Blockchain: Challenges and Applications

Pinyaphat Tasatanattakool
Faculty of Science and Technology
Rajamangala University of Technology Suvarnabhumi
Bangkok, Thailand
namenoon@msn.com

Chian Techapanupreeda
Faculty of Business Administrator
Thonburi University,
Lampoon, Thailand
wichian.tech@gmail.com

Abstract— **The technology that has had the most impact on our lifestyles in the last decade is Blockchain. A word that often arises when talking about Blockchain is Bitcoin. Many people still confuse Blockchain with Bitcoin; however, they are not the same. Bitcoin is just one of many applications that use Blockchain technology. In this paper, the authors conduct a survey of Blockchain applications using Blockchain technology and the challenges these face.**

Keywords—Blockchain; Bitcoin; smart contract; cryptocurrency; centralized; distributed

I. Introduction

Blockchain is a form of database storage that is non-centralized, reliable, and difficult to use for fraudulent purposes. Bitcoin, on the other hand, is a form of digital currency that uses a Blockchain public ledger to make transactions across peer to peer networks. Bitcoin is just one of the financial applications that use Blockchain technology, there are also others such as smart contract and hyperledger. Blockchain technology can therefore be used to create many applications.

II. Background and Related Work

Blockchain is a database used for storage in a decentralized network. However, Blockchain is not only used in financial applications. Moreover, we can design a transaction to match our application. In this section we will discuss Blockchain technology.

A. *Technical Terms*

First, it is important to clarify the meaning of several technical terms relating to Blockchain. Table I provides a list of these terms and their meaning.

TABLE I. Technical Terms

Term	Description
Decentralized	The system that stores data across the network.
Transparent	Everyone in the node and can see the ledger that share amount decentralized network.
Miner	Transaction verifier
Consensus	A v method used to verify the transaction.
Forks	The problem that arises when the node is used for different version of Blockchain.
Hash	One-way hash function to check the integrity of a transaction or message.
Node	The ledger in the Blockchain system.
Timestamp	A date and time in the computer system used as an electronic time stamp for the transaction.

B. *Blockchain*

Wikipedia defines Blockchain as *[2] "…a decentralized and distributed digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network."* Figure 1 describes a formation of Blockchain where the longest chain, called the main chain (active chain), comes from the genesis block and the orphan block is the block that exists outside the main block. According to Christian Cachin *et al.* [7] the Blockchain has 4 elements that are replicated: the ledger, cryptography, consensus and business logic. For more information about these characteristics the reader can consult [7].

C. *Bitcoin*

The Bitcoin was invented by an unknown group or person under the pseudonym Satoshi Nakamoto as stated in "Bitcoin: A peer-to-peer electronic cash system.", a research study completed after the United States Subprime mortgage crisis [6] in 2008. CNNMoney [3] define Bitcoin as *"…a new currency that was created in 2009 by an unknown person using the alias*

Satoshi Nakamoto. Transactions are made with no middle men. There are no transaction fees and no need to give your real name. Wikipedia, on the other hand describe Bitcoin as "*… a worldwide cryptocurrency and digital payment system called the first decentralized digital currency, as the system works without a central repository or single administrator [4].*" Thus, we can infer that Bitcoin is a cryptocurrency and digital payment system that is decentralized with no middle men and no transaction fees, however the miners will get their reward if they can prove the transaction, otherwise known as proof of work (PoW) or Proof of Stake (PoS).

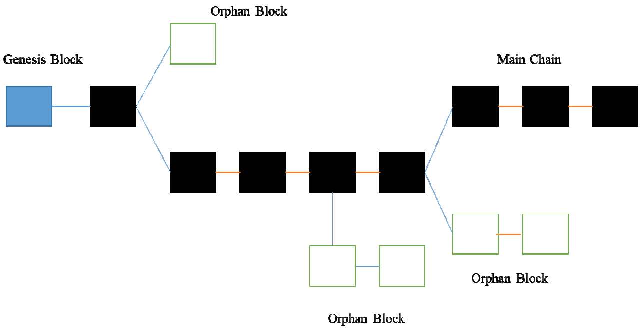

Fig. 1. A Blockchain formation

III. Blockchain Applications

As noted previously, the Blockchain is not a Bitcoin but a form of database stored in a decentralized system. The Blockchain can therefore be adapted for use in a variety of areas. The following are just some of the Blockchain applications active today.

A. *Financial Applications*

- Bitcoin

The Bitcoin or digital currency was first introduced by an anonymous person or group under the alias Satoshi Nakamoto in 2008 [1]. Bitcoin uses a Blockchain public ledger to make transactions across a peer to peer network. Examples of active Bitcoins are Bitbond, BitnPlay, BTC Jam, Codius and DeBuNe.

- Ripple

The Ripple is a currency exchange, remittance and real-time gross settlement system (RTGS) [8] that uses ripple protocol across a peer-to-peer network, a decentralized exchange that focuses on the banking market. Other well-known currency exchange and remittance systems are Coinbase, BitPesa, Billion, Stellar, Kraken and CryptoSigma.

B. *Non finanancial Applications*

- Ethereum

A Next-Generation Smart Contract and Decentralized Application Platform was created by a cryptocurrency researcher and programmer named Vitalik Buterin [5]. It uses a Blockchain-based distributed computing platform with a Turing complete scripting language that enables the processing of smart-contracts on the Blockchain.

- Hyperledger

The Hyperledger is a Linux foundation project that develops Blockchain technologies for business, supporting only registered members. Hyperledger is an open source collaborative effort created to advance cross-industry Blockchain technologies. This is a global collaboration, hosted by The Linux Foundation, which includes leaders in finance, banking, the Internet of Things, supply chains, manufacturing and technology.

There are also many other non-financial applications using Blockchain technologies such as Election Voting (Follow My Vote), Smart Contracts (Otonomos, Mirror, Symbiont), and Blockchain in IoT (e-Plug, Filament).

IV. Challenges

Blockchain technology can also be used in various fields of business. One interesting implementation of Blockchain technology is in the healthcare system. This satisfies all stakeholders such as Hospitals, Healthcare, Health Authorities by meeting information consumer's needs and protecting patient privacy by using Blockchain to pay fees with Bitcoin. In the paper system, if information consumers need to see a patient's health record they had to filled in a request form and sent it to the registration office for approval. After receiving approval, the information consumer will pay a copy fee to the cashier and obtain a bill of receipt. The information consumer then shows the receipt to the registration office to obtain a copy of the patient's health record. However, a patient's health records can be lost, or copies may be made for illegal purposes. The concept of an electronic health records system using Blockchain technologies is depicted in Figure 2.

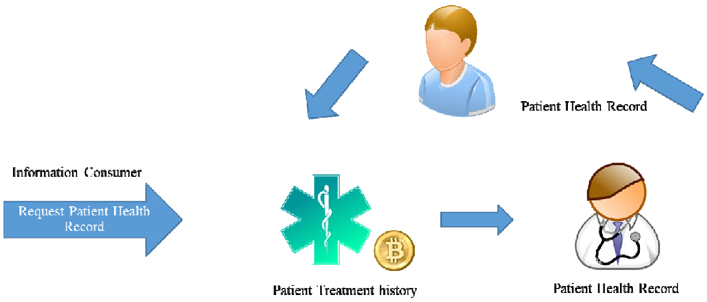

Fig. 2. E-health system using Blockchain

When an information consumer sends a request for a patient's health records to an issuer (hospital or healthcare), and the issuer agrees with the information consumer, the Bitcoin will be placed. Before sending a patient's health records to an information consumer, approval from a primary doctor and the patient is needed so that only specific records are sent, for example mental health records. The details of this process will be explained in subsequent research.

V. CONCLUSIONS AND FUTURE WORK

We have defined Blockchain as a form of database used to store data in a distributed system. We also clarified the differences between Blockchain and Bitcoin. Future work will focus on implementing Blockchain technology for use in electronic health records. It will consider how an external party (external stake holder) can use or request a patient's health records from the hospital or health authority without contravening patient privacy.

ACKNOWLEDGMENT

The authors would like to thank the Rajamangala University of Technology Suvarnabhumi and Thonburi University for their support and sponsorship of this research.

REFFERENCES

[1] Nakamoto, S., 2012. Bitcoin: A peer-to-peer electronic cash system, Oct,2008.

[2] Wikidia,“Blockchain”,https://en.wikipedia.org/wiki/Blockchain #cite_note-te20151031-1.

[3] CNNMoney “What is Bitcoin” http://money.cnn.com/infographic/technology/what-is-Bitcoin/

[4] Wikipedia, “Bitcoin”,https://en.wikipedia.org/wiki/Bitcoin.

[5] Vitalik Buterin, “Ethereum and The Decentralized Future". Future Thinkers Podcast. 2015-04-21. Retrieved 2016-05-13.

[6] Hyperledger,“AboutHyperledger”,https://www.hyperledger.org /about.

[7] Christian C., Elli A., Angelo De Caro, Andreas K., Mike O., Simon S., Alessandro S., Marko V,. et al, “Blockchain, cryptography, and consensus”, IBM Research Zurich, June 2017.

[8] Ripple, “RippleNet”, https://ripple.com