin, was introduced by Satoshi Nakamoto, although he disappeared from the public in April 2011 and nowadays, any new development in Bitcoin and handed over to a group of volunteers (Jaiswal Manishaben, 2020).

Bitcoin was created to have a system that entirely does not rely on a central authority or financial intermediaries. By using distributed computation systems and other innovations such as peer-to-peer and b-money. This has helped address a significant weakness in previous digital currencies, such as the double-spent problem (Antonopoulo, 2014).

On the other hand, bitcoin faced major challenges, such as the volatility of the currency leading to a decrease in users' trust in the ability of these digital currencies to replace the traditional system. Another challenge is that by 2013, government agencies worldwide have been trying to introduce regulations and legal frameworks that are expected to limit the idea of Bitcoin being decentralised (Antonopoulo, 2014).

However, since 2009, the adoption of Bitcoin has increased exponentially and reached a total market value of more than 135 billion US dollars. Moreover, the number of merchants using cryptocurrencies and Bitcoin for payments is increasing as it is viewed as a way to achieve a secure payment transaction (Antonopoulo, 2014).

In terms of how a single bitcoin transaction is structured, the first element is the transaction output which includes an integer value as a multiple of Satoshis. Next, bitcoin nodes compute the spendable outputs, called "unspent transaction outputs" (UTXO), which are currently estimated to be in millions. Any transaction is a change in the collection of all UXTO (Antonopoulo, 2014).

In general, the bitcoins balance of every user is the total of UTXOs that can be spent. Those will be located in that user's wallet and are managed by the wallet application, which maintains a database of all the UTXOs which can be spent along with the associated keys. These transactions will be recorded in the wallet as a UTXO until it is consumed. Once a bitcoin is transferred to a user, one of the keys controlled by that wallet will detect the UTXO. On the sender side, a UTXO must at least be equal to the transaction amount plus the fees. Moreover, in case UTXO (i.e. 50) is more than the desired transaction value (30), the entire the transaction will generate two outputs, one to the recipient while the remaining value will be transferred back to the sender address as a change (20), keeping in mind the miners' fees (Antonopoulo, 2014).

In general, the bitcoin is generated from a chain of previous UTXOs, which ensures that each transaction's output has an input, except for the first constructed block called the Coinbase transaction that miners create. Therefore, to ensure that the money is not created, each input must retrieve at least one previous transaction except the Coinbase transaction (Antonopoulo, 2014).

Subsequently, to permanently confirm the legitimacy and record a bitcoin transaction on a blockchain, there is a four-step validation process:

- During transactions, To prevent double-spending, other transactions are not allowed any access to the database until the initiated transaction is completed (Murugan & Vijayalakshmi, 2019)
- Version verification: The transaction version is checked for compliance with the standards
- Simple verification: This will focus on the transaction input to ensure that it is not already saved or referenced in the UTXO as an input. Also, there is a check that the transaction amount and fee must be positive and less than 21 million. The total of the input amount must be more than the output
- Signature verification: This step checks that the public key is identical to the signature; otherwise, the transaction is discarded

(Vallois & Guenane, 2017)

2. ERC-20:

ERC20 (Ethereum Request for Comment) was initially issued in 2015 to support the community of Ethereum users. Later in 2017, it was augmented into the Ethereum protocol and became an official standard protocol mainly utilised for tokens and smart contracts within the Ethereum blockchain ecosystem. The protocol is now considered the most widely adopted token standard and defines a set of rules for any development of Ethereum-based tokens, including tokens transfer, transactions approval and access to the token's data (ViCA foundation, 2022).

Millions of ERC-20 digital tokens have been traded and transferred from various physical fungible items such as real estate and private currency; however, this poses a challenge while retaining the linkage between the digital token and physical good. Moreover, various companies have relied on the ERC20 protocol within the Ethereum network for their ICO (Initial Coin Offerings), mechanism companies follow to raise funds required for their new applications, services and any new invention. These companies aim to develop smart contract platforms and decentralised storage network systems (Somin et al., 2020).

ERC-90 offers the opportunity to exchange and transfer tokens by only providing the address of the token's contract, and it allows wallets to provide balances for many other tokens. This is achieved by ensuring the token complies with ERC-20 standards (McDonald Jim, 2017). It can be concluded that ERC-20 and bitcoin have a lot in common since both are blockchain-based and can be exchanged. However, a significant difference in ERC-20 compared to bitcoin is that it is issued primarily with the Ethereum ecosystem rather than its blockchain network (Reiff Nathan, 2022).

ERC-20 transactions represent one of the fascinating examples of decentralised networks in creating decentralised records during any exchange between the users, similar to financial transactions. However, there are two advantages compared to traditional interactions: the ability to have an unlimited number of wallets and tokens. Moreover, Ethereum Blockchain, through the ERC-20, introduced the concept of "Smart Contracts", which allow for every transaction to store the ownership and the execution code, which helped launch new forms of digital tokens (Somin et al., 2020).

By looking at the conceptual schema of the ERC-20 token standard, it is observed that a single token belongs to an instance of an ERC-20 contract account. Each instance is defined with three attributes (name: which is used for token usability, symbol: such as EUR and decimals: which returns how many decimals are used in the token). These attributes are common for all contracts and define the contract state (Olivé, 2020).

Upon deploying smart contracts, ERC-20 tokens are created and exchanging those tokens requires using Ethereum currency (ETH). These details are specified in the contract along with other details. For example, 5% of the ETH received in a particular contract will be transferred to another address.

Processing transactions on the Ethereum ecosystem require computing power and is usually measured by computational effort referred to as "Gas". Generally, there is a positive correlation between the transaction complexity and the computational effort required. Hence, the upper limit of gas consumed in every transaction is determined.

One of the most famous implementations of ERC-20 standards is OpenZeppelin. OpenZeppelin allows the development of custom smart contracts and complex systems on top of the Ethereum development framework and other blockchains (Weston Georgia, 2022).

3. Ripple:

In 2012, another blockchain-based digital currency was released, called Ripple. Although it is similar to bitcoin in principle. However, the source code for Ripple is privately owned in contrast to bitcoin. Furthermore, the verification in Ripple does not depend on miners but on the transactions, which can be verified only by Ripple company and other validators such as the Massachusetts Institute of Technology (MIT). Moreover, Ripple technology is designed to be more energy-efficient and faster than bitcoin by using Ripple Transaction Protocol (RTXP) which offers instant money transfer between sender and receiver (Jani, 2018).

Ripple security is preserved by allowing only a network of independent servers belonging to, for example, banks or market makers to validate transactions and manage a shared ledger. Another crucial factor is that Ripple company introduced their digital currency, Ripple's internal currency (XRP), which allowed financial institutions and banks to reduce the time and cost of transferring money (Jani, 2018; Somin et al., 2020).

Ripple's ecosystem is an open-source back-end infrastructure rather than a currency. The infrastructure enables banks, financial institutions, and non-banking services to augment Ripple protocol within their process and systems and accordingly allow customers to access this service (Jani, 2018).

The main parties involved in the transaction are regulated financial and market makers. The regulated financial is responsible for funds and issuing the customers' balance. In contrast, market makers provide the market with the currency.

Ripple offers integration with multiple protocols and financial institutions. Users must specify who they trust and the number of transactions to ensure validation. The balance will be adjusted based on the limits users have defined during any payment. If the trust is unavailable, the ripple system will establish a path between users and adjust the balance (Jani, 2018).

4. Compare and Contrast Different Currencies Mechanisms:

	Bitcoin	Ripple	ERC20
Flexibility	- bitcoin application can run in different operating systems. Therefore, anyone can install the bitcoin software (Jani, 2018) - It is suitable for unbanked people because it does not require customer ID (*Bitcoin Wiki*, 2010) - Transaction processing speed is not efficient for a high number of transactions (Cekerevac, 2019)	- peer to peer and open-source platform that deals with a different kind of currency. - To confirm a transaction, the consensus approach is used, which offers limited cost, few energy consumptions and rapid time confirmation (Frankenfield Jake, 2021)	- It offers a smart contract concept, and also there is no limitation on the number of tokens and wallets (Somin et al., 2020)
Privacy	- It provides robust financial privacy (*Bitcoin Wiki*, 2010) - Transactions can have various inputs from several accounts. While the users' identity is secure, the number of transactions and the time is leaked (Jani, 2018)	- The payment has one input account. While the users' identity is secure, the number of transactions and the time is leaked (Jani, 2018) - The use of smart contracts as transactions are executed automatically without users' intervention.	- The currency exchange should be done by activating a privacy protocol.
Security	- Proof of Work (PoW) ensures high security, and the transaction security is controlled by a few entities (Jani, 2018)	- It offers high security because the source code is owned by a private company. Thus the verification cannot be done by outsider nodes (Jani, 2018). Thus, the transaction is assured by utilising vote per validating server.	- Provide high security while offering medium amounts in transferring (Cekerevac, 2019) - A third party deploy the security audits to achieve high efficiency in the verification phase. Thus, improving the time and cost (ViCA foundation, 2022)

Table 1: Compare and Contrast Different Transaction and Verification Mechanisms

5. References:

Antonopoulo, A. M. (2014). Mastering Bitcoin. *Sermaye Piyasası Kurulu Araştırma Dairesi*, *9*(1), 75–82. http://dergipark.gov.tr/doi/10.29048/makufebed.365066%0Ahttp://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/1130

Bitcoin Wiki. (2010). https://en.bitcoin.it/wiki/Main_Page

Cekerevac, Z. (2019). *MEST Journal BLOCKCHAIN AND THE APPLICATION OF BLOCKCHAIN TECHNOLOGY Petar Cekerevac Independent researcher, Belgrade, Serbia*. https://doi.org/10.12709/mest.10.10.02

Frankenfield Jake. (2021). *Ripple*. https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp

Jaiswal Manishaben. (2020). *Cryptocurrency an era of digital currency*. https://ssrn.com/abstract=3919919

Jani, S. (2018). *An Overview of Ripple Technology & its Comparison with Bitcoin Technology*.

McDonald Jim. (2017). *Understanding ERC-20 token contracts*. Medium. https://medium.com/@jgm.orinoco/understanding-erc-20-token-contracts-a809a7310aa5

Murugan, A., & Vijayalakshmi, J. (2019). *Preventing the bitcoin Double Spend using Transaction Hash and Unspent Transaction Output*. https://doi.org/10.35940/ijrte.C5352.098319

Olivé, A. (2020). *The Conceptual Schema of Ethereum* (pp. 418–428). https://doi.org/10.1007/978-3-030-62522-1_31

Reiff Nathan. (2022). *What Is ERC-20 and What Does It Mean for Ethereum?* Investopedia. https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/

Somin, S., Gordon, G., Pentland, A., Shmueli, E., & Altshuler, Y. (2020). *ERC20 Transactions over Ethereum Blockchain: Network Analysis and Predictions*. https://doi.org/10.48550/arxiv.2004.08201

Vallois, V., & Guenane, F. (2017). *Bitcoin transaction: From the creation to validation, a protocol overview*. 1–7. https://doi.org/10.1109/CSNET.2017.8241988

ViCA foundation. (2022). *The ERC-20 Standard Protoco*. Medium. https://medium.com/@vicafoundation/the-erc20-standard-protocol-b72f2d88afdb

Vogelsteller Fabian, & Buterin Vitalik. (2015). *EIP-20: Token Standard*. https://eips.ethereum.org/EIPS/eip-20

Weston Georgia. (2022). *A Beginner's Guide to OpenZeppelin Blockchain*. 101 Blockchains. https://101blockchains.com/openzeppelin-blockchain/

6. Word Count:

Total number of words: **1806** words