ORTA DOĞU TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

TEZ ŞABLONU ONAY FORMU
THESIS TEMPLATE CONFIRMATION FORM

1. Şablonda verilen yerleşim ve boşluklar değiştirilmemelidir.
2. Jüri tarihi Başlık Sayfası, İmza Sayfası, Abstract ve Öz'de ilgili yerlere yazılmalıdır.
3. İmza sayfasında jüri üyelerinin unvanları doğru olarak yazılmalıdır.
4. Tezin son sayfasının sayfa numarası Abstract ve Öz'de ilgili yerlere yazılmalıdır.
5. Bütün chapterlar, referanslar, ekler ve CV sağ sayfada başlamalıdır. Bunun için **kesmeler** kullanılmıştır. **Kesmelerin kayması** fazladan boş sayfaların oluşmasına sebep olabilir. Bu gibi durumlarda paragraf (¶) işaretine tıklayarak kesmeleri görünür hale getirin ve yerlerini **kontrol edin**.
6. Figürler ve tablolar kenar boşluklarına taşmamalıdır.
7. Şablonda yorum olarak eklenen uyarılar dikkatle okunmalı ve uygulanmalıdır.
8. Tez yazdırılmadan önce PDF olarak kaydedilmelidir. Şablonda yorum olarak eklenen uyarılar PDF dokümanında yer almamalıdır.
9. **Bu form aracılığıyla oluşturulan PDF dosyası arkalı-önlü baskı alınarak tek bir spiralli cilt haline getirilmelidir.**
10. Spiralli hale getirilen tez taslağınızdaki ilgili alanları imzalandıktan sonra, Tez Juri Atama Formu ile birlikte bölüm sekreterliğine teslim edilmelidir.
11. Tez taslağınız bölüm sekreterliğiniz aracılığıyla format ve görünüm açısından kontrol edilmek üzere FBE'ye ulaştırılacaktır.
12. FBE tarafından kontrol işlemleri tamamlanan tez taslakları, öğrencilere teslim edilmek üzere bölüm sekreterliklerine iletilecektir.
13. Tez taslaklarının kontrol işlemleri tamamlandığında, bu durum öğrencilere METU uzantılı öğrenci e-posta adresleri aracılığıyla duyurulacaktır.
14. Tez taslakları bölüm sekreterlikleri tarafından öğrencilere iletileceği için öğrencilerimizin tez taslaklarını enstitümüzden elden alma konusunda ısrarcı olmamaları beklenmektedir.
15. Tez yazım süreci ile ilgili herhangi bir sıkıntı yaşarsanız, **Sıkça Sorulan Sorular (SSS)** sayfamızı ziyaret ederek yaşadığınız sıkıntıyla ilgili bir çözüm bulabilirsiniz.

1. Do not change the spacing and placement in the template.
2. Write defense date to the related places given on Title page, Approval page, Abstract and Öz.
3. Write the titles of the examining committee members correctly on Approval Page.
4. Write the page number of the last page in the related places given on Abstract and Öz pages.
5. All chapters, references, appendices and CV must be started on the right page. **Section Breaks** were used for this. **Change in the placement** of section breaks can result in extra blank pages. In such cases, make the section breaks visible by clicking paragraph (¶) mark and **check their position.**
6. All figures and tables must be given inside the page. Nothing must appear in the margins.
7. All the warnings given on the comments section through the thesis template must be read and applied.
8. Save your thesis as pdf and Disable all the comments before taking the printout.
9. **Print two-sided the PDF file that you have created through this form and make a single spiral bound.**
10. Once you have signed the relevant fields in your thesis draft that you spiraled, submit it to the department secretary together with your Thesis Jury Assignment Form.
11. Your thesis draft will be delivered to the GSNAS via your department secretary for controlling in terms of format and appearance.
12. The thesis drafts that are controlled by GSNAS, will be sent to the department secretary to be delivered to the students.
13. This will be announced to the students via their METU students e-mail addresses when the control of the thesis drafts has been completed.
14. As the thesis drafts will be delivered to the students by the department secretaries, we are expecting from our students no to insist about getting their theses drafts from the Institute.
15. If you have any problems with the thesis writing process, you may visit our **Frequently Asked Questions (FAQ)** page and find a solution to your problem.

☒ **Yukarıda bulunan tüm maddeleri okudum, anladım ve kabul ediyorum. / I have read, understand and accept all of the items above.**

Name : Salar
Surname : Ahmadisheykhsarmast
E-Mail : salar_ahmadi69@yahoo.com
Date :
Signature : ________________________

SMART CONTRACT SYSTEMS FOR GUARANTEED AND TIMELY PAYMENT OF CONSTRUCTION PROJECTS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

SALAR AHMADISHEYKHSARMAST

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CIVIL ENGINEERING

JANUARY 2020

Approval of the thesis:

SMART CONTRACT SYSTEMS FOR SECURE AND TIMELY PAYMENT OF CONSTRUCTION PROJECTS

submitted by **Salar Ahmadisheykhsarmast** in partial fulfillment of the requirements for the degree of **Master of Science** i**n Civil Engineering, Middle East Technical University** by,

Prof. Dr. Halil Kalıpçılar
Dean, Graduate School of **Natural and Applied Sciences** ____________

Prof. Dr. Ahmet Türer
Head of the Department, **Civil Engineering** ____________

Prof. Dr. Rifat Sönmez
Supervisor, **Civil Engineering, METU** ____________

Examining Committee Members:

Prof. Dr. İrem Dikmen Toker
Civil Eng., METU ____________

Prof. Dr. Rifat Sönmez
Civil Eng., METU ____________

Assist. Prof. Dr. Aslı Akçamete Güngör
Civil Eng., METU ____________

Assist. Prof. Dr. Güzide Atasoy Özcan
Civil Eng., METU ____________

Assist. Prof. Dr. Saman Aminbakhsh
Civil Eng., Atılım University ____________

Date: ...

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Salar Ahmadisheykhsarmast

Signature :

ABSTRACT

SMART CONTRACT SYSTEMS FOR GUARANTEED AND TIMELY PAYMENT OF CONSTRUCTION PROJECTS

Ahmadisheykhsarmast, Salar
Master of Science, Civil Engineering
Supervisor : Prof. Dr. Rifat Sönmez

January 2020, 108 pages

Delay in progress payment is a widespread problem in the construction industry which adversely affects the entire processes of the projects. Difficulties in the cashflow of the contracts, and consequently the subcontractors are the main consequences of delayed payments. Despite its significance, few research focused on development of methods guaranteeing timely payments of the participants throughout the project. Recent developments in blockchain and smart contract technologies presents a potential for development of a secure platform for the construction projects. Smart contract based payment systems not only provides an opportunity for minimizing the payment problems, but also enables building trust among the project parties for successful completion of construction projects. By taking advantage of the blockchain and smart contract technologies, this thesis aims to design and develop smart contract-based payment systems for guaranteed and timely payment of construction projects. A Smart Contract System for Security of Payment of Construction Contracts (SMTSEC)is presented to ensure security of payment of construction progress payments. , BIM-smart-contract-based progress payment system (BIMSMRTPAY) is developed to expedite the conventional progress payment process and to minimize potential payment disputes. The smart contract based retention payment system (RETPAY) is designed to expedite and automate the retention payments. The contributions and limitations of the SMTSEC, BIMSMRTPAY, and RETPAY are illustrated and discussed through case projects.

Keywords: Smart Contract; Blockchain Technologies; Construction Projects; Project Payments; BIM

ÖZ

İNŞAAT PROJELERİNİN GÜVENCE ALTINDA VE ZAMANINDA ÖDENMESİ İÇİN AKILLI SÖZLEŞME SİSTEMLERİNİN GELİŞTİRİLMESİ

Ahmadisheykhsarmast, Salar
Yüksek Lisans, İnşaat Mühendisliği
Tez Yöneticisi: Prof. Dr. Rifat Sönmez

Ocak 2020, 108 sayfa

Ödemelerin gecikmesi inşaat sektöründeki projelerin tüm süreçlerini olumsuz etkileyen yaygın bir sorundur. Geç yapılan ödemeler, hem yüklenicilerin hem de alt yüklenicilerin nakit akışlarında önemli problemlere sebep vermektedir. Arz ettiği öneme rağmen, çok az sayıda araştırma, katılımcıların proje boyunca zamanında ödemesini garanti edecek sistemlerin geliştirilmesine odaklanmıştır. Blok zincir ve akıllı sözleşme teknolojilerindeki son gelişmeler inşaat projelerinin ödemelerinin vaktinde ve garantili olarak yapılabilmesi için güvenli bir platform sunmaktadır. Akıllı sözleşme tabanlı ödeme sistemeleri hem ödeme problemlerinin için hem de taraflar arasındaki güvenin sağlanması için önemli bir potansiyel içermektedir. Bu tezde, inşaat projelerine ait ödemelerin zamanında ve garantili şeklide ödenmesi için akıllı sözleşme tabanlı sistemlerin tasarlanmasını ve geliştirilmesini hedeflemektedir. Hakediş ödemelerinin garanti altında ödenmesi için akıllı-sözleşme-hakediş-ödeme-sistemi (SMTSEC) sunulmuştur. BIM-akıllı-sözleşmeye dayalı hakediş ödeme sistemi(BIMSMRTPAY) ise mevcut hakediş ödeme sisteminin hızlandırılması ve ödeme sebebi ile olabilecek anlaşmazlıkların en aza indirgenmesi amacıyla geliştirilmiştir. Teminat kesinti ödemelerini hızlandırmak ve otomatikleştirmek için ise akıllı-sözleşmeye-dayalı-kesinti-ödeme-sistemi (RETPAY) önerilmiştir. SMTSEC, BIMSMRTPAY, and RETPAY sistemlerinin katkıları ve kısıtları örnek inşaat projeleri kullanılarak tartışılmıştır.

Anahtar Kelimeler: Akıllı Sözleşme; Blok zinciri Teknolojisi; Yapım Projeleri;
Proje Ödemeleri; BIM

In dedication to my beloved family, who instilled in me the virtues of perseverance and commitment and encouraged me to strive for excellence.

ACKNOWLEDGMENTS

The past year has been an incredibly enriching life experience for me, both in the academic and personal sense. Achieving the goal of this study has been a long road, here I am at the end, but there are so many people to whom thanks I extend.

I would like to express my gratitude to Prof. Rifat Sönmez for pushing me to my limits and for being a friend more than just a supervisor to me. He always encouraged me to go on and reassured me my ideas are valuable to be said. As a friend, the words cannot describe the change he has made in my vision, professional and personal growth. Thanks to the guidance of him, I was able to shape my academic knowledge.

Moreover, I would like to pay my deepest gratitude to Assist. Prof. Dr. Aslı Akçemete for her valuable comments and feedbacks. I wish to thank to the rest of my dissertation committee members: Prof. Dr. İrem Dikmen Toker, Assist. Prof. Dr. Güzide Atasoy Özcan., Assist. Prof. Dr. Saman Aminbakhsh for generously offering their time, guidance and review of this document.

I would like to extend my sincere thanks to my cousins, or maybe it is just better to call them my brothers Dr. Amin Nouri, Dr. Sina Golmohammadi, and Dr. Ali Golmohammadi. I would like to acknowledge your enthusiasm which always showed me the light at the end of tunnel. You all were there even when you had nothing to offer but your presence. This journey may have not been even started without your motivations and supports. I would also thank to Yaser Mohammadi for standing by my side, no matter how situation is.

I would also express my deepest gratitude to Dr. Kerem Tanboğa for assisting me in my professional path. I would also like to thank AGE Construction staff, especially Sezai Azizoğlu, Emre Işıl, Hakan Cabaluz, Utku Karapınar, and Mehmet Boğut for providing me the opportunity to develop my career alongside with pursuing my academic goals.

I take this opportunity to thank my precious friends specially those who turned into family. You should know that your contribution not only in this journey but also at any moment of my life was worth more than I can express on paper. You all mean a lot to me. Cheers to our friendship.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

APP	Actual Progress Payment Amount
BIM	Building Information Modeling
Bloc	Amount to be Blocked
Cong	Contingency Amount
CryT	Cryptocurrency Type
Cur	Fiat Currency
DApp	Decentralized Application
DLT	Distributed Ledger Technology
EM	Employer
EOA	Externally Own Account
ETH	Ether
IoT	Internet of Things
LoC	Letter of Credit
MC	Main Contractor
Pay_i	Progress Payment Amount of Subcontractor & Suppliers
PayMC	Progress Payment Amount of Contractor
PBA	Project Bank Account
PerChange	Percentage of Change
PeriBloc	Period Block

PeriBloc	Period Block
PeriPay	Progress Payments Period
PoS	Proof of Stake
PoW	Proof of Work
PPP	Projected Progress Payment Amount
SC	Subcontractor
WAdEM	Employer's Wallet Addresses
WAdMC	Contractor's Wallet Addresses
WAdSCi	Subcontractor's Wallet Addresses

CHAPTER 1

INTRODUCTION

Payment is an essential part of any business since it is the best incentive for accomplishment of works. The payment is the lifeblood of construction industry and obviously continuity of the works and performance of the various parties mainly depends on the consistent and uninterrupted payment flow among the project participants. Regularity of monetary flow is significant in the industry since the activities take a long time, the overhead expenses should be afforded, and also because the payments are made for the works already done (Ameer-Ali, 2006). Despite its importance, issues regarding payments such as delayed payment is still the cardinal problems of the construction industry (Ramachandra & Rotimi, 2014).

Hillebrandt, Hughes, & Murdoch, (1998) highlight that the payment problems are generally risen from the deliberate default by payers (delayed or postponed), arbitrary devaluation of invoices or claims, and non-payment. In addition Tran & Carmichael, (2012) states that payments are delayed intentionally in construction projects since the upper tiers of supply chain use them as a strategy to finance the other projects. Hence, the delayed payment has become a feature of the construction industry culture of most countries.

According to the report provided by Euler Hermes Global, (2016), late payments rose by a devastating 27% during 2015 and the average payment time for construction companies rose up to 82 days to 120 days. Large companies who cannot service large upfront costs and continuous payment while maintaining health cash flows are vulnerable to putting the entire supply chain at risk. To that end, study conducted in 2012 found that 97% of the 250 companies surveyed experienced some of unfair or overdue payments (Penzes, 2018). In a sector in which 18% of firms are considered small or medium-sized, these practices are hurtful. (Farmer, 2016). This situation leads to undesirable consequences which could threaten the success of the parties and consequently, the completion of projects. Project delay, cost overrun, performance reduction, disputes, business bankruptcy, and contract termination could be also associated with delayed problem (Sambasivan & Soon, 2007; Tran & Carmichael, 2012). Odeyinka & Kaka, (2005) suggest that contractor becomes subject to additional financing and transaction cost as a result of failure to get paid on the stipulate period of time which eventually puts the parties further down the chain at the risk of insolvency. Abdul Kadir, Lee, Jaafar, Sapuan, & Ali, (2005) declare that payment delays cause stoppage to material delivery which in turn affect the labors' productivity adversely. As a result, success of the project and ultimately the survival of the industry is affected.

Progress payment plays a crucial role in each project to carry out the project scopes successfully (Ansah, 2011). Because, the contractor or subcontractors generally plan the payment to the lower tiers based on the progress payment cash flow of the contract (Enshassi & Abuhamra, 2015). Practically, the interim payments are initiated by the issuance of the interim certificates. Interim certificate is defined as provisional periodic certification for the payment due to contractor (Ansah, 2011). In practice, it is generally observed that the main contractors have difficulties getting the on-time payments. Once a contractor gets paid late by the employer, difficulties are encountered in the contractor's cash flow, which in turn, causes the payments of subcontractors and suppliers to be also deferred (Enshassi & Abuhamra, 2015).

Even if the contractor gets paid on time, the prompt flow of payment down to the subcontractors is not always guaranteed because of the contractor's intentions such as earning interest, financing other projects, increasing the individual profit margins and etc. Amoako, (2011) reports that subcontractors are mostly paid by contractors according to "pay-when-paid" and "pay-if-paid" clauses outlined in most contract forms. The consequences of the subcontractors being paid late may cause bankruptcy. In such situations, some subcontractors tend to increase their quotations, which in turn increases total project cost, an undesirable condition for owners. The postponed payments not only prevent both the contractor and subcontractors from financially surviving to accomplish the tasks, but the trust between parties can also be severely damaged in this circumstance (Manu, Ankrah, Chinyio, & Proverbs, 2015). In perspective of the subcontractors, the payment approach of the contractors is directly related with their trustworthy. Thus, the late payments also influence the trust in the supply chain relationships adversely. (Manu et al., 2015). Besides, late payment results motivation reduction of the parties and effects activities performance negatively.

Theoretically, integrating specific provisions into contracts address the information regarding payment commitments and payment specific acts (Ramachandra & Rotimi, 2011). Nevertheless, the industry still suffers from various payment issues. Therefore, there is a growing need for a reliable payment platform to eliminate the problems discussed above.

As a solution , Project Bank Accounts (PBAs) has been proposed in recent years to improve the conventional progress payment system by taking back control of payment from upper tiers, by securing payment in the supply chain, and by decreasing the length of progress payment cycle. A PBA is a ring-fenced bank account from which payments are made directly and simultaneously to the main contractor and lower tires of the supply chain (UK Cabinet Office, 2012). Under PBA, the employer may deposit the entire project lump sum amount into the PBA or may pay amounts due once the progress payment reports are approved (Macaulay & Summerell, 2019). Upon issue of an authorization by the employer, due amounts are released from the PBA to the main contractor and subcontractors according to the breakdown included in the progress payment reports. The advantages of PBAs include accelerated payments, savings as a result of reduced financing and debt chasing expenses, and protection in the event of contractor insolvency (Biddell, 2015). Despite its advantages, PBAs have been only used in public projects mainly in the United Kingdom and Australia by government enforcement. Set-up and administration burdens and costs are often cited as the key barrier (Griffiths, Lord, & Coggins, 2017; Price, 2011) for adaptation of the PBAs.

Moreover, the industry has tried to remedy this situation, for example, utilizing open source standards such as NEC, JCT, or FIDIC to institute best practices. In addition, Construction Supply Chain Payment published by the Construction Leadership Council, (2013) implement fair payment commitments that reduce payment time to 30 days, these measures are intended to support companies. Furthermore, Housing Grants, Construction and Regeneration Act 1996 (United Kingdom, England), Building and Construction Industry of Payment Act 2004 (Queensland, Australia), and Building and Construction Industry Security of Payment Act 2004 (Singapore) are such solutions which have been provided by different countries to improve payment action and reduce the late progress payments within the industry. (Ramachandra, 2013; Sahab & Ismail, 2011; Din & Ismail, 2014). Although the mentioned solutions may reduce the delayed payment risk, the problem still persists in the construction industry (Ramachandra & Rotimi, 2011). As a result, there is an evident need for transparent, traceable, and efficient payment environment in the industry.

Inherited features of blockchain and smart contracts offer an opportunity to integrate payment clauses of construction contracts to establish a secure, efficient, and expedited payment system within the construction industry according to recent research studies (Ahmadisheykhsarmast & Sonmez, 2018; Cardeira, 2018; Hunhevicz & Hal, 2019; J. Li, Greenwood, & Kassem, 2018; Wang, Wu, Wang, & Shou, 2017). The blockchain is a decentralized data management technology which transacts the data among the participants within the network and is managed by cluster of computers (Anuradha, Yamini Gupta, Udayasree, & Tabassum, 2017). Blockchain was originally introduced for Bitcoin (a decentralized digital currency), but then the recent developments in blockchain technology have led to the invention of smart contracts as a creative alternative for automated execution of contract conditions. Smart contract is a code-based computer program which is run on the blockchain public network to automatically execute the specified clauses and transact the digital assets among the parties, under certain conditions (Szabo, 1996). The payment transaction in smart contracts is not applicable without using the cryptocurrency. Cryptocurrency is a digital currency, or a digital cash created through blockchain encryption process and is used as a mean of payment transaction within the system. Unlike the existence money such as dollar cryptocurrency does not have a physical form. Bitcoin and Ether (ETH) are among the most well-known cryptocurrencies.

Despite the fact that the potentials of the blockchain and smart contract in payment domain of the construction industry have been highlighted in numerous research studies, very few researchers have developed the application to demonstrate its use in the industry. Hence, the main purpose of this study is to develop three smart contract-based applications for payment domain of the construction industry namely Smart Contract System for Security of Payment of Construction Contracts (SMTSEC),BIM-smart-contract-based Progress Payment System (BIMSMRTPAY), and Smart Contract Based Retention Payment System (RETPAY) to narrow this gap. The proposed SMTSEC system is for security of payment of construction projects which disciplines the employer to plan and make payments on time, hence, assures timely payments to the contractor and lower tires of supply chain; subcontractors and suppliers. The smart contract of SMTSEC system make the parties' payment simultaneously based on the specified conditions and the cost-schedule data obtained from a management software. The BIMSMRTPAY system was resulted from the integration of the Building Information Modeling (BIM) and the smart contract technologies. The adopting of BIM in the BIMSMRTPAY aims to present a novel and object-based progress payment which enable the users to determine the completed objects through the model and also visualizes the progress which facilitates the control of the on-site progress through model. Information such as the cost of material or the total cost of each objects is enabled by the BIM section of the system. The BIMSMRTPAY offers a transparent and expedited progress payment system for the industry within the contract clauses are executed without involving of the banks and lawyers. Moreover, smart contract section of the BIMSMRTPAY system, expedites and facilitates the progress payment calculation process, reduces the vagueness and uncertainties of the contract payment clauses. RETPAY provides a decentralized application for payment of retention to the contractor by the employer for the works completed. The RETPAY is mainly designed for the project contracts in which partial completion and partial payment of retention is allowed. RETPAY not only enables automated payment of retention but also performs storage and record keeping of the project completion data on a secure, reliable and trustworthy blockchain platform Applying the achieved improvements on different case projects to demonstrate their applicability is also in the scope area of this thesis study.

The rest of the paper is organized as follows: Chapter 2 starts with a detailed review of payments practice, related challenges, and existence remedies in the construction industry, followed by a comprehensive review regarding application of blockchain and smart contract technologies in the construction. Chapter 3 is dedicated to a brief introduction on blockchain and smart contract technologies. In Chapter 4 the proposed systems followed by application on the case studies are discussed in detail. Chapter 5 is devoted to a detailed discussion on the proposed systems to illustrate their advantages and limitations. Finally, Chapter 6 includes the conclusions and points out potential topics for future research.

CHAPTER 2

LITERATURE REVIEW

2.1 Types of Payments in Construction Industry

The main types of payments in construction industry are mainly classified in three categories namely advance payment, interim or progress payment, and retention payment.

Advance payment is defined as sum of money which is paid to the contractor by the employer before any work has been started in order to ensure contracts are able to meet startup costs and finance their contract without requiring them to enter into unnecessary external borrowing. When an employer makes an advance payment to a contractor, it obtains a bank guarantee as security against that payment. The guarantee is payable on demand and contains optional wording for the value of the guarantee to reduce as interim payments are made under the contract (Hussin & Omran, 2009).

The interim payment which is also known as progress payment could be defined as provisional payment is paid to the project participants such as contractor by the employer and to the subcontractors by the contractor progressively in turn of the works or services which they perform (Judi & Rashid, 2010). According to Kenley, (2003) this type of payments is made to the contractor so that he can recover the money for work as they progress and thereby avoid the burden of the contractor funding the project. There is often a time lag between the time the contractor incurs the expenses and get paid for them. Hence, late payment to the contractor drive them to seek additional funding (Odeyinka & Kaka, 2005).

It is common practice in construction that the payer, which is commonly employer or upper tire contractors, deducts a certain percentage (less than 10% and usually up to a limit of 3-5% of the contract sum) of each progress payment and withholds it until the completion of work to assure that the contractor will finish the works according to the specifications. These retentions are repaid to contractor once the completed works are tested and approved by the employer. This is called retention payment which is withheld until the completion of the project to secure full performance of the contractor’s obligation. Retention payment is also considered as a security for the cost of rectifying any defective works. Similarly, the contractors also withhold a percentage of subcontractor’s contract payment.

2.2 Challenges in Payment Practice

Most of the contractors' face difficulties to afford the construction expenses when the payments are delayed (Doloi, Sawhney, Iyer, & Rentala, 2012). Payment delay for completed work lead to disputes between all project parties and it can lead to arbitration or litigation if it is not resolved amicably (Sambasivan & Soon, 2007). Also, it is obvious that the speed of work progress depends mainly on the efficiency and availability of workers. Most of contractors hire sub-contractors to perform the construction work and when they are paid late, they have limited resource to work with and consequently reduce the number of workers or suspend the work until they get payment from the contractors. Although there are abundant of workers in the construction sector, the reluctant of the contractors or sub-contractors to hire more workers contribute to shortage of site workers and then delay in the project period occurred (M. R. Abdullah, Abdul Azis, & Abdul Rahman, 2009).

The hierarchical or multi-tiered structure of the contractual framework of the construction industry gives rise to the payment problems (Griffiths et al., 2017). The owner transfers the payment to the main contractor in return of the progress that the contractor made. Afterward, the contractor is expected to make payments to the subcontractors for the subcontracted tasks. Hence, cascade payment structure affect contractors and suppliers in the lower levels even more due to poor payment practices of a contractor at the top of the contracting chain. (Latham, 1994). Thus, a payment delay by one party may affect the whole supply chain of payment of a construction project. For instance, if an employer delays in making payment to the contractor, this in turn will result in contractor's delay in making payment to the sub-contractor and lower tires. In many cases, the owner may not arrange the payment of the contractor on time, due to poor financial management, lack of financial resources, and etc. (Ye & Abdul-Rahman, 2010). The importance of the payment problem and failure of construction projects and companies worldwide due to the problem has been stated by previous research (Abdul-Rahman, Kho, & Wang, 2014; Ramachandra & Rotimi, 2014).

Delay in progress payment by the owner has been highly ranked among the factors that cause dispute and conflict among the parties within the project (Jaffar, Tharim, & Shuib, 2011; Mahamid, 2016; Tazelaar & Snijders, 2010). Duration of the project is also affected by the late progress payments to the contractor and subcontractors accordingly (Assaf & Al-hejji, 2006; Lessing, Thurnell, & Durdyev, 2017). Because, the work may be suspended until the conflicts among the participants are resolved and payment due to the contractor is fully paid (Ansah, 2011). Furthermore, late payments make the contractor's cash flow negative and make him financially unable to proceed the work and pay subcontractors and suppliers which in turn creates the cash flow problems for the subcontractors (Mei Ye & Abdul-Rahman, 2010). Ramachandra & Rotimi, (2011) analyzed the payment losses and delays in New Zealand and concluded that payment delays and losses are prevalent within the industry. Abdul-Rahman et al., (2014) focused on the underlying causes of late payment issues in Malaysia and revealed the cash flow problems due to employer's poor management as the most significant 5 cause. Liu et al., (2019) performed a comprehensive literature review on the dispute causes and determined payment delays as one of the top owner related causes.

Timely payment of the contractor does not ensure that subcontractors are get paid promptly (Cheng, Soo, Kumaraswamy, & Jin, 2010). The results of an investigation which has been conducted by Arditi & Chotibhongs, (2005) declares that the payment of the 89% of subcontractors which is made by the contractor is delayed by more than 45 days after the completion of the work. Furthermore, according a report provided by the Senate Economics References Committee, the contractors can employ tactics to subcontractors for accepting long payment claim periods, ranging anywhere between 30 and 90 days (ERC, 2015). Hence, the subcontractors face financial difficulties to accomplish the tasks. In-depth interviews with senior management personnel in a cross section of contractors, sub-contractors, suppliers, and consultants performed by the UK Office of Government Commerce revealed that payment delays up to 60 days for the payments from the employers were common (OGC, 2007). According to the survey conducted by Master Builders Association of Malaysia (MBAM) among contractors and sub-contractors, about 80.3% indicated that they had encountered slow progress payment similarly in government and private sector’s projects. The contractors are facing delays of payment for more than 91 days and up to 12 months compared to the contractual date.

Cash flow indicates the financial health of a business and measures its payment ability. So, effective cash flow will help to protect the financial security of a business. The payment delay from owners will affect the cash flow of the contractor and retainage withheld by the owner will also create cash flow problem to the payment delay problem is interrelated with the cash flow problem. Cash flow in the construction industry is critical because of the relatively long duration of projects. Any deviation due to either project delays or cash flow delays can have diverse impact on the project (Mei Ye & Abdul-Rahman, 2010). According to Frimpong, Oluwoye, & Crawford, (2003) monthly payment difficulties is the most important cost overruns factor in construction industry.

One of the main consequences of the delayed payments would be the interest due on capital borrowed by considering the fact that contractors often borrow working capital from banks in order to finance their construction operations and in turn have to pay interest on these borrowings. As a result, contractors are highly dependent on regular interim payments from employers during the course of construction to help discharge the debt so accrued. Once the contractors fail to receive the progress payment timely or in accordance with the terms agreed or for the proper amount, the interest they face hardship to finance the expenses which result in increased costs such as interest charges on loans, late-payment penalties, and loss of vendor discounts for paying bills promptly. Late payment also affects the contractor’s performance adversely.

Llangakoon, (2017) stated that frequent payment delays result in disputes and drive construction parties to suspend and terminate projects. Besides, At a larger scale, payment delays drive down the productivity of the industry and cause liquidation and insolvencies. Ansah, (2011) and Danuri, Munaaim, Rahman, & Hanid, (2006) declared that payment delays cause stress on contractors and creates financial hardship, creates adverse chain effect on other parties, results in delay in completion of projects, creates negative social impacts, leads to abandonment of projects, results in formal dispute resolution, leads to bankruptcy.

Ayudhya, (2012) identified twenty-four factors which causes of delay in payments. According to the result the main contractors faced moderately severe impact from the payment delays because of the five reasons which are owner financial problems, delay in work approval, major accidents, inaccurate bill of quantities and substandard workmanship.

The study of M. Abdullah, Abdul Azis, & Abdul Rahman, (2009) found that the payment delay causes in the industry are the employer's poor financial and business management, withhold of payment by employer, contractor's invalid claim, delay in valuation and certification of progress payment by consultant, inaccuracy of valuation for work done, inadequate documentation and information for valuation, involvement of numerous parties in the honoring certificates process, heavy work load of consultant to do evaluation for work done, contractor's misinterpretation of employer's requirement of variation order.

Danuri, Munaaim, Rahman, & Hanid, (2006) listed the payment delay reasons as delay in certification, poor financial management of payer, local culture, payer's failure to implement good governance in business, underpayment of certified amounts by the payer, the use of "pay when paid" clauses in contracts, disagreement on the valuation of work done, payer's wrongful withholding of payment, short of current year project budget, poor communication among parties involved, delay in submitting contractor's payment claim, conflict among parties involved, poor understanding of the contract.

The results of Mei Ye & Abdul-Rahman, (2010) study revealed that the main payment delay factors out of a total of forty-one variables include the cash flow difficulties due to deficiencies in employer’s management capacity, employer’s improper utilization of funds, scarcity of capital to finance the project, and poor cash flow due to the improper process implementation, delay in releasing of the retention payment to contractor and delay in the evaluation and certification of interim and final payment.

Aaron Yao, (2015) revealed that the delay in payments rise from poor financial management by the employer and contractor, employer insufficient fund to pay contractor, employer withholding of payment due to misinterpretation of change orders or arguments over amounts to be paid for work completed, use of “pay-when-paid” clauses in general contractor’s contract with sub-contractors, construction “culture” that delayed payment are expected or acceptable, delays in certification e.g. inaccurate evaluation of work done, defects in work, verbal instructions/changes are not clarified in writing, miscommunications, contractual provisions and technical problems e.g. delayed processing for approvals, lack of clear project specifications, errors in submitting claims, failure to identify technical problems.

2.3 Remedies for Delay Payment

In order to cope with the delayed payments, suggestions have been declared in both literature and practice (Judi & Rashid, 2010; Ramachandra & Rotimi, 2014).

Claim for the interest by contractor is one of the possible remedies to late payment caused by the employer. This affords some relief to the contractor, but this can be a double-edged sword for the contractor for it effectively allows the employer to suspend payment and not commit a breach of contract. Suspension of the further performance of his obligations under the contract by the contractor is referred as another remedy for late payments. According to the FIDIC contract type, the contractor has the right to either suspend work or reduce the rate of work, and even has the authority to terminate his employment under the contract after giving notice to the owner, with a copy to the engineer. This can be a safe and common position taken by the contractors when they face non-payment from the employer. However, for late payment, this action might be too harsh and impose another problem at site such as suspension of work by the contractor.

It shall be established that in the case that progress payment is not paid to the contractor within the stipulated time in the contract, by notifying the owner, the contractor may ask the employer to affect a progress payment. If the employer fails to pay after receipt of the contractor's notice, the employer could negotiate with the contractor for payment on deferred terms. Otherwise, the employer should pay delayed interest. However, if both of them do not come to an agreement and the contractor is unable to continue his work, the contractor may suspend work and the employer should bear the liability for breach of contract (Meng, 2002).

Payment delays may also occur at the end of the project after the construction process. In practice, employers often take over completed projects before making completion payment to contractors (Arditi & Chotibhongs, 2005). Danuri et al., (2006) stated that the possible solutions according to contractors are the right to regular periodic payment, the right to a defined time frame for payment, the right to a speedy dispute resolution mechanism e.g. adjudication, the right to interest due to payment delay, the mandatory creation of a trust account for retention sums, a right to suspend work, the restriction of the right to set-off or withhold sums due, the creation of a right to a lien, the prohibition of "pay when paid" clauses in contracts. Contractors and subcontractors indicated that payment bonds, direct payments and the use of trust accounts were preferred solutions to the payment problems experienced by industry (Ramachandra & Rotimi, 2014). The right of suspension is an important remedy which by contractor allows to stop work until the payment is made. It can be an effective means of securing overdue payment without the need to instigate other formal procedure such as arbitration and litigation (Pettigrew, 2005).

Griffiths et al., (2017) has been stated that adoption of the PBA in the construction industry could be a solution for the delayed progress payment problem. In recent years, PBAs were proposed to overcome the delayed progress payment by providing a secure payment system in the supply chain, followed by reduction of the payment length. The PBA which was initiated by the National Audit Office, (2005) to improve the payment practices in UK, is a payment mechanism from which the payment are made simultaneously to the main contractor and lower tires in supply chain by a bank account as shown in Figure 2.1.

Contrary to the traditional payment mechanism, employer deposits the payment of one or two months in advance into the PBA before any progress of works. To keep the balance of account positive, the employer usually has a detailed and frequently updated payment schedule which sets out the estimated construction costs in each month of the project.

Employer can also pay amounts due once the progress payment reports are approved. The contractor provides a declaration to the employer of what is due to the supply chain along with its application for payment. The breakdown of what is due between the contractor and the sub-contractors is included in progress payment certificate. The employer deposits the due payment into the PBA and then bank send out the due sums simultaneously to all the parties. Once the payment has been certified, each party can withdraw the payment instead of waiting payment from the employer or up tiers of the supply chain (Towey, 2013).

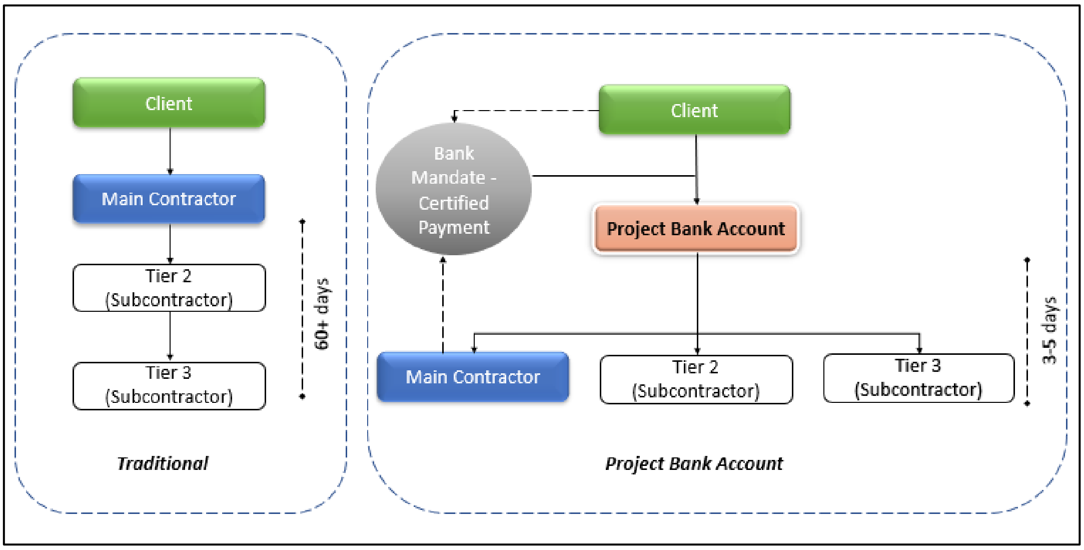

Figure 2.1 PBA Payment Route

In September 2009, Government Construction Board required Central Government Departments, their Agencies and Non-Departmental Public Bodies in the UK to use PBAs in the case that they extend down to at least tier 3 contractors and 80% of the value of sub-contract payments (UK Cabinet Office, 2012). Although expedited payment, enhanced trust among the supply chain participants, protection in the event of contractor insolvency are resulted from the using of PBAs (Biddell, 2015), employers and contractors are still unwilling to apply the PBAs, especially in the private projects (Griffiths et al., 2017; Price, 2011). PBAs have been only used in public projects mainly in the United Kingdom and Australia by government enforcement.

Although PBAs could be a remedy for payment issues of the construction industry, disadvantages such as establishment and administration burdens and costs, staff training and company policy, complex and confusing nature of PBAs, loss of cash flow benefits, and loss of control from employer (funder's perspective) because of the payment tiding in PBA are highlighted as the main barriers of adoption of PBAs (Griffiths et al., 2017; Macaulay & Summerell, 2019; Price, 2011).

Although the aforementioned solutions could be remedy for payment problems in the industry, very limited research focused on development of methods to prevent industry from facing with payment problems. The advantages of having a protective scheme against late payments in the construction industry is a major incentive for seeking the novel technologies. Blockchain technology accompanied by smart contract have the potential to establish a robust payment system in which the payments are done on time and all project participants receive the payment with no delay.

2.4 Building Information Modeling

BIM model is an intelligent visual and data based process that gives architecture, engineering, and construction (AEC) experts the perception and authoring tools in delivering a more efficient plan, design, construct as well as a facility management (Barnes & Davies, 2015). Build it twice once virtually and once physically is the process benefit encouraging virtual construction. Building Information Modelling presents various 3D Models such as design models (architectural, structural, mechanical, electrical and plumbing and site/civil models),

4D BIM modelling is adding the fourth-dimension schedule to the 3D model. The fourth-dimension model links the 3D elements with the project delivery timeline to provide users a virtual simulation of the project in the 4D environment. The linkage to project timeline makes it possible to graphically visualize the projects schedule and users can simulate the building site and construction at any point developing real time schedule and workspace planning. This type of simulation provides considerable insight and allows for early detection of planning errors. By adding ‘time’ to the information in the project model (linking attributes to the construction schedule), it becomes possible for contractors to review the construction of the building.

Fifth dimension makes possible the calculation of cost for the entire construction project as well as if it is necessary for project parts. The total cost of projects based on information about cost of labor, materials, etc. those currently could be set up manually or automatically with help of selected software tools. 5D BIM process allows contractors, employers and the project team to generate accurate cost and essential estimating information with model element attributes like size, area, object family type, and productivity projections (Barnes & Davies, 2015). 5D BIM model is the linking of the fifth dimension to the 3D BIM model extracting non-graphical data and model attributes to generate cost information and material quantities within a level 2 BIM collaborative environment. Evolving design changes within the model automatically adjusts to improve progressive accuracy of cost performance. 5D model is expected to link BIM model to cost data through a digital model information for quantity takeoff generating accurate project cost estimation. The ability of BIM models to generate cost information and quantity schedules will allow for faster cost value of a given design.

ND BIM model contains advanced information such as materials, components, schedules, energy analysis, and more. This allows information to be secured as well as available to each key discipline team member to access and contribute their intelligence to the project. The model simplifies the collaboration workflow of a project as well as savings in costs, time, and human errors. Any change, alteration or variations to the model instantly updates all the data reflecting in update of sources such as schedules, constructability, costs and risks (Andersson, Farrell, Moshkovich, & Cranbourne, 2016).

Although the BIM is applied in various domain of construction such as scheduling, cost control, cost estimation and etc., there is lack of BIM application in progress payment domain of the construction industry. Emergence of the blockchain and smart contracts may pave the road for the BIM to be used in payment domain of the industry and results establishing of the novel progress payment methods which by payment process is expedited and progress valuation is facilitated.

2.5 Blockchain and Smart Contracts in Construction Industry

Advantages of smart contracts make it superior to the legal contracts in terms of contract payment clauses execution. Blockchain and the smart contract technologies have significant implications for contract management of projects. Automating the payment process by considering the payment clause of the contract could be referred to as an example for the transaction within the system. As the outlined contract milestones are reached and payments are made, they are recorded in such a way that neither party can repudiate, remove, and manipulate the record .

One of the substantial features of the smart contract is that it enables the funds in cryptocurrency to be embedded within the contract against the insolvency of the late payments (Ahmadisheykhsarmast & Sonmez, 2018; Wang et al., 2017). In other word, the smart contract does not allow the funds to be transacted among the parties of the contract (by blocking and holding them) until the preconfigured conditions in the contract are satisfied. Applying smart contracts accompanied by cryptocurrencies ensure guaranteed payments to an extent never before seen in the construction industry (Cardeira, 2015; McNamara & Sepasgozar, 2018). Moreover, the smart contracts could facilitate the payment practice, expedite the payment process, save time and cost besides decreases the risk of late payment and disputes within the industry (J Mason & Escott, 2018; Wang et al., 2017).

In Li & Kassem, (2019), authors declared solutions that the smart contract, blockchain, BIM, and IoT can bring to overcome the delay payments, trust issues and deficient collaboration problems in the industry. In the proposed system the performance of the delivery of the physical asset can be detected via IoT. The data required to verify against is provided by the digital information models. Payments regarding activities are triggered by smart contract automatically if the outlined performance requirements of the contract meet. afterward, the blockchain records the completion and payment events.

(Blycha, 2018) claimed that the information regarding the date of the physical delivery of materials to the site could be recorded in the blockchain. In addition, the payment related to the materials could also be paid by the smart contract when they are delivered to the site. So, applying the blockchain technology in supply chain phase of the construction project significantly increases the performance of the supply chain management due to the fact that it allows a real-time tracking of construction materials to a particular site from the initial phase of the process (J. Li et al., 2018).

With a smart contract the funds could be embedded in the contract and are initiated automatically when the drafted conditions of the contract meet. Ahmadisheykhsarmast & Sonmez, (2018) have claimed that in the procurement phase of the construction projects the payment regarding to the materials could be embedded in the smart contract and it is triggered automatically to seller when they are delivered to the site. Hence, could eliminate the need for the letter of credit (LoC), a document which is provided by the bank to guarantee the payment of seller and create trust among the parties, could be eliminated. So, the high time and cost of the LoC process, transaction fees, administrative cost to follow the process reduce significantly. Wang, Wu, Wang, & Shou, (2017) declared that funds or cryptocurrencies can be embedded into the contract against the insolvency of the delayed payments so as to eliminate the payment and cash-flow issues. In addition, it improves the efficiency of the contract administration process since the codes of the contract are unambiguous and predictable when compared with the traditional contracts. Mason, (2017) pointed out that the smart contracts could be extremely useful for collaborative construction foremost for project bank accounts and project insurance. Also, according to a vast review and analysis of the current state of blockchain in the construction provided by J. Li, Greenwood, & Kassem, (2019), PBAs are mentioned as potential area for blockchain use case in construction.

Moreover, In the construction projects, especially in the international ones the payment transaction fees are noticeably high. However, transaction costs are reduced 40% to 80% when the payments are transacted through the blockchain (Khandaker, 2019). Furthermore, it takes an average of four to six seconds to finalize the transaction compared to transfer process of the banks which is two to three days.

Many challenges in the industry such as delays, cost overruns, poor productivity, poor quality, disputes, and etc. could be mitigated by the solutions which are provided by the digital innovations (J. Li & Kassem, 2019). Blockchain and the smart contract are such novel technologies which have attracted the increasing attention of the various industries and fields such as healthcare industry, finance and banking industry, built environment, energy industry and etc. Numerous studies have declared the challenges of the construction industry and determined the extent to which blockchain and smart contract technologies are able to address these problems (Cardeira, 2017; Heiskanen, 2017; J. Li et al., 2018; J Mason & Escott, 2018; Jim Mason, 2017; Turk & Klinc, 2017).

BIM technology is used in the construction industry to enhance collaboration among the parties, data exchange, and results in the most efficient plan, design, construct and management (Shou, Wang, & Wang, 2015).. Turk & Klinc, (2017) have highlighted that the blockchain coupled with BIM ensure the trust and transparency of the network. Besides, the blockchain could be a remedy for the inadequate collaboration and information sharing, which are among the issues that slow the adoption of the BIM. Shou, Wang, & Wang, (2015) and Wang et al., (2017) have presented that the blockchain accompanied by the BIM provide a powerful tool for keeping the records of any modifications to the BIM model during the design and construction phases. In addition, blockchain ensures accuracy of information through immutability and identification of the person making changes along with details of the changes to allow better recording and tracking of the data (Stougiannos & Magneron, 2018). Hence, results in enhanced confidence and trust among the parties. Nawari & Ravindran, (2019) claimed that the blockchain integrated with BIM increases the confidentiality and eliminate repudiation. Besides, it addresses the existence challenges such as change tracing, traceability, provenance tracking and data ownership. As a result, the provided trust by the blockchain could maximize the efficiency of the collaborative design process and integrated project delivery strategies. In addition, secure cryptography behind the blockchain presents a promising method to address cybersecurity threats such as storage device failures, information corruption and disruption of BIM operations by abuse of authorized access, malicious intent of involved participants, which can affect BIM workflow and its connected systems furthermore, the Proof of Delivery method, which is secured and transparent via blockchain, allows collaboration between team members of a design project using BIM.

All the certificates related to the materials and quality checks throughout construction can be recorded, stored, and shared through a participants within the blockchain system (Penzes, 2018). This facilitates the measurement of the sustainability aspects such as total carbon footprint, percentage of reusable materials changing in time, and etc. Besides, it supports the planning of the waste management plan which generally requires the supply chain data such as invoices, specifications. Wang, Wu, Wang, & Shou, (2017) presented that the visibility of the transaction in the blockchain system makes the parties to trace the supply of each product or service with authenticity from quality assurance perspective. Thereby, the transparency and traceability in the supply chain phase of the projects enhances owing to the blockchain ecosystem.

(Pilagos, 2018) has been stated that the project data which are recorded by on-site sensors could be transfers to the smart contract and BIM system which results in contemporaneous report on progress. Hence, this data could be used to value the works automatically according to the pre-agreed prices and are paid to the parties paid on time. The author also stated that, the information related to the weather could retrieved form the weather sensor on site. Once the data are sent to the smart contract, it enables compensation events under a contract to be determined. Afterwards, the data is used to provide automatic extension of time decisions.

Health and safety accidents or unsafe conditions such as unauthorized actions on site, risky events, etc. can be recorded in the blockchain risk mitigation can be initiated (Penzes, 2018). To put simply, the critical data which are automatically provided by the IoT or the onsite sensors are processed in a smart contract. The smart contact has a built-in risk mitigation plan if certain thresholds or triggers reached, notifying the related parties and prompting them to change construction plan. The data such as the events occurrence date, alarm from the smart contract, etc. are registered on the blockchain system. In this way the system creates a tamper-proof source of health and safety information with accountability.

Potential of smart contracts for construction industry was mentioned in several studies in recent years, however, very limited research has developed applications to explore their use in the construction industry. Also, adapting these technologies for designing the application for guaranteed payment in the industry has not been declared. Integration of these smart contracts with BIM in few domains of the industry such as construction data management has been declared in the studies (Turk & Klinc, 2017), however, there is inadequate studies regarding developing an smart contract-based and BIM-integrated applications for progress payment phase of the industry. Hence, the main focus of this research is to narrow these gaps in the literature by designing and developing a smart contract system for security of payment of construction contracts.

CHAPTER 3

BLOCKCHAIN AND SMART CONTRACTS

3.1 Blockchain Definition

The blockchain was firstly introduced by Nakamoto, (2008) as the fundamental technology of Bitcoin; a person to person (peer-to-peer) digital cash exchange system. The distributed ledger technology (DLT), also known as blockchain technology is a community-based and decentralized data management technology which transacts the data among the participants within the network and records the transaction in the system (Anuradha et al., 2017). The technology functions through a person-to-person or peer-to-peer network, which is based on numerous of computers. Blockchain could be also referred as a chain of the blocks which each block contains a record of information or transaction (Fortney, 2019) that is locked in a chronological order and secured by cryptography, the science of coding and decoding for protecting and securing of the information and communication respectively. Each transaction is verified and performed directly thorough the computers over the internet by consensus of a majority (more than %50) and the entities which are known as nodes within the network respectively (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanamaran, 2016). Mougayar, (2016) defines the blockchain as a “value exchange network” which is able to store and transmit data in a decentralized way.

Technically, each block of the blockchain includes three elements which are data, hash, and hash of the previous block. The data is stored in a block, which mainly depends on the type of the blockchain is used, could be transactional data which details such as the amount of the transaction amount, sender and receiver information would be the data within the block. Once a block is created, hash (string of numbers and letters) is being calculated. The cryptographic hash uniquely identifies the block and all of its contest which allows us to distinguish it from every other block. Each block also contains the hash of the previous block which effectively establishes the public chain of the blocks since each block references the hash of the block that came before it (Christidis & Devetsikiotis, 2016).

3.2 How Blockchain Works

The transaction process in the blockchain has been demonstrated in the Figure 3.1. At the initial stage a blockchain user requests for a transaction e.g. bitcoin transaction. Public and private cryptographic keys are assigned to the transaction that the both sender and receiver holds. Every user of the blockchain owns a digital signature which is a pair of private key and public key. The private key which should be kept in privacy, is used to sign the transaction and once they are signed, they are broadcasted throughout the whole blockchain network. The usual digital signature is completed in two stages: signing and variation phases (Aung & Tantidham, 2017). In the signing phase, transaction initiator encrypts its data with its unique private key and sends the encrypted result and original data. During the verification phase, when the transaction has been broadcasted to the network, the nodes validate the initiator's public key value.

Afterwards, a new block which represents the transaction is created and is broadcasted to the participants (nodes) within the network to validate the transaction. However, creation of a new block takes few steps to be completed. New blocks are created through a process called mining by miner nodes. These miners operate anonymously by working together which all try to solve mathematical puzzles, which creates new blocks to the blockchain (Jutila, 2017). Mining nodes associate together and collect new transaction data. Upon receiving such data, each node independently verifies each and every transaction against many criteria such as tracking the source of the data, checking the sender balance to determine if there is enough amount to be transacted in case of the payment transaction. Afterwards, the verified transactions are aggregated into transaction pool, also called memory pools where they are held until they are included into a block. As miners compete with each other to be the first to come up with a new valid block to win right to mine the block to the blockchain , they need to make sure the transaction in their memory pool have not already been included in previous blocks (Dorri, Kanhere, Jurdak, & Gauravaram, 2017).

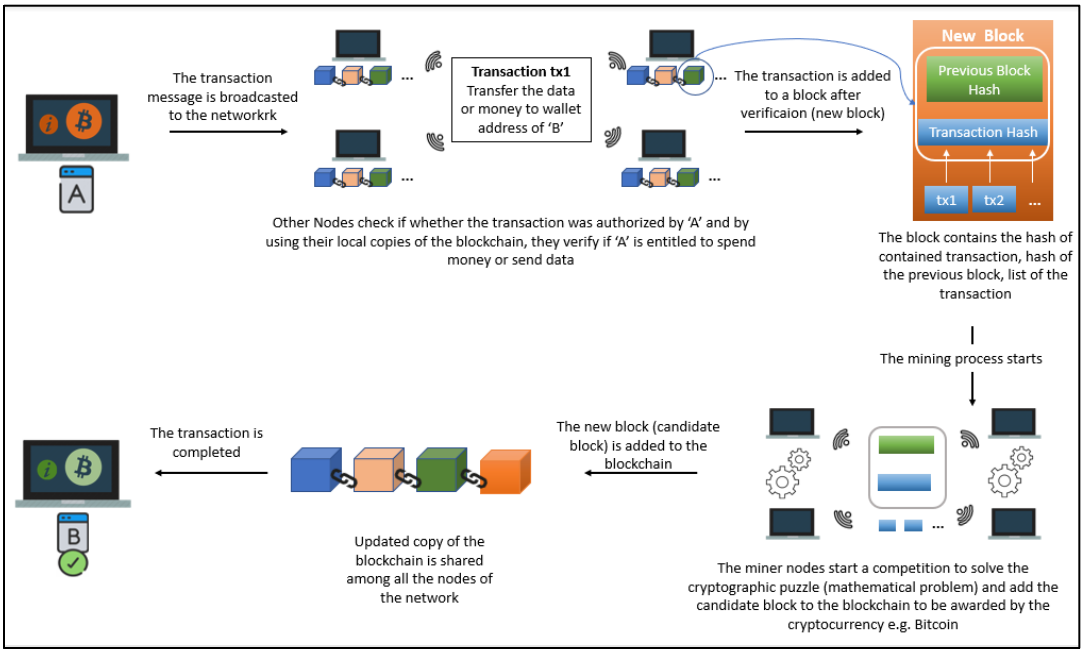

Figure 3.1 Transaction Process of Blockchain

When the transaction is broadcasted to the nodes of the network, its existence verified and validated through a consensus mechanism such as a Proof-of-Work (PoW) protocol which uses complex mathematics to solve equations across a distributed, decentralized, and peer-to- peer network. The transaction is received by all nodes that validate and verify its existence through pre-defined checks with regards to its structure and activity (Karafiloski & Mishev, 2017). Once a consensus is reaches, i.e. 50% of nodes agreeing on the transaction validity, then the block is appended to the blockchain and each node's copy within the blockchain is updated respectively (Biswas & Muthukkumarasamy, 2016; J. Li et al., 2018). On the mining side each node's version of the blockchain is renewed (Gatteschi, Lamberti, Demartini, Pranteda, & Santamaría, 2018). On another note, the blockchain itself is a distributed ledger without the ability to perform computations, these are handled elsewhere by miners who then verify and validate the chain's blocks through mining (Mik, 2017). Miners are then are rewarded for their service, for example with bitcoins in case of the Bitcoin blockchain network.

3.3 Types of Blockchain

The blockchains are categorized into public, private, and hybrid blockchains depending on their applications (Allens, 2016; Buterin, 2014). All types of the blockchains carry the similar benefits which is provided by the blockchain. They are executed in a peer-to-peer networks (Viriyasitavat & Hoonsopon, 2019). In addition, consensus process is fulfilled by the multiple nodes of the network.

In public blockchain network, anyone can access the data and can read, write, and participate in consensus process of the network (Zheng, Xie, Dai, Chen, & Wang, 2017). The success of the network totally relies on the number of anonymous participants. The Bitcoin blockchain could be mentioned as an example of the public blockchain.

In contrast, in private blockchain only the pre-defined nodes by a single entity can participate in the network and fulfill the consensus process of the system (Massessi, 2018). Private blockchains are able to restrict the operations of the participants such that specific nodes can only make certain transactions or the accessibility of the participants to the information may be limited (Wang et al., 2017). Although all operations are conducted on the blockchain network, it adds an additional layer of the privacy. As a result, it motivates the organizations to apply the blockchain in their business since adapting blockchain without making the data public is enabled by the private blockchain.

Hybrid or consortium blockchain are public only to the groups which are predetermined by a specific entity of the network. In other words, the production of block is determined and presented via a preselected internal group of nodes of transaction recorders (Pass & Shi, 2017). This consensus process is guided by a known and privileged server that utilizes a set of rules agreed upon by all parties, these rules also dictate the degree of data openness defined by access controls determined by the consortium that varies access to participants and data within the Blockchain (Viriyasitavat & Hoonsopon, 2019; Ye, Yin, Tang, & Jiang, 2018). The Permissioned blockchain method is designed for a semi-closed system involving few enterprises, collectively in the form of a consortium.

3.4 Key Features of Blockchain

Being decentralized and distributed are among the substantial features of the blockchain technology. The inherit algorithm behind this technology serves a secure mechanism for electronic collaboration without depending on a central power for trust (Huckle, Bhattacharya, White, & Beloff, 2016). As shown in Figure 3.2 (a) in a centralized system, parties are directly dependent on a certain trusted authority or enterprise to perform a service or to enable trust between the parties by assuring them that they have the authority and transparency (Penzes, 2018). The banks could be an example of the central organization which play the role as a financial intermediary to validate and process the transaction among the parties (Crosby et al., 2016).

According to the Figure 3.2 (b), in the decentralized blockchain system transactions are performed directly between the independent entities which are known as nodes within the network thorough the computers over the internet (Atlam, Alenezi, Alassafi, & Wills, 2018). This direct exchange of information among the interacting parties is enabled by the consensus mechanism of the blockchain which means validation and modifications in data must be agreed by all parties on the network, without reliance on any intermediaries (Penzes, 2018). The distributed aspect of the blockchain enables the participants to access the same data in the system at any location since list of the transactions are shared public among the peers. Hence, assures the system transparency and diminish the single point of failure and data integrity (Zhu & Zhou, 2016). However, in a central system the data is generally kept by a single authority. Since the information regarding the transaction is synchronized with all nodes in the network, the data could not be tempered in the system (Johansson & Nilsson, 2018).

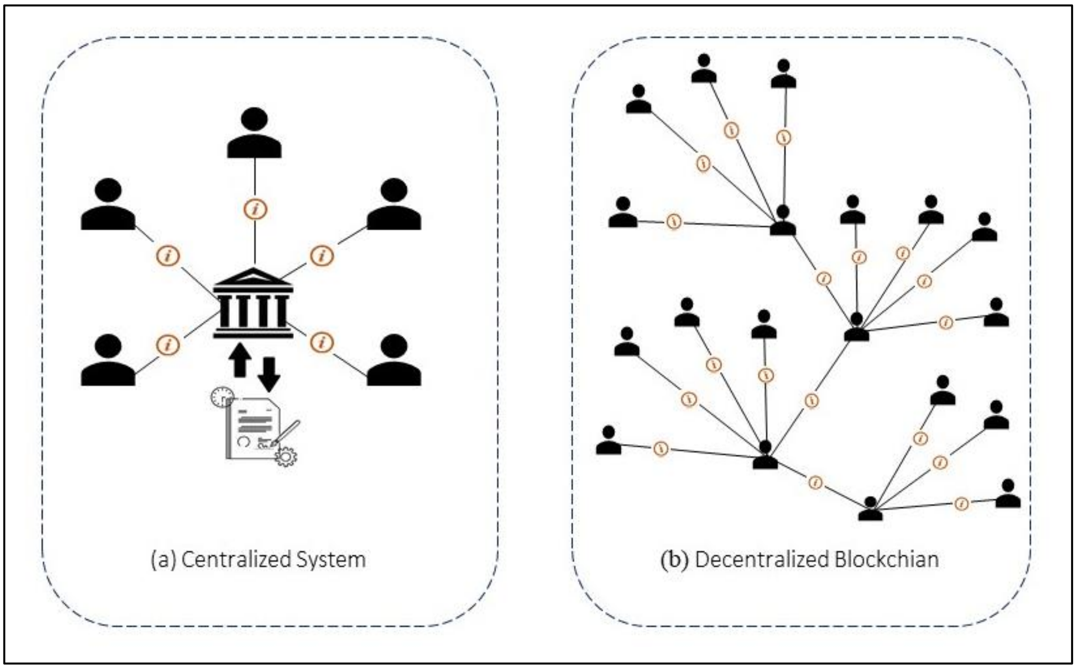

Figure 3.2 Centralized & Decentralized Systems

The structure of the blockchain is such way that the stored data are immutable, secure, and tamper-proof. As mentioned before, each block points the previous block that linked to the chain. The hash of each block is very useful in detection of the changes to the blocks since changing something inside the block will cause the hash to change. Hence, it will not match the following blocks anymore (Chen, Xu, Lu, & Chen, 2018) which would cause the tempering to be detected by the other nodes utilizing the exact same validation algorithm. In addition, miner nodes continuously follow the transactions and prevent to accept the transactions that are not coherent. Once a peer in the network tries to temper the data inside the block, it should make the block valid and resolve the cryptographic puzzle again which takes 10 minutes in case of Bitcoin. Also, it should make the next blocks valid. Meanwhile, the other blocks continuously are added to the blockchain. So, it can never outrun the creation of the blocks and cheat the system. Over 51% of ledgers within the stored network would need to be changed for successful tampering (Tschorsch & Scheuermann, 2016).

Transaction are recorded in the blockchain in a permanent way as they are share across the network, where each node in the network keeps and controls its records (Sultan, Ruhi, & Lakhani, 2018). Transparency, immutability, and temper resistance properties are derived from persistency feature of the technology which proves the verification of the blockchain (Viriyasitavat & Hoonsopon, 2019). As each transaction within the blockchain is recorded and validated using a timestamp, users are able to verify and trace previous records by accessing nodes within the distributed network, this process boosts the transparency and traceability of data stored within the blockchain (Zheng, Xie, Dai, Chen, & Wang, 2018). The extent of verification and the degree of auditability depend on the implemented blockchain system (Viriyasitavat & Hoonsopon, 2019). To that end, private Blockchains are least verifiable due their single administrator nature, permissioned Blockchains are second because encrypted of encrypted data preventing full verification, and lastly public Blockchain have the highest verification since nodes are totally decentralized.

Anonymity is other characteristic of this technology. Each user connects and access the blockchain network with a generated unique public address. The public key is large numerical value (27 to 32 characters) that makes it impossible to identify the participants (Swan, 2015). By virtue of design, its distributed consensus mechanism is most secure since it offers anonymity, resilience, fault-tolerance, and persistence (Hamida, Brousmiche, Levard, & Thea, 2017). Anonymity of the blockchain provides an efficient environment of assuring the transaction privacy in the network and keeping the users identification private (Atlam et al., 2018).

3.5 Limitations of Blockchain

Although blockchain technology has the potential to substantially change the current approach of value exchanges, few challenges and limitations of the system still exist which need to be overcome (Karafiloski & Mishev, 2017).As mentioned before, every block in the blockchain network is methodically validated and mined by the miner nodes with a proof of work consensus mechanism. In order to accomplish the process of mining (validation of the block), miners compete to find the right value of the block component (solving the cryptographic puzzle) namely nonce by trial and error method. In mining process, the miner who has the more hash rate (amount of computational power) has the high chances of finding a valid solution for the next block. This effort to reach the right value is implemented by the running of power-hungry mining equipment e.g. computers. Hence, vast amount of electricity is consumed by the machines in mining process so that a new block is created, or a transaction validated. It is undeniable that the number of participants nodes and blocks of the blockchain network grow exponentially. Hence, the requirement for miners to validate the blocks in the network also increased. Attending more miners in the network to reach consensus results in a need of more amount computational resources and electricity consumption accordingly**.** As a result, blockchain such as Bitcoin which uses proof of work mechanism to validate the transactions entail heavy energy consumption which is neither environmentally friendly nor feasible. Furthermore, As blockchain network gets larger, it adversely affects the processing speed hence the time required to validate transaction increases (Law, 2017).

Addition to the problem of vast electricity consumption of miner machines to participate in consensus process, scalability has been remained a challenge for the blockchain from technical level. In case of Bitcoin blockchain, Bitcoin block size is currently set 1 MB and it takes about 10 minutes so that a new block be generated (be mined). Moreover, Bitcoin network is not cable to handle the high frequency transactions by considering the fact that the network can currently guarantee 7 transactions per second (Zheng et al., 2017). As mentioned before, all the transactions are recorded on the common transaction ledger which is distributed among all nodes within the network. This transaction ledger grows exponentially faster than the number of network participants. Thus, the storage and computational burden on network members will eventually become too large for network members to handle as the network size grows. Size of the blocks gets larger if blockchain be adapted to high volumes of transactions which result in larger storage space, slower distributing process, and expensive participation cost in the network (Ammous, 2016). Consequently, the number of blockchain users who want to keep such a large blockchain will be decreased hence it will lead to centralization gradually. Therefore, there is a clear trade-off between scale and decentralization.

The 51 % attack which was also highlighted by the Nakamoto, (2008) is the most serious security problem of all blockchain. In the proof of work process of blockchain, more computational power of the computers (hash rate) means more trial per second to solve the mathematical puzzle. Consequently, more hash rate a miner node has, the higher the chances of finding a valid solution for the next block. So, 51% attack is defined as a potential attack on a blockchain network whereby the majority of the network hash rate is controlled by an entity or organization which potentially causing a network disruption (X. Li, Jiang, Chen, Luo, & Wen, 2017; J. L. Zhao, Fan, & Yan, 2016). In this situation, the attackers mining power could exclude or change the order of transactions, however, 51% attacks are improbable due to the size of the network, hence the likelihood of an attacker with enough computing power to overwhelm other participants drops exponentially as the Blockchain grows larger.

To tackle with some challenges superseded consensus mechanism such as proof of stake (PoS) have been proposed over proof of work. PoS protocol requires far fewer computational power for mining the blocks since, in proof of stake, miner nodes do not compete to solve the computational puzzle by mean of mining matachins; instead, the likelihood of a node mining the next block are related to that node's relative wealth (or stake) in the cryptocurrency balance (Christidis & Devetsikiotis, 2016; Saleh, 2019). Henceforth, the more Bitcoin or altcoin a miner has, the more mining power they have. PoS consensus mechanism reduces energy consumption and can result in faster transaction within the network (David, Gazi, Kiayias, & Russell, 2018). In addition, it can decrease the probability of 51% network attack since the nature of its structure makes an attack from another miner less fruitful (Frankenfield, 2019).

3.6 Blockchain 1.0 & 2.0

The evolution of the blockchain is mainly divided into two major stages namely Blockchain 1.0 for digital currency and Blockchain 2.0 for digital finance (Swan, 2015; J. L. Zhao et al., 2016).Blockchain 1.0 is for the decentralization of the payment system enabled by the well-known digital money; Bitcoin, which represent a store of value as well as provide value to the protocol itself (Burgess & Colangelo, 2015). The main functionality of blockchain 1.0 is that the individuals are able to make payment transaction directly in secure and fast way over the internet all over the world without intermediaries' involvement such as banks. Unlike the fiat currencies which rely on a central bank to regulate the money supply, the money supply of the Bitcoin is limited to the 21 million units (Efanov & Pavel, 2018). The supply of the new units is being issued at a regular interval which has been currently catch 17.9 million growing to capped amount of 21 million.

Blockchain 2.0 refers to the decentralization of markets which enables the transfer of the assets through blockchain beyond the simple payment transaction by the creation of a unit of value whenever it is transferred (Wang et al., 2017). Blockchain 2.0 supports financial applications such as stocks, mutual funds, and bonds, banking instruments such as loans and mortgages, as well as legal instruments such as contracts and other assets or properties that can be monetized (Burgess & Colangelo, 2015). Moreover, smart contracts, smart property, Decentralized Applications (DApps), Decentralized Autonomous Organizations, and Decentralized Autonomous Corporations appeared in this stage of the blockchain evolution. Verification is executable by the blockchain for proof of insurance and ownership as well as notarized documents. This process extends to physical and intangible assets like cars or patents to be encoded, protected and transferred through the blockchain

(Wang et al., 2017). The most relevant property of Blockchain 2.0 is the integration with smart contract which is provided by Ethereum.

3.7 Smart Contract Definition

The contracts are the backbone of any enterprise. So, these contracts need to be managed efficiently. Separate from financial constraints in reliable contract lifecycle management, companies are also exposed to legal risks in the execution and administrative phases of their contracts. As a result, many of these contracts are better served by a technical approach. Automation of contracts is a viable option to solve the ever-amplifying difficulties of contract management. Suppose a contract which is self-executing: for instance, the contract will initiate the payment automatically once the delivery has taken place. This self-executing contract is in theory far more functional than the traditional paper-based contracts, since it decreases the burden on company's contract management functions (Szabo, 1996).
Smart contracts are among the key emerging use cases of the blockchain technology (Efanov & Pavel, 2018). In the first blockchain generation; Bitcoin, it is not possible to condition the transactions. In other words, the capability of the Bitcoin blockchain is very limited to use it for any purpose other than transferring bitcoins from one account to another. However, defining conditions and clauses to make transaction (smart contract) among the parties could be established by well-known blockchain; Ethereum (Wood, 2014). So, the main objective of Ethereum creation was to provide programming capability to a blockchain platform (Buterin, 2014). Beyond a cryptocurrency; Ether, Ethereum is a platform for smart contracts and a decentralized platform that runs smart contracts on its blockchain (Nagpal, 2017).

The smart contract, which was initiated by (Szabo, 1996) is a computerized transaction protocol which implements the conditions and terms within a contract automatically. Smart contracts could be referred as piece of computer codes between multiple parties that runs on the blockchain by a unique address and include set of rules to fulfil common contractual conditions such as payments, legal obligations, etc. which are agreed upon by the involved parties (Pratap, 2018). Simply put, the smart contracts are similar to the traditional legal contracts except that the computer code dictates the contract terms and clauses instead of legal language. The program enforces the coded functions and controls the transfer of digital currencies or assets in a digital environment which is provided by the blockchain once the outlined conditions satisfy.

The coded terms and conditions in the smart contract are deployed to the blockchain network so that the parties can interact with them. As a result, the transactions are made in a peer-to-peer environment by taking the predefined conditions and terms within the smart contract into the consideration. Transactions that happen in a smart contract are enabled and guaranteed by the co-operating nodes; blockchain (Mik, 2017). The contracts are automatically executed by consensus mechanism; miner nodes, once they have been deployed on blockchain (Hamida et al., 2017; Zheng et al., 2018). Hence, the smart contract allow the users to accomplish data exchange or any transaction without need of any intermediary or trusted authority (X. Li et al., 2017).

3.8 How Smart Contracts Work

In the Ethereum blockchain network, there are accounts which exchange information or anything which has value among themselves. The state (address) of each account and transactions are tracked and recorded by the Ethereum blockchain similar to the other blockchains e.g. Bitcoin. There are two types of account in the Ethereum blockchain namely Externally Own Account (EOA) and Contract Account. EOAs which are allocated to users, are controlled by private keys and do not have code associated with them. Whereas, Contract Accounts, where the smart contracts are stored on blockchain, are governed by their contract codes. The conditions and policies are set in the contract account to fulfill the transactions accordingly (Aung & Tantidham, 2017). The value transaction is possible only between the EOAs and from an EOA to a contract account by creating and cryptographically signing a transaction using their private key. So, the contract accounts are not able to initiate a new transaction on their own. Instead, by a transaction from EOAs to the contract accounts, the codes within the contract accounts are activated automatically and then execute various coded functions such as payment transaction, performing some calculations, etc. (Law, 2017). When a transaction is sent by the EOA to a contract account, the transaction data payload is used to provide input to the contract function to be executed (Bahga & Madisetti, 2016).

The contracts deployed on the blockchain are able to communicate with each other. To put it simple, contracts are able to send messages to other contracts. Transferred message comprises the address of the both sender and the recipient, value to transfer and a data field which includes the input data to the recipient contract (Bahga & Madisetti, 2016). Transaction and message are produced by an EOA and a contract respectively as shown in Figure 3.3.

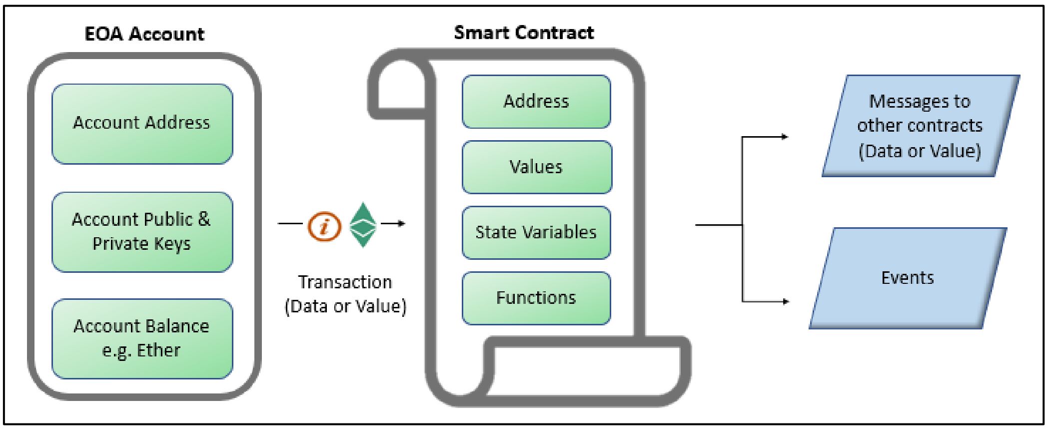

Figure 3.3 Smart Contract Accounts

To establish a smart contract, parties primarily should determine and set the necessary conditions that must be reached to exchange happen. Conditions may be triggered by the parties themselves, external events or milestones. All the contractual agreements are then programmatically written in form of the codes by using programming languages such as Solidity for smart contracts. Afterwards, the coded smart contract is deployed to the blockchain, where it will be self-enforcement when the specified conditions meet.

For a smart contract to initiate, users must utilize an EOA to create a transaction with a Contract Account. This is then encrypted by the initiating users private key and transmitted to nodes across the blockchain. Other uses are able to verify the originality of the transaction using generated public key and that the initiating user indeed the one who triggered the transaction (Smart Contracts Alliance, 2016). Once the majority of the network validate the transaction (consensus), it is linked to the blockchain, the smart contract is successfully enforced, and its outcomes are recorded. Since the computational resources required to carry out the proof-of-work mechanism, every transaction that creates a change in state in the Ethereum platform requires a transaction fee. The miners in Ethereum network are rewarded by the Ether which is paid by the initiator of the transaction. Further, Deploying and executing of the smart contract, transactions that changes the state of the contract, and payment transaction to the parties of the contract cost a fee which is paid by the initiator of the transaction (Wedrowicz, 2018).

Each line of code and every instruction in contract need a certain amount of Gas to be executed. Gas is a unit which is used to calculate the amount of computational effort and related fees that need to be paid to the network (miners) in order to execute an operation e.g. transaction (Rosic, 2017). In other words, the gas fee paid is proportional to the amount of work that is needed to execute the transaction, in terms of the number of instructions (Bahga & Madisetti, 2016). Each transaction within the smart contract is actually is performed by calling of smart contract's functions and instructions. The required Gas for the execution of each contract instructions has been clarified in Ethereum Yellow paper by Wood, (2014).

Gas price refers to the amount of Ether the initiator willing to pay for every unit of gas and is usually measured in "Gwei" Gas prices are specified in Gwei which is fraction of the Ether (1 Ether = 109 Gwei). The initiator of transaction can also determine the gas limit that he is willing to pay for transaction. As a result, the limit of gas and gas price are two main factors which state the total cost of the transaction.

Setting the gas price higher will ensure that the transaction is processed faster since lower gas price is generally less alluring to miners. Hence, transactions that have a lower gas price, take longer to be completed. However, setting a lower gas price is a great idea to make the transactions more cost efficient.

3.9 Key Features of Smart Contracts

Execution of the paper-based contracts mainly rely on vast chain of middlemen such as lawyers, notary and etc. intervention to be fulfilled. This type of enforcement may not be only time-consuming process, but also very ambiguous and costly. However, as discussed before, the obligations of the parties related to the contract enforcement could be written as a computer code in the smart contract. These coded agreements consist out the conditions and related consequences. For instance, if A condition is met, then the consequence B will be carried out by the smart contract automatically without involvement of any intermediaries. Smart contracts play the role of an autonomous agents that run on the blockchain and eliminate the human engage in the execution phase of the contract. Therefore, based on the stipulated instructions that are outlined in the code of smart contracts, they are entirely self-executing with the blockchain immutability acting as a judge's ruling. Hence, the contract execution is guaranteed in case the predefined criteria are satisfied by thanks to this feature of smart contracts.

The decentralized feature of the smart contract could be referred as crucial advantages of the smart contract since the need for the personal and administration involvement to track and enforce the contract such as contract managers, banks, accountants, and even lawyers is removed. As a result, it does not only minimize the cost related to the third parties involvement e.g. administrative cost and transaction cost (Christidis & Devetsikiotis, 2016; Crosby et al., 2016; Fanning & Centers, 2016), but also means contracts are not as dependent on inferences from third parties, as a result, smart contracts are less sensitive to the vulgarities of the other party.

Moreover, the risks of manipulation and nonperformance are eliminated as execution is managed via the network as opposed to any individual party.

Furthermore, Self-executing and decentralized features of the smart contracts expedite the contract execution process. This is in contrast to human participation and time associated with traditional contracts in terms of compliance and execution, smart contracts require less time to execute because of its automatability feature. The contract execution is initiated once the outlined conditions within the contract met.

Beside the self-executing and decentralized properties, immutability is also among the inherited features of the smart contracts. Once the smart contracts are deployed on the blockchain, the block that manages the smart contract cannot be tampered and influenced by different interpretations by an involved party unilaterally without the consent of all the participants (nodes) (Zheng et al., 2017). The smart contracts execute exactly the coded terms of contract and decide the outcome of the contract accordingly which means that interpretation of contracts cannot be conducted in different ways affected by external factors or third parties, hence, there is no place for misunderstands and malicious (Christidis & Devetsikiotis, 2016). In addition, contrary to the traditional contracts where interpretation of the contract terms is performed via human cognition and affected by subjective projections, smart contract terms are interpreted by the binary logic (Savelyev, 2017). Also, by using such contract, parties to the contract commit to the rules and ultimatums of the code. As a result, all the parties are aware of the outcomes of the contract terms once they met and parties cannot interpret the contract in their favor due to the fact that the code execute regardless of subjective criteria.

3.10 Challenges Facing Smart Contract

Prior to wider adoption of the smart contracts and blockchain, main fundamental challenges regarding these technologies should be solved. From a legal perspective, for now there are still regulatory uncertainty and lack of policies on these technologies (Hu et al., 2018) which may arise the concern of the corporation to adopt these technologies. Blockchain and smart contacts have not obtained the government approval yet. Hence, there is an issue of enforceability and control within the technology. As a result, there is a need for the technology to be regulated in a more comprehensive and simple way for a technical and non-technical crowd.

Smart contracts are vulnerable to mismanagement of privacy since all transaction information are visible, transparent, and accessible to all participants of the smart contracts. Although keeping the data secret is in contrast with the nature of the public blockchain, measures need to be drawn up to mitigate concerns over privacy (Bahga & Madisetti, 2016). Moreover, the human errors could be defined as a main challenge of smart contracts application by considering the fact that success of the smart contract is mainly dependent on the written code into it and individuals who draft the codes. As a result, the professionality of the coder directly affects the quality of the contract in executing the conditions properly (J. Li et al., 2018). Hence, care and determination are required to understand the code for contract developers and parties to the contract. For example, there have been scenarios where smart contracts were exploited leading to sizeable financial harm (Popper, 2016; W. Zhao, 2017).

In aspect of usability, there are few limitations exist in these technologies. Firstly, all clauses of a traditional paper-based contracts cannot be coded in the smart contracts since they can only execute specific clauses of a contract such as payment clauses. Secondly, once the smart contracts are deployed on the blockchain, improvement and making changes of the contract clauses based on the later agreed modifications is almost impossible. Hence, it makes the smart contracts inflexible. Thirdly, by involvement of the cryptocurrencies in these technologies, the fluctuation in the cryptocurrencies rate may also raise the concern to apply the blockchain and smart contract. If aforementioned issues are handled without losing reliability and enforceability, smart contracts shall become more mainstream.

As mentioned previously, smart contracts execute the coded functions of contract by examining if predefined conditions of execution have been satisfied or not. The problem arises from the validation of these conditions. In the case that the conditions of execution are outside the blockchain, smart contracts rely on trusted third parties; Oracles. Simply put, Oracles take the data from the real world and inject them to the blockchain (Gatteschi et al., 2018). This issue may decrease the trust of the system because of the intermediary involvement.

3.11 Decentralized Application (DApp)

One of the emerging use cases of the blockchain and smart contract is DApp. Zhang, Schmidt, White, & Lenz, (2018) stated that smart contracts can enable development of DApps to interact with blockchains and provide seamless services to the application users. DApps could be defined as blockchain-empowered website applications, where use the smart contracts to run and manage the state of all network participants (Bahga & Madisetti, 2016). DApps provide a user-friendly interface to smart contracts hence the core logic behind a DApp is presented by the smart contract. Smart contracts are building blocks of blockchain that help maintain the state of all network actors by processing information from outside events (Voshmgir, 2019). Like the applications, DApps also consist of frontend and backend codes with the difference that the instead of a centralized server, backend code of DApps run on the blockchain network which cannot be shut down or restricted as shown in Figure 3.4. (Sultan et al., 2018). The user interface of DApps are similar to Web application. However, its frontend is hosted on decentralized storage networks.

Both traditional web applications and DApps use HTML, CSS, and JavaScript or the like programming language to render a webpage. However, they differ in some respects. In the traditional web page, the data are stored on a centralized server e.g. physical or virtual servers. This web page interacts with a centralized database by calling an API (application programming interface) function to process data and other information stored on servers. User of the web pages generally use ID and passwords for identification and authentication, and since personal information is stored on the service provider's server, security is less (Voshmgir, 2019).

The "wallet" is an application that manages Dapps connection to the blockchain, acting as manager to cryptographic keys and record keeper of private keys and blockchain address, that represents the 30 unique identities and point of reference. A wallet software triggering activity of a smart contract, using a public-key infrastructure, as opposed to an identification and validation method utilizing an API connected to a database, that interacts with a Web3 compatible site. Eschewing wallets means an inability to manage our digital identity and hence not being able to interact with the blockchain. As a result, the Web3 back end provides a layer of infrastructure necessary for Dapps to interact with the decentralized protocol stack. In conclusion, decentralized apps require a tool to manage user's private keys, that allows users to sign transactions on the state layer, i.e. the blockchain.

The features of the DApps are inherited from the blockchain and smart contract since they consist the basis of the DApps. Firstly, the Dapps are stable. The transaction history, information regarding the operations, the behaviors of DApps, the bytecodes of smart contracts are stored on blockchain. Thanks to the distributed feature of the blockchain, each node holds the information of the blocks. As a result, the operation of the system will not be affected by the failure of some nodes e.g. a fire in a central server. This mechanisms ensures that DApps can run stably and guarantee the traceability of DApps (X. Li et al., 2017). The consensus mechanism of blockchain along with public key cryptography ensure security and right operation of smart contracts, so as to maximize DApps security.

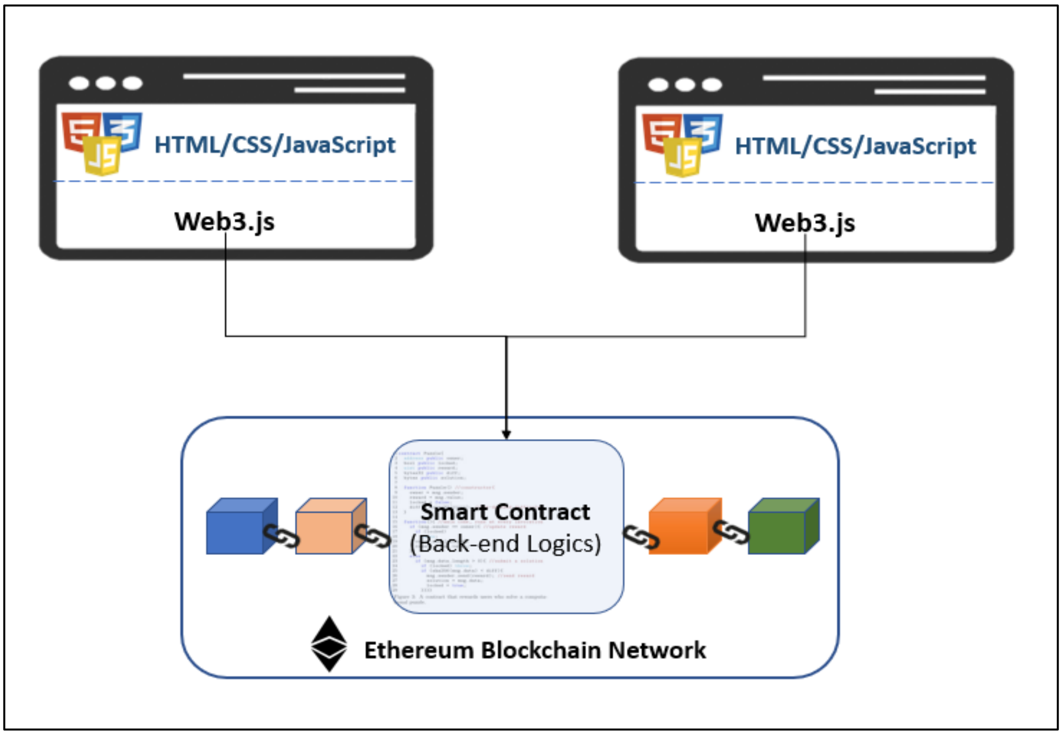

Figure 3.4 Decentralized Application

CHAPTER 4

SMART CONTRACT SYSTEMS FOR GUARANTEED AND TIMELY PAYMENT OF CONSTRUCTION PROJECTS

In this section three smart contract-based systems that are developed for guaranteed and timely payment of construction projects are explained. SMTSEC is presented to ensure security of payment of construction progress payments. BIMSMRTPAY is developed to expedite the conventional progress payment process and to minimize potential payment disputes. RETPAY is designed to expedite and automate the retention payments.

4.1 Research Method

As shown in Figure 4.1, first a vast literature review regarding the payment problems in the construction industry was conducted at the first stage of the research. The reasons behind the payment problems and their impact on project process followed by the existence remedies for these problems were reviewed in this section. As a result of the research, lack of efficient solutions for payment problems which could assure the payments in the construction projects, was identified as the gap. In addition, literature regarding application of the blockchain and smart contracts in construction industry were comprehensively surveyed. Although many research have stated the benefits which blockchain and smart contract could bring to the various phases of construction projects such as data management, contract management, and specially payment domain, very few research have focused on developing smart contract applications to explore their potentials. By taking these gaps into consideration, SMTSEC, BIMSMRTPAY, and RETPAY smart contract systems were developed.

The smart contract of each system , which is backend of the systems, was designed according to the function of each system. Contract parties, the payment clauses, conditions of the contract execution, and etc. are part of the conditions of the systems were outlined in smart contract design phase of the systems. The smart contract of the systems was deployed to a virtual blockchain. Next, user interfaces ,which are frontend of the systems, were developed to notify the smart contract whether the conditions were met or not, so that the smart contract protocol is executed accordingly. In order to reveal the contributions of the systems along with their limitations, each system was applied on a different real case project.

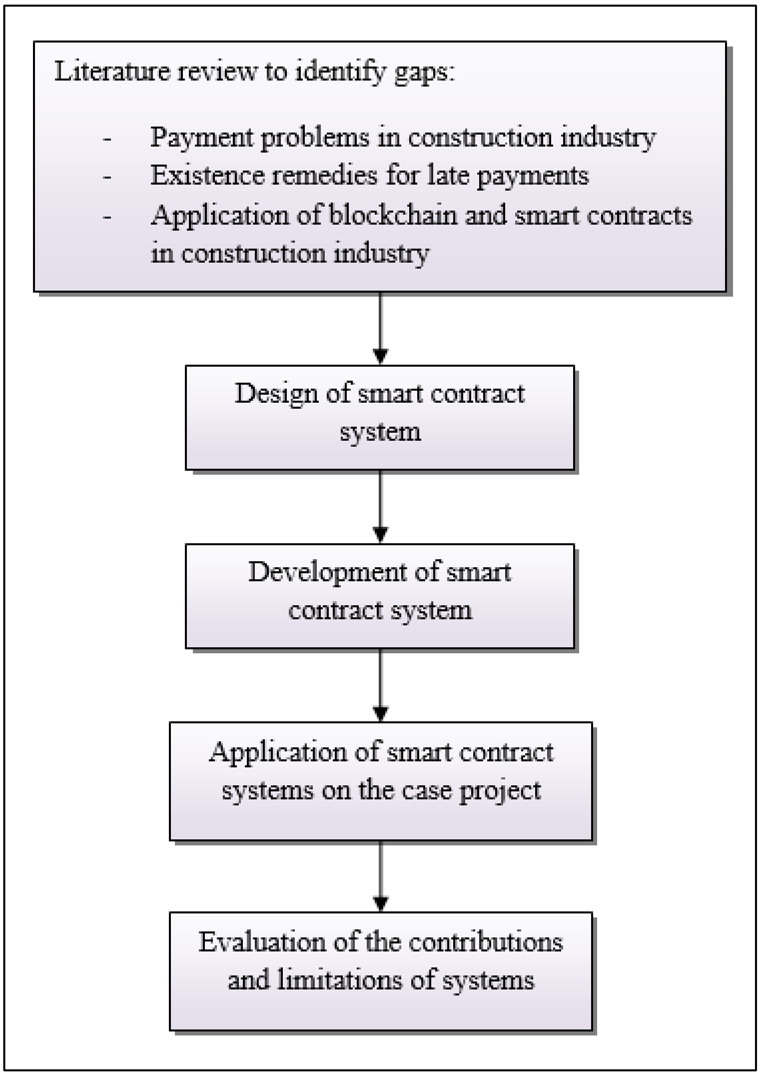

Figure 4.1 Research Method

4.2 SMTSEC

4.2.1 SMTSEC System Overview

SMTSEC is designed and developed to enable a platform for secure, efficient, timely and transparent payment of construction projects by enabling security of payments for works under construction. SMTSEC consists of two modules. The first module is an add-on developed for one of the well-known management software, Microsoft Project 2019, and the second module is a DApp. In this section, the system of using smart contract for secure payment of construction contracts is stated along with the SMTSEC.

In SMTSEC, the employer (EM) and main contractor (MC) as contractor's parties, agree on payment terms of the contract. The agreed terms are then coded (smart contract) and deployed on the blockchain so that smart contract is enabled to execute the coded functions and interface with the parties. The progress payment period is assumed to be made on monthly basis in SMTSEC since generally the interim payments are made monthly in construction projects. Before the project starts, the projected progress payment amount for the upcoming progress payment period is determined using the planned cash flow of the project. Smart contract enables the SMTSEC to block the projected related month's payment at the beginning of the month to ensure security of progress payments. Smart contract automatically transfers the progress payment amount to the contractor's and subcontractor's wallets according to the predefined terms, immediately after employer's approval of the progress payment as shown in Figure 4.2. Smart contract of the SMTSEC then blocks the projected progress payment amount for the next period(s) along the transfer of the funds to secure the payments for the next payment period(s). The procedure is repeated for the next progress payment period until the project is completed.

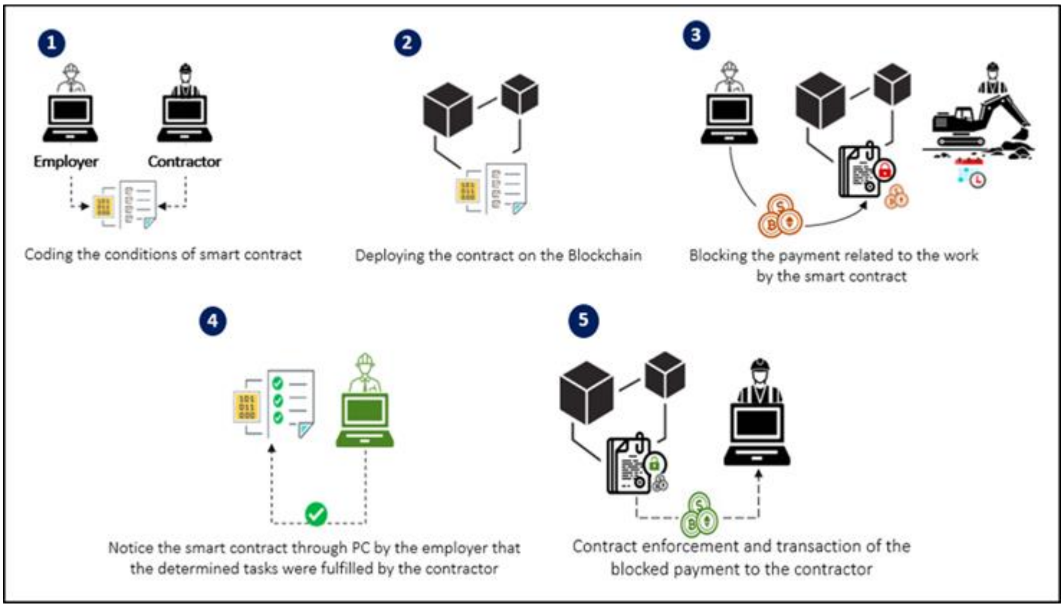

Figure 4.2 Payment Process of SMTSEC According to Determined Conditions

4.2.2 Smart Contract Conditions

Unique to each project, the smart contract conditions include but are not limited to a number of major criteria: , the fiat currency (Cur) that the payments are to be made according to the contract document, The Cryptocurrency Type (CryT) that the Cur will be converted, Period Block (PeriBloc), i.e. the period within the smart contract blocks and holds the funds of the EM until the date of progress payment application by the MC, the period that the owner's blocked funds can only be used for payment of progress payments (PeriPay), a contingency amount (Cong) which is the additional amount of CryT that will be blocked to manage possible CryT/Cur fluctuations and potential increases in the progress payments, the percentage amount that is paid to SCs for the subcontracted tasks and is called Percentage Subcontractors ($SubPer_i$) throughout this study, and finally The employer's (WAdEM), contractor's (WAdMC), and subcontractor's ($WAdSC_i$) wallet addresses (WAd) should also be included in the smart contract.

4.2.3 Microsoft Project Add-on

The first module of SMTSEC is an add-on which was developed for Microsoft Project 2019 in C# with Visual Studio 2019. The first module named “MPP Parser” enables the contractors to use their existing schedule and cost data to determine the projected and actual progress payment amounts and to facilitate the data exchange among the proposed system. The schedule and payment data (including planned and actual completion dates, planned and actual quantities, unit prices and responsible party of the tasks) of all of the progress payment items should be included in a Microsoft Project file to initiate the SMTSEC process.

The contractor then should select the month of the progress payment and the Microsoft Project file which includes the progress payment and schedule data using the MPP Parser as shown in Figure 4.3. In the beginning of the project the project, the contractor should select the month that corresponds to the month before the first progress payment to initiate blocking of the first month’s projected progress payment amount (PPP). At the end of each month, the contractor should update the Microsoft Project file by entering the actual quantities completed, and actual start and completion dates of the activities. MPP Parser will calculate the progress payment amount (APP) and its breakdown for the selected month and the projected progress payment amount for the next month. As demonstrated in Figure 4.3, once the contractor selects the “PPP Export” and “APP & Pays Export” button of the MPP Parser, it will create two separate “.TXT” files to transfer the actual and projected progress payment amounts to the second module of SMTSEC.

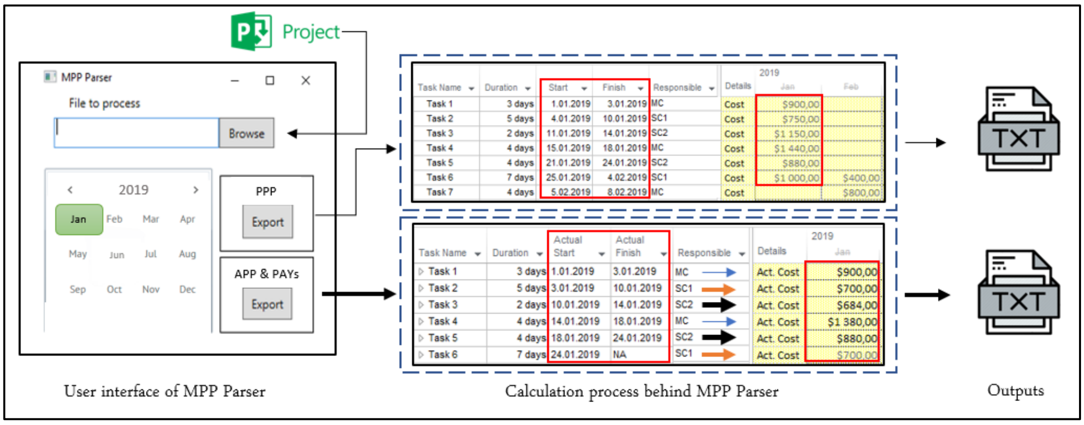

Figure 4.3 MPP Parser Module of SMTSEC

Each project contains many tasks which are distributed throughout the project period according to their start dates, duration, relationships among tasks and etc. which are determined during the planning phase of the project. The PPP related to a specific period e.g. the first month of the project is the sum of the estimated cost of the works (tasks) that are planned to be proceeded by the project parties such as the main contractor and the Subcontractor (SC) and suppliers in that period of time. Since these tasks involve resources e.g. material, machinery, manpower, and etc. assigning the quantity and cost of every resource to the corresponding activity provides the planned budget of the project. Spreading out the monetary values added by these resources over the project duration provides the periodic PPP for the project.

The PPP calculation behind the MPP Parser is that it looks at ‘’task Usage’’ sheet of the MS Project. Afterwards, it looks for the activities that have the start date and or start-finish date in the selected period thorough the calendar of the system. It also checks the actual start and actual finish date of those activities which should be N/A, to ensure that those activities have not been started yet. Then it looks cost of those activities in the selected period and it sums all those costs and export it as a single number to a “.TXT” file.

In the construction projects actual progress payment is prepared by the contractor which includes the payment the owner makes to the contractor based on the contract conditions and the progress that has been made. The total of Actual Progress

Payment (APP) mainly includes the actual cost of the works that have been carried out by the contractor, subcontractors and suppliers. In order to calculate the APP of the selected period, actual progress values, monetary values of the progress, cost information, and updated schedule information are entered in MS Project at the end of each month.

In the ‘’Task Usage’’ sheet of the MS Project, MPP Parser looks for the activities that their actual start and or both actual start- actual finish are in the selected period. When the MPP Parser retrieves the APP amount from the MS Project, it also obtains the exchange rate to calculate the payment amount that should be paid to the contractor (PayMC), the subcontractors and suppliers (Pay_i). In order to calculate the amount to be paid to the parties separately, the MPP Parser is coded such a way that it looks for the tasks that have been fulfilled and proceeded in the selected period. Also, it looks for the response of those tasks which are MC, SCs and suppliers. MPP Parser calculates the PayMC and Pay_i by adding the actual payment of the tasks within the selected period and in the responsibility of the MC, SCs and suppliers respectively. Finally, it exports those amounts in a ‘.TXT’ file to transfer to the second module of SMTSEC.

4.2.4 Decentralized Application

The second module of SMTSEC is a DApp. The frontend of the DApp web page is developed by HTML5, CSS3, PHP, JavaScript programming languages. The smart contract part of the DApp (backend) is developed in Remix IDE with Solidity 0.4.0 language and Web3.js is used for interacting HTTP web page with the blockchain node and the smart contract. The smart contract is deployed on Ethereum blockchain, the most commonly used blockchain among the blockchains supporting smart contracts. The tests of SMTSEC were performed on the Ganache blockchain which is a virtual Ethereum blockchain that does not require any deployment or transaction fees. In this study, CryT is taken as Ethereum (ETH), Cur is taken as the United States Dollar ($), and progress payment period is taken as 30 days. However, other fiat currencies that can be converted in a cryptocurrency exchange can also be used in SMTSEC.

4.2.4.1 PPP Blocking

By the mean of the DApp, the contractor should request blocking of the first month's PPP right after start of the project. The DApp will get the PPP amount for the first month from the ".TXT" file which was previously provided by the contractor through the MPP Parser module. Once the DApp is executed, it will acquire the latest ETH/Cur exchange rate form a website and display the amount to be blocked (Bloc) by considering the Cong amount for the first month in both Cur and ETH on contractor's screen as shown in Figure 4.4. The contractor should enter WAdMC 's private key and press the "Blocking Request" button to complete the blocking request.

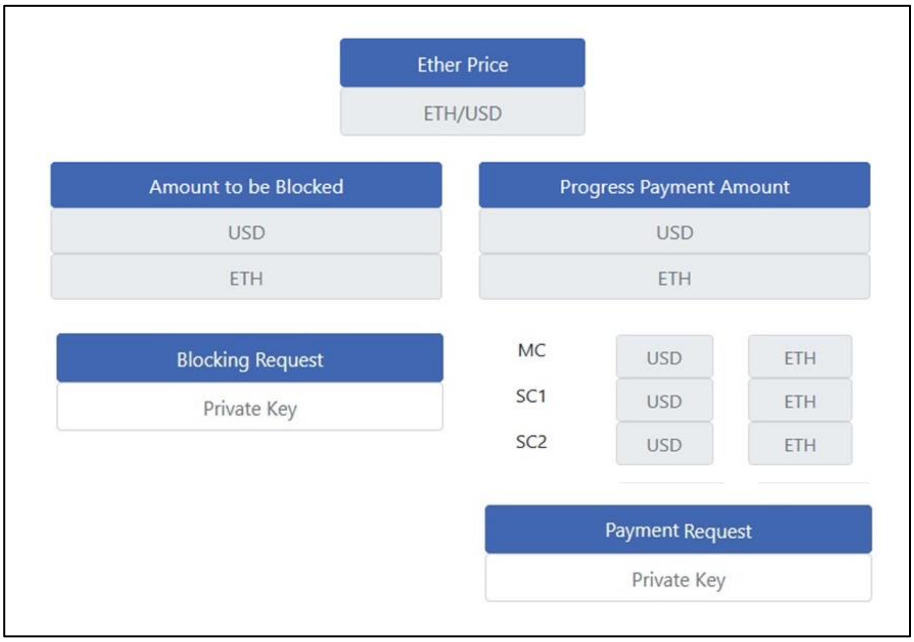

Figure 4.4 Contractor's Screen for DApp Module of SMTSEC

The DApp will then show the request on the employer's screen under the "Amount to be Blocked" as shown in Figure 4.5. The employer has to deposit the required funds in ETH to the WAdEM and then the enter the private key of the WAdEM to approve the blocking of the funds. If the balance of EM's WAdEM is adequate, smart contract automatically deducts the Bloc amount from it and blocks it such a way that no single party can access or withdraw it before PeriBloc is over. The pseudo code of blocking process is given in Figure 4.6.

Figure 4.5 Employer's Screen for DApp Module of SMTSEC

```
function PPP Blocking {
    require MC's claim through SMTSEC;
    Retrieve the PPP amount from MS Project cashflow;
    Convert the fiat currency (Cur) of the PPP amount into the CryT;
    Bloc= (Cong) × (PPP) ;
    require EM's approvement  through SMTSEC;
    if WAdEM's balance ≥ Bloc Then
        Reduce Bloc from the WAdEM;
        Block Bloc for the PeriBloc = true;
     else
            Alert the EM through SMTSEC to deposit the deficit (Bloc – WAdEM's Balance);
     end;
     }
```

Figure 4.6 Pseudo-code of Blocking Process Decentralized Application

4.2.4.2 Payment and Release

The contractor could request the progress payment of the first month and blocking of the projected progress payment for the second month consecutively after PeriBloc is over. Once the PeriBloc period is over, the actual payment amounts of related period is obtained from the MS Project through MPP Parser. The afterwards, DApp will display the total APP, progress payment amounts of the main contractor (PayMC) and the subcontractors (Pay_i) in both Cur and ETH.

The contractor should first enter its private key and then press the “Payment Request” button to send a request of payment to the employer as shown in Figure 4.4, which will be displayed on the employer’s screen under the “Actual Amount”. The payment amounts will be transferred to the specified wallet address of main contractor and subcontractors immediately after employer’s approval if the blocked funds are sufficient to make the payments. The excess amount of the blocked amount will be released and transferred to the WAdEM along with the payments. The DApp will request the employer to deposit the deficit amount if the blocked amount is not sufficient to make the progress payment. The pseudo-code of payment process is provided in Figure 4.7. Once the contractor and subcontractors receive the payments in ETH, they can convert it to any fiat currency in the local cryptocurrency exchanges. The contractor can request blocking of the second month’s after the payments of first month are made. The procedure is repeated every month until the project is completed. The flow chart of the blocking and payment processes is shown in Figure 4.8.

```
function Payment {
require MC's claim through SMTSEC;
Retrieve the APP amount from the cash flow;
Convert the (Cur) of the APP amount into the CryT;
if PeriBloc period passed Then
     require MC's claim through SMTSEC;
     require EM's approvement through SMTSEC;
                    if APP = Bloc Then
                         Unblock Bloc = true;
                         Transfer the Payi of the SCi to their WAdSCi according to the SubPeri;
                         Transfer the PayMC to WAdMC;
                    elseif APP < Bloc Then
                         Unblock the embedded Bloc = true;
                         Transfer the Payi of the SCi to their WAdSCi according to the SubPeri;
                         Transfer the PayMC to WAdMC;
                         Transfer the excess amount (Bloc – APP) to WAdEM;
                    else
                         Do not unblock the Bloc = true;
                         Alert the EM to deposit the deficit amount (APP – Bloc) through SMTSEC;
                    end;
else
      Alert the MC through SMTSEC that the APP could not be claimed before the PeriBloc is over;
end;
}
```

Figure 4.7 Pseudo-code of Payment Process

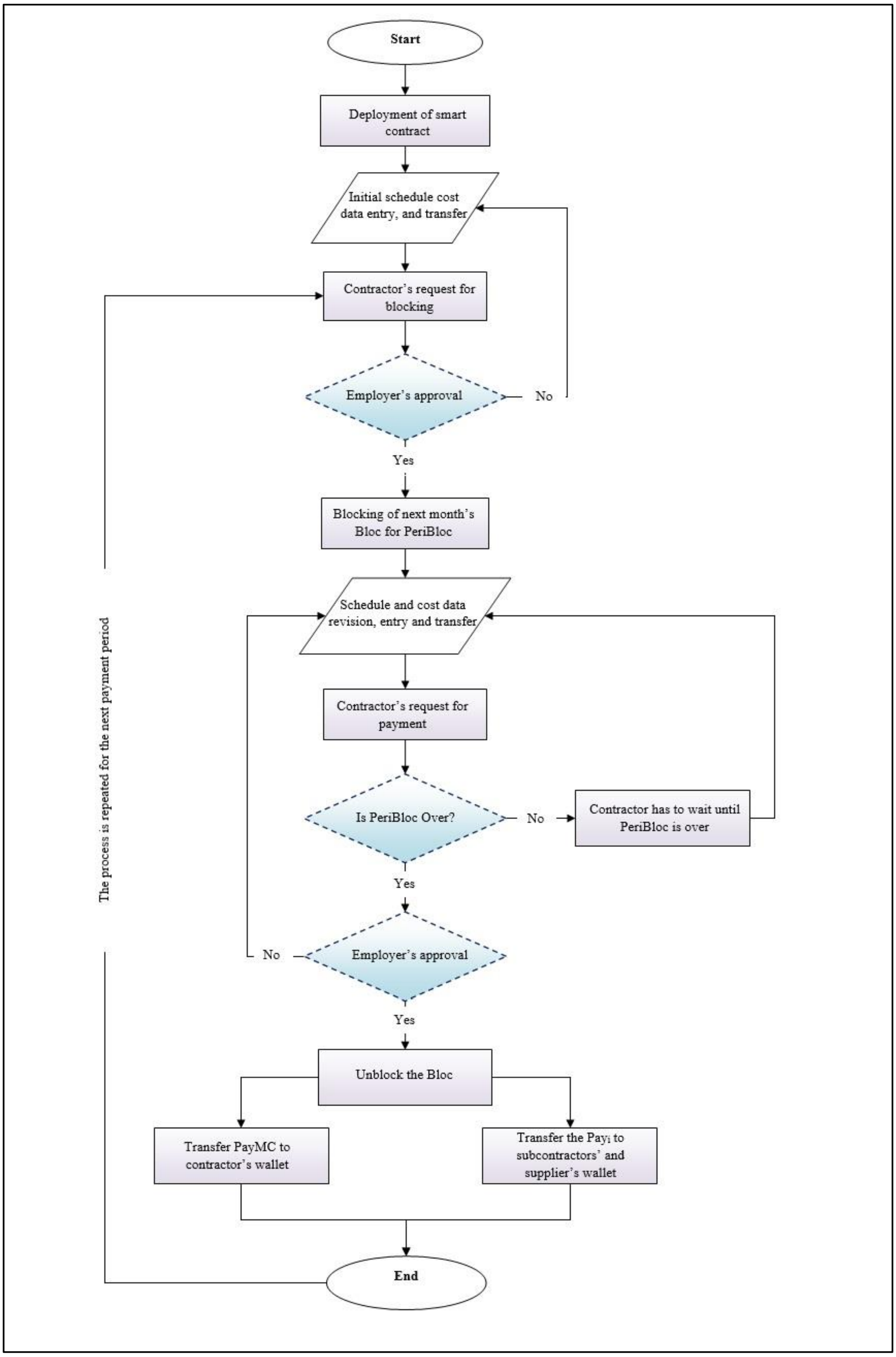

Figure 4.8 Flow Chart of Blocking and Payment Processes

Smart contract enables the blocked amount to be released and SMTSEC enables the employer to withdraw that amount if the contractor does not request a progress payment or the employer does not approve the contractor's payment request within PeriPay. Hence, the maximum period that the funds of the employer will be blocked is PeriBloc plus PeriPay. After the maximum blocking period, SMTSEC will release the blocked funds and will transfer them to WAdEM, if the employer presses "Withdraw Blocked Funds" button on the employer's screen. The release procedure prevents the employer's funds to be blocked indefinitely. The pseudo code of release process is provided in Figure 4.9.

```
function Release of {
    if PeriBloc + PeriPay period is over Then
        Unblock the Bloc and allow the EM to withdraw the Bloc;
        require Private key of WAdEM;
        require EM to press 'Withdraw Blocked Funds' button through SMTSEC;
        Transfer the Bloc to WAdEM;
    else
        Do not unblock the Bloc = true;
        Alert the EM that Bloc could not be withdrawn ;
    end;
    }
```

Figure 4.9 Pseudo-code of Release Process

4.2.5 SMTSEC Case Study

In order to demonstrate the SMTSEC applicability within the industry, it was applied to a real construction project. The case project compromised of civil works of a 3,000 m^2 powerhouse building that is under construction in Turkey. The budgeted cost of civil works of the powerhouse building is $20 Million. The parties in the case study are Employer (EM), Main Contractor (MC), and two Subcontracts. Subcontractor 1 (SC1) is responsible for reinforcement works whereas the structural concrete works are carried out by Subcontractor 2 (SC2).

At the first stage, information regarding payment clauses such as project participants, WAdEM, WAdMC, WAdSC1, WAdSC2, PeriBloc, PeriPay, and $SubPer_i$ were coded in the Ethereum smart contract. Moreover, the functions discussed in the second module of SMTSEC were specified in the smart contract. The PeriBloc and PeriPay period was considered as 30 days and 60 days respectively. In addition, the SubPer1 and SubPer2 were considered as %50. Furthermore, the Cong percentage was considered as 20%. The developed smart contract was deployed to a virtual blockchain environment named Ganache to execute the condition and transaction of the data so that the proposed system is validated.

The civil works of the case project started on March 1, 2019. MPP Parser module of SMTSEC was used to calculate the PPP amount for March 2019 and to create the ".TXT" file to transfer the first PPP amount to the DApp. then the Bloc amount was presented in EM and MC screen under "Amount to be blocked" section as shown in Figure 4.10. The DApp was executed on March 1, 2019 to convert the first month's PPP of $272,417.74 to 1,980.50 ETH at the exchange rate of 137.55 ETH/$. Hence, with a Cong of 20%, the Bloc was calculated as 2,376.60 ETH by the DApp. The blocking request was submitted to the EM once the MC entered the private key of the WAdMC and pressed the "Request" button. The EM approved the Bloc amount by entering the private key of the WAdEM and pressing "Approve" button. Consecutively, the smart contract reduced the 2,376.60 ETH from WAdEM and embedded it in the contract for the 30 days. The balance of employer's wallet deduced to 8,664.34 ETH from 11,040.94 ETH as shown in Figure 4.11.

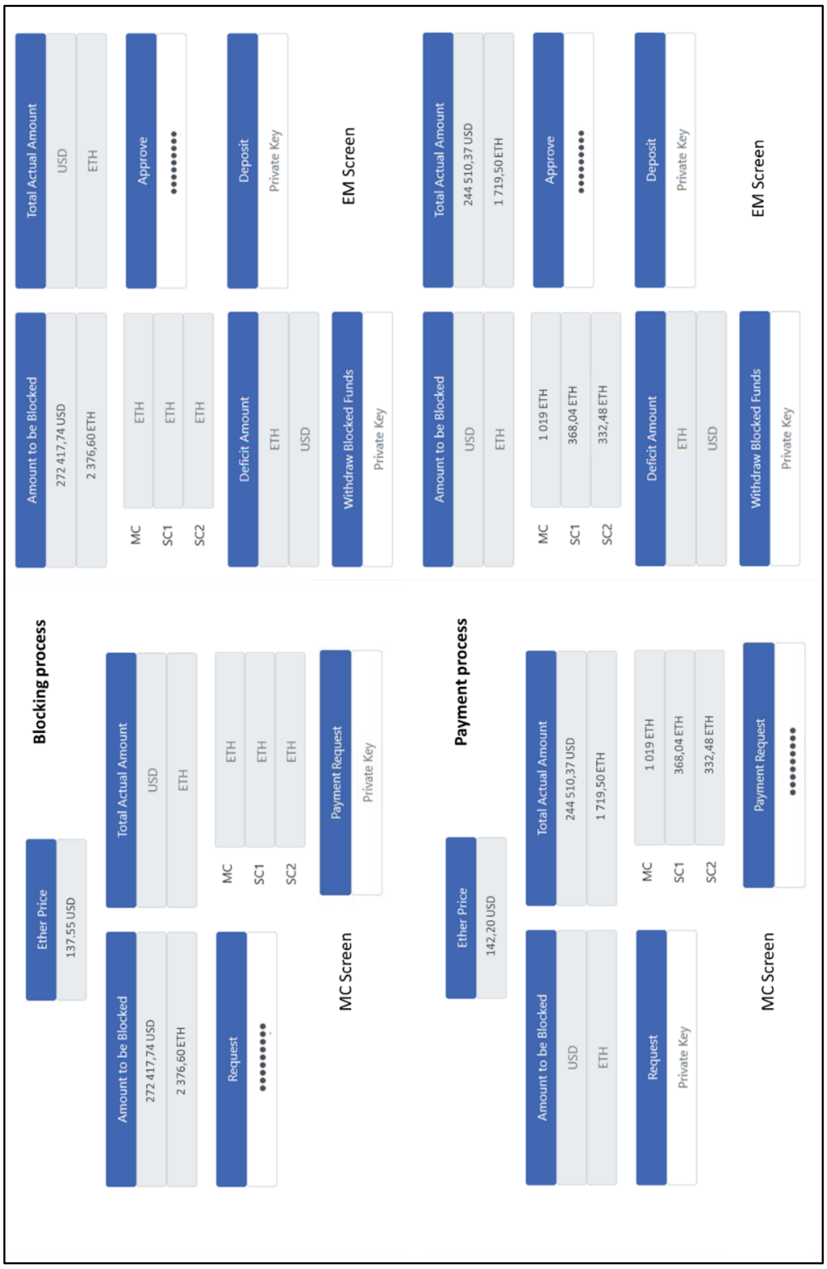

Figure 4.10 Screen of Contractor and Employer in DApp Module for The Case Project

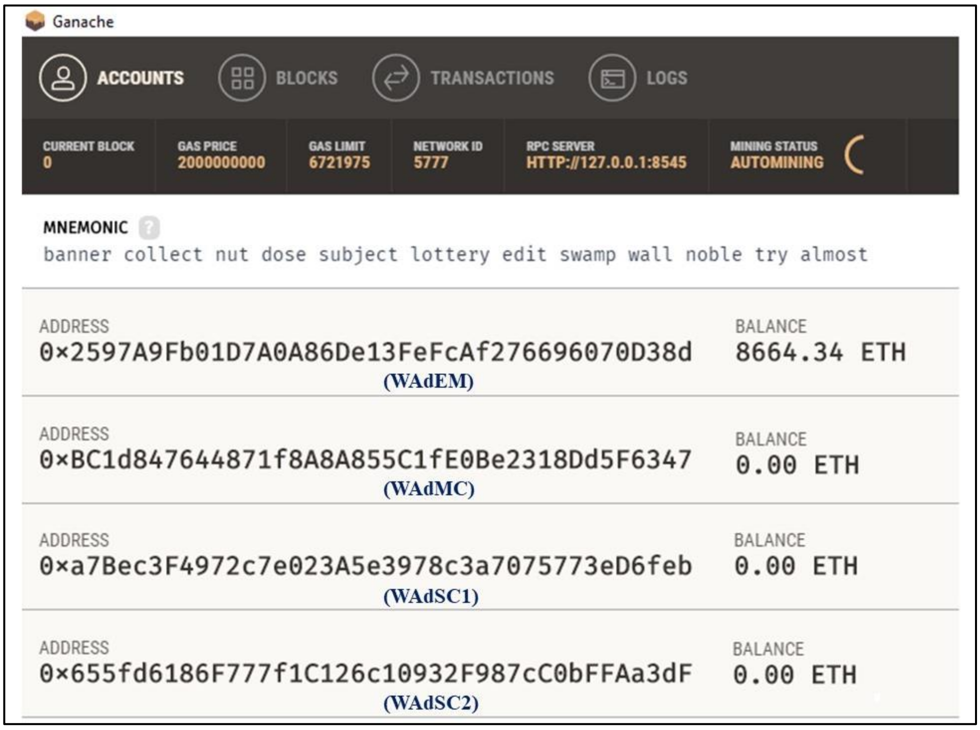

Figure 4.11 Balances of Wallets for SMTSEC Case Project After Blocking Process

On April 1, 2019 the schedule was updated according to the actual progress carried out by the parties. The MC requested for the progress payment by entering its private key and pressing “Payment Request”. The amounts of total progress payment, PayMC, PaySC1, and PaySC2 which are $244,510.37, $144,897.92, $52,334.95 and $47,277.5 were retrieved form the MPP Parser module which is presented in Figure 4.12 and were converted by the DApp to the ETH at the rate of 142.20 $/ETH as 1,719.5 ETH, 1,019.00 ETH, 368.04 ETH, 332.48 ETH. The amounts were shown on both EM and MC’s screen as declared in Figure 4.10. Once the EM approved the progress payment by entering its private key and pressing “Approve” button, the smart contract released the blocked amount and transferred to WAdMC, WAdSC1, WAdSC2. In the transferring stage, smart contract considered the SubPerSC1 and SubPerSC2 (50%) so they eventually received half of the payment accordingly. So, the amounts that were transferred to WAdMC, WAdSC1, and WAdSC2 were 1,369.23 ETH, 184.02 ETH, and 166.24 ETH respectively.

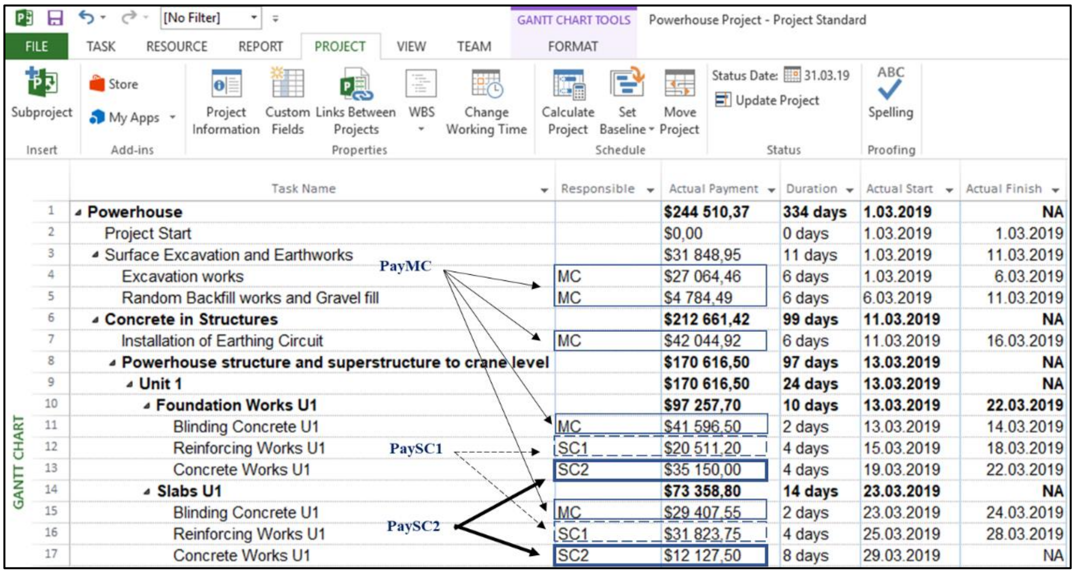

Figure 4.12 Actual Progress of Case Project at End Of March 31 2019

In the presented case, since progress payment amount 1,719.50 ETH was less than Bloc 2,376.60 the excess amount; 657.12 ETH was transferred to the WAdEM. Figure 4.13 illustrates the final balance amount of the WAdEM, WAdMC, WAdSC1, and WAdSC2 respectively from up to down.

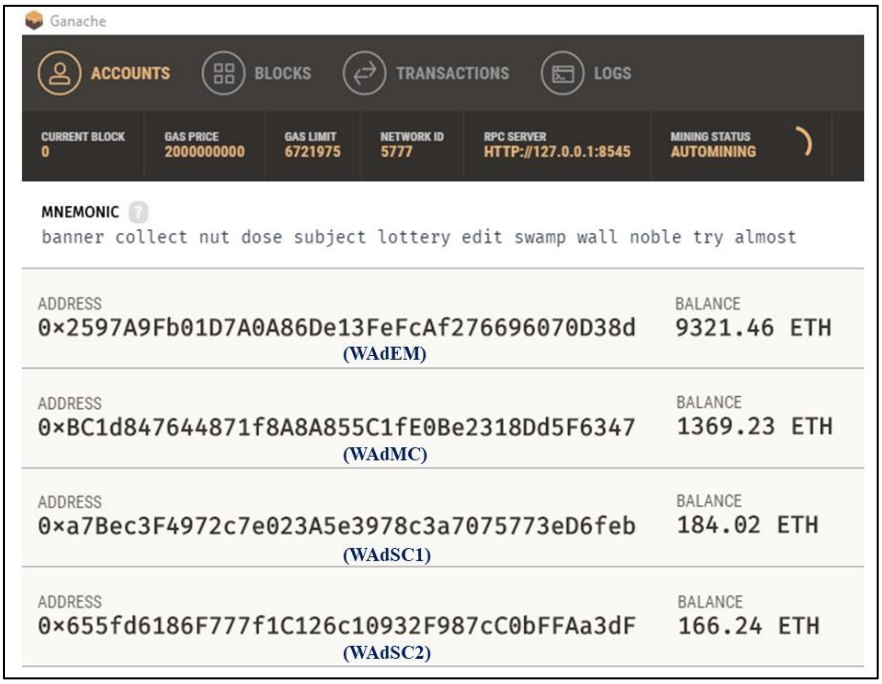

Figure 4.13 Balances of Wallets for Case Project After Payment Process

4.3 BIMSMRTPAY

In order to expedite the payment process, automate the calculation of the progress payment amount, reduce the uncertainties at the time of the progress measurement, guarantee the simultaneous payment to the contractor and lower tiers, and minimize the vagueness of payment clauses, a novel object-based progress payment system namely BIMSMRTPAY was developed. In BIMSMRTPAY the BIM model is applied to determine the progress followed by 3D visualization of the progress. Besides, the cost of the objects, objects' name, and etc. are outlined in the smart contract. The smart contract performs the progress payment calculation and transaction of the progress payment to the specified parties in the contract.

4.3.1 BIMSMRTPAY System

BIMSMRTPAY consists of two sections. The first module is a plug-in developed for the main BIM software, Revit 2019, and the second module is a DApp. In BIMSMRTPAY the 3D BIM model of the project is needed to initiate the process. 3D model of the project consists of separate objects which they constitute the whole project. At the first stage, the employer and main contractor agree on the price of each object to be specified in the smart contract. Moreover, the shares of the subcontractors are determined in this stage. In the progress payment period, the contractor determines the completed objects within that period through the BIM model via Revit and then progress payment amount is calculated by the smart contract. Once the employer approves the payment claim, the payment amount is paid to the contractor, subcontractors, and suppliers simultaneously. Moreover, the visualization of the progress is also in the scope of the BIMSMRTPAY system. Figure 4.14 presents the overall BIMSMRTPAY process.

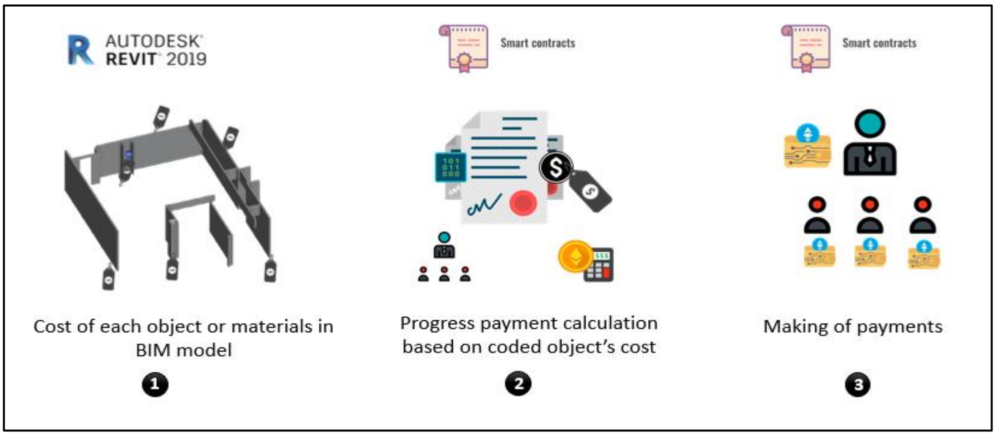

Figure 4.14 BIMSMRTPAY

The conditions of the smart contract include Cur, CryT, WAdEM, WAdMC, and WAdSC$_i$ wallet addresses. As shown in Figure 4.15, the name of each object of the 3D BIM model is defined in the smart contract to calculate the progress payment amount accordingly. Besides, the amounts in Cur that should be paid to main contractor (PayMC) and to the subcontractors (PaySC$_i$) at the completion of each object, are also included in the smart contract. Furthermore, any change in the works of the contractor (PerChangeMC) and subcontractors (PerChangSC$_i$) which may affect the payment amount of the related party, are also outlined as variables in the smart contract.

```
constructor() public {

        addObjects("Beam-0-1", PayMC*PerChangeMC, PaySCi*PerChangeSCi, , ,);
        addObjects("Column-0-2", PayMC*PerChangeMC, PaySCi*PerChangeSCi, , ,);
        addObjects("Roof-0-3", PayMC*PerChangeMC, PaySCi*PerChangeSCi, , ,);
        addObjects("Floor-0-4", PayMC*PerChangeMC, PaySCi*PerChangeSCi, , ,);
        addObjects("Wall-0-5", PayMC*PerChangeMC, PaySCi*PerChangeSCi, , ,);
```

Name of the objects | Amount to be paid to MC and the PerChangeMC | Amount to be paid to SC$_i$ and the PerChangeSC$_i$

Figure 4.15 Smart Contract Clauses Related to the Objects

4.3.2 Revit Plug-in

In the modeling phase of the project, a unique ID or name is assigned to each object of the model. These object names or IDs are necessary to recognize each completed object in the proposed BIMSMRTPAY system. In order to retrieve the completed object names and then visualize the progress, a plug-in named PROGITVIS was developed for Revit 2019 in C# with Visual Studio 2019 as shown in Figure 4.16. To initialize the PROGITVIS plug-in, shared parameters are defined in the 3D BIM model. These parameters include Object Name, Period, Completed checkbox, and PerChange. The PROGITVIS performs two functions which are exporting the names of the completed objects within the progress payment period and progress visualization as shown in Figure 4.17.

By the mean of 3D model in Revit, in the progress payment period, the contractor checks the tick box for the completed objects of the progress payment period through "Completed" parameter. It also determines the completion date of each completed object in "Period" section. In the cases of change orders by the owner, change in the price of object, and change in the required materials for the related objects, the contractor can determine percentage of the change through "PerChange" section. The PerChange also could be used as percentage of the completion at the time of applying the system in unit price type of the contracts. In the progress payment period, the contractor should select the month that corresponds to the progress payment month and then press "Export Completed Object's Name" button through PROGITVIS. A ".TXT" file including the names of the completed objects of selected period and change percentages value is exported to initiate the second section of BIMSMRTPAY. In the exporting process, the PROGITVIS is coded such a way that it considers the "Completed" and "Period" parameters of the objects and then it exports the information. Hereby, the information related to the uncompleted objects and those which were completed before the selected period are ignored to be appended into the ".TXT" file.

Moreover, a visualized report of progress is provided by the PROGITVIS plug-in. The PROGITVIS visualizes the completed objects related to the last progress payment period and previous periods by just selecting the period through calendar and then pressing the "Visualize Progress" button as presented in Figure 4.16. It also visualizes the changes made on any object in any period. Furthermore, the upcoming works could be easily identified since the uncompleted objects are visualized in this module.

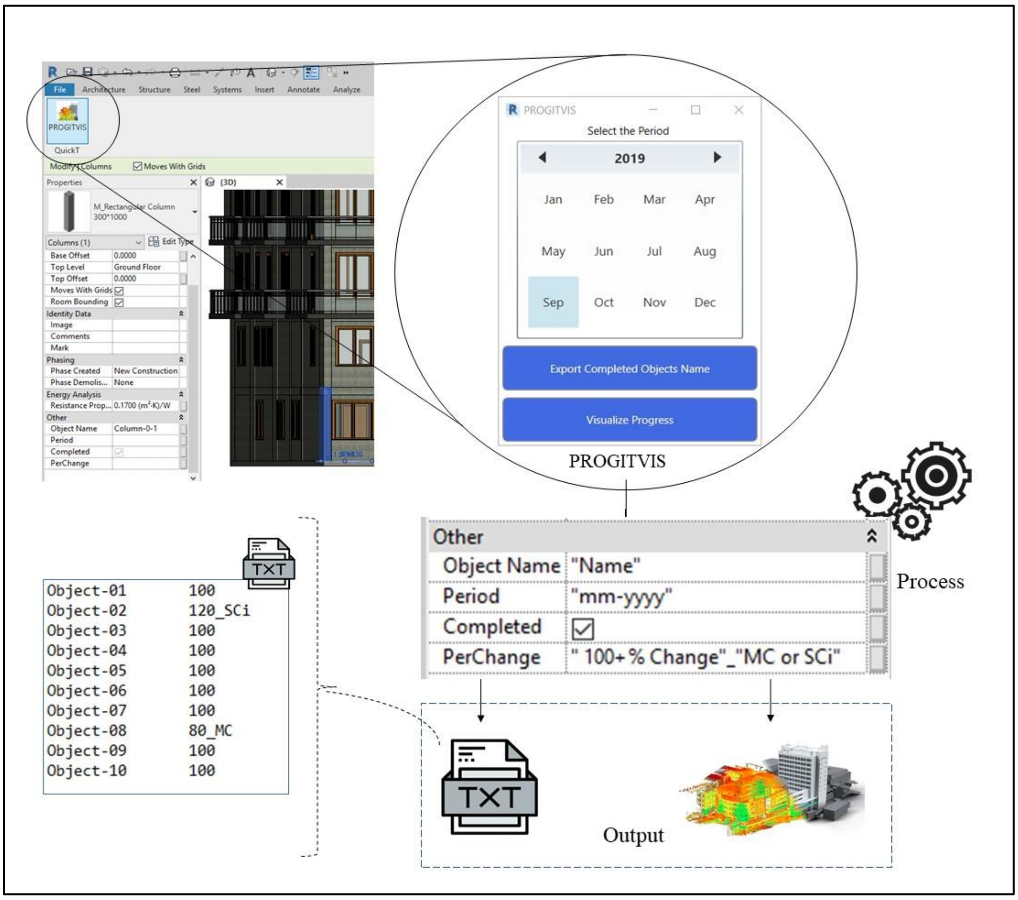

Figure 4.16 PROGITVIS Section of BIMSMRTPAY

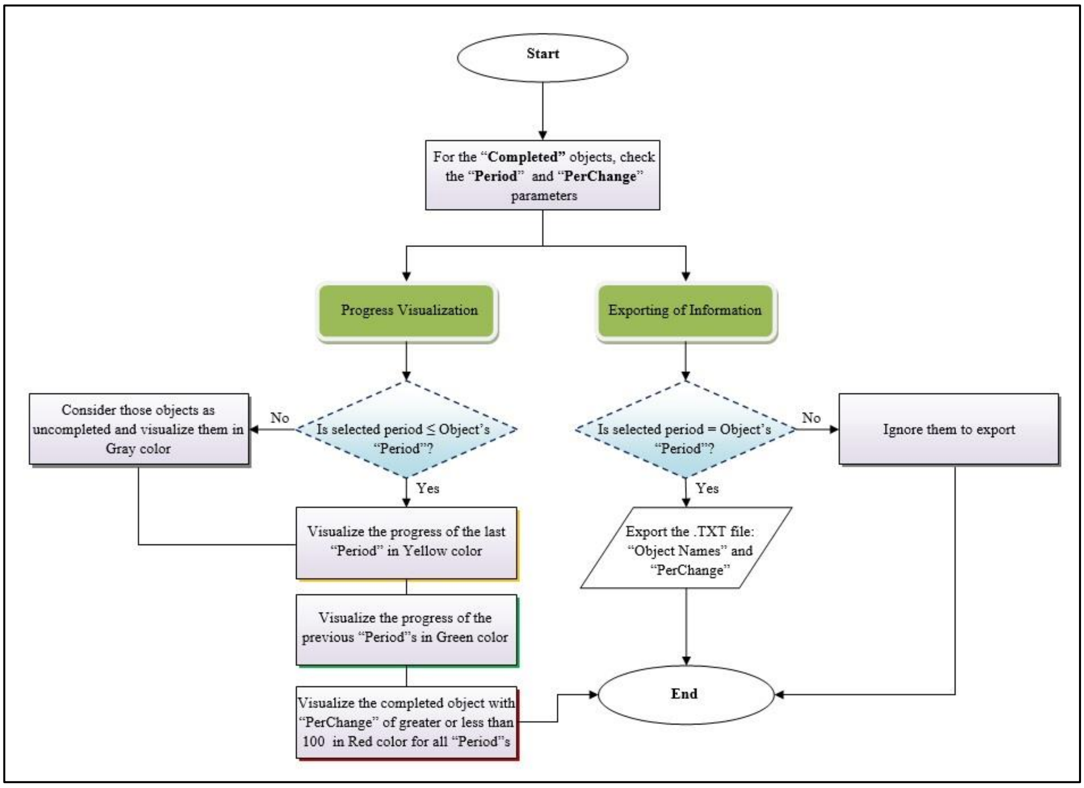

Figure 4.17 Functions of PROGITVIS Section

4.3.3 Decentralized Application

A DApp is developed for the second module of the BIMSMRTPAY. HTML5, CSS3, PHP, JavaScript are used to develop the frontend of the DApp webpage. The web part is developed using the PHP Laravel 5.8 Framework in the backend. The smart contract is developed in Remix IDE with Solidity 0.5.2 language and Web3.js is used for interacting web page with the blockchain node and the smart contract. The smart contract is deployed to a virtual Ethereum blockchain, namely Ganache to test the DApp section of BIMSMRTPAY. In this section, ETH and United States Dollar ($) are taken as CryT and Cur respectively. Moreover, to increase the security of the system, instead of private keys, MetaMask is used as the user interface for identity management on the Ethereum blockchain. The DApp is linked to the first module PROGITVIS through the ".TXT" file as shown in Figure 4.18.

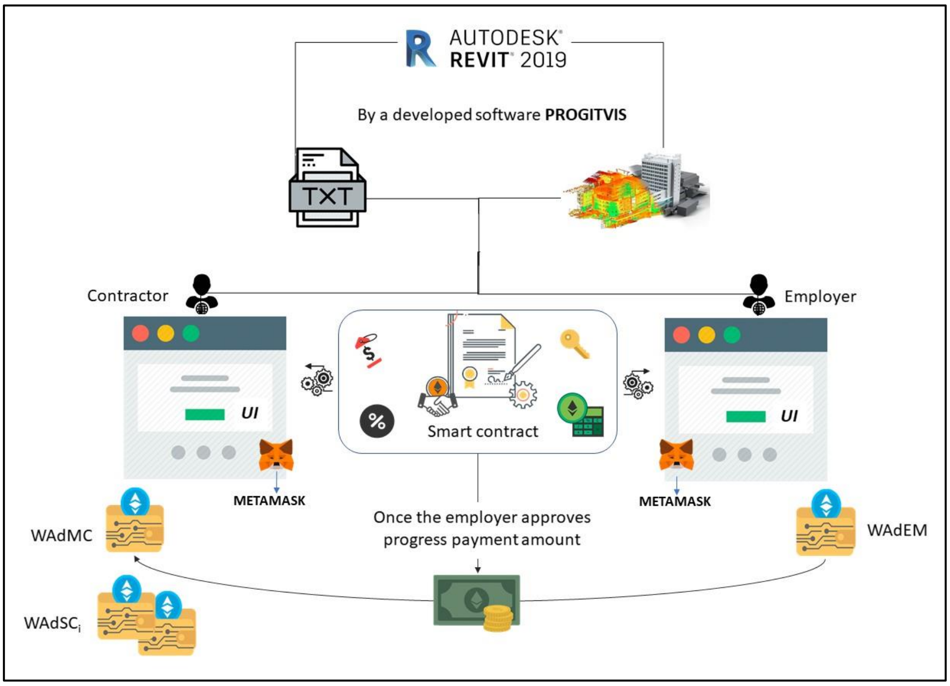

Figure 4.18 BIMSMRTPAY Overall Process

The contractor has to login the MetaMask using his account password to start the process. By the mean of the DApp, the latest ETH/Cur is retrieved form an exchange website and then contractor presses the "Calculate the Payment" button, as shown in Figure 4.19, so that the progress payment amount be calculated and be converted to ETH. The DApp will get the names of the completed objects and related PerChange from the ".TXT" file which was previously provided by PROGITVIS section. Since the completed objects' names along with objects' price are embedded into the smart contract, the smart contract automatically calculates the payment amounts by considering the PerChange and then they are shown on the MC's screen in both ETH and Cur. Also, the smart contract gets the PerChange of corresponding party to multiply the amount to the paid with the PerChange of related party.

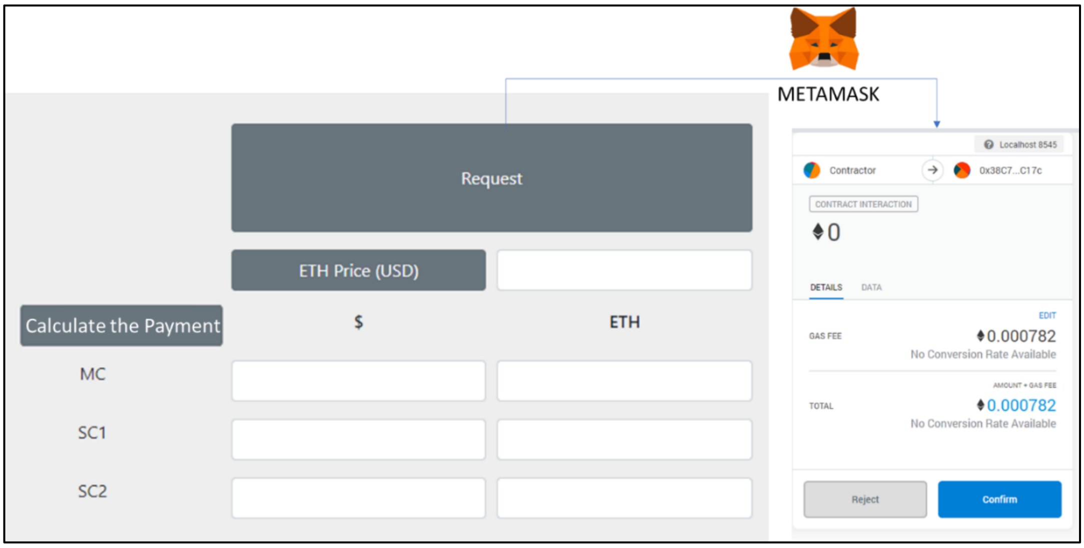

Figure 4.19 Contractor’s Screen for The DApp Section of BIMSMRTPAY

The MC uses “Request” button of the DApp to request the approval for progress payment, as shown in Figure 4.19 . Once the MC presses the “Request” button, the DApp directs the MC to login the MetaMask using his wallet specified in the smart contract. DApp will then check whether the MC’s wallet address is same as the address specified in the smart contract. If the addresses are same, the request will be submitted and then DApp notifies the employer by displaying “You have a request to approve” massage on the employer’s screen along with showing the requested amount under the “Payment Amounts” section of the employer’s screen as declared in Figure 4.20. Notifications are shown from interface on the information fetched from smart contract.

In progress payment calculations, smart contract checks whether the payments of the requested works have been paid previously to prevent double payment, using the latest list of completed objects which are stored on the blockchain as shown in Figure 4.21.

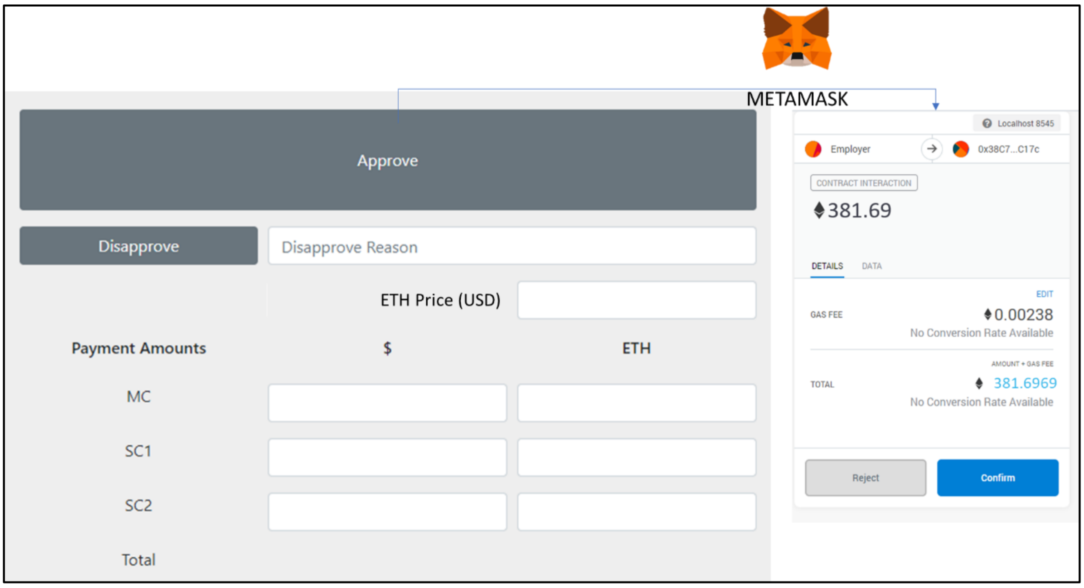

Figure 4.20 Employer's Screen for The DApp Section of BIMSMRTPAY

The DApp requires EM's approval to complete the progress payment process for the specified period. The employer has to login the MetaMask using his account password to start the approval process. Once the employer logins, the MetaMask will also show the requested amount and transaction fee as well as the DApp. If the employer does not approve the requested payment amount through pressing "Disapprove" button, he will be able to describe the reason of the disapproval through "Disapprove Reason" section of DApp. The DApp will then notify the contractor and will provide the reasons of rejection of the employer. If the employer approves the request by pressing the "Confirm" and "Approve" buttons through MetaMask and DApp respectively, the DApp directs the employer to check whether the employer's wallet address is same as the address specified in the smart contract. If the addresses are same, the progress payment amount is transferred from the WAdEM to the WAdMC and $WAdSC_i$, and the list of paid objects that are stored in the blockchain are updated. The employer, however, has to make sure that there are sufficient funds in WAdEM before approval. Once the contractor and subcontractors receive the payment amount in ETH, they can convert it to any fiat currency in the local cryptocurrency exchanges.

```
function getObjectPrice(bytes32 _item) public view returns (uint, uint, uint) {
  for(uint j = 0; j < objectsPaid.length; j++){
    if(objectsPaid[j] == _object){
      return (0, 0, 0);
```

Figure 4.21 Prevention of Double Payment in Smart Contract

4.3.4 BIMSMRTPAY Case Study

The proposed BIMSMRTPAY system was applied to a four-story construction project. The parties in the case project include Employer (EM), Main Contractor (MC) , and two Subcontracts. MC is responsible for structural works whereas the Subcontractor 1 (SC1) and Subcontractor 2 (SC2) carry finishing works. As per the condition of the contract, the progress payment period is considered as monthly basis. Initially, the contract clauses such as WAdEM, WAdMC, WAdSC1, WAdSC2, were coded in the Ethereum smart contract. Moreover, the Object's Name, PayMC, PaySC1, PaySC2, and variables of PerChangeMC, PerChangeSC1, and PerChangeSC2 were included in the contract. As shown in Figure 4.22, after the parties' agreement on the contract clauses, it was deployed to Ganache Ethereum network to execute the condition and transaction of the data so that the proposed system is illustrated through a case project.

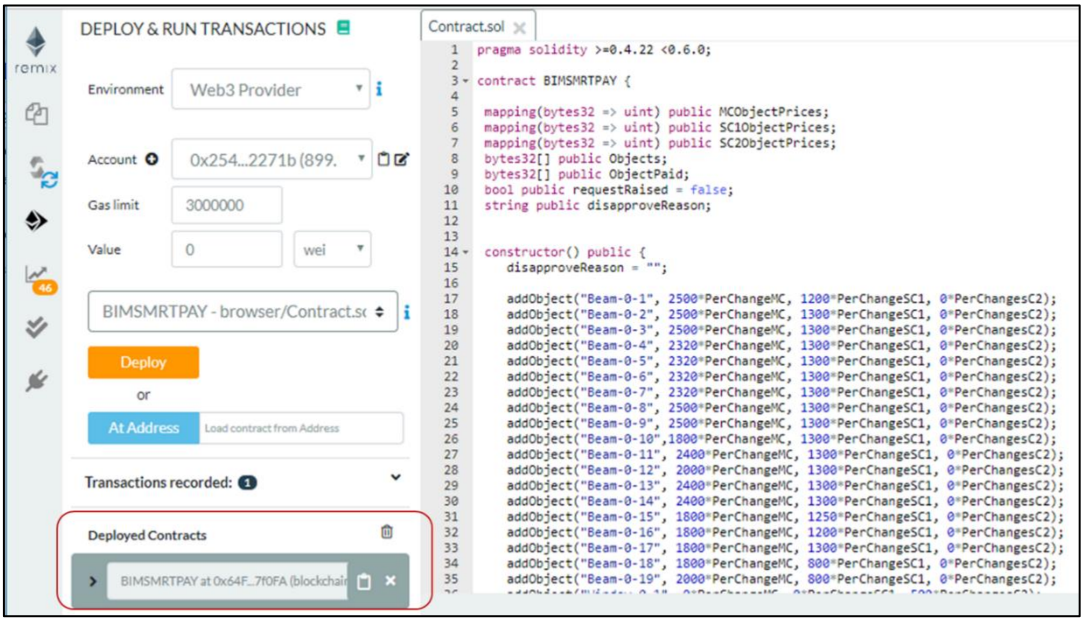

Figure 4.22 Deployment of Smart Contract on Blockchain

The case project started on September 01,2019. At the end of month, the contractor controlled on-site progress of works and used BIM model to determine the objects that were completed within the month of September as shown in Figure 4.23 (A). At this stage, the contractor also filled the "PerChange" and "Period" parameters for the completed objects. Since there were not any changes in design or costs, the "PerChange" section was filled as 100 %. Moreover, the "Period" was filled as 09-2019 for the completed objects within month of September.

Afterwards, the PROGITVIS was used to export the object's name and PerChange of the completed objects followed by progress visualization of the selected period. The contractor selects the month of the September through the calendar of PROGITVIS section and then a ".TXT" file including the information was provided to initialize the second section of the BIMSMRTPAY. Also, the visualized progress report was provided by this section and then sent to the employer to review the progress as shown in Figure 4.23 (B).

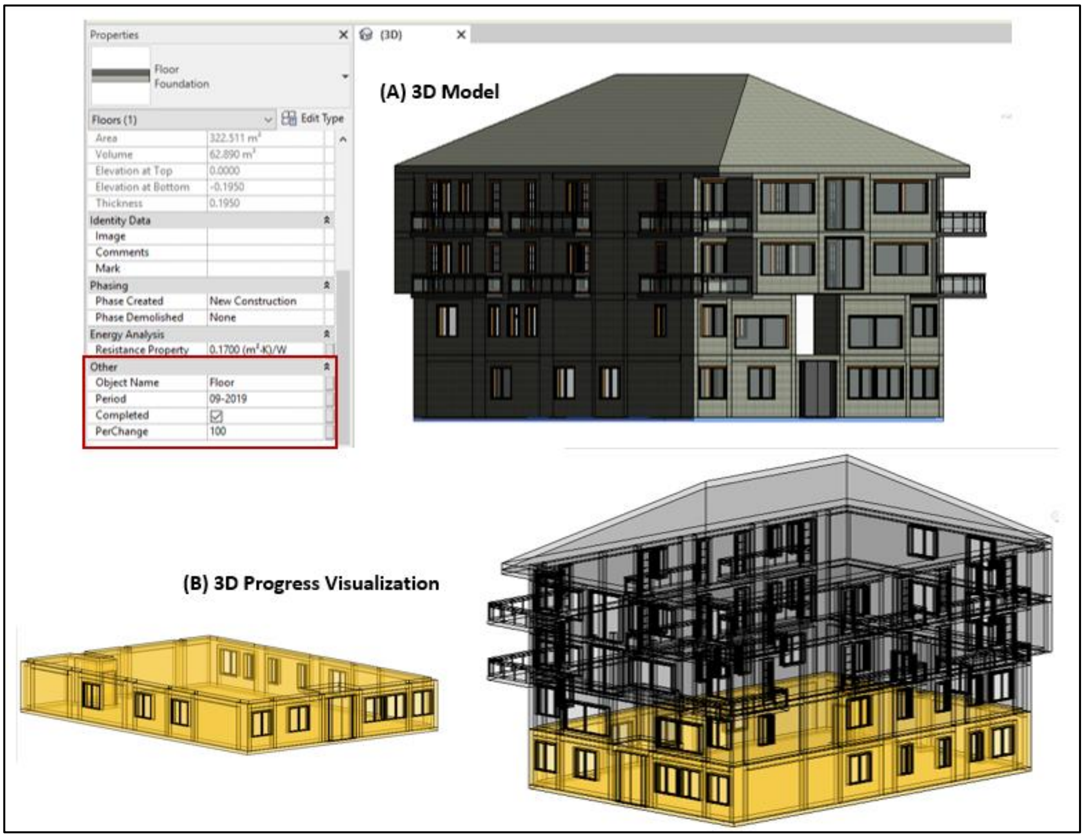

Figure 4.23 Visualized Progress of Case Project

The contractor should login in his MetaMask account to initiate payment process through DApp section. The DApp obtains the list of the completed objects in the “.TXT” file provided by the first section of the BIMSMRTPAY. Consecutively, the contractor presses the “Calculate Payment” button and then the progress payment amount and its breakdown are calculated by the smart contract according to the objects’ costs defined in the contract as shown in Figure 4.24. The PayMC, PaySC1, and PaySC2 was calculated as $58,760.93, $17,625.45, $6,370.60 respectively and converted by the DApp to the ETH at the rate of 177.07 $/ETH as 331.85 ETH, 99.54 ETH, 35.98 ETH. Once the payments are calculated, the contractor can send the payment request to the employer by pressing the “Request” button through the DApp as shown in Figure 4.24.

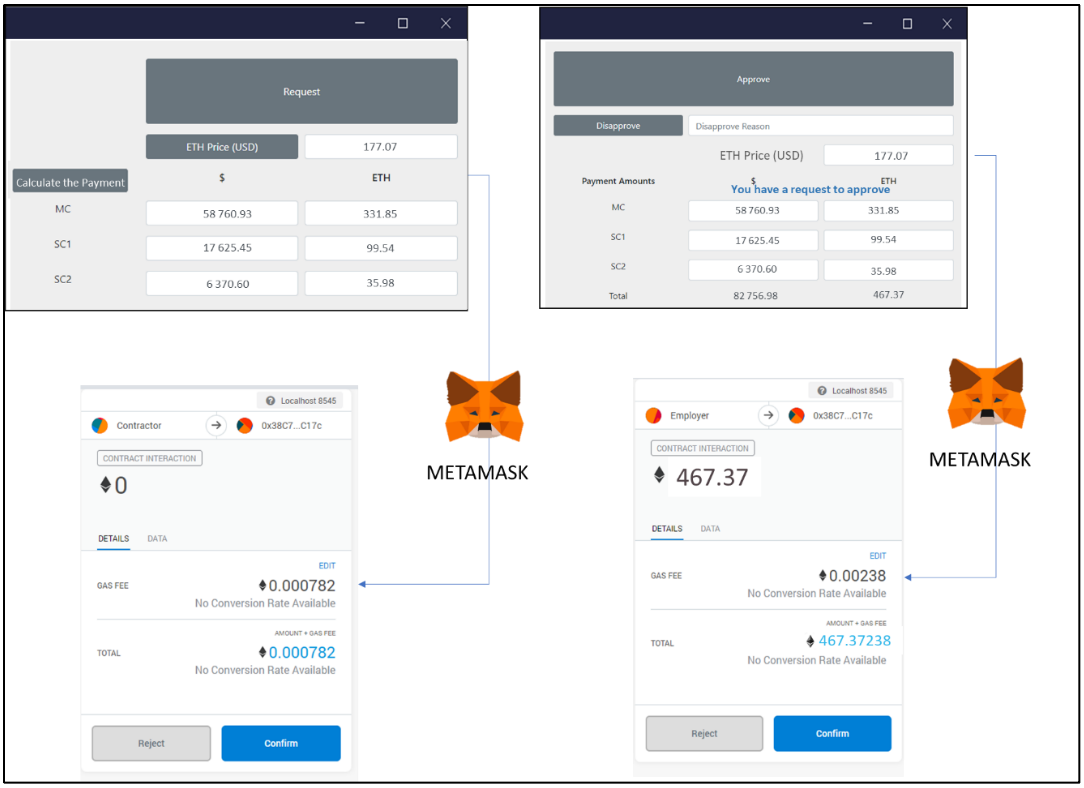

Figure 4.24 DApp and MetaMask Interface for Case Project

At the time that the employer receives the payment request, the payment amounts appeared on his screen. The employer should press the "Approve" and "Confirm" button of DApp and MetaMask accordingly so that the smart contract deduces the payment amount from WAdEM balance and then transfers it to the WAdMC, WAdSC1, and WAdSC2. The Balance of WAdEM is reduced from 900 ETH to 432.63 ETH and the balance of WAdMC, WAdSC1, WAdSC2 became 331.58 ETH, 99.54 ETH, 35.95 ETH respectively. The final balance of the accounts is presented in Figure 4.25.

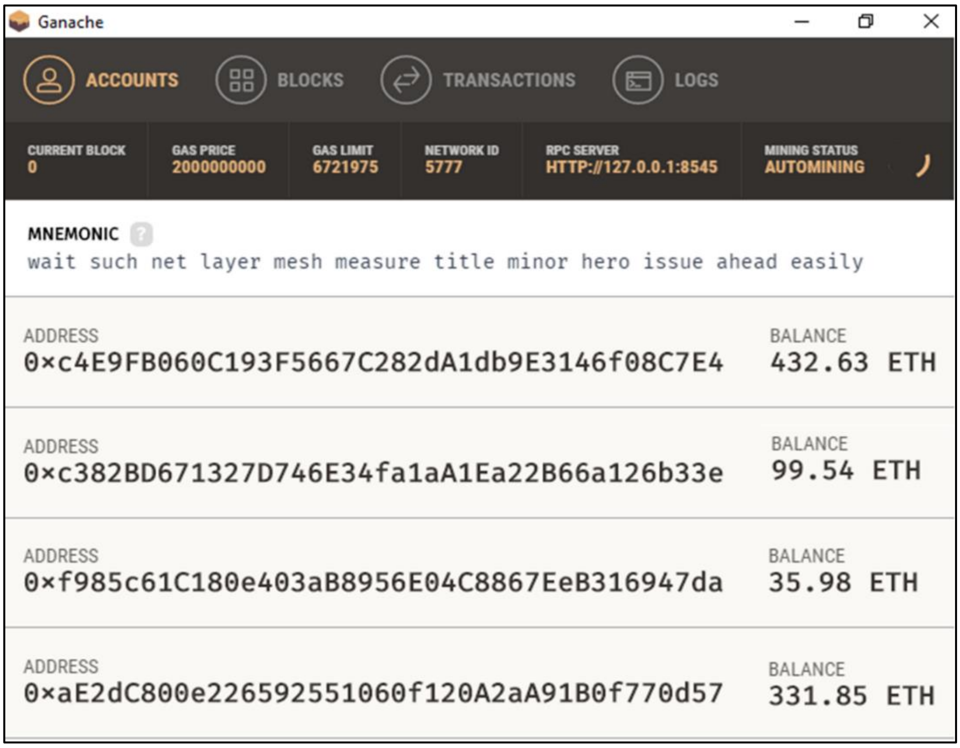

Figure 4.25 Balances of Wallets for BIMSMRTPAY Case Project After Payment Process

4.4 RETPAY

The RETPAY system was mainly designed for the construction project contracts in which partial completion and partial payment of retention is allowed. RETPAY not only enables automated payment of retention through smart contract but also performs storage and record keeping of the project completion data on a secure, reliable and trustworthy blockchain platform.

4.4.1 RETPAY System Overview

The proposed smart contract application performs execution of retention clauses of a typical project contract by performing automated payment of retention immediately after the employer's approval of partial completion of works. The application also enables storage of project completion and retention payment data on the blockchain. . In this part, while the business logic and terminologies are described textually, the design of the system will be provided through the use of top level architecture design description including the selected technologies, and the flow of activities, the changes on the sample data with respect to system activities, description of code parts via pseudo coding and end user interface screenshots. The system of RETPAY is presented in Figure 4.26.

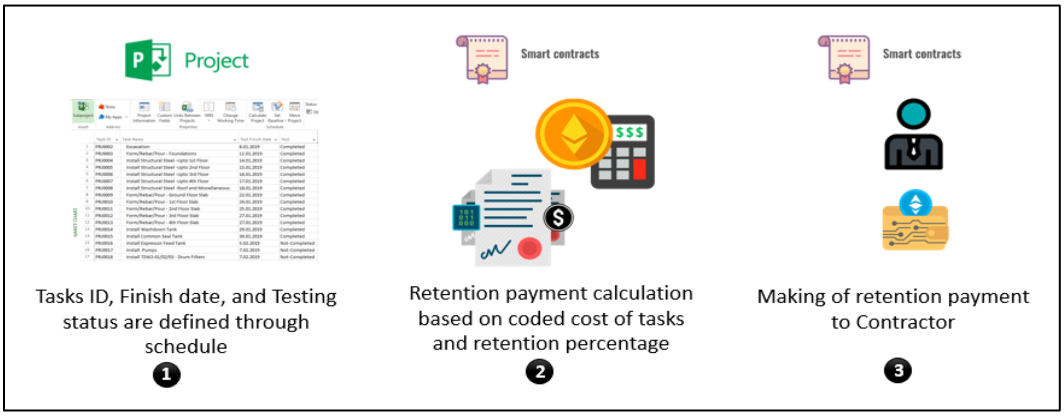

Figure 4.26 RETPAY system

In RETPAY the contract conditions related to the retention payment for partial completion are coded as a smart contract. The retention payments for each work are also embedded in the smart contract and then it is deployed on Ethereum blockchain. Once completion of a work is confirmed by the contractor and employer, RETPAY transfers the retention amounts of the works completed from WAdEM to the WAdMC and stores the partial completion data on the blockchain.

RETPAY consists of two modules. The first module is an add-on software named “Data MSP” that was developed to capture data from Microsoft Project 2019 using the C# language and Visual Studio 2019 platform. The second module of the RETPAY is a DApp consisting of two parts; the web part, and the smart contract part. The top-level design which shows the main flow of activities of the RETPAY is presented in the Figure 4.27.

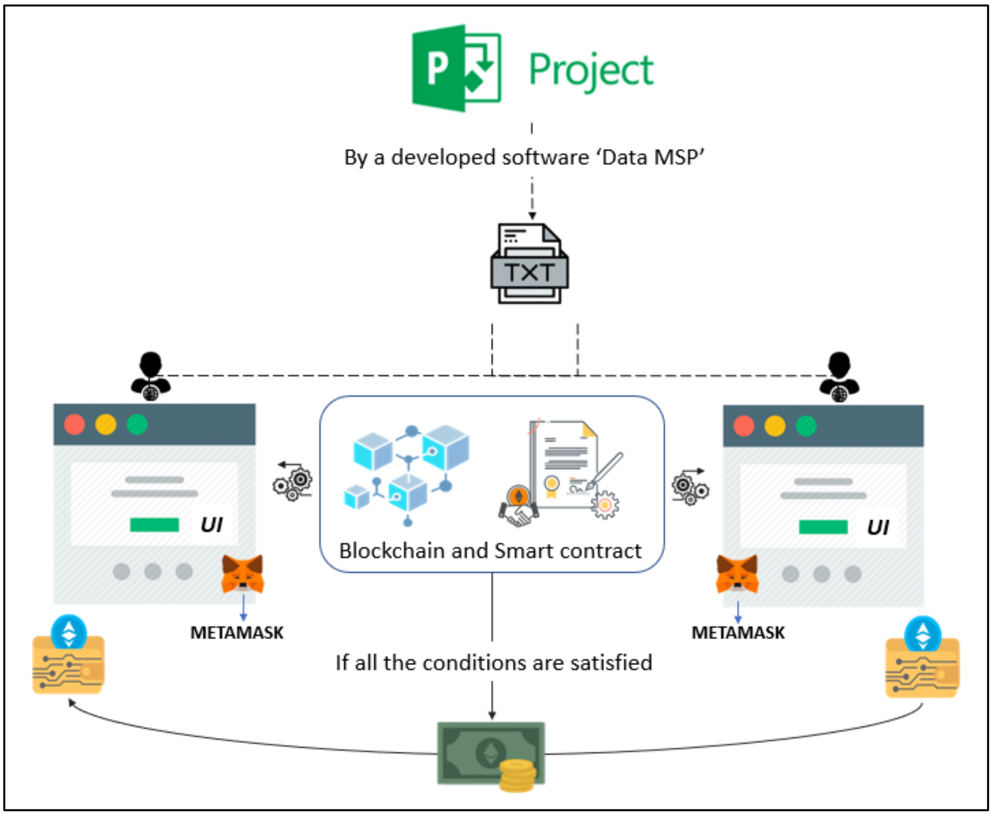

Figure 4.27 RETPAY Process

4.4.2 Microsoft Project Add-on

The purpose of the first module is to enable the contractors to use their existing project data and software for preparing the list of works completed to facilitate the data exchange among the proposed system. through the schedule the contractor determines the completion date of the tasks and their testing status whether the completed tasks have been tested and confirmed by the employer or not. Followingly, in the add-on, the contractor first selects a report period and then presses on the "Prepare List of Works Completed" button as shown in Figure 4.28. Once the button is pressed, the add-on exports the list of completed works' "Unique ID"s and their completion dates to a ".TXT" file as shown in Figure 4.28.

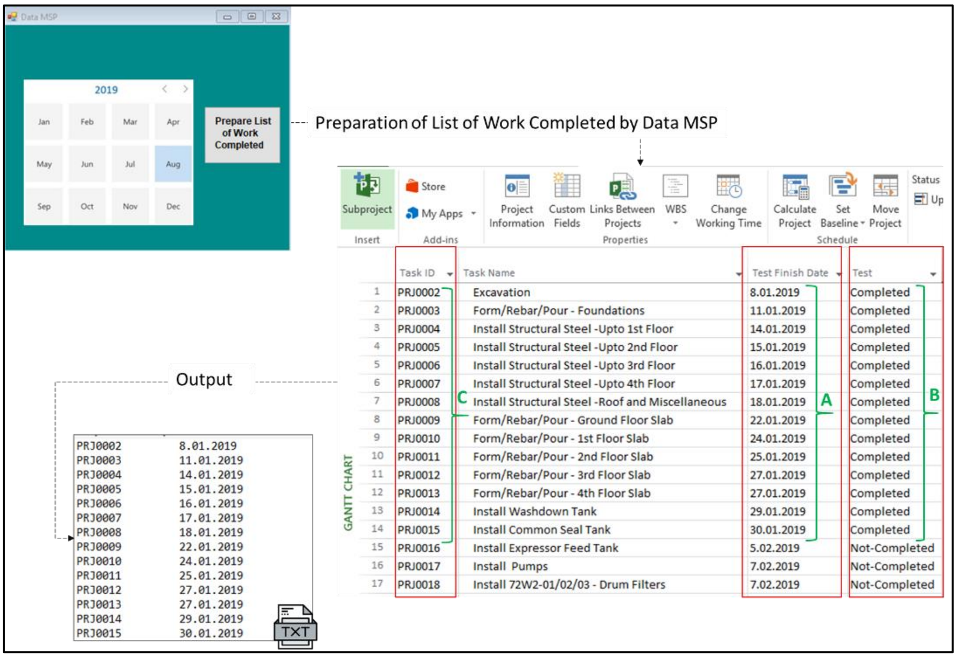

Figure 4.28 First Module of RETPAY

4.4.3 Smart Contract Conditions

The smart contract is developed in Remix IDE using the Solidity 0.5.2 language. Like the SMTSEC and BIMSMRTPAY systems the Cur, CryT and finally WAdEM and WAdMC are included in the smart contract. The retention amounts of works are embedded into the smart contract along with their unique IDs, as shown in Figure 4.29. Also, the retention percentage of each task which withhold by the employer is specified in the contract.

```
constructor() public {

   TaskIDs("PRJ-0-1", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-2", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-3", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-4", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-5", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-6", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-7", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-8", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-9", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-10", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-11", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-12", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-13", Cost*RetentionPercentage);
   TaskIDs("PRJ-0-14", Cost*RetentionPercentage);
```

Figure 4.29 Retention Amounts of Works Embedded into Smart Contract

4.4.4 Decentralized Application

The web part of the system is developed using the PHP Laravel 5.8 Framework in the back-end and HTML5, CSS3, and JavaScript in the front-end. For integrating HTTP web page (UI) with the Ethereum node and smart contract, Web3.js is used. MetaMask is used as the user interface for identity management on the Ethereum blockchain. The smart contract is deployed to a Ganache virtual Ethereum blockchain to test the DApp.

The contractor will have to login the MetaMask using his wallet specified in the smart contract to start the partial project completion and retention payment process. The contractor will use the “Request” button of the second module to request the approval for partial completion and retention payment, as shown in Figure 4.30. DApp will then check whether the contractor’s wallet address is same as the address specified in the smart contract. If the addresses are same, DApp will use the list of completed activities in the TXT file to determine the amount of retention payment in the currency of the contract, and in Ethereum (ETH) based on the latest exchange rate. Smart contract part calculates the total retention payment amount through the cost of each task specified in the contract.

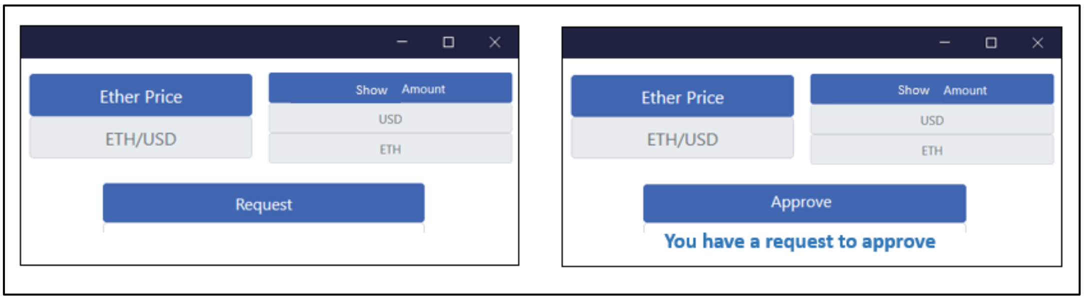

Figure 4.30 Second Module of RETPAY

The DApp will display the total retention amount to be paid for list of completed works on the contractor's screen. The contractor can change the list of completed works by clicking on the "Reject" button, and then by using the first module. Once the contractor approves the completed works and the retention amount, by pressing the "Confirm" button, the DApp notifies the employer by displaying "You have a request to approve" massage on the employer's screen. Notifications are shown from interface (JavaScript) on the information fetched from smart contract.

The DApp requires employer's approval to complete the partial completion and retention payment process for the report period. The employer will have to login the MetaMask using his wallet specified in the smart contract to start the approval process. Once the employer logins with the specified wallet, the DApp will display the requested retention payment amount of the employer's screen as shown in Figure 4.30. If the employer does not approve the list of works completed and the retention payment amount, the DApp will notify the contractor and will provide the reasons of rejection of the employer. If the employer approves the completed works, the agreed retention amount for the report period is transferred from the employer's wallet to the contractor's wallet, and the list of completed activities that are stored in the blockchain are updated along with their completion dates. The employer, however, has to make sure that there are sufficient funds in his wallet before approval. Once the contractor receives the retention amount in ETH, he can convert it to any fiat currency in the local cryptocurrency exchanges.

4.4.5 RETPAY Case Study

The proposed RETPAY system was applied to a construction project which had a contract with retention clauses similar to the majority of construction projects. The project was a process plant project contracted on engineering procurement and construction (EPC) bases. The January 2019 period consisted of a month which included partial retention payments for the works completed within the specified period. As shown in Figure 4.31, in the given case project 5% of the total costs of works will be transferred from the employer's wallet to the contractor's as retention payment after the completion of the works. The cost, retention percentage, and task IDs of each task were outlined in the smart contract.

```
constructor() public {
    TaskIDs("PRJ0002", 44850*5/100,);
    TaskIDs("PRJ0003", 127430*5/100,);
    TaskIDs("PRJ0004", 267545*5/100,);
    TaskIDs("PRJ0005", 245830*5/100,);
    TaskIDs("PRJ0006", 238432*5/100,);
    TaskIDs("PRJ0007", 214800*5/100,);
    TaskIDs("PRJ0008", 129325*5/100,);
    TaskIDs("PRJ0009", 26830*5/100,);
    TaskIDs("PRJ0010", 18460*5/100,);
    TaskIDs("PRJ0011", 18460*5/100,);
    TaskIDs("PRJ0012", 18460*5/100,);
    TaskIDs("PRJ0013", 18460*5/100,);
    TaskIDs("PRJ0014", 4532*5/100,);
    TaskIDs("PRJ0015", 9618*5/100,);
}
```

Figure 4.31 Part of RETPAY Smart Contract of Case Project

As presented in Figure 4.32 the schedule of the contractor was available in MS Project software format. So, the contractor initiates the RETPAY process through the "Data MSP" module of the system and the ".TXT" file including task IDs and completion date of the tested tasks was exported.

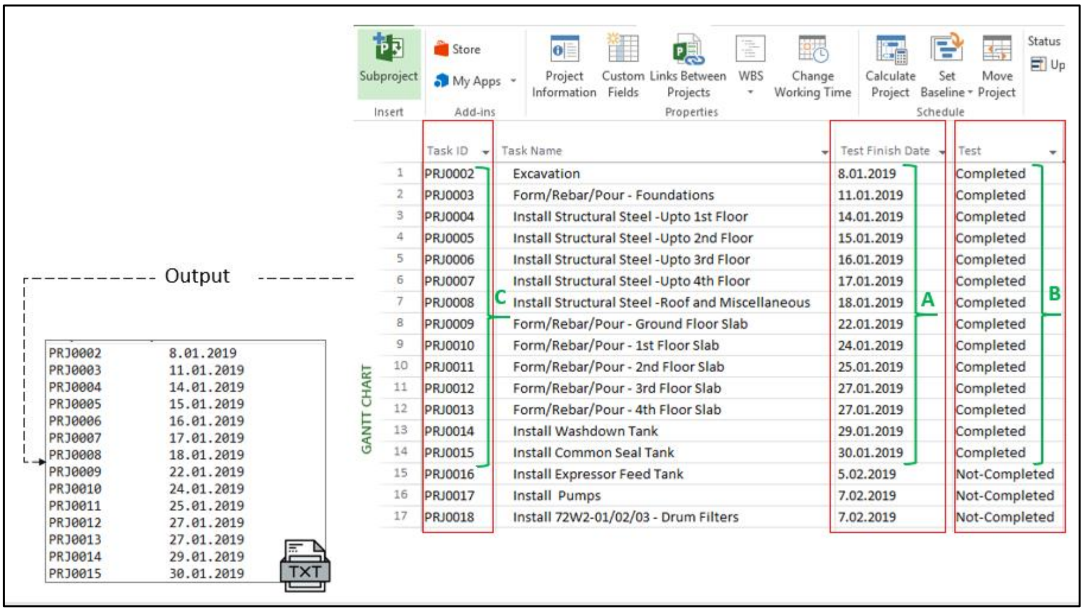

Figure 4.32 Work Schedule of RETPAY Case Project

The contractor logged in his MetaMask account to initiate retention payment process through DApp section. The DApp obtained the information from ".TXT" file provided by the first section of the RETPAY. Consecutively, the contractor pressed the "Show Amount" button and then the total retention payment amount calculated by the smart contract according to the tasks' cost and percentage defined in the contract. The total retention payment amount was calculated as \$69,151.6 and converted by the DApp to the ETH at the rate of 181.17 \$/ETH as 381.7 ETH. Once the payments were calculated, the contractor sent the payment request to the employer by pressing the "Request" button through the DApp as shown in Figure 4.33.

Once the employer received the payment request, the retention payment amount appeared on his screen. The employer pressed the "Approve" and "Confirm" button of DApp and MetaMask accordingly so that the smart contract deduces the payment amount from WAdEM balance and then transact it to the WAdMC. The final balance of the WAdMC which became 381.7 ETH is presented in Figure 4.33.

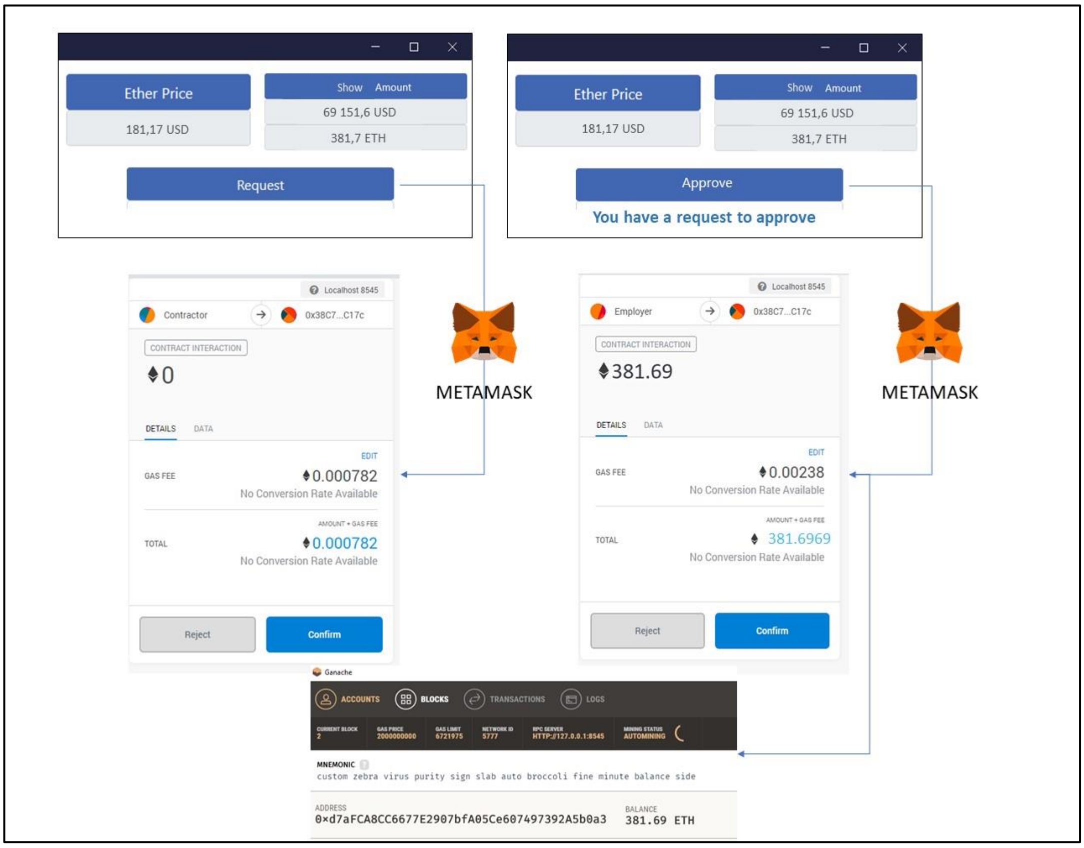

Figure 4.33 DApp Module of RETPAY Case Project

CHAPTER 5

DISCUSSION

In this section the advantages and limitations of the proposed smart contract systems; SMTSEC, BIMSMRTPAY, and RETPAY are discussed along with their limitations.

5.1 Discussion of SMTSEC

The proposed SMTSEC and its implementation on a case project, support the fact that it provides a secure, traceable, transparent, efficient and trustworthy platform for the secure payment of the construction industry. As a result, the SMTSEC and smart contract as a core of the system, present an innovative alternative for enhancing the traditional payment system within the industry. Availability of funds for progress payment periods is guaranteed since the projected progress payment amount of upcoming period is blocked in advance in the smart contract. The SMTSEC enables the payments to be transferred directly, promptly and simultaneously from employer's wallet to the subcontractors' and suppliers' wallets . Hence, the cash flow problems of the contractor and lower tiers resulting from the late payment could be significantly reduced.

The SMTSEC also increases the transparency by recording the content of each operation, transaction information such as sender and receivers, and date of transaction, in the blockchain which adds additional reliability and traceability to the process. SMTSEC could minimize disputes between the employer and the contractor on the payment issues because the smart contract carries out the payment clauses based on automated protocol, which leaves no chance for the parties to disobey, reinterpret or alter the contract's conditions. So, the need for a costly and time-consuming arbitration process for dispute resolution for payment issues could be reduced. The payment conditions such as Cong, PeriBloc, PeriPay, and SubPeri in the SMTSEC are flexible which could be coded in the smart contract based on the agreements made between the employer and the main contractor. The SMTSEC could be used globally as an alternative for the PBAs for both public and private projects.

Despite the benefits of the proposed system, SMTSEC has few limitations. The fluctuation in the cryptocurrencies prices may raise the concern to apply the blockchain and smart contract in the industry. Bitcoin Futures, a risk hedge approach provided by Chicago Mercantile Exchange (CME) could be used to mitigate and hedge the variation risks of the cryptocurrency prices. Moreover, Ethereum futures which might be also a possibility in the near future would provide a better hedge, however, both of these alternatives come at a cost. Use of smart contracts which support the stable coin, cryptocurrencies backed by fiat currency which has always a fixed value against a fiat currency, would also minimize the risk of CryT/Cur fluctuations. Contrary to the PBAs which enables the interest payment, interest is not accrued to the blocked funds in SMTSEC system. However, once the Ethereum moves to the PoS from PoW consensus mechanism, earning interest might be a possibility with the SMTSEC in the future.

The current market cap of smart contract cryptocurrencies also presents a limitation on the use of smart contract-based security of payment systems for large size construction projects. With the current supply of 108,850,825 and at a current exchange rate of 150.06 ETH/$, the current market cap of ETH is at $16.334 Billion. The large amount of buying demand from an employer for a mega project may lead to rapid appreciation of ETH against Cur, similarly large amount of selling orders from the contractors, subcontractors, and suppliers may result in a rapid depreciation of ETH against Cur. Hence the proposed SMTSEC is more suitable for small or medium size construction projects.

5.2 Discussion of BIMSMRTPAY

Smart contracts are well-known for transaction of digital assets. On the other hand, BIM enables the information of the building to be digitally represented. As a result, integration of smart contract with the BIM and developing the BIMSMRTPAY system, followed by applying on a case project revealed numerous advantages. In progress measurement phase, the objects which have been totally completed are determined the sum of progress payment amount. In other words, rather than calculation of progress percentage of ongoing works, the objects which has been accomplished within the progress payment period, are considered and the ongoing objects are neglected. Hence, this binary progress tracking method by the mean of BIM model, reduces the progress measurement minimizes potential disputes about progress calculations process an. Moreover, it minimizes the uncertainties during collecting data to calculate the progress. Visualization of the completed objects enable employer and contractor to observe the progress and superimposed model. In addition, it enables the parties to discriminate the upcoming objects to be started or completed.

Calculation of the progress payment by the smart contract based on the determined prices of the objects, will accelerate the payment calculation process. The BIMSMRTPAY transfers the payment to from the employer’s wallet to the contractor, subcontractors and suppliers’ wallet concurrently, hence could also make the payments of the lower tiers of supply chain along with the contractor’s payment. The transparency and auditability of operations are also promised by the BIMSMRTPAY. Transaction hashes which are generate at the time of time a transaction is recorded to the blockchain and are accessible to the contract participants. Hence, these records indicate information regarding to the pertinent transactions (e.g. when payments have been transacted, or when clauses have been executed, which objects have been paid).

Since the blockchain is the core logic of the proposed systems, payment length and fees are significantly reduced in both SMTSEC and BIMSMRTPAY systems

Further, all the payment clauses in both systems are enforced by the smart contract. Thus, the need for the intermediaries such as banks and lawyers to transact the payments and to execute the contract terms respectively are minimized. Both SMTSEC and BIMSMRTPAY are suitable for both unit price and the lump sum type of the contracts which increase the application area of the systems in different types of the construction contracts.

MetaMask is chosen in the BIMSMRTPAY system design and implementation. Using of MetaMask to store the wallet provides a secure web wallet. It is open source; thus, its code is open to be evaluated by a large community of users currently reaching one million active user population. It also allows connection of hardware wallets such as Ledger (Gentilal, Martins, & Sousa, 2017) and Trezor (Boireau, 2018) which would result in increasing the security level of the application instantly.

Despite the SMTSEC, the proposed BIMSMRTPAY application relies on the availability of sufficient funds in the employer's wallet for paying the progress payment. Although BIMSMRTPAY does not guarantee the payments in advance, the employer is not impacted by the CryT/Cur fluctuations since the funds are not blocked.

5.3 Discussion of RETPAY

Applying the smart contracts for the retention clauses promised a significant potential to reduce the duration of retention payments substantially. DApp presented in RETPAY includes general retention payment procedures that can be implemented to the majority of projects that include standard partial retention payment clauses. The tests of RETPAY on the case project revealed that the retention payments could be made within seconds after approval of the employer. The proposed RETPAY system expedites the payment process and reduces the transaction cost because of the inherited features of the smart contracts. Further, all the retention clauses are enforced by the smart contract. Thus, the need for the third party such as banks and lawyers to transact the payments and to execute the contract terms respectively are minimized. In addition, all the data regarding the transactions and operations are recorded in the blockchain and shared among the contract parties in the secure blockchain environment. Hence, the disputes, misunderstandings, and obscurities among the parties could be significantly reduced. RETPAY also enabled the contractors to use their existing project data for preparing the list of works completed and did not require a long document preparation and approval process for payment of retention.

Despite its advantages, RETPAY has some limitations. One of the main limitations is that it does not lock the funds of the employer but rather relies on the availability of sufficient funds in the employer's wallet for paying the retention. In case the funds are not available, RETPAY cannot execute automated payment of retention. RETPAY will also incur deployment and transaction costs as it uses the Ethereum blockchain. Since RETPAY includes a small size of source code for the smart contract, the deployment cost is insignificant. For, example the deployment and two transactions costs for the case project was $4.0 at the exchange rate of $180.0/ETH. There will be also be a developments cost if the employer wants to develop their own DApp.

5.4 Blockchain and Smart Contract Adoption

Blockchain, smart contract, and cryptocurrencies are quite new technologies and have not been mainstream yet. So, few construction corporations are aware of the advantages of these technologies. Implementing of the mentioned technologies in the construction application requires trained people. Thus, it is necessary to continue to educate the public about blockchain technology. This will ultimately help organizations to see the value proposition that blockchain brings to them.

The lack of standards and regulations to govern the blockchain and smart contract usage could be a barrier to the organizations to adopt these technologies. The legal aspects of smart contracts have to be further explored and industries have to come up with best practices that are most applicable to their particular industry. With the presence of both public and private blockchains, standards and agreements will also be needed to ensure interoperability. Being a public ledger that is not owned by any single entity, divisions can arise when addressing the technology's development. For example, both Bitcoin and Ethereum have had to deal with disagreements in their open-source communities, making it difficult to agree on protocol upgrades and causing 'forks', where smaller groups split off from the main group. Thus, much volatility still exists in the progression of blockchain technology.

The blockchain technology is considered as a driver for disintermediation, which means that third parties’ and intermediaries’ involvement are eliminated. This may disrupt current business models within construction or other industries.

Although blockchain and smart contracts provide a very secure platform for the development of decentralized applications such as SMTSEC, BIMSMRTPAY, and RETPAY they are not risk free. (Li et al., 2017) provides a systematic review of security threats of the blockchain and smart contract systems and presents enhancements to minimize the security risks.

Aforementioned 51% attack of blockchain is the most well-known risks to blockchain application. In general, this risk mainly towards the integrity of blockchain data. It is believed that the nature of the SMTSEC, BIMSMRTPAY and RETPAY would result in the interest of a closed group of related users, rather than a vast amount of blockchain users. Thus, having the possibility of 51% risk for this specific application is very low. Another risk for blockchain applications is the risk of security of private keys for the blockchain. This may end of confidentiality problems for both the users and data. This issue, storage of private keys, is depicted more during the description of use of wallets for this application.

Unlike, some other web browsers which store the keys in the wallet vendors’ server, MetaMask stores the public and private key information on the wallet owner’s browser. This results in user having more control over his/her keys. However, it supports limited number of browsers, namely Google Chrome, Mozilla Firefox, Opera, and the newly emerged Brave browser. The users who does not want to store their keys on browsers by the mainstream vendors, may choose the latter one, or simply reject using MetaMask at all

Being a distributed application, and running on a specific platform, blockchain, brings additional vulnerabilities to the smart contract applications. Primitive codes caused by either development languages/platforms or lack of experience in distributed application design result in problems which may cause important security issues. (Luu, Chu, Olickel, Saxena, & Hobor, 2016) proposed a system called OYENTE which investigates the smart contract code for vulnerabilities. OYENTE provides an output as a result of this investigation pointing out possible vulnerabilities for smart contract applications. This application was also used during the case study resulting for both systems with no significant security related bug of the listed types.

CHAPTER 6

CONCLUSION

The blockchain and smart contracts are highly potential technologies in terms of self-executing of the clauses respectively which can bring value and opportunities to the construction industry. One area in which these technologies promise to be particularly beneficial is payment domain of the construction business. With so many participants involved and cascade payment process, there tends to be major payment issues among the supply chain of the project which adversely affect the success of the project. Blockchain accompanied by the smart contracts have the potential to address payment challenges with distributed ledger technology that provide an open, immutable record of transactions which is accessible by all the participants of the system and could perform automatically execution of the payment clauses r.

By taking the advantages of blockchain and smart contract technologies, this thesis presented three smart contract systems namely SMTSEC, BIMSMRTPAY, and RETPAY with the aim of securing the progress payment, expediting of the progress payment process, and minimizing the third parties' involvement such as lawyers and banks in execution phase of the contract clauses.

The SMTSEC enables the security of the payments by blocking the projected progress payment amount of the upcoming period provided by a management software in the smart contract. Afterwards, it directly releases the blocked amount and pays the actual payment at the progress payment period. It transfers the payment amount of the contract parties; contractor, subcontractors and suppliers to their wallet address simultaneously.

The main contribution of the proposed SMTSEC is that it offers a secure, transparent, and efficient platform for security of the payment for construction contracts globally without relying on the intermediaries such as notaries, lawyers, and banks. The presented process of blocking of the payments of works that will be constructed for the next progress payment period enforces the employer to plan and arrange the payments ahead of time and guarantees timely payment of progress payments to the main contractor, subcontractors, and suppliers. Mitigation of time and cost overruns, dispute, overhead and administrative cost besides expedition of the payment process and increasing trust among parties in the project are some of the advantages of the proposed system. In addition, the payments log is saved in the blockchain database which adds additional reliability to the process. The proposed framework was also applied on a real-life construction project to assess its applicability.

BIMSMRTPAY, novel object-based progress payment system for construction industry is presented based on the integration of smart contracts with BIM. In BIMSMRTPAY, only the payment related the objects that have been totally completed are made in the progress payment period. Modeling and breaking the project into small objects will facilitate to recognize and determining of the completed objects based on the on-site progress.

Since the price of each object are outlined in the contract, the calculation of the progress is performed by the smart contract, hence, payment calculation becomes automated. As a result, potential disputes in progress payment calculation could be significantly reduced. The tests of BIMSMRTPAY on the case project revealed that the progress payment could be made within seconds after approval of the employer. The proposed system expedites the progress measurement, payment calculation, and payment processes followed by reduction of the transaction cost because of the inherited features of the smart contracts. Further, all the payment clauses are enforced by the smart contract. So, the need for the third party such as banks and lawyers to transact the payments and to execute the contract terms respectively are minimized. Last but not least , all the data regarding the transactions and operations are recorded in the blockchain and shared among the contract parties in the secure blockchain environment. Hence, the disputes, misunderstandings, and obscurities among the parties could be significantly reduced. RETPAY system is designed to establish a decentralized platform for the retention payment of the construction contracts. The tasks' IDs and deduced retention amounts are outlined in the smart contract. Once the testing process is completed, the data such as test completion date of the tasks and tasks IDs is retrieved from a management software and transferred to the smart contract. Once the employer approves the tested tasks, the system instantly transfers the deduced retention amount from the employer to the contractor. In addition, the information such as payment amount, test completion date, and payment date are recorded by the blockchain of the RETPAY system. Hence, it expedites the retention payment process and eliminate the third parties' involvement such as banks.

Although the proposed systems offer numerous advantages for construction payment contracts, there are still potentials to improve these systems. BIMSMRTPAY relies on manual data collection and entry to initiate the payment process. Therefore, future research focusing on use of robots or sensors in data collection and data exchange could provide a fully automated progress payment system for construction payment contracts.

As this thesis has been investigating blockchain and smart contract technologies as a solution to construction project issues from payment perspective, it does however, require further investigation in other areas. The technology may affect the industry in a broader sense, from all aspects rather than just from a payment point of view. Thus, investigating the solutions that these technologies can offer to overcome the challenges beyond the delayed payments can also be considered as the topics which may draw the researchers' attention.

The construction industry is a heavily contract oriented industry. There are agreements between different parties of the project e.g. agreement between subcontractor and suppliers, contractor and suppliers, contractor and insurance companies and etc. Since the smart contracts could communicate with each other, integrating the contracts together to execute the mutual clauses could be the subject of the future studies. Integrating of the blockchain with the data trackers such as IoT sensors or BIM could be among the further research topics by considering the vast potential of the blockchain in the data management domain. In addition, the data management, exchange, protection, and recording process need to be enhanced to establish a traceable, transparent, and immutable data management environment in construction industry.

REFERENCES

Aaron Yao, E. (2015). *Effects of Delayed Payment on Projects and Stakeholders: A Case Study of Keta Municipal Assembly*. Kwame Nkrumah University of Science and Technology.

Abdul-Rahman, H., Kho, M., & Wang, C. (2014). Late payment and nonpayment encountered by contracting firms in a fast-developing economy. *Journal of Professional Issues in Engineering Education and Practice*, *140*(2), 04013013. https://doi.org/10.1061/(ASCE)EI.1943-5541.0000189.

Abdul Kadir, M. R., Lee, W. P., Jaafar, M. S., Sapuan, S. M., & Ali, A. A. A. (2005). Factors affecting construction labour productivity for Malaysian residential projects. *Structural Survey*, *23*(1), 42–54. https://doi.org/10.1108/02630800510586907

Abdullah, M., Abdul Azis, A., & Abdul Rahman, I. (2009). Potential effects on large Mara construction projects due to construction delay. *International Journal of Integrated Engineering*, *1*(2), 53–62.

Abdullah, M. R., Abdul Azis, A. A., & Abdul Rahman, I. (2009). Potential Effects on Large Mara Construction Projects Due To Construction Delay. *International Journal of Integrated Engineering*, *1*(2), 53–62.

Ahmadisheykhsarmast, S., & Sonmez, R. (2018). Smart Contracts in Construction Industry. In *5th international Project and Construction Management Conference (IPCMC2018)* (pp. 767–774). North Cyprus.

Allens. (2016). *Understanding the opportunities and navigating the legal frameworks of distributed ledger technology and blockchain*.

Ameer-Ali, N. A. N. (2006). A "Construction Industry Payment and Adjudication Act": Reducing payment-default and increasing dispute resolution efficiency in construction. *Master Builders*, *3*, 4–14.

Ammous, S. (2016). *Blockchain Technology : What is it good for ?*

Amoako, K. B. (2011). *The effect of delayed payment on cash flow forecasting of Ghanaian road contractors*.

Andersson, L., Farrell, K., Moshkovich, O., & Cranbourne, C. (2016). *Implementing Virtual Design and Construction Using BIM: Current and Future Practices. Routledge*. Taylor and Francis Group.

Ansah, S. K. (2011). Causes and effects of delayed payments by clients on construction projects in Ghana. *Journal of Construction Project Management and Innovation*, *1*(1), 27–45.

Anuradha, M. N. L., Yamini Gupta, N., Udayasree, R., & Tabassum, F. (2017). The blockchain (R) evolution. *International Journal of Innovations & Advancement in Computer Science*, *6*(7), 129–133.

Arditi, D., & Chotibhongs, R. (2005). Issues in Subcontracting Practice. *Journal of Construction Engineering and Management*, *131*(8), 866–876. https://doi.org/10.1061/(asce)0733-9364(2005)131:8(866)

Assaf, S. A., & Al-hejji, S. (2006). Causes of delay in large construction projects. *International Journal of Project Management*, *24*(4), 349–357. https://doi.org/10.1016/j.ijproman.2005.11.010

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of Things : Benefits , Challenges , and Future Directions. *Nternational Journal of Intelligent Systems and Applications*, *10*(6), 40–48. https://doi.org/10.5815/ijisa.2018.06.05

Aung, Y. N., & Tantidham, T. (2017). Review of Ethereum: Smart home case study. In *2017 2nd International Conference on Information Technology (INCIT)* (pp. 1–4). https://doi.org/10.1109/INCIT.2017.8257877

Ayudhya, B. (2012). Factors causing delay in payment of residential building projects in Thailand. *TS01C - Construction Economics and Management*.

Bahga, A., & Madisetti, V. K. (2016). Blockchain Platform for Industrial Internet of Things. *Journal of Software Engineering and Applications*, *9*(10), 533–546. https://doi.org/10.4236/jsea.2016.910036

Barnes, P. T., & Davies, N. (2015). *BIM in Principle and in Practice* (2nd Editio). Institute of Civil Engineers (ICE) Publishing.

Biddell, L. (2015). *Implementation of Project Bank Accounts across Highways England*.

Biswas, K., & Muthukkumarasamy, V. (2016). Securing Smart Cities Using Blockchain Technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)* (pp. 1392–1393). https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

Blycha, M. (2018). Smart contracts in the construction industry. Retrieved December 2, 2019, from https://www.lexology.com/library/detail.aspx?g=78d1740e-bb52-4c67-9135-3d0193a2b2b7

Boireau, O. (2018). Securing the blockchain against hackers. *Network Security*, *2018*(1), 8–11. https://doi.org/10.1016/S1353-4858(18)30006-0

Burgess, K., & Colangelo, J. (2015). *The Promise of Bitcoin and the Blockchain*.

Buterin, V. (2014). *Ethereum white paper, 2014. A next-generation smart contract and decentralized application platform*. Retrieved from www.github. com/ethereum/wiki/wiki/White-Paper%0Ahttps://s3.us-east-2.amazonaws.com/bci-static/downloads/ethereum_whitepaper.pdf%0Ahttps://ethereum.github.io/yellowpaper/paper.pdf

Cardeira, H. (2015). Smart contracts and possible application to the construction industry. In *New Perspectives in Construction Law Conference* (Vol. 1).

Bucharest.

Cardeira, H. (2017). The Benefits of Integrating Smart Contracts and BIM Using an XML Protocol. In *The New Wave annual conference*. Gold Coast.

Cardeira, H. (2018). *The advantages of using a web payments platform in the construction industry based on smart contracts and cryptocurrencies*.

Chen, G., Xu, B., Lu, M., & Chen, N. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, *5*(1), 1–10. https://doi.org/10.1186/s40561-017-0050-x

Cheng, T., Soo, G., Kumaraswamy, M., & Jin, W. (2010). Security of payment for Hong Kong construction industry. *Proceedings of Institution of Civil Engineers: Management, Procurement and Law*, *163*(1), 17–28. https://doi.org/10.1680/mpal.2010.163.1.17

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, *4*, 2292–2303.

Construction Leadership Council. (2013). *Construction Supply Chain Payment Charter*.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanamaran, V. (2016). BlockChain technology: Beyond bitcoin. *Applied Innovation Review*, (2), 6–19.

Danuri, M. M., Munaaim, M. C., Rahman, H. A., & Hanid, M. (2006). Late and non-payment issues in the Malaysian Construction Industry Contractor’s perspective. In *International Conference on Construction, Culture, Innovation and Management (CCIM)*.

David, B., Gazi, P., Kiayias, A., & Russell, A. (2018). Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 66–98).

Din, N. M. D. N., & Ismail, Z. (2014). Construction Industry Payment and Adjudication Act (CIPAA) Remedying Payment Issues: CIDB G7 Contractor's Perspective. *Journal of Technology Management and Business, 1*(1), 21–38.

Doloi, H., Sawhney, A., Iyer, K. C., & Rentala, S. (2012). Analysing factors affecting delays in Indian construction projects. *International Journal of Project Management*, *30*(4), 479–489. https://doi.org/10.1016/j.ijproman.2011.10.004

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017* (pp. 618–623). IEEE. https://doi.org/10.1109/PERCOMW.2017.7917634

Efanov, D., & Pavel, R. (2018). The All-Pervasiveness of the Blockchain Technology. In *8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017* (pp. 116–121).

Enshassi, A., & Abuhamra, L. (2015). Delayed Payment Problems in Public Construction Projects: Subcontractors' Perspectives. In *International Conference on Construction and Real Estate Management* (pp. 567–575). Luleå.

ERC. (2015). *The Senate: Economics References Committee*.

Euler Hermes Global. (2016). Euler Hermes: UK late payments hit two-year high at 2015 year-end. Retrieved October 31, 2019, from https://www.eulerhermes.com/en_global/media-news/news/press-release-eh-uk-late-payments-hit-two-year-high-at-2015-year.html

Fanning, K., & Centers, D. P. (2016). Blockchain and Its Coming Impact on Financial Services. *Journal of Corporate Accounting & Finance*, *27*(5), 53–57. https://doi.org/10.1002/jcaf.22179

Farmer, M. (2016). *The Farmer Review of the UK Construction Labour Model:*

Modernise or Die Time to decide the industry's future. *Construction Leadership Council*. Retrieved from www.cast-consultancy.com

Fortney, L. (2019). Blockchain Explained. Retrieved November 5, 2019, from https://www.investopedia.com/terms/b/blockchain.asp

Frankenfield, J. (2019). Proof of Stake (PoS). Retrieved November 10, 2019, from https://www.investopedia.com/terms/p/proof-stake-pos.asp

Frimpong, Y., Oluwoye, J., & Crawford, L. (2003). Causes of Delay and Cost Overruns in Construction of Groundwater Projects in a Developing Country: Ghana as a Case Study. *International Journal of Project Management*, *21*, 321–326. https://doi.org/10.1016/S0263-7863(02)00055-8

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). To Blockchain or Not to Blockchain : That Is the Question. *IT Professional*, (April), 62–74. https://doi.org/10.1109/MITP.2018.021921652

Gentilal, M., Martins, P., & Sousa, L. (2017). TrustZone-backed bitcoin wallet. In *Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems* (pp. 25–28). Stockholm, Sweden. https://doi.org/10.1145/3031836.3031841

Griffiths, R., Lord, W., & Coggins, J. (2017). Project bank accounts: the second wave of security of payment? *Journal of Financial Management of Property and Construction*, *22*(3), 322–338. https://doi.org/10.1108/jfmpc-04-2017-0011

Hamida, E. Ben, Brousmiche, K. L., Levard, H., & Thea, E. (2017). Blockchain for Enterprise : Overview , Opportunities and Challenges. In *The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017)* (pp. 83–88).

Heiskanen, A. (2017). The technology of trust: How the Internet of Things and blockchain could usher in a new era of construction productivity. *Construction Research and Innovation*, *8*(2), 66–70.

https://doi.org/10.1080/20450249.2017.1337349

Hillebrandt, P., Hughes, W., & Murdoch, J. (1998). *Financial Protection in the UK Building Industry: Bonds, Retentions and Guarantees*. London: Taylor & Francis.

Hu, Y., Liyanage, M., Manzoor, A., Thilakarathna, K., Jourjon, G., Seneviratne, A., & Ylianttila, M. (2018). The Use of Smart Contracts and Challenges, *1*(1), 1–12.

Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. *Procedia Computer Science*, *98*, 461–466. https://doi.org/10.1016/j.procs.2016.09.074

Hunhevicz, J. J., & Hal, D. M. (2019). Managing mistrust in construction using DLT: a review of use-case categories for technical decisions. In *Proceedings of the 2019 European Conference for Computing in Construction* (pp. 100–109). Chania, Greece. https://doi.org/10.35490/ec3.2019.171

Hussin, A. A., & Omran, A. (2009). Advance Payment: To What Extend It "Save" The Construction Works? In *The International Conference on Economics and Administration, Faculty of Administration and Business (ICEA – FAA)* (pp. 238–247). Bucharest.

Jaffar, N., Tharim, A. H. A., & Shuib, M. N. (2011). Factors of conflict in construction industry: a literature review. *Procedia Engineering*, *20*, 193–202. https://doi.org/10.1016/j.proeng.2011.11.156

Johansson, J., & Nilsson, C. (2018). *How the blockchain technology can enhance sustainability for contractors within the construction industry*.

Judi, S. S., & Rashid, R. A. (2010). Contractor's Right Of Action For Late Or Non-Payment By The Employer. *Journal of Surveying, Construction and Property*, *1*(1), 65–95.

Jutila, L. (2017). *The blockchain technology and its applications in the financial* *sector*.

Karafiloski, E., & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In *17th IEEE International Conference on Smart Technologies, EUROCON 2017 - Conference Proceedings* (pp. 763–768). https://doi.org/10.1109/EUROCON.2017.8011213

Kenley, R. (2003). *Financing Construction: Cash Flows and Cash Farming*. Spon Press (Taylor & Francis). https://doi.org/10.4324/9780203467398

Khandaker, S. (2019). How Blockchain Is Transforming Cross-Border Payments. Retrieved November 15, 2019, from https://www.forbes.com/sites/forbestechcouncil/2019/03/12/how-blockchain-is-transforming-cross-border-payments/#61c20ead7df2

Latham, M. (1994). *Constructing the team:Final report of the government industry review of procurement and contractual arrangements in the UK construction industry*. London.

Law, A. (2017). *Smart Contracts and their Application in Supply Chain Management*.

Lessing, B., Thurnell, D., & Durdyev, S. (2017). Main factors causing delays in large construction projects: Evidence from New Zealand. *Journal of Management, Economics, and Industrial Organization*, *1*(2), 63–82.

Li, J., Greenwood, D., & Kassem, M. (2018). Blockchain in the built environment : analysing current applications and developing an emergent framework. In *Creative Construction Conference* (pp. 59–66). Ljubljana. https://doi.org/10.3311/CCC2018-009

Li, J., Greenwood, D., & Kassem, M. (2019). Blockchain in the built environment and construction industry : A systematic review , conceptual models and practical use cases. *Automation in Construction*, *102*, 288–307. https://doi.org/10.1016/j.autcon.2019.02.005

Li, J., & Kassem, M. (2019). A Proposed Approach Integrating DLT, BIM, IoT and Smart Contracts: Demonstration Using a Simulated Installation Task. In *International Conference on Smart Infrastructure and Construction 2019 (ICSIC)* (pp. 275–282). https://doi.org/10.1680/icsic.64669.275

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.020

Liu, J., Li, H., Skitmore, M., & Zhang, Y. (2019). Experience mining based on case-based reasoning for dispute settlement of international construction projects. *Automation in Construction*, *97*, 181–191. https://doi.org/10.1016/j.autcon.2018.11.006

Llangakoon, D. H. S. . (2017). *STUDY ON PAYMENT DELAYS IN SMALL SCALE CONSTRUCTION PROJECTS IN SRI LANKA (BASED ON CASE STUDIES)*. University of Moratuwa.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making Smart Contracts Smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 254–269). Vienna, Austria. https://doi.org/10.1145/2976749.2978309

Macaulay, M., & Summerell, T. (2019). UK: Project Bank Accounts: Making Payment Fair. Retrieved October 24, 2019, from http://www.mondaq.com/uk/x/786636/Building+Construction/Project+bank+accounts+making+payment+fair

Mahamid, I. (2016). Micro and macro level of dispute causes in residential building projects : Studies of Saudi Arabia. *Journal of King Saud University - Engineering Sciences*, *28*(1), 12–20. https://doi.org/10.1016/j.jksues.2014.03.002

Manu, E., Ankrah, N., Chinyio, E., & Proverbs, D. (2015). Trust influencing factors in main contractor and subcontractor relationships during projects.

International Journal of Project Management, *33*(7), 1495–1508. https://doi.org/10.1016/j.ijproman.2015.06.006

Mason, J, & Escott, H. (2018). Smart contracts in construction: Views and perceptions of stakeholders. In *Proceedings of FIG Conference*. Istanbul.

Mason, Jim. (2017). Intelligent Contracts and the Construction Industry. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *9*(3), 04517012. https://doi.org/10.1061/(ASCE)LA.1943-4170.0000233.

Massessi, D. (2018). Public Vs Private Blockchain In A Nutshell. Retrieved November 10, 2019, from https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f

McNamara, A., & Sepasgozar, S. M. E. (2018). Barriers and drivers of Intelligent Contract implementation in construction. In *The 42nd Australasian Universities Building Education Association Conference* (pp. 281–293). Singapore.

Mei Ye, K., & Abdul-Rahman, H. (2010). Risk of Late Payment in the Malaysian Construction Industry, World Academy of Science, Engineering and Technology. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, *4*(5), 503–511.

Meng, X. (2002). Guarantees for contractor‟s performance and owner‟s payment in China. *Journal of Construction Engineering and Management, ACSE*, *3*, 232–237. https://doi.org/10.1061/(asce)0733-9364(2002)128:3(232)

Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. In *Law, Innovation and Technology* (Vol. 9, pp. 269–300). Taylor & Francis. https://doi.org/10.1080/17579961.2017.1378468

Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.

Nagpal, R. (2017). 17 blockchain platforms — a brief introduction. Retrieved October 10, 2019, from https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

National Audit Office. (2005). *Improving Public Services through better construction*.

Nawari, N. O., & Ravindran, S. (2019). Blockchain Technologies in BIM Workflow Environment. In *Computing in Civil Engineering* (pp. 343–352).

Odeyinka, H. A., & Kaka, A. (2005). An evaluation of contractors' satisfaction with payment terms influencing construction cash flow. *Journal of Financial Management of Property and Construction*, *10*(3), 171–180. https://doi.org/10.1108/13664380580001074

OGC. (2007). *Guide to Best "Fair Payment" Practices*. *Office of Government Commerce*. Office of Government Commerce.

Pass, R., & Shi, E. (2017). Hybrid consensus: Efficient consensus in the permissionless model. In *Leibniz International Proceedings in Informatics, LIPIcs* (Vol. 91). Schloss Dagstuhl- Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing. https://doi.org/10.4230/LIPIcs.DISC.2017.39

Penzes, B. (2018). *Blockchain Technology In The Construction Industry*.

Petre, A. (2017). Blockchain use cases in healthcare. *LinkedIn Pulse*, *111*, 1–41. Retrieved from https://www.linkedin.com/pulse/blockchain-use-cases-healthcare-anca-petre

Pettigrew, R. (2005). *Payment Under Construction Contracts Legislation*. London: Thomas Telford.

Pilagos, N. (2018). Disrupting the building blocks: smart contracts and blockchain in construction. Retrieved November 25, 2019, from https://www.taylorwessing.com/download/article-disrupting-building-blocks.html

Popper, N. (2016). A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency. Retrieved October 5, 2019, from https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html

Pratap, M. (2018). Everything You Need to Know About Smart Contracts: A Beginner's Guide. Retrieved November 8, 2019, from https://hackernoon.com/everything-you-need-to-know-about-smart-contracts-a-beginners-guide-c13cc138378a

Price, R. (2011). The problem of pay. *Construction Research and Innovation*, *2*(2), 34–39. https://doi.org/10.1080/20450249.2011.11873802

Ramachandra, T. (2013). *Exploring Feasible Solutions to Payment Problems in the Construction Industry in New Zealand*. Doctoral dissertation, Auckland University of Technology.

Ramachandra, T., & Rotimi, J. O. (2011). The Nature of Payment Problems in the New Zealand Construction Industry. *Australasian Journal of Construction Economics and Building*, *11*(2), 22–33. https://doi.org/10.5130/ajceb.v11i2.2171

Ramachandra, T., & Rotimi, J. O. B. (2014). Mitigating Payment Problems in the Construction Industry through Analysis of Construction Payment Disputes. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *7*(1), A4514005. https://doi.org/10.1061/(asce)la.1943-4170.0000156

Rosic, A. (2017). What is Ethereum Gas? [The Most Comprehensive Step-By-Step Guide Ever!]. Retrieved November 1, 2019, from https://blockgeeks.com/guides/ethereum-gas/

Sahab, S. . S., & Ismail, Z. (2011). Construction Industry Payment And Adjudication Act ; Enhancing Security Of Payment In The Malaysian Construction Industry.

In *International Conference on Business, Engineering and Industrial Applications (ICBEIA)* (pp. 153–159). IEEE. https://doi.org/10.1109/ICBEIA.2011.5994231

Saleh, F. (2019). *Blockchain Without Waste : Proof-of-Stake*.

Sambasivan, M., & Soon, Y. W. (2007). Causes and effects of delays in Malaysian construction industry. *International Journal of Project Management*, *25*(5), 517–526. https://doi.org/10.1016/j.ijproman.2006.11.007

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information and Communications Technology Law*, *26*(2), 116–134. https://doi.org/10.1080/13600834.2017.1301036

Shou, W., Wang, J., & Wang, X. (2015). A Comparative Review of Building Information Modelling Implementation in Building and Infrastructure Industries. *Archives of Computational Methods in Engineering*, *22*(2), 291–308. https://doi.org/10.1007/s11831-014-9125-9

Smart Contracts Alliance. (2016). *Smart Contracts: 12 Use Cases for Business & Beyond*. Washington, D.C.

Stougiannos, L., & Magneron, A. (2018). BIM, Blockchain and the Smart Construction Contract. Retrieved November 15, 2019, from https://www.millerthomson.com/en/blog/breaking-ground-mt-construction-law/bim-blockchain-smart-construction-contract/

Sultan, K., Ruhi, U., & Lakhani, R. (2018). CONCEPTUALIZING BLOCKCHAINS : CHARACTERISTICS & APPLICATIONS. In *11th IADIS International Conference Information Systems 2018* (pp. 49–57).

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly.

Szabo, N. (1996). Smart Contracts : Building Blocks for Digital Markets. *EXTROPY: The Journal of Transhumanist Thought*, *16*(18), 1–11.

Tazelaar, F., & Snijders, C. (2010). Dispute resolution and litigation in the construction industry . Evidence on conflicts and conflict resolution in The Netherlands and Germany. *Journal of Purchasing and Supply Management*, *16*(4), 221–229. https://doi.org/10.1016/j.pursup.2010.08.003

Towey, D. (2013). *Cost Management of Construction Projects*. United Kingdom: John Wiley & Sons.

Tran, H., & Carmichael, D. G. (2012). Contractor's Financial Estimation based on Owner Payment Histories. *International Journal of Organization, Technology and Management in Construction*, *4*(2), 481–489. https://doi.org/10.5592/otmcj.2012.2.4

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084–2123. https://doi.org/10.1109/COMST.2016.2535718

Turk, Ž., & Klinc, R. (2017). Potentials of Blockchain Technology for Construction Management. *Procedia Engineering*, *196*, 638–645. https://doi.org/10.1016/j.proeng.2017.08.052

UK Cabinet Office. (2012). *Government Construction; A Guide to the Implemetation of Project Bank Accounts (PBAs) in Construction for Government Clients*. *UK Government*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62118/A-guide-to-Project-Bank-Accounts-in-construction-for-government-clients-July-2012.pdf

Viriyasitavat, W., & Hoonsopon, D. (2019). Journal of Industrial Information Integration Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*(July 2018), 32–39. https://doi.org/10.1016/j.jii.2018.07.004

Voshmgir, S. (2019). *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*.

Wang, J., Wu, P., Wang, X., & Shou, W. (2017). The outlook of blockchain technology for construction engineering management. *Frontiers of Engineering Management*, *4*(1), 67–75. https://doi.org/10.15302/J-FEM-2017006

Wedrowicz, K. (2018). Ethereum gas: how to pay it on behalf of your users. Retrieved November 9, 2019, from https://espeoblockchain.com/blog/ethereum-gas-price/

Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, *151*, 1–32.

Ye, Z., Yin, M., Tang, L., & Jiang, H. (2018). Cup-of-Water theory: A review on the interaction of BIM, IoT and blockchain during the whole building lifecycle. In *ISARC 2018 - 35th International Symposium on Automation and Robotics in Construction and International AEC/FM Hackathon: The Future of Building Things*.

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial*, 1–7. https://doi.org/10.1186/s40854-016-0049-2

Zhao, W. (2017). $7 Million Lost in CoinDash ICO Hack. Retrieved November 5, 2019, from https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology : Architecture , Consensus , and Future Trends. In *2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557–564). https://doi.org/10.1109/BigDataCongress.2017.85

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities : a survey. *International Journal of Web and Grid Services*, *14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.10016848

Zhu, H., & Zhou, Z. Z. (2016). Analysis and outlook of applications of blockchain technology to equity crowdfunding in China. *Financial Innovation*, *2*(1), 1–11. https://doi.org/10.1186/s40854-016-0044-7