CHAPTER 2
LITERATURE REVIEW

In this chapter, the focus will cover on the technologies that are used by the blockchain and the examination system. Besides that, this chapter will discuss more about Ethereum blockchain technology and its critical component to have a better understanding about the project.

2.1 Introduction

In this chapter, the focus will cover on the technologies that are going to be used to develop the secured exam management system. Besides that, this chapter will also discuss more about the blockchain technology, decentralized website and the smart contracts in more details. Some related works will also be included so that the readers can have a better understanding. After conducting a lots of research by reviewing the articles and journal from past researchers, eventhough the blockchain technology is famous for its security but it is not widely used in developing a website.

2.2 Overview

Data security, integrity, availability and confidentiality are some of the crucial point in data management. In this era advanced technology, where everything is stored digitally in order to replace the traditional ways of data management, which have a lot of loophole in it (Karl, 2017). However, there is also a downside of it. When we are talking about sensitive data or information in can be represent in various form from sound, picture and document and this digital data are expose to threat whether from inside or outside. A majority of system today, used a client-server based model or involved third parties in the process. Therefore, the data is expose to a lot of threat such as man-in-the-middle attack (MITM), data tampering and distributed denial of service (DDoS). A system such as decentralized web application that implement a

blockchain technology to manage the data not only save a lot of trouble for the user but also provide a more secure environment (Jacobovitz, 2016)

2.3 Blockchain Technology

2.3.1 Architecture

Blockchain is a sequence of block and each of the blocks refer to the previous block hash contained in the block header. Each of the blocks also have a parent block except for the genesis block, which is the first block that are created in the blockchain. The figure 2.1 below illustrate the architecture of the blockchain.

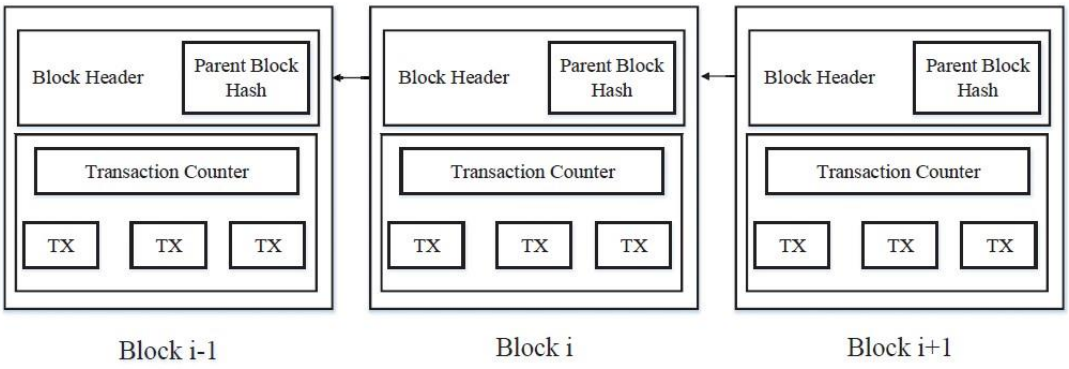

Figure 2.1 Architecture of Blockchain

A block inside the blockchain consists of two parts, which the block header and the block body as shown in figure 2.2. In particular, the block headers includes a couple of field inside it, which is a block version, merkle tree root hash, timestamp, nBits, nonce and parent block hash.

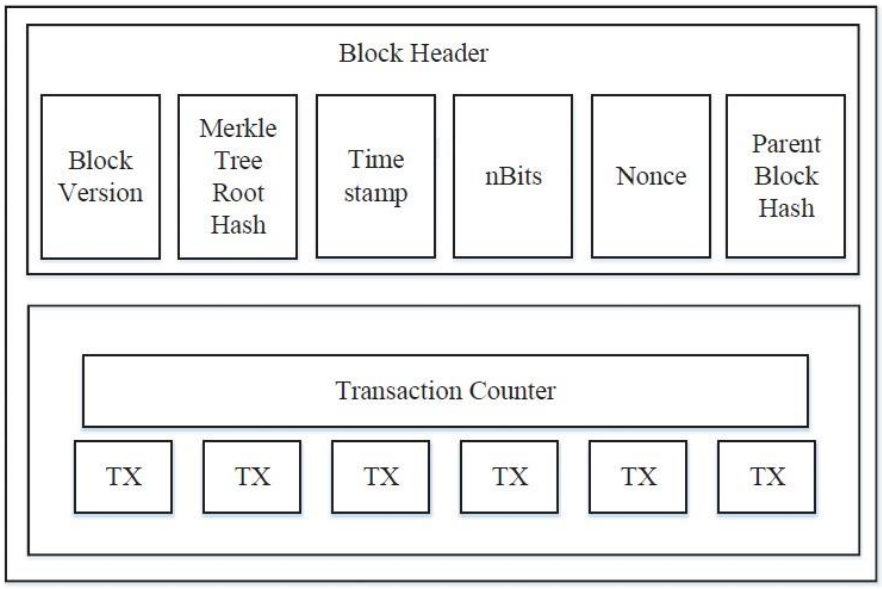

Figure 2.2 Block Structure

Table 2.1 Block Structure Description

Field	Description
Block version	Indicates which set of block validation rules to follow
Markle tree root hash	The hash value of all the transactions in the block
Timestamp	The timestamp of the block in UNIX
nBits	The target threshold of a valid block hash
Nonce	The counter used by miners to generate a correct hash
Parent block hash	A 256-bit hash value that points to the previous block

The block body on the other hand, is composed of a transaction counter and transactions. The size of the block and the size of each transaction is important to determine the maximum number of transaction that can be stored in the block.

Blockchain is also decentralised, which means that the blockchain sits on every nodes of the network (Toshendra, 2018). Nodes of the network or network node is participant or user in the network that can receive, create, store or send data to the other nodes. The blockchain contains by each nodes are the exact duplicate in the network. Due to the the decentralised nature of blockchain, no central database is required in the system to host the data or involvement of third parties. By storing data across

its peer-to-peer network, this is not only benefits the user by making the information public and easily verifiable but also prevent a hacker to temper or corrupt the information because there is no central point of failure to be exploit or taken down (Michael et al., 2016).

There are millions of websites that are up and running, and the vast majority of them are based on centralized server-client model. Some are distributed and only a few of them are decentralized (Siraj, 2016). Figures 2.3 below show these three models for web hosting.

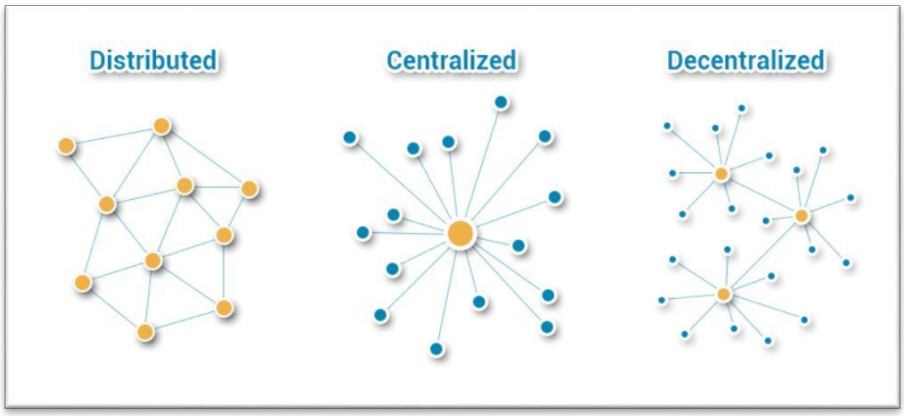

Figure 2.3 Types Web Hosting

Centralized systems are currently the most favorite model for websites application. Centralized system directly controls the flow of information from one single center and the operation of the individual units. While distributed means that the computation are handled by the multiple nodes inside the network instead of just one. Decentralized on the other hand, means that no node is instructing any other nodes as to what to do. (Siraj, 2016).

Blockchain database is managed using a peer-to-peer network and a distributed time stamping server (Don et al., 2016). The peer-to-peer (P2P) computing itself is a distributed application architecture that partitions task or workloads between peers. This allows the participants to verify, audit or share the information among themself. In peer-to-peer networks, the exchange of data is still directly done using the TCP/IP network, but at the applications layer peers

are able to communicate with each other directly, via the logical overlay links. Thus bypassing the need for traditional trusted third parties.The figures 2.4 below shows the structure of peer-to-peer network.

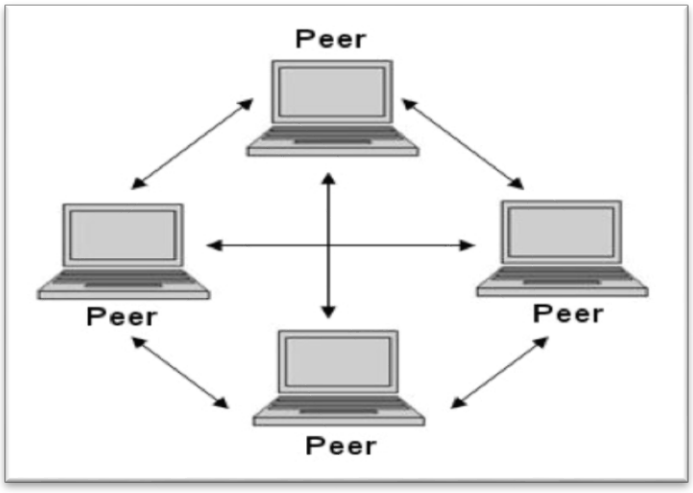

Figure 2. 4 Peer-To-Peer Network Topology

2.3.2 Consensus Model

Blockchain platforms use a variety range of consensus models whether in their original form such as Proof-of-Work (PoW). There are also a few new models proposed such as Proof-of-Stake (PoS) providing advantages desired over the original model (Arati, 2017).

a) Proof of Work (PoW)

Ethereum is one of the example of blockchain platform that supports smart contracts and use Solidity programming language for writing the smart contracts and a virtual machine called Ethereum Virtual Machine (EVM) for executing the smart contacts code on Ethereum nodes (Arati, 2017). Same as bitcoin, Ethereum network is an open source that allows any user to download the Ethereum client and join the Ethereum network. The crypto currency used by Ethereum are called Ether, which is used to pay for any data written to the blockchain and paid to miner. Ether also serve

as anti- spamming and DDOS defense measure (Arati, 2017). Ethreum is designed to be used by any kind of application that requires blockchain support and secure the integrity of data. Figure 2.5 below shows the structure of smart contract applied for transportation system.

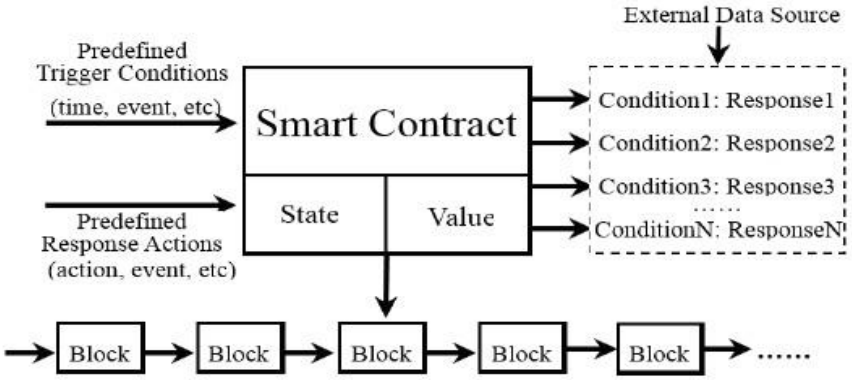

Figure 2.5 The Structure of Smart Contracts

The figure 2.5 depicted that smart contracts are a group of self-verifying, self-executing and self-enforcing state-response rules that is stored on the blockchain (Yong, 2016). When the predefined conditions are triggered, the smart contracts will self-executed and trigger a corresponding response action all by itself without any intervention of third parties (Yong, 2016).

The main purpose of PoW is to prevent cyber-attack such as distributed denial-of- service attack (DDoS) which has the purpose of exhausting the resources of a computer system by sending multiple fake requests. With PoW consensus model, Ethereum uses PoW called Ethhash to counter 51% attacks that bitcoin is susceptible to (Arati, 2017) by providing a fast confirmation times and build ASIC resistance. The Ethhash uses two technique for combating mining centralization which is memory hardness and GHOST. Memory hardness is the ability of the computer to move data around memory, which have been designed perfectly fine but are not efficient on ASICs. Therefore, by making the algorithm ASICs resistant, it prevents any large companies from seizing control of the mining power. As for GHOST, the node producing uncle block (orphaned blocks) are given a less reward to encourage them to continue with the latest block in the Ethereum blockchain (Arati, 2017).

b) Proof of Stake Model (PoS)

Proof-of-Stake algorithms are created to overcome the disadvantages of PoW algorithms in terms of the high electricity consumption involved in mining operation (Arati, 2017). With PoS instead of user, spending their money to buy mining equipment to engage in PoW algorithm and winning a mining reward, with PoS the user can use the money to buy crypto currency and use it as stake to buy proportionate block creation by becoming a validator. The PoS algorithm selects validators for block creation randomly; therefore, no validator can predicts it turns in advance. Unlike PoW, where the user need to compete with each other to find a solution for the mathematical problems and there is also no block reward, so the miners can only take the transaction fees.

The Ethereum PoS algorithm called casper uses the concept of security deposit and bets to achieve consensus (Arati, 2017). In this method, the validators stake a portion of their own Ether as stake. When they discover a blocks which they think can be added to the chain, the will validate it by placing a bet on it. If the block get accepted, the validators will get a reward based on their bets. However, it the validator acts in malicious manner, they will be punished and all of their stakes is going to be slash.

2.3.3 Blockchain Application

With the modern internet where almost we stored every bit of information and assets online, without a doubt we thrive for a protection in order to protect our valuable assets and ensure its integrity and validity. With blockchain, the assest are stored in an encoded form on a network-to-network chain called blockchain. By doing so each participant can sees who is doing business with whom. This is not only protects the data integrity and validity but also prevents theft as the blockchain is almost tempered proof. Not only that, it also quickens the process, reduces error and eliminated the involvement of the third parties. There are a lot of fields affected by the emerging of this new technology such as transportation system and online transaction.

a) Transportation System

The rapid development of modern sensing in the recent years have resulted in the industry growth in intelligent transportation systems (ITS). However the ITS suffer a few critical issues such as the evolving trends have grown towards centralization which will might causes the service to be temporarily unavailable due to malicious attack and the lack of trust issues among ITS entities (Yong, 2016). With a blockchain-based ITS it provides decentralization so that there is no central point of failure in the system, promoting trusted communication and cooperation among vehicles, chronological data and programmability (Yong, 2016).

Figures 2.6 below illustrate the ITS-Oriented Blockchain Model, which consist of seven-layer conceptual model for characterizing and standardizing the typical architecture and major components of blockchain system (Yong, 2016).

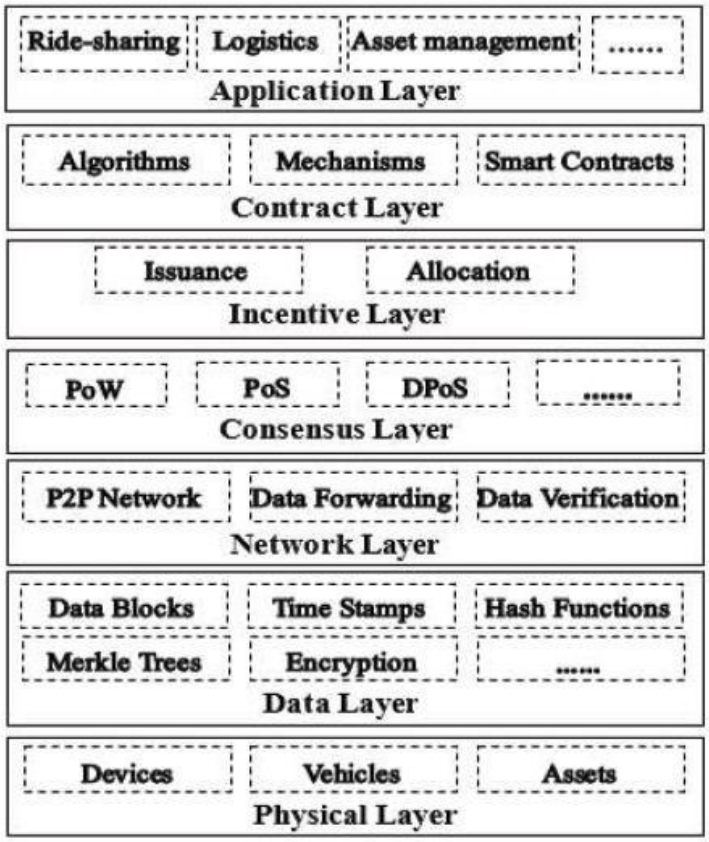

Figure 2.6 ITS-Oriented Blockchain Model

Table 2.2 ITS Blockchain Model

Layer	Description
Physical Layer	▪ The key techniques in this layer is IoT, which enjoys enhanced device security. ▪ Contains a chip specifically design for connecting to the Internet and for mining.
Data Layer	• Provides the chained data blocks including asymmetric encryption, time stamping, hash algorithms and Merkle trees.
Network Layer	• Specifies the mechanism of distributed networking, data forwarding and verifications. • Topologically modelled as a P2P network.
Consensus Layer	• Packages all consensus algorithms to validate the data.
Incentive Layer	• Incorporates economic reward into blockchain and specifies its issuance and allocation mechanism. • Once a new block is created, a certain amount of coins will be generated as reward to encourage participant in data verification.
Contract Layer	• Packages various scripts, algorithms and smart contracts which served as activators to the static data. • Control and manage both physical and digital assets in ITSs, making them programmatic "smart properties".
Application Layer	• Packages potential application scenarios and use cases of Blockchain ITS.

b) Open Bazaar

OpenBazaar is like an online e-bay with no central server involvement at all. By using the peer-to-peer client architecture, it avoids any interruption from government entity to restrict access on user and does not operates under the approval of any laws. Without the involvement of third parties, the buyer can connect directly to seller to buy goods without any transaction fee.

OpenBazaar application is actually two programs in one, the OpenBazaar server is the back end application which allows OpenBazaar to function and each user need to runs the server in order to connect to the network. The next program is the OpenBazaar client which is the front end application that allows user to communicate, control the server and provide the visual interface for the user. The server does not necessarily to be run on the user's computer but can also be run on another computer such as Raspberry Pi to host the user store.

2.4 Examination System

Conducting an examination is important to evaluate the student understanding in the subject that they are taking. Therefore, it is very important to ensure its integrity and who have access to view or edit it to prevent any paper leakage because the process of making it is time consuming. There are a lot of types of examination from handwritten, oral to online examination. For the handwritten, the question paper need to be made by the lecture or teacher itself before it was chosen to be used on the examination day.

2.4.1 Handwritten Examination

Table 2. 3 Staff Involved and Responsibilites

Staff	Responsibilities
Dean	▪ Dean of a faculty of Computer Sciences and Mathematics is a staff that we appointed by the vice chancellor to accept the circular preparation of question papers from BPA. ▪ Inform about the circular preparation of question papers from BPA to TD(A) for the next step.
TD(A)	▪ Distribute circulars to all academic staff (lecturers) and Acedemic Management Office. ▪ Monitor the preparation of question papers following the date, which is set by CPA.
Provider (Penyedia)	▪ FSKM lecturer (master campus or branch) who teaches a code in the current semester that provides question papers and answer schemes. ▪ Prepare the exam papers and answer schemes. ▪ Submit the question paper and answer scheme to the General Provider (Ketua Penyedia).

General Provider (Ketua Penyedia)	▪ Formulate and set up at least one set question paper and answer scheme. ▪ Correct the question paper and the answer scheme if needed. ▪ Submit the question paper and answer scheme to the vetter. ▪ Deliver the documents to the Office of the Academic Management in the following manners. ▪ The finalized exam papers and answer scheme are in the form of hard copy and soft copy. ▪ Customer Product Form (signed by the General Provider and Vetter). ▪ Staff Recognition Form.
Vetters	▪ Check and ensure the structure and contents of the paper questions reach the prescribed cognition level. ▪ Submit the reviewed question papers and answer schemes to the General Provider (Ketua Penyedia).
Central Examination Committee (JK Peperiksaan Pusat Pengajian)	▪ Ensure the finalized question paper provided by the Provider follows the guidelines that has been set by CPA. ▪ Ensuring the Customer Product Form and Staff Recognition Form has been filled and completed by the General Provider. ▪ Submit the finalized question paper and answer scheme to the Office of Academic Management.
JKPep / PE 1 & 2	▪ Collect all the finalized question papers and answer schemes. ▪ Provide a copy of the answer scheme for all involved campuses branch. ▪ Record the submission of question paper and answer scheme from the School Examination Committee into the Question Paper Receipt Form.

The procedure for the preparation of final examination paper in Universiti Teknologi Mara (UiTM) and responsibilities can be illustrate in the form as flow chart shown in figure 2.7 below (Noorwahida, 2016).

Carta Alir Prosedur Penyediaan Kertas Soalan Peperiksaan Akhir

Orang yang bertanggung jawab	Aliran kerja	Proses Kerja	Rekod
		Mula	
Dekan		Terima arahan dan edar	Peraturan Penyediaan Kertas Soalan [600-FSKM(2/1/3)]
KP		Kenalpasti Penyedia dan PK	
Dekan / TD(A)		Keluarkan surat lantikan kepada Penyedia dan PK.	Surat Lantikan (600- FSKM(2/3/15)]
Penyedia		Sedia kertas soalan peperiksaan dan skema jawapan	
PK		Semak kertas soalan mengikut format yang ditetapkan dan skema jawapan.	Borang *Vetting Sheet* FSKM/AKA/BSV/2010
	tidak	Kelulusan	
Penyedia	ya	Serah kertas soalan dan skema jawapan kepada Koordinator/KP	
	A		

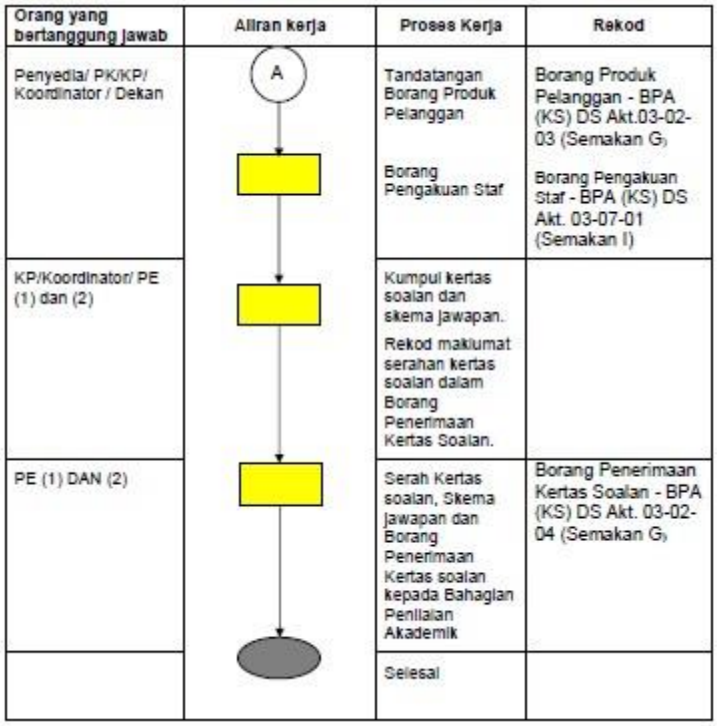

Figure 2.7 Flowchart for the Drafting Process of Exam Question Paper

2.4.2 Online Examination

Another approach to conduct an examination system is by making it online, which will save cost in printing, lessen the workload of the lecturers to draft a new examination question paper by recycling the past question, and randomly generate the exam paper in standard format and its answer could be output. The examination system could also be easily update and add questions to the question bank to make the teaching content developing with the technology synchronously (Zhaou, 2012).

2.5 Related Works

There are many developers and researcher that tried to enhance their method of handling the examination process be it manually through written test or an online examination. This topic will discuss and differentiate every researcher development based on their techniques to develop the system, features of the system and domains.

The comparison will be further explain by comparing each of the technique, feature, domain and comparison with blockchain technology.

2.5.1 Technique

In the article “Research and Development of Online Examination System” written by Zhao et al., in 2012. The authors elaborate about the importance of examination system to separate teaching and testing through an online examination. The examination system was developed with Java Web technology and the combination of client- side programming and server-side programming. The systems uses Java Web technology, which is JSP or Java Server Pages. The developers use JSP to create a dynamically generated web page that allows Java code to be interleaved with static web markup content.

Next, in the article written by Fagbola et al., 2013 about “Computer-Based Test (Cbt) System for University Academic Enterprise Examination”. The author emphasizes on the uses of online examination to replace the problems faced on writing examination method by using Microsoft Visual Studio 2012 and Microsoft SQL Server 2008 for developing the CBT system.

In the article written by Deepankar et al., 2016 about “ONLINE EXAMINATION SYSTEM”. The author emphasizes on conducting examination via online environment. The online examination system uses Random Number Generators (RNG) to produces a sequence of zeros and one bits, that may be together combined into the sub-sequences or blocks of random values for the purposes of generating a random question.

In the article written by Xueping et al., 2017 about “ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability”. The developers developed ProvChain on a blockchain network to monitored user operations in real time to collect provenance data and stored it in the blockchain network.

Finally, in the book “Decentralized Applications” written by Siraj in 2016, the author explained about developing a decentralized web applications, which operated

using a peer-to- peer technology, and a few running web application such as OpenBazaar. In OpenBazaar trust between users is establish through proof-of-burn and proof-of-time lock.

2.5.2 Features

Zhao et al., 2012 develop an online examination system using JSP model 1. The system have a few highlighted features such as the it is possible to add, delete, and modify the question paper stored in the database. The system also equipped with exam paper generating function according to specified requirements. The student user could also benefit from the system login the system at any time within the campus network, self-test online, and understand their learning level.

Fagbola et al., 2013 develop a Computer- Based test (Cbt) that uses Microsoft SQL Server 2008 and Microsot Visual Studio 2012 to create a system that provide a time analysis of responses to the question level and includes video in questions. The system also used a question banks and randomization of questions and response orders to reduce cheating and automated analysis of results from entire candidate.

Deepankar et al., 2016 uses JSP and JavaBeans to develop a system that can auto-generate multiple choice test paper and works in business logic tier to react to customer demand.

Xueping et al., 2017 developed ProvChain architecture to collect and verify cloud data provenance by embedding the data into blockchain transactions. The ProvChain operates mainly in three phases; the first one is provenance data collection. Once the user performs actions on the data files in the cloud, the corresponding operations are recorded. For this phases, only RecordID, Date and Time, Username,Filename, AffectedUSer and Action attributes are recorded. ProvChain is built on top of an open source application called ownCloud to collect the provenance data. Next, is the phase of provenance data storage, for provenance data storage, they use Tierion API to publish data records to blockchain network. The in the last phase which is provenance data validation, the provenance auditor will request the

blockchain receipt via Tierion API. The blockchain receipt contains information of the blockchain transaction and Merkle proof are used to validate the transaction.

Finally, in the book of "Decentralized Applications" written by Siraj in 2016, the author exercised more on using OpenBazaar network. User in OpenBazaar network is a node in the P2P network. Every user is assigned three roles that they can build on which is merchant, buyer or arbiter. The currency presently in use is Bitcoin. The merchant have the ability to communicate with their buyers, either directly on OpenBazaar using a messaging protocol built on ZeroMQ or by using a third-party communication protocol.

2.5.3 Domain

From the obervation, Zhao et al., 2012 and Fagbola et al., 2013 develop a system, which covers the education, information technology and programming domain. Deepankar et al., 2016 also cover the same domain as the first two system but he added cryptography to further enhance the system security. The remaining two also have the same domain, which is developing a security system but at the same time, they implement it in different areas. For Xueping, Sachin, Deepak, Charles, Kevin and Laurent, 2017 project, the implement it on cloud. Which as discuss, they used the blockchain to collect, store and validate data on cloud environment. While, Siraj, 2016 project he decided to implement a blockchain to create an open source market that uses the bitcoin currency for trading purposes.

2.5.4 Comparison with Secure Exam Question Management System

In the Zhao et al., 2012 project, the system uses a client / server model while the SEQM uses decentralized model to host the website and stored the data to eliminate central point of failure. Their project also does not implement security measure therefore the integrity of the question paper could be question as any unauthorized could temper with the question. The access to system also restricted within the campus network to limit the user accessibility will result in troubling the user.

In Fagbola et al., 2013 project, same as the first project is used a centralized database to store all the data which creates a central point of failure. The project also did not implement any other security measure beside password. Therefore, it is susceptible to cyber-security attack. The system can only support multiple choice and structured question, unlike SEQM where the question paper are changed every year and the support theory based questions because it was made by a human and not recycling past question paper.

In Deepankar et al., 2016 project, it rely on examination office to create and secure the inquiry paper. Meanwhile, SEQM uses an Ethereum based to ensure the integrity of the document and eliminates any third parties involvement. The system also only produces multiple-choice questions but not structured or theory based questions like SEQM.

In the Xueping et al., 2017 project has several advantages that provide a secured and reliable cloud. In the project, there is a few disadvantages such as the data is stored in cloud. Therefore, the involvement of third parties is still there. The client might not trust this project this entirely unlike a SEQM, which uses a peer- to-peer network. The development process of the project is also a lot more complex than SEQM.

Finally, in Siraj, 2016 project. The author did use a P2P network called OpenBazaar network but still the OpenBazaar are still in alpha phases. Therefore there is a risk that Bitcoin can be stolen because of the lack of reputable notaries and reputation takes time to build.

2.5.5 Summary of Related Works

Table 2.4 Comparison of Related Works

Title / Author	Domain	Technology	Strength	Weakness	Limitation
Research and Development of Online Examination System (Zhao et al., 2012)	▪ Education ▪ Information Technology ▪ Programming	▪ JavaScript ▪ JSP ▪ Web Application ▪ HTML ▪ Tomcat	▪ autogenerate exams question ▪ question management ▪ able to generate the question type, difficulty and chapter for the exam paper	▪ Client/Server model ▪ No security implementation	▪ access are restricted within the campus network
ONLINE EXAMINATION SYSTEM (Deepankar et al. , 2016)	▪ Education ▪ Information Technology ▪ Cryptography	▪ Random number generator algorithm ▪ HTML ▪ JSP ▪ JavaBeans ▪ MS ACCESS ▪ Tomcat	▪ auto-generating test paper algorithm ▪ Business logic tier(react to customer demand)	▪ rely on examination office to create and secure the inquiry paper	▪ only produce multiple choice question

Computer-Based Test (Cbt) System For University Academic Enterprise Examination (Fagbola et al.,2013)	▪ Education ▪ Information Technology	▪ HTML ▪ Microsoft Visual Studio 2012 ▪ Microsoft SQL Server 2008 ▪ Macromedia Dreamweaver 8.0	▪ Automated analysis of result ▪ Include video in question ▪ Auto-generate exams question ▪ System run on distributed networks	▪ All of the data are stored in a single/centralized database ▪ No security measure other than password implement in the system	▪ The system only support multiple choice, structured question and not theory based questions
A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability (Xueping et al., 2017)	▪ Security ▪ Information Technology	▪ Cloud data storage ▪ ProvChain ▪ Merkle tree	▪ Enable cloud auditing ▪ Preserve user privacy ▪ Increase availability	▪ The development process is more complex than SEQM.	▪ The involvement of third parties to stored data in cloud
Decentralized Applications (Siraj, 2016)	▪ Security ▪ Information Technology	▪ ZeroMQ ▪ Proof of Burn ▪ Proof of Time lock	▪ Provides an online trading market. ▪ Decentralized ▪ The user are able to communicate with each other	▪ Bitcoin can be stolen ▪ Storing data in local SQLite data store	▪ Lacks of internal currency

2.6 Summary of Related Works

In conclusion, the concepts of blockchain have been widely used in the real environment. In addition, each of the system have different method on how to secure the system and the digital asset from being tamper or stolen. The used of blockchain also provides availability as it operates using mostly P2P network meaning that the chance for the network to collapsed is nearly zero as long as there is one nodes up and running. This chapter also shows that there are a few different ways to implement a blockchain whether using a smart contracts or asymmetric cryptography.