Blockchain

Student’s Name

Institution

Blockchain

**Introduction**

Blockchain refers to an easy transition in creating, keeping, and updating financial records. It is a distributed ledger containing all financial records of transactions that have ever been made in cryptocurrency by many interlinked computer systems. Instead of having a single owner, records from blockchain are distributed among all users. This approach is genius because it uses a sophisticated agreement and validation to make sure that as much as there is no central owner, a single version that is agreed upon applies to all users. This system brings about a universal bookkeeping method, whereby one entry is identical and permanent with all the other participants. On the other hand, auditing is done to check the transparency of finances in a company. Issues of auditing have been on the rise as CPA auditors are unable to deliver their work due to the rise in online fraud. Since the legitimacy and originality of transactions made are protected by cryptography, the blockchain has proved to improve auditing and offer solutions in the management of cryptocurrency. Ways blockchain can improve auditing are discussed below.

**Opportunities to Apply Blockchain for Improving Auditing**

The first opportunity that blockchain can present in improving auditing is auditing smart contracts. One captivating ability of blockchain is distinct in smart contracts. It creates an avenue for computer programs to transfer assets digitally between different parties.The second opportunity is the services that auditors offer, which relate to consortium blockchains. The blockchain business offers an opportunity for the auditors to engage their practice because they will have to give assurance.The blockchain administrator is also another opportunity for auditors. Some organizations may need independent auditors in case they may require private blockchains. The last opportunity is arbitration. Blockchain technology can execute contracts (Underwood, 2016).

**Solving financial problems with blockchain solutions**

           Companies, as well as the public, expect the financial auditors to increase trust and transparency in the finances of the company. However, auditing a job is not all that easy for auditors. Sometimes the books of accounts can be adjusted to hide sketchy transactions and frauds, and auditors may lack enough information to expose fraud in a company. This is a major financial auditing issue many CPA auditors face. For instance, an unauthorized user can make and still reverse a transaction to form a scenario known as double-spending, whereby already transacted money seems like it is still in the account. This is where blockchains come in. Blockchain technology records all activities involved in transitions from when the transaction is initiated to when it is reported. This means that blockchains can make the work of CPAs easier. They do not have to run a financial statement audit since all transactions are recorded. They only need to assess if the recorded transactions are reinforced by appropriate and correct evidence.

In a blockchain, every participant is referred to as a node. They are supposed to keep a copy of the historical transaction, which is added to the ledger. They do this by comparing their copy to that of other nodes, which are synchronized in a consensual process (Gupta, 2017). Contrary to the common ledger system, nodes do not have particular rights of editing or deleting transactions. No central party exists in this case. It is oneof the reasons why blockchains are useful when trusted central parties are too expensive or unavailable (Gupta, 2017). The perception of requiring ledgers, which is uniform to all participants, has always been in existence for long. However, there are existing limitations to overcome. The major one is ordering transactions and the subsequent double-spending problems. In large networks, transactions are consistently broadcast from various nodes. These transactions reach various terminals of the network in the varying duration of time (Iansiti, &Lakhani, 2017). Therefore, it is never easy to have an order of transaction that is well defined, particularly in case two different transactions try to credit one resource. If this happens, it will cause double-spending. Besides, two parties will disagree on the party that has the right to a particular asset.

In blockchains, transactions are recorded in blocks. A transaction takes about 15 minutes to be validated, and a permanent block is created. However, these blocks do not assure authenticity because unauthorized users may tamper with transactions and make double-spending transactions. Therefore, the auditors need to check every original transaction to ensure the validity of every blockchain. Companies being audited may be the miners of the blockchains and may manipulate the records of the blockchains. Thus, an auditor ought to understand the dependability of a certain blockchain and understand if the corporation is using a public or private blockchain. Auditors can use blockchain-enabled digitization to ensure computerization and machine learning, which can alarm parties when unusual transactions are made. Thus, with blockchains, much time can be saved while performing financial audits of a company. Also, an auditor has a shoot at improving transparency by verifying the original transactions by studying all blocks created (Underwood, 2016).

**The use of smart contracts for fraud solutions**

**Smart contracts solutions architecture**

As stated, blockchains cannot guarantee total originality of the transactions as some times a user can perform double-spending transactions. Here, a company could use a smart contract. Smart contracts can be defined as digital contracts that automate transaction processes once the nodes meet the encrypted terms and conditions. Smart contracts can be incorporated into blockchains to streamline business transactions. They can offer a solution to double-spending transactions and other frauds that occur in a company. The smart contracts solutions are incorporated into a new blockchain system, and the users ought to update their software so that their transactions can now follow the new rules presented by the new contract. The smart contracts will entail terms and conditions of the arrangement between buyers and sellers, which are directly inscribed into the lines of codes. The codes are arrangements that will be incorporated in the publicly shared decentralized blockchain networks (Sharma, 2019). These codes are the basis of the contracts such that if any transaction does not follow them, then it is rejected. The auditor’s role is that of an administrator. In this case, he verifies the interface between the company’s network and the external networks and watches out for any unusual transactions.

The smart contracts will be developed using the Ethereum. The ethereum is a public blockchain that is based on a distributed operating system. It is an open source. The Ethereum comes hand in hand with a decentralized machine called the Etherum Virtual Machine (EVM). EVM uses global networks of public codes to implement scripts. Using the Ethereum also provides the network with other components, which include the mining nodes, who control transactions, gas, ether, which refers to the bitcoins, digital signatures, hash, and encryption features. The Ethereum disregards the importance of a central body, which is usually expensive or even hard to find. However, Ethereum is prone to cybersecurity threats. The feature commonly attacked is the DAO codes. Thus, the program will be tested through checking for any security issues in its codes to ensure that it is free from cyber-attacks (Sharma, 2019). Smart contracts will also promote data tokenization. Data tokens are simply a numerical illustration of data. In Ethereum blockchain, tokens can be developed to symbolize a whole or a part of actual property. These properties include gold, oil, land, stock, cash, etc. With asset tokenization, a buyer and seller can liquidize assets to ease trading (ConsenSYs, 2019). Data tokenization will be used as a protocol in the smart contracts. In a contract, protocols are vital as they standardize the transfer of assets. In this case, tokens will be used as a protocol, where trading will only be done through the exchange of tokens. This will make auditing quite easy because the actual value of a property will be represented by a specific data.

**The workflow in smart contracts**

The smart contract will function like any other contract, only that it will make transactions faster. For instance, when one is buying a very valuable item such as a car, they cannot pay cash, rather, they ought to first involve other third parties such as a lawyer, insurance, etc., and when involving these people, there is always a fee that will be involved. However, for the smart contract, all these will be overlooked. A user can buy a product directly without having to involve third parties. They will just set the terms and conditions between the two parties. Then the transaction will be made. Since the transactions can never be tampered with, the smart contract will have eliminated the need of a lawyer and other parties, making the purchase faster and cheaper. Also, there are records to prove ownership in case things do not go as planned. This will also make auditing easy, as any transactions made and the exact cost are recorded (Modi, 2018).

**Security and reliability**

**Promoting integrity in the blockchain**

The smart contracts will ensure that trustworthy transactions and arrangementsare made by unrelated parties without the need for a central body or administration by an external legal system. Smart chains promote integrity in the blockchains by ensuring that financial records in various blockchains are transparent, noticeable, and permanent. This means that the sellers, as well as the buyers, can see every transaction happening in the network. Also, once the transaction takes place, it cannot be edited. Moreover, every transaction can be tracked as from its initiation to its recording. This will ensure that there is transparency between the buyers and the sellers.

The Ethereum also provides the company with other components, which include digital signatures, hash, and encryption. There are two types of encryption offered: symmetric and asymmetric encryption. Asymmetric encryption will allow the nodes to code their messages through the use of the available public keys. When one node sends an encrypted message to a second node, the recipient can use their private key to decode the message and understand the content. This ensures security such that no one else can decrypt and understand the content of the message. For symmetric encryption, participants can use the same keys to share messages (Modi, 2018).

The hashing feature describes the process through which a series of information is transferred into another fixed series of information to regenerate new data. This feature promotes security in that it will be quite hard to change the algorithm of the new data. This way, when a transact is made, a node can generate the new information of a transaction using the hashing feature. This information can no longer be changed, and if an outsider tries to change the transactions, the node will notice. A digital signature is another way through which smart contracts on the Ethereum promote security. Digital signatures are created through the use of asymmetric keys. Every user will have their private keys, which only they will know of. When sending a message, the Ethereum will provide a chance to sign the message to assure the recipient that the message was actually sent by the authorized sender (Modi, 2018).

**Defenses to hacking, and theft**

The Ethereum has vulnerabilities to cybersecurity, and thus, the new software ought to be protected from hackers and malicious malware. The use of data tokenization is one measure for eliminating theft. Hackers will not understand the coded assets and cannot really know what to target. Hackers mostly use the DoS attacks and malware to exploit vulnerabilities in the system and lockout users, limiting them from making transactions. Thus, in this case, the software could be protected through the use of anti-viruses, which fight all malicious software such as viruses, Trojan horses, and worms. Ethereum allows for the tokenization and encryption of data, which will protect the data from being stolen by malicious users. Also, the use of a strong password is essential. These passwords ought to be unique in that hackers or other unauthorized users will not get past them. The use of password managers and biometrics strengthen passwords. Vulnerabilities could also be protected through the use of intrusion detective systems (IDS) and preventive intrusion systems (IPS), which detect any unusual activities in the blockchains and lockout the users (Horbenko, 2019).

**Implementation of the smart contracts**

Implementation of smart contracts needs the public's consent. To see to this, the new software updates will be displayedon the old software in the networks. As participants sign into their accounts, they will get an alert, and the information on smart contracts will be displayed. They will be enlightened on the importance of the contracts and how they protect their ethers. They will also be cautioned that the old software might not incorporate with the new software. Users are then given the option to update their software to adaptto the new rules presented by Ethereum blockchain.

**Solution limits, and bottlenecks**

Smart contract platforms entailone blockchain, whose network is shared. This reduces the number of transactions that can be done in a minute; the Ethereum blockchain processes just 900 transactions in a minute, unlike other accounts such as Facebook, which transact hundreds of thousands in a minute. The smart contract platform is thus an open project which works as a closed platform proprietary. Moreover, these limits in transactions have caused an issue of invalidation in transactions. In the Etherium, there is the use of both the public and private keys. Since the Etherium is a public blockchain, the network is open and could create vulnerability to nodes’' accounts. A user who uses public keys to communicate private messages will have soiled their privacy as the message can be read by everyone. Also, even if the transactions cannot be tampered with, they can also be used to trace the user's IP address. If a hacker gains the IP address of a user, then they may steal from them in other ways (Daniel, 2019).

Implementation of new contacts and the Ethereum introduces a hard fork in the network. A hard fork is a shift of rule whereby since the software is authenticating transactions according to prior rules before the implementation of new contracts, it may invalidate the new blocks formed according to the new rule. This calls for all users of the platform, i.e., the nodes to upgrade to the new software with the new smart contracts to avoid the case where some nodes are using old software and others the new software (Daniel, 2019).

Smart contracts do not necessarily require to be registered as a security. When using the blockchains smart contracts, the regulators will have full access to the terms of the agreement between the two parties. This makes it easy for the firms since they are dismissed of the compliance duties and risks of involving lawyers, waiting for contracts to be due, etc. These exemptions can be relied upon because even if something goes a miss, the parties can present evidence to the regulatory bodies even if they did not involve them at the beginning of the contract.

**Conclusion**

Blockchains that can be used to improve the profession of auditors are drive transparency. When they act as blockchain administrators, they should not give one party an advantage over the other. Auditors can exercise their skills when they handle blockchains at various stages. It is also clear that the blockchain offers a good solution to the transactions. They are distinct and transparent. It is not easy to tamper with any information. If any participant attempts to alter the information, they will be easily recognized. With the changing technology and the many things that it brings along, the blockchain is ideal and keeps people up to date. Therefore, such technologies are important because they enhance the skills of some professionals. In this case, the skills of the auditors are enhanced significantly.

References

ConsenSYs. (2019). An Exploration of 5ways Enterprises Can Benefit from Tokenization. Retrieved from <https://media.consensys.net/an-exploration-of-5-ways-enterprises-can-benefit-from-tokenization-e3110c66bcb8>

Daniel, K. (2019). Smart Contract Platforms: The Design & Its Limitations. Retrieved from <https://komodoplatform.com/limitations-of-smart-contract-platforms/>

Gupta, S. S. (2017). *Blockchain*. John Wiley & Sons, Inc.

Horbenko, Y. (2019). Using Blockchain Technology to Boost Cyber Security. Retrieved from <https://steelkiwi.com/blog/using-blockchain-technology-to-boost-cybersecurity/>

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118-127.

Modi, R. (2018). Introduction to Blockchain, Ethereum, and Smart Contracts- Chapter 1. Retrieved from <https://medium.com/coinmonks/https-medium-com-ritesh-modi-solidity-chapter1-63dfaff08a11>

Sharma, K. (2019). Best 5 Blockchain-based Smart Contract Platforms. Retrieved from <https://www.blockchain-council.org/blockchain/best-5-blockchain-based-smart-contract-platforms/>

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15-17.