Blockchain model and use case for data protection through examination and certification

Dina Darwish

Abstract— From its start as the premise of cryptocurrencies to more extensive applications in areas like property registration and insurance, Blockchain has arisen as a groundbreaking technology, because of its property as a distributed ledger which can eliminate the requirement for a trusted third party to encourage exchange. The expansion of this technology to new application areas has been caused by the presence of smart contracts, which are blockchain-based protocols which can automatically process a contract. Higher education is one of the areas that has being considered for the types of issues related to blockchain in many situations, since it can perform tasks with more speed, and minimize time and error while protecting data privacy. Blockchain can be implemented in higher education in many situations, such as, examination, training and certification and many others. This paper has proposed the design of an automated blockchained system for online examination and certification based on using student, instructor and university authorities secured signatures for verification of identity. The design is based on using Ethereum platform and NoSQL database for storage due to their advantages.

Index Terms— Blockchain, model, use case, data protection, examination, certification, education.

1 Introduction

The basic of Blockchain used today was published in a White Paper at October 2008 on a cryptography mailing list, but some of the principles included in Blockchain technology were already discussed in earlier cryptography papers. The paper title was, "Bitcoin: A Peer-to-Peer Electronic Cash System", and was published by an author, or a group of authors, under the pseudonym Satoshi Nakamoto. Thus, expressions such as 'chain of blocks' and 'blocks are chained' were mentioned in the original paper instead of term 'Blockchain'. The term "blockchain" was firstly used on the same mailing list in following discussions related to the original Nakamoto paper.

Satoshi Nakamoto released on 8 January 2009 Version 0.1 of the Bitcoin software [1], which was the first software to implement the principles described in the October 2008 paper. This was done on an open-source software site called SourceForge. Until mid 2010, Satoshi Nakamoto continued to collaborate with other developers on the Bitcoin software. Around that time, the control of the source code repository and updates are taken by Gavin Andresen, who transferred several related Internet domains to other known members of the bitcoin community, and ended his involvement. The development of Blockchains is another important step in the evolution of Blockchain technology, because blockchains could use small computer programs called smart contracts, which are written in computer languages, and possess a complete set of programming capabilities (these are named "Turing complete" computer languages).

Smart contracts [2] have given Blockchains the ability to implement a varied set of business functions involving the transfer of information and/or value, while leaving transparent and reliably auditable information trails.

The first Blockchain to use smart contracts was Ethereum [3] which was invented by Vitalik Buterin. He first described the use of smart contracts on a Blockchain in a White Paper in late 2013. Then, when he failed to gain agreement on this concept within the Bitcoin community, he proposed the development of a new platform called Ethereum. This new network, launched on 30 July 2015, is today the Blockchain with the largest number of transactions and is among the top three in market capitalization.

2 Overview of Blockchain Technology

2.1 Blockhain Technology

The blockchain is a decentralized data structure with internal consistency maintained through consensus reached by all the users on the current state of the network. It's an enabling technology that resolved the Byzantine generals' problem (message communication between untrusted parties) and opened up a new horizon of possibilities for trustless transactions and exchange of information. If the Internet democratized the peer-to-peer exchange of information, then the blockchain has democratized the peer-to-peer exchange of value. This section explores how transactions work between users on the Bitcoin network.

To understand how transactions occur between two users (Alice and Bob), we first need to understand the structure of blocks that hold the transactions. In the simplest terms, the blockchain is a collection of blocks bound by two main principles:

- Internal consistency: There are a few design principles inherent to the functioning of each block that make the blocks internally consistent. For instance, each block links to the previous one in the chain and has a creation timestamp. Such mechanisms in the blockchain allow it to be an internally coherent data structure that can keep a consistent record of transactions.

• *Dina Darwish, Ahram Canadian University, giza, Egypt. E-mail: dina.g.darwish@gmail.com.*

- Consensus on transactions: The concept of mining represents one implementation for verifying transactions; there are different methods where no brute-force hashing is involved. We can generalize this verification of transactions for a decentralized system by either using some sort of PoW (Proof of Work) or a similar strategy that pools transactions that are then checked by users on the network.

To discover the process, a transaction is essentially a data structure carried on a block, and each block has at least two unique components: the block header, which contains a unique hash (called the merkle root) [4] that uniquely identifies a block, and the transaction list, which contains new transactions. Each block contains the same amount of transactions in the list, but the precise transactions between users are different. This is because only one block wins the mining race every ten minutes on the blockchain, other candidates are rejected, and the race starts again. In this simplified model, there are only two other components of a block: the block size, which is kept consistent for the entire network, and a counter for the number of transactions in each block.

In this example [5], Bob wants to send one BTC to Alice. The BTC owned by Bob is used as the input of the transaction and the output is two parts, one sent to Alice for one BTC and the second one returned as change back to Bob. It should be noted here that the initial transaction, the newly assigned transaction, and the change are recorded on the blockchain as the input and output. Alice initiates the transaction from her wallet, which contains multiple addresses. Each address has a certain amount of Bitcoin balance (the sum of all UTXOs, representing the amount that is transferred to a Bitcoin address, associated with that address) that can be used to create new transactions. The transaction is then signed using Alice's private key and it enters the mining phase, where it will be packaged into a candidate block. As the mining concludes, the winning miner announces the block on the network and the block is included into the blockchain. The remaining transactions are thrown into the pool of transactions to be added. The transaction propagates to Bob, who can now use his private key to unlock the transaction output amount and use it. Fig. 1 [5] introduces the concept of the wallet, which can be used to initiate transactions.

2.2 Different Types of blockchains

Blockchains comes in many forms, but one of the fundamental aspects with blockchain is that there is always a network of nodes (computers/actors) participating in the network. A blockchain is often distinguished between three different types: private, public and a consortium. They have many similarities, but the difference lies in who is allowed to participate in the network, how the agreement of truth (consensus) is established, and the maintenance of the ledger.

In blockchain the network of nodes is also called peer-to-peer system. "Peer-to-peer systems are distributed software systems that consists of nodes (individual computers), which make their computational resources directly available to another " [6]. The members can interact with each other without having central coordination. The relation between a peer-to-peer system and blockchain is that the system uses blockchain as a tool to achieve and maintain integrity [6].

Public blockchain

In a public blockchain anyone is allowed to participate, anyone can send transactions and participate in the consensus process. The ledger is publicly available to all participants, which means that everyone in the network has the same information at all times [7]. Most crypto currencies in the blockchain sphere are built as public blockchains, they draw the benefits of value transaction without going through a bank, and thereby have lower transaction costs.

Private blockchain

In a private blockchain you need an invitation and a validation from the other participators in the network to be accepted as a part of the private blockchain. The rules for participation, consensus, and restrictions to the ledger may vary from each private blockchain [7]. In a private blockchain write permission are normally centralized and kept to one organization, while the read permission can be either public or restricted to selected participators [8].

Consortium blockchain

A consortium blockchain is a constellation of participators that have pre-selected a set of nodes that control the consensus process, illustrated with red nodes in Fig. 2. A consortium blockchain is a hybrid of a public and a private blockchain. Consortium blockchains can be considered as partially decentralized, which gives the advantage of providing multiple defaults for the transaction process [8].

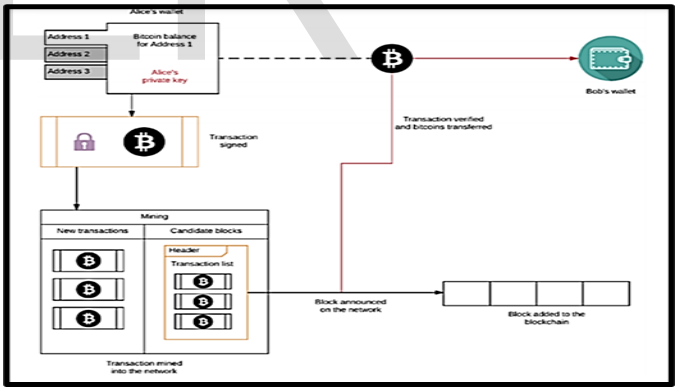

Fig. 1. Overview of a transaction on the network

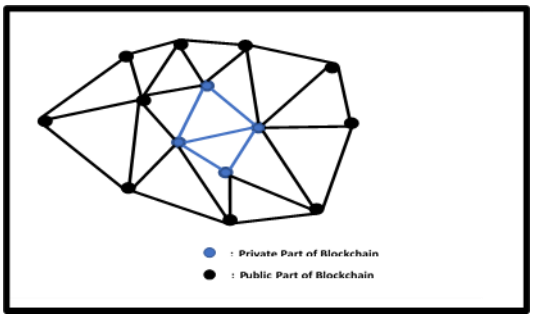

Fig. 2. Illustration of Consortium blockchain

3 IMPACT OF BLOCKCHAIN

Blockchain is an innovative solution for disrupting the inefficiencies in the financial system. Kastelein [9], publisher of Blockchain News (BCN), noted that there are five basic principles underlying the blockchain technology that allows blockchain to change how financial market transactions are created. It's worth repeating here the five basic principles underlying the technology:

- ***Distributed database*:** Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.
- ***Peer-to-peer transmission*:** Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes.
- ***Transparency with pseudonymity*:** Every transaction and its associated value are visible to anyone with access to the system. Each node, or user, on a blockchain has a unique 30-plus-alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others.
- ***Irreversibility of records*:** Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, because they're linked to every transaction record that came before them (hence the term chain).
- ***Computational logic:*** The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. Users can therefore set up algorithms and rules that automatically trigger transactions between nodes.

For the first time in human history, two or more parties, be they businesses or individuals who may not even know each other, can forge agreements, make transactions, and build value without relying on intermediaries (such as banks, rating agencies, and government bodies such as the US Department of State) to verify their identities, establish trust or perform the critical business logic—contracting, clearing, settling, and record-keeping tasks, that are foundational to all forms of commerce.

Blockchain applications can reduce transaction costs for all participants in an economy via peer-to-peer transactions and collaboration. Blockchain is truly a game-changing financial markets solution using new technology and empowered by thought leadership. Blockchain technology was used due to a number of features and characteristics that can enhance the overall ability to meet reporting requirements: Data integrity, Reliability, Storage, Speed, Analytics, and Proof-of-Concept (PoC).

4 BLOCKCHAIN MODEL AND USE CASE IN EXAMINATION AND CERTIFICATION IMPLEMENTING DATA PRIVACY

A number of researchers have explored the use of Blockchain to store university grades, i.e. university transcripts. A group at the University of Glasgow has developed a functional prototype for storage of student grades at the institution [10]. The platform chosen was Ethereum, hence it was built on a public blockchain. This was exploratory research, and they identified several challenges, including in the use of smart contracts to calculate grades in an algorithmic manner. Another project giving a prototype implementation is [11], where a private BigChainDB blockchain is used for storage of student transcripts (not grades within a course). Yokubo [12] describes a prototype implementation of a university transcript system using an Ethereum private blockchain and ERC-20 tokens (a standard for tokens, which are needed to carry out smart contracts, on Ethereum) on that blockchain. Students are able to read their grades, while professors and administrative personnel can record grades. EduCTX [13] is an ambitious project for the development of a higher education credit platform based on the concept of the European Credit Transfer and Accumulation System (ECTS), a framework which has been approved by the EU. The decentralized higher education credit and grading system can offer a globally unified viewpoint for students, higher education institutions, and other potential stakeholders such as prospective employers. A prototype implementation has been built on the ARK blockchain platform [14].

Several platforms for building blockchain systems have been developed in recent years. Amongst the most popular of these are the following; Ethereum [15] is an open-source, public blockchain platform first proposed by Vitalik Buterin in 2013. Ethereum features Ether, a token (cryptocurrency) which can be used to pay for "gas", a unit of computation performed by smart contracts (scripts) which run on the Ethereum Virtual Machine (EVM). Ethereum supports a modified version of Nakamoto consensus (Bitcoin's consensus protocol). Ethereum is widely used for the development of Peer to Peer (P2P) Distributed (or Decentralized) Apps (Dapps).

4.1 Proposed Education system using BC

The proposed education system, depending on the automated examination, correction and certification is to be implemented using Ethereum. In this section, the proposed educational university system processes and the initial implementation model of the system using blockchain and NoSQL databases were explained. Ethereum is a promising platform for implementation of this system, because it is an open-source, public, blockchain-based distributed computing platform and operating system that provides smart contract functionality. Ethereum has also proven to be a common platform in higher education projects due to its smart contracts and general usage, but other platforms have been widely used as well.

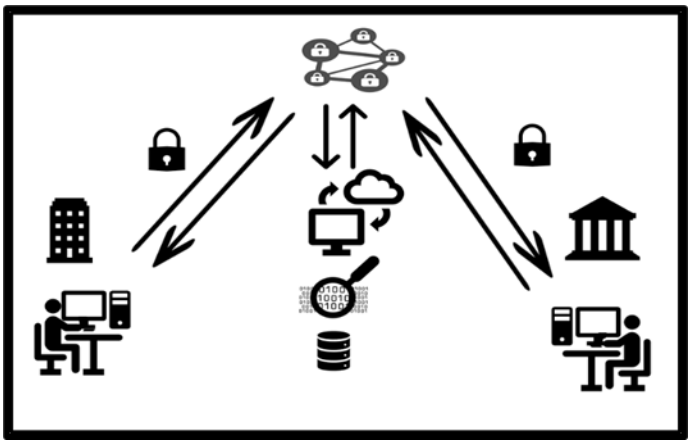

Fig. 3. Education system processes

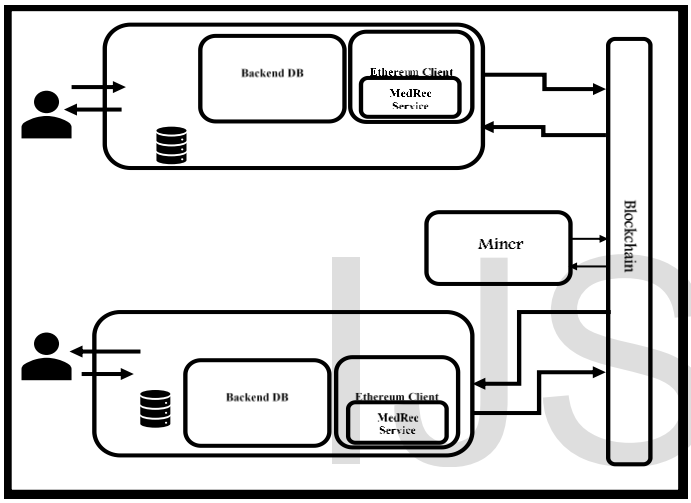

Fig. 4. Initial implementation model for the system

Fig. 3 and Fig. 4 above show the processes and the initial implementation model of the proposed educational university system. The first figure shows how the proposed automated system for correction, and certification works beginning from the student performing an online exam and submits it after entering his signature, then all the answers and the signature are encrypted and blockchained then sent to an automated university system for exams correction, and all students results records are stored after verifying the students signatures on this automated system and then all results are sent to the instructor to review them, after reviewing the results, a certificate for the student is generated and the signatures of instructor, university authorities are added to the certification, encrypted and blockchained, and sent to the automated system for storage, which in turn send at the end the certificate to the student to print it. This process protects student, instructor and university authorities data privacy, especially during transactions. The second figure shows the system implementation using the Ethereum and NoSQL database, beginning from the student which send his exam, along with his signature after encrypting and blockchaining them using Ethereum platform connected to a NoSQL database to reach the miner, here which represents the automated system for correction and certification, which makes the correction of the exam, and sends the results to the instructor for review, which in turn, appends his own signature as well as the university authorities signatures and approves the certificate generation using the Ethereum platform and the NoSQL database, then encrypts it and blockchains it to be sent to the miner for storage, and sent to the student to print the certificate at the end of the process.

5 Conclusion

The paper has presented the design of an automated blockchained system for online examination and certification based on using student, instructor and university authorities secured signatures to verify their identities and achieve authentication. The design is based on using Ethereum platform and NoSQL database for storage because they have many advantages.

References

[1] Blockchain. https://en.wikipedia.org/wiki/Blockchain.
[2] Smart Contract. https://en.wikipedia.org/wiki/Smart_contract.
[3] Ethereum. https://en.wikipedia.org/wiki/Ethereum
[4] Merkle tree. https://en.wikipedia.org/wiki/Merkle_tree
[5] V. Dhillon, D. Metcalf and M. Hooper, "Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You", 2017.
[6] D. Drescher, "Blockchain Basics, a non-technical introduction in 25 steps", *apress*, 2017.
[7] P. Jayachandran, "The difference between public and private blockchain," *IBM Blockchain Blog*, 31 May 2017. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
[8] V. Buterin. Ethereum White Paper, "A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM", 2015. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentrali--zed_application_platform-vitalik-buterin.pdf
[9] R. Kastelein. https://www.richardkastelein.com/
[10] J. Rooksby and K. Dimitrov, "Trustless education? A blockchain system for university grades," *New Value Transactions Understanding and Designing for Distributed Autonomous Organisations Workshop at DIS 2017*, 2017.
[11] T. Arndt, "Empowering university students with blockchain-based transcripts," in Proc. *CELDA 2018*, Budapest, Hungary, October 21-23, 2018.
[12] B. Yokubov, "Blockchain based storage of students career," Master degree thesis, Politecnico di Torino, 2018.
[13] M. Turkanović et al., "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112-5127, 2018.
[14] ARK Blockchain Framework. https://ark.io
[15] Ethereum. https://www.ethereum.org