

**Xiamen University Malaysia Research Fund (XMUMRF)**

**Application Form**

|  |  |  |  |
| --- | --- | --- | --- |
| **Year** | 2021 | **Cycle** | 8 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PERSONAL DETAILS OF PRINCIPAL INVESTIGATOR (APPLICANT)** | | | | | | | | | | | | | | | | | | | |
| **Full name** | | | | | | | | Mahdi Hassan Miraz | | | | | | | | | | | |
| **Abbreviated name (as in a publication)** | | | | | | | | Mahdi H. Miraz | | | | | | | | | | | |
| **Position** | | | | | | | | *Assistant Professor* | | | | | | | | | | | |
| **School / Department** | | | | | | | | Electrical and Computer Engineering / Information and Communication Technology | | | | | | | | | | | |
| **Highest academic qualification(s)** | | | | | | | | PhD (and Postdoc) | | | | | | | | | | | |
| **Staff number** | | | | | | | |  | | | | | | | | | | | |
| **Nationality** | | | | | | | |  | | | | | | | | | | | |
| **New identity card number** | | | | | | | | N/A | | | | | | | | | | | |
| **Passport number (non Malaysian)** | | | | | | | |  | | | | | | | | | | | |
| **Gender** | | | | | | | | *Male* | | | | | | | | | | | |
| **Starting date at XMUM** | | | | | | | |  | | | | | | | | | | | |
| **Contract end date (if applicable)** | | | | | | | |  | | | | | | | | | | | |
| **Correspondence address** | | | | | | | |  | | | | | | | | | | | |
| **E-mail address** | | | | | | | | mahdi.miraz@xmu.edu.my | | | | | | | | | | | |
| **Office telephone number** | | | | | | | | 5032 | | | | | | | | | | | |
| **Mobile number** | | | | | | | |  | | | | | | | | | | | |
| **RESEARCH CLUSTER**  *(Please tick √)* | | | | | | | | | | | | | | | | | | | |
| **( ) Pure and Applied Science**  *(Chemistry, Physic, Biology, Biochemistry, Material Science, Biotechnology, Mathematics and Statistics)* | | | | | | | | | | | | | | | | | | | |
| **( ) Engineering and Technology**  *(Electrical and**Electronics, Chemical and Process Engineering, Material and Polymer, Green Technology, Energy, Mechanical and Manufacturing)* | | | | | | | | | | | | | | | | | | | |
| **( ) Traditional Chinese Medical Sciences**  *(Basic Medical Sciences, Clinical Studies)* | | | | | | | | | | | | | | | | | | | |
| **( √ ) Information and Communication Technology**  *(Software, Artificial Intelligence, Computer Networks, Information System, Theory of Computation, Hardware Design)* | | | | | | | | | | | | | | | | | | | |
| **( ) Social Science**  *(Anthropology, Sociology, Political Science, Business, Management, Economic, Communication, Ethnography)* | | | | | | | | | | | | | | | | | | | |
| **( ) Arts**  *(Language and Linguistic, Literature, Religion, Philosophy, History, Art, Culture, Education, Policies and Law* | | | | | | | | | | | | | | | | | | | |
| **DETAILS OF CO-RESEARCHER(S)**  *(Please attach the curriculum vitae of each co-researcher)* If necessary, please add additional rows with the appropriate details. | | | | | | | | | | | | | | | | | | | |
| **1. Name:** Maaruf Ali CEng, SMIEEE, FHEA **Position:** Assistant Professor **Staff /student number:** N/A **School / Department:** Department of Computer Engineering, Epoka University, Albania **Email address:** maaruf@ieee.org **Contribution:** External Consultant/Collaborator | | | | | | | | | | | | | | | | | | | |
| **2. Name: Teh Jia Yew Position: Assistant Professor Staff / student number: School / Department: Email address: Contribution:** | | | | | | | | | | | | | | | | | | | |
| **3. Name: Position: Staff / student number: School / Department: Email address: Contribution:** | | | | | | | | | | | | | | | | | | | |
| **DETAILS OF PROPOSED RESEARCH PROJECT**  *(Please include problem statement, hypothesis/research questions, literature reviews and related reference)* | | | | | | | | | | | | | | | | | | | |
| (A) Title: Lightweight Blockchain of Things (BCoT) Architecture for Enhanced Security and Performance of Health Level Seven (HL7) IoT Network  (B) Research area/field: Blockchain/Digital Ledger Technology (DLT), Internet of Things (IoT) and Health Level Seven (HL7) Network  (C) Duration (Maximum 3 years): From 1 July 2021 to 30 June 2024  (D) Abstract (Not more than 500 words):  Both Blockchain (BC) and Internet of Things (IoT) are the two major disruptive emerging constituents of the contemporary internet-enabled era of technology. In fact, both of these technologies are distributed, autonomous and mostly decentralised systems. That being said, both of these technologies have their own innate technological confines to some extent, possessing connatural potentials to act as complementary to each other. IoT is in need of hardening its security measures while Blockchain or Distributed Ledger Technology (DLT) intrinsically provides secure platform by making extensive use of cryptography and consensus algorithms along with distributed networks. On the contrary, Blockchain requires significant contributions from the participants of its distributed network to make its P2P (Peer-to-Peer) consensus model function properly, while IoT intrinsically embodies P2P participants in its architecture. Most Health Level Seven (HL7) Networks, providing multifaceted healthcare services including remote monitoring, comprise IoT and Wireless Sensor Networks (WSN). The healthcare data streams, passing through such wired or wireless networks, are a prime target of cyber criminals. This is because healthcare data possesses greater black-market cyber value even when compared to financial data. With the proliferating number of personal healthcare records being digitised and being transmitted through the local networks or the Internet, the volume of cyber-attacks on Health Information System (HIS) has drastically increased in the recent past years. One major concern is the incapability of the resource constrained IoT or wireless sensor devices to efficiently utilise the traditional cryptographic techniques. Therefore, a light-weight smart contract enabled fusion of Blockchain technologies with the Internet-of-Things, also known as Blockchain-of-Things (BCoT), architecture can be adopted as a smart alternative of data obfuscation. For enhanced performance, the resource constrained IoT devices will act as Light nodes (opposed to the full nodes holding the entire copy of the ledger) of the blockchain network. To address concerns related to access control, identity management and other relevant aspects, blockchain-enabled smart contracts can be utilised. While Blockchain-of-Things (BCoT) is a recent popular research trend, the concept of developing a light-weight BCoT enabled smart contract based secure architecture for ICS/SCADA Health Level Seven (HL7) Network with enhanced security and performance, is the novelty of this project. Thus, the project will lead to the development of a framework and prototype, making the BC consensus very light-weight and safeguarding the data streams from eavesdrop attacks by any man-in-the-middle (MiTM) exploits, while enhancing the performance of the network including energy consumption aspects. In fact, upon completion of the study, this fundamental framework can then be used for any other IoT enabled smart networks. This research project, therefore, will intensely investigate the viability as well as the prospective challenges of integrating Blockchain with IoT technologies—inducing the notion of Blockchain of Things (BCoT)—as well as the benefits such consolidation can offer to Health Level Seven (HL7) or any other IoT enabled smart networks. Furthermore, the project will develop solutions, such as light-weight BC consensus algorithm/framework and prototype, eliminating the current challenges and enhancing the overall performance of the fusion, to some extent. The solutions will be then tested and verified.  (E) Objective(s) (May include problem statement, hypothesis, research questions):  Objective(s) of the Research:   1. To conduct a detailed/systematic review on the fusion of Blockchain and IoT (BCoT) and its application in smart IoT environments, including the healthcare sector. 2. To identify, design and develop a light-weight consensus algorithm/mechanism in order to address the current challenges and enhance the performance of Blockchain of Things (BCoT) for securely exchanging Health Level Seven (HL7) data streams amongst ISO/IEEE 11070 compliant healthcare and other IoT/computing devices. 3. To develop a proof-of-concept (PoC) prototype and testbed, to facilitate continuously monitoring, diagnosis and treatment of the patients remotely, who are in critical situation or suffering from infectious diseases. 4. To test and verify different parameters, particularly security and performance, of the developed algorithm/framework as well as the PoC testbed prototype.   Problem Statements:  Based on the situation evolved due to the current COVID-19 [1] pandemic, the significant importance of being able to provide uninterrupted remote monitoring of the health parameters, for those who are either elderly or suffering from any critical or infectious diseases, has been (re)realised. This technology led innovations in healthcare sector provides with multifaceted advantages over the traditional manual process, such as being able to remotely monitor and treat the patients without the healthcare professionals being exposed to the infections, automatically moving and handling a bedridden patient using IoT enabled medicare equipment with (pressure) sensors, remote access to various healthcare related data at the doctors’ desk without physically visiting the patients, treatment related decision making powered by Artificial Intelligence (AI) through the collection of machine-generated data and thus performing the required actions automatically etc.  This remote monitoring systems not only provides efficiency, cost-effectiveness, improved performance etc. but also helps contain any infectious diseases. Therefore, this has recently become a popular trend. As a result, tremendous amount of patients’ health related as well as other personal data are being digitalised and communicated over various networks to and from multifaceted systems including IoT devices and cloud computing [2]. Therefore, healthcare data are being prevalently targeted by the cyber criminals [3]. In fact, Malaysia’s healthcare sector is no exception to this phenomenon, as evidenced by the recent medical data breach claim [4,5] which asserts that the medical data of approximately 20,000 Malaysians were also leaked on the Internet amongst the millions of others globally. In Malaysia, cybersecurity cases, including healthcare ones, has gone up by 82.5% compared to the previous year, as reported in April 2020 by Cybersecurity Malaysia [6], during the first phase of the movement control order (MCO) imposed by the Malaysian government to contain the spread of COVID-19 infections.  The ISO/IEEE 11073 Personal Health Data (PHD) [7] family of standards enable the seamless exchange of medical/healthcare data amongst various healthcare devices as well as external computing platforms including cloud computing. The Health Level Seven (HL7), along with its successor Fast Healthcare Interoperability Resources (FHIR), has been acting as the key data enabler for data modelling and standardisation support for more than 30 years [8]. While the implementation and specification of HL7/FHIR fall out of the scope of this project, we consider to use HL7 for its maturity, proven track-record and widespread adoption as a healthcare information sharing standard. However, HL7/FHIR does not provide any data security features by default. To ensure privacy and security, HL7/FHIR data streams also need to be protected by adopting routine procedures.  To ensure data security of the healthcare records while they are being transmitted, e.g. the data-in-transit, the data needs to be obfuscated so that even if the data are captured by the MiTM, they cannot be meaningfully interpreted. Obviously, there are many established encryption techniques to cipher the data, which have been prudently used thus far, including financial sectors. However, these encryption techniques demand high processing power, due to the mathematical calculations and/or permutations and  combinations required to perform the tasks.  The IoT devices and sensors, including the Nano-scaled ones, are considered to be highly resource constrained, particularly in terms of computational processing power and source of energy. Therefore, traditional encryption and data obfuscation mechanisms, even including traditional lightweight communications, are not a well-fit for such resource limited devices. In addition, the lack of industrial standardisation and regulation enforcement is also another concern. Hence, a very simple but efficient approach, combining blockchain enabled smart contract and IoT technologies, will be a good fit for this purpose and have been advocated in our project proposal. However, such lightweightness of any cryptographic algorithms is usually achieved by trading off level of security measures. This is where the application of blockchain comes into the scenario and can significantly contribute. Our aim is to fortify the level of security compromised for the leightweightness through the implementation of blockchain and smart-contracts. Thus, the system will not only inherit the underlying security features of the blockchain architecture, implementation of smart-contracts will also strengthen many aspects of the existing security measures, such as by the introduction of authentication, identity management of the devices, role-based access controls, etc.  For security and privacy purposes, these data-in-rest will be stored in encrypted forms using cryptographic tools. Considering the fact that a major share of the blockchain peers/nodes will comprise resource constraint IoT Healthcare devices, the blockchain ecosystem will incorporate the concept of implementing role-based peers. The peers, based on their computing and processing capability, shall have two distinct roles: light nodes and full nodes. While the light nodes, such as the lightweight IoT devices, will actively take part in the consensus process, they will not hold the complete copy of the ledger - rather, only the hashes using Markle Tree will be held. However, the full nodes of the blockchain ecosystem only will hold copies of the ledger. If additional storage is required, cloud based distributed off-chain storing process can also be implemented, depending on the yet-to-be-evaluated need of the project. Access controls, identity management and other associated measures of these devices shall be administered by smart contracts to ensure that only legitimate devices (users) have access to the authorised data upon authentication.  The integration IoT with blockchain technologies and smart contacts, for such HL7/FHIR healthcare monitoring system, delivers the novelty of the project. Upon successful completion of the project, the derived light-weight but efficient framework can be extended for multifaceted IoT enabled applications and/or smart platforms.  Hypothesis:  This is a dire necessity to develop and deploy an efficient and light-weight consensus based BCoT architecture, considering both computational processing power and energy consumptions as well as security measures of the resource limited smart IoT devices. While traditional encryption mechanism fails to fulfil this demand for ISO/IEEE 11073 compatible healthcare devices, the smart contact enabled BCoT technique holds the promise to address these issues. However, deployment of suitable smart contact enabled BCoT technique, has its own respective challenges, particularly in terms of authentication, authorisation, identity management etc. with respect to the newly installed or reconnected devices. Therefore, developing a secure but light-weight architecture for ICS/SCADA Health Level Seven (HL7) Network with the fusion of Blockchain-enabled Smart Contract can serve as a key strategy to effectively address the aforementioned issues.  Research Questions:  1. How to theorise the development of a light-weight consensus algorithm based BCoT architecture/framework for efficient and secure ICS/SCADA Health Level Seven (HL7) Network, considering the resource constrained ISO/IEEE 11073 healthcare and other IoT devices?  2. How to test, evaluate and validate the security and performance parameters of developed proof-of-concept (PoC) prototype and testbed and/or any (remote monitoring) healthcare systems developed using the proposed architecture, facilitating continuous monitoring, diagnosis and treatment of the patients, who are in critical situation or suffering from infectious diseases?  (F) Literature review/Research background (Concise, with some relevant key references):  To continuously monitor, diagnose, medicate and treat critical and/or isolated patients, such as COVID-19 positive ones, sensor and IoT enabled healthcare monitoring system is a must. However, the benefits of the “connected” healthcare system come with their own cost i.e. the risk of data breach and leaks. In fact, healthcare (and associated personal) data is a popular target of the cyber criminals. Therefore, when deploying the emerging technologies to enable and automate the aforementioned healthcare related tasks,  data security needs to be given high importance. While the traditional encryption techniques have been proven to be efficient for regular networks, they are not a well-fit for the resource constrained sensor and IoT devices. These necessitates the need for innovating, developing and deploying other smart alternatives.  Both Blockchain technologies and IoT are distributed, autonomous and *mostly* decentralised systems possessing connatural potentials to act as complementary to each other [9]. Similar to other computing domains, security and privacy issues of Internet of Things (IoT) ecosystem are considered to be the major concerns [10]. Since Blockchain already possesses proven security measures, in their integrated platform i.e. BCoT, Blockchain can play a vital rôle in fortifying IoT’s security and privacy backbone [11]. Furthermore, most of the communication in an IoT ecosystem takes place in the form of Machine-to-Machine (M2M) interactions – without the need for human intervention. Therefore, establishing the “trust” amongst the participating is a major challenge that IoT technologies yet require to address. However, a fusion with Blockchain can act as a paradigm shift in this regard, by enabling extra layer of security, scalability, privacy and reliability [9,11]. This can be engineered by implementing Blockchain/DLT to track and trace IoT’s billions of connected devices and then to enable and/or coordinate the processing of transaction of messages/data. Such fusion of IoT with Blockchain/DLT will further enhance IoT’s reliability by eliminating any Single Point of Failure (SPF). The major foundation of Blockchain’s security feature is laid on the extensive utilisation of hashing techniques and cryptographic algorithms. Therefore, the combined ecosystem can offer better security services. That being said, to deploy the required cryptographic algorithms and carry out the hashing techniques, higher amount of processing power will be required, which devices IoT currently suffers from. To address this current limitation, further research will be required, “including extending the longevity of the in situ powering source” [11].  Blockchain/DLT is also a perfect fit to record sequence or chronological information, stored as Blockchain transactions, “as it may be seen as an enormous networked time-stamping system” [11]. It can also be used “to prevent tampering and spoofing of data by managing and securing industrial IoT and operational technology (OT) devices” [3]. After a device, sensor or controller is deployed in the IoT ecosystem and is working, tampering it becomes nigh impossible if integrated with Blockchain. Any comprised devices will be recorded in chain and be easily identifiable. Furthermore, the consensus algorithm will also reject any unauthorised changes.  Most of the communication of IoT takes place utilising wireless sensor network (WSN) technologies. Therefore, it inherits the threats and vulnerability to security and privacy from WSN. In contrast, Blockchain/DLT is considered as a “Trust Machine” [11] as it is highly secure by its architecture and design which includes consensus method, hashing, cryptography and distributed network. Therefore, it seems possible that the majority of IoT’s security concerns can be addressed by integrating with Blockchain technologies. As was pointed out in the abstract section to this proposal, Miraz and Ali [11] argues “[that both IoT and Blockchain are] complementary technologies for each other: BC requires participating nodes for consensus approach which can be supplemented by IoT devices while IoT requires security features which can be met by BC such as: transparency, privacy, immutability, operational resilience and so forth”.  Internet of Things (IoT) is a “cyber-physical system” replicating the “connected” physical world into part of a large dominion of the information system – i.e. the “cyber world” [12]. Be that as it may, for various reasons, the security aspects of the IoT were not properly focused and addressed at the design phase of the technology -e.g. devices and products [12]. With the mushrooming popularity of BC, there is a growing body of literature that recognises the importance of IoT research coupled with BC [13-14] to materialise a robust but secure cyber world.  Despite these, since both the technologies are yet not quite mature, there are many unaddressed challenges and concerns arising from such integration [15]. A growing number of studies [9, 11, 16, 17] suggest that the application of Blockchain/DLT has the potentials to help fulfil the security limitations of IoT ecosystem, including the protection from the “Stalker” [16] attack. As mentioned above, IoT’s communication mechanisms are mainly built on the foundation laid by the wireless sensor network (WSN) [18], archetypally IoT platforms are vulnerable to similar attacks, such as from the Distributed Denial-of-Service (DDoS) [19] threat and may serve as a point of failure if compromised.  Within the IoT influenced “Machine Economy”, the data generating IoT devices or sensors can now proficiently exchange, share and even trade the generated data with different autonomous marketplaces and systems. That being said, uplifting the “trust” amongst the transacting parties is still considered as a core challenge. A publicly verifiable audit-trail system, as offered by the blockchain technologies, to establish trust without needing a third-party, is vital to address the non-repudiation problem [20]. To date, few such blockchain/DLT based applications were implemented, amongst which TransActive Grids [21] and FileCoins [22] are noteworthy.  [23] adopts pseudonymization approach by splitting the data into small chunks before sending to a smart IoT device, such as in smart homes. The hashes of these data are stored on the Blockchain which acts as a certificate provider. Since blockchain has been integrated into different layers of this framework, viz. application, database, communication and physical layers, security issues and relevant limitations of these layers were satisfactorily addressed. Applying blockchain as a distributed database, Smart Contract functionalities were implemented using Ethereum platform. The application layer, having Blockchain integrated, further strengthen the security through restricting fraudulent access to the dependent processes by any intruders.  Filament [24] implemented a different approach by applying the Telehash protocol to adopt Blockchain. With the utilisation of smart contracts, Filament enabled smart IoT devices and sensors “to discover, interact and communicate (message exchange) with each other with the freedom to act independently without the need for any central control” [11]. As a pre-requisite to any communication process, the transacting devices need to successfully authenticate themselves through pertinent security protocols, e.g. Secure Socket Layer (SSL) and Transport Layer Security (TLS) utilising through public key infrastructure (PKI).  Some intermediate devices, in an IoT ecosystem, may perform the roles of hops. As a result, considering the significance of such private communication protocols, it is necessary to design a secured architecture. To facilitate such secure communications amongst the smart IoT devices, the Moeco prototype adopted “Domain Name System (DNS) of things” [25] by applying Blockchain for IoT data routing, utilising Ethereum platform. However, Moeco’s future research direction includes shifting from Ethereum to a tailor-made Byzantine consensus approach namely Exonum [26].  To date, one of the unaddressed key challenges of securing IoT data is designing and developing an access control and authentication mechanism which solely fulfils the especial requirements of decentralised IoT platforms encompassing devices having low processing power. With the aim to address this issue, Deters [27] proposed a smart contract enabled Blockchain based solution – a data recorded on the ledger can only be accessed by sending a request transaction to the address of the smart contract which administers the access control.  Zhenyu et al. [28] advocate the application of large-scale internet of things (IoT) networks for healthcare systems through fog computing. While edge/fog computing reduces the transmission overhead and provides faster performance compared to a traditional cloud computing approach, unless the underlying flaws of the supportive technologies get addressed, data security is seemingly to remain a major cause of concern.  There have been quite a few research advocating the application of blockchain technologies. However, these mainly focused on the security of the data-in-rest. Data-in-transit still remains vulnerable to eavesdropping attacks by the Man-in-the-middle (MiTM) exploits. To address this research gap, we aim to derive a lightweight but efficient and secure BCoT framework, along with blockchain-enabled smart contracts. The major benefits that this scheme, proposed in this project proposal, will be able to offer the reduced (lightweight) cryptographic processing, scalability and portability with very nominal overhead to secure the data-in-transit. To administer authentication and authorisation of the devices, particularly for the newly installed and/or reconnected ones, for accessing the data-in-rest stored on distributed digital ledger, blockchain-enabled smart contracts will be utilised.  References:  [1] David T. Huang et al., “Implementation of the Randomized Embedded Multifactorial Adaptive Platform for COVID-19 (REMAP-COVID) trial in a US health system—lessons learned and recommendations”, Trials, ISSN: 1745-6215, 22(1), pp. 100-110, 2021, DOI: 10.1186/s13063-020-04997-6. Available: https://link.springer.com/article/10.1186/s13063-020-04997-6.  [2] Rohit Ranchal et al., “Disrupting Healthcare Silos: Addressing Data Volume, Velocity and Variety With a Cloud-Native Healthcare Data Ingestion Service”, IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 11, pp. 3182-3188, Nov. 2020, DOI: 10.1109/JBHI.2020.3001518. Available: https://ieeexplore.ieee.org/document/9113446.  [3] Hai Tao et al., “Secured Data Collection With Hardware-Based Ciphers for IoT-Based Healthcare”, IEEE Internet of Things Journal, vol. 6, no. 1, pp. 410-420, Feb. 2019, doi: 10.1109/JIOT.2018.2854714. Available: https://ieeexplore.ieee.org/document/8409278.  [4] Kevin Davasagayam, “Ministry probes medical data breach claims”, The Sun Daily, 19 September 2019. Available: https://www.thesundaily.my/local/ministry-probes-medical-data-breach-claims-FK1387412.  [5] Jerry Choong, “Health Ministry says working with MCMC, Nacsa to contain patient data breach”, Malay Mail, 19 September 2019.  Available: https://www.malaymail.com/news/malaysia/2019/09/19/health-ministry-says-working-with-mcmc-nacsa-to-contain-patient-data-breach/1792174.  [6] Yuen Meikeng, “Cybersecurity cases rise by 82.5%”, The Star, 12 April 2020. Available: https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825.  [7] Kabsu Han, Minwoo Jung and Jeonghun Cho, “Implementation of the personal healthcare services on automotive environments”, Personal and Ubiquitous Computing, 18 (3), pp. 523–533, 2014, DOI: 10.1007/s00779-013-0672-0. Available: https://doi.org/10.1007/s00779-013-0672-0.  [8] Rita Noumeir, “Active Learning of the HL7 Medical Standard”, Journal of Digital Imaging, vol. 32, pp. 354–361, 2019, DOI: 10.1007/s10278-018-0134-3. Available: https://link.springer.com/article/10.1007/s10278-018-0134-3.  [9] Mahdi H. Miraz, “Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies”, In: “Advanced Applications of Blockchain Technology”, Studies in Big Data, Vol. 60, pp 141-159, Published by Springer Nature, 25 September 2019, DOI: 10.1007/978-981-13-8775-3\_7, Print ISBN: 978-981-13-8774-6, Online ISBN: 978-981-13-8775-3, Available: <https://link.springer.com/chapter/10.1007%2F978-981-13-8775-3_7>.  [10] Zainab Alansari, Nor Badrul Anuar, Amirrudin Kamsin, Mohammad Riyaz Belgaum, Jawdat Alshaer, Safeeullah Soomro, Mahdi H. Miraz, “Internet of Things: Infrastructure, Architecture, Security and Privacy”, 2018 Int. Conf. on Computing, Electronics & Communications Engineering (iCCECE), Southend, United Kingdom, 2018, pp. 150-155, doi: 10.1109/iCCECOME.2018.8658516.  [11] Mahdi H. Miraz and Maaruf Ali, “Integration of Blockchain and IoT: An Enhanced Security Perspective”, Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 52-63, Vol. 4, No. 4, 1st October 2020, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2020.04.006, Available: <http://aetic.theiaer.org/archive/v4/v4n4/p6.html>.  [12] Mahdi H. Miraz, Maaruf Ali, Peter S. Excell, and Richard Picking, “Internet of Nano-things, Things and Everything: Future Growth Trends”, Future Internet, vol. 10, no. 8, July 2018, article 68, doi: 10.3390/fi10080068. Available: <http://www.mdpi.com/1999-5903/10/8/68>  [13] Mayra Samaniego, U. Jamsrandorj and Ralph Deters, “Blockchain as a Service for IoT”, Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 2016, pp. 433-436, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102. Available: https://ieeexplore.ieee.org/document/7917130  [14] Jianjun Sun, Jiaqi Yan and Kem Z. K. Zhang, “Blockchain-based sharing services: What blockchain technology can contribute to smart cities," Financial Innovation, vol. 2, article no. 26, pp. 1-9, Dec. 2016, doi: 10.1186/s40854-016-0040-y Available: https://link.springer.com/article/10.1186/s40854-016-0040-y  [15] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler and Manuel Díaz, “On blockchain and its integration with IoT. Challenges and opportunities”, Future Generation Computer Systems, vol. 88, pp. 173-190, Nov., 2018, doi: 10.1016/j.future.2018.05.046. Available: <https://www.sciencedirect.com/science/article/pii/S0167739X17329205>.  [16] Emanuel Ferreira Jesus, Vanessa R. L. Chicarino, Célio V. N. de Albuquerque and Antônio A. de A. Rocha, “A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack”, Security and Communication Networks, vol. 2018, article ID: 9675050, 27 pages, April 2018, doi: 10.1155/2018/9675050. Available: https://www.hindawi.com/journals/scn/2018/9675050/  [17] Djamel Eddine Kouicem, Abdelmadjid Bouabdallah and Hicham Lakhlef, “Internet of things security: A top-down survey”, Computer Networks, vol. 141, pp. 199-221, August 2018, doi: 10.1016/j.comnet.2018.03.012.  [18] Ahmed S. Abu Daia, Rabie A. Ramadan, and Magda B. Fayek, “Sensor Networks Attacks Classifications and Mitigation”, Annals of Emerging Technologies in Computing (AETiC), vol. 2, no. 4, pp. 28-43, October 2018, doi: 10.33166/AETiC.2018.04.003. Available: <http://aetic.theiaer.org/archive/v2/v2n4/p3.html>.  [19] Md Mehedi Hassan Onik, Nasr Al-Zaben, Hung Phan Hoo and Chul-Soo Kim, “A Novel Approach for Network Attack Classification Based on Sequential Questions”, Annals of Emerging Technologies in Computing (AETiC), vol. 2, no. 2, pp. 1-14, April 2018, doi 10.33166/AETiC.2018.02.001. Available: http://aetic.theiaer.org/archive/v2/v2n2/p1.html  [20] Florian Hawlitschek, Benedikt Notheisen and Timm Teubner, “The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy”, Electronic Commerce Research and Applications, vol. 29, pp. 50-63, May-June, 2018, doi: 10.1016/j.elerap.2018.03.005. Available: <https://www.sciencedirect.com/science/article/pii/S1567422318300292>.  [21] LO3 Energy, “EXERGY: Electric Power Technical Whitepaper: Building a Robust Value Mechanism to Facilitate Transactive Energy”, White Paper, 14 December 2017. Available <http://www.truevaluemetrics.org/DBpdfs/Initiatives/Exergy/Exergy-2018-Technical-Whitepaper-v8.pdf>.  [22] Protocol Labs, “Filecoin: A Decentralized Storage Network”, USA, White Paper 2017. Available: <https://filecoin.io/filecoin.pdf>.  [23] Kamanashis Biswas and Vallipuram Muthukkumarasamy, “Securing Smart Cities Using Blockchain Technology”, 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), Sydney, NSW, Australia, 2016, pp. 1392–1393, doi: 10.1109/HPCC-SmartCity-DSS.2016.0198. Available: <https://ieeexplore.ieee.org/document/7828539>.  [24] Filament, "Filament Security Overview—Networking Devices at the Edge of Risk", Nevada, USA, White Paper 2017. Available: <https://www.scribd.com/document/366876418/Filament-Security>.  [25] M. Gorilovsky, "Global IoT Connectivity Platform—MOECO", MOECO, White Paper 2017. Available: <https://moeco.io/>.  [26] Exonum, “Exonum Documentation”, White Paper 2018. Available: <https://exonum.com/doc/version/0.12/>.  [27] Ralph Deters, “Decentralized Access Control with Distributed: Using Blockchain to Manage IoT Access”, International Conference on Cloud and Robotics, Saint Quentin, France, 2017. Available: <https://www.cloudrobotics.info/files/papers/ICCR17_paper_6.pdf>.  [28] Zhenyu Wen, Renyu Yang, Peter Garraghan, Tao Lin, Jie Xu and Michael Rovatsos, “Fog Orchestration for Internet of Things Services”, in IEEE Internet Computing, vol. 21, no. 2, pp. 16-24, 2017, DOI: 10.1109/MIC.2017.36. Available: https://ieeexplore.ieee.org/document/7867735.  (G) Research methodology (Brief descriptions and attach a **FLOWCHART** depicting your research activities):  This project will involve identifying, designing and developing a light-weight BCoT consensus framework, implementing blockchain enabled smart contract, for ICS/SCADA health level seven (HL7) network. A proof-of-concept (PoC) prototype and testbed will then be developed to test the performance of the system and validate the framework. The project will encompass the following steps:  Step-1: A systematic literature review will be conducted comprising the available literatures from the last 10 years. An inclusion and exclusion criteria shall be implanted for the systematic review of literature, which will be strictly followed. This will help to refine the identified research gaps, as outlined in this proposal and comprehend the current status of research in the domain.  Step-2:  An algorithm/approach will be designed and developed to strengthen the security measures of BCoT and enhance the performance of the fusion, to address the needs of exchanging Health Level Seven (HL7) data streams amongst ISO/IEEE 11073 compatible 11073 Personal Health Data (PHD) devices and/or other IoT/computing platforms, to ensure the security of the data-in-transit during the transmission. To achieve this, we propose to the application of smart contracts.  A smart contract is a computer program intended to automatically execute specific actions based on set terms. Programming language that is used to deploy smart contracts is called “Solidity”. The system can be implemented in either the Ethereum Platform or on any other suitable blockchain platform. Ganache can be used for storing smart contracts, which is part of the Truffle suite of Ethereum development tools. For the test environment, Rinkeby can be utilised. Rinkeby is an Ethereum testnet for tests and prototypes.  The data series, i.e. the data-in-rest, will be stored on the tamper-proof digital ledger hosted on a blockchain platform. For security and privacy purposes, these data-in-rest will be stored in encrypted forms using cryptographic tools. Therefore, any newly installed and/or reconnected devices will not only have full access to the required data, but also be able to decrypt them using the appropriate keys, provided that they are authenticated and authorised through the smart contract. Smart contracts will thus ensure legitimate  access to the data as well as the system as a whole, through implementing appropriate access controls, identity management and other associated measures.  Step-3:  Upon successful derivation of the proposed algorithm/approach and developing the required architecture to support the proposed framework, a proof-of-concept (PoC) prototype and testbed will be developed enabling continuous monitoring, diagnosis and treatment of the patients remotely, who are in a critical situation or suffering from infectious diseases such as COVID-19.  Based on the real scenario selected at the time of implementation, the testbed prototype will comprise various sensors that generate events that generate time series data. These sensors must be “smart” enough to be able to communicate with the Personal Healthcare Device (PHD) agent as well as other IoT/Computing devices. The implementation of the PHD will be through an Arduino board connected with the sensors.  Step-4:  The final stage will comprise testing and evaluating different parameters, particularly the security and the performance aspects, of the developed fundamental framework as well as the PoC testbed prototype.  Established security testing mechanisms such as Injection, Broken Authentication and Session Management, Insecure Direct Object References, Missing Function Level Access Control etc. will be deployed to test the robustness of the system. IBM’s Appscan and Microsoft’s FxCop security testing tools will be utilised for this purpose.  The following work-flow diagram demonstrates how each of the above steps will fulfil the research objectives, showcase their alignment with the research questions (RQ).  Fig. 1: Alignment of Research Methodology Steps with Research Objectives and Questions    Finally, at the end of the successful completion of the project, we aim to submit a patent application.  N. B. Flow Chart has been provided with this grant application, in a separate file. Please find attached. | | | | | | | | | | | | | | | | | | | |
| **MATTERS RELATED TO THE PROPOSED RESEARCH PROJECT** | | | | | | | | | | | | | | | | | | | |
| (A) Expected results or benefits: **Publications** (specify national / international, ISI / WoS / Scopus / SSCI / A&HCI / CSSCI and number) – Primary aim is to achieve one ISI/WoS Q1/Q2 ranked journal article, one Scopus ranked journal article and two conference articles. Targeted journals include IEEE Transactions on Wireless Communications, (IF 6.779, Q1), IEEE Internet of Things Journal (IF 9.515, Q1), etc.  **Knowledge creation** – The research will add knowledge to the existing knowledge domain by investigating possible solutions for providing enhanced security and performance through the fusion of IoT and Blockchain, for Health Level Seven (HL7) and other similar IoT-enabled smart networks and applications. A real-time healthcare remote monitoring communication framework through the fusion of IoT and blockchain enabled Smart Contract based secure architecture for ICS/SCADA Health Level Seven (HL7) Network consisting of sensors, IoT and/or (cloud) computing devices will be produced. This novel integrated system is designed to be inherently secure, stable and fault-tolerant. The standardised interface across multiservice sectors will introduce its wide adoption by its reduced learning time through harmonisation.  **Human capital development** (specify undergraduate or postgraduate, number of students) – One undergraduate junior student will be formally recruited to work on the project for a year. Apart from that, FYP and/or other enthusiastic students will have the opportunity to join the group voluntarily. These students will be trained and supervised as required.  **Collaboration with external institutions/agencies** – Dr. Maaruf Ali, from EPOKA University in Albania, agreed to act as a consultant to the project. In addition, I (the principal investigator) is a visiting fellow at Wrexham Glyndwr University (WGU), UK and Senior Fellow, CFRED, The Chinese University of Hong Kong. If deemed to be necessary, external collaborators from these universities will be invited to join.  **External research grant (national or international) application for further research –** The researchers did not apply for any such funding on this particular project. However, the funding of this project, if granted and upon successfully completion of it, may act as a seeding fund for future large-scale projects originating from it.  **Consultancy –** Initially with already established close network of research academics.  **Patent –** The researchers have plan to apply for any innovative application process duly created.  **Commercialisation –** Any possibility arising will be explored and exploited wherever possible.  (B) Benefits of the proposed research to XMUM, the economy, and the society:  Due to Malaysia’s recent technological drive towards the “smart” notion, the usages of multifaceted smart connected objects, i.e. sensors and IoT devices, is mushrooming in every aspect of life, from simple consumer to complicated industrial applications, including sensitive and mission critical domains such as remote healthcare monitoring systems. This move towards the adoption of industry 4.0 or above, significantly contributes to the overall socio-economic development of the relevant communities in Malaysia, aligning and conforming with various national policies and strategies of the Malaysian government. The project falls within the scopes of several 10-10 Malaysian Science, Technology, Innovation and Economy (MySTIE) Framework [20], as outlined by the Academy of Sciences Malaysia. It fully aligns with the 2nd, 6th and 8th Science and Technology Drivers of 10-10 MySTIE which are Sensor Technology, Cyber-security & Encryption and Blockchain [20, pp. 16]. The scope of the project also fully aligns with the 4th Socioeconomic driver (i.e. Medical and Healthcare) as well as partially aligns with the 5th and 6th ones which are Smart Technology and Systems (Next-generation Engineering & Manufacturing) and Smart Cities & Transportation [20, pp. 17]. It also positions it well within the Science and Technology Application Map: Application of the 10-10 MySTIE Framework to the Medical and Healthcare Socioeconomic Driver [20, pp. 29]. The project also falls well within the goals of the National Internet-of-Things (IoT) Strategic Roadmap, as outlined by the Malaysian government [21]. In accordance to satisfy the sustainable development goals (SDG) [22], the deliverables of the project will assure the 3rd and the 11th goals which are good health & well-being and sustainable cities & communities, respectively. Out of the 15 proposed key economic growth activities (KEGA), as outlined in the shared prosperity vision 2030 (SPV 2030), the project highly aligns with KEGA 3 (i.e. Industrial Revolution 4.0) [23]. To summarise, the project significantly comprises different aspects of computing and communications engineering along with healthcare, i.e. IoT, blockchain and security of cyber based healthcare systems in the cyberspace. Thus, it satisfies and falls into multiple categories as outlined by different government strategic plans.  Application of blockchain has become truly multifaceted – far beyond its initial purpose of serving the cryptocurrencies, particularly Bitcoin. Therefore, this research will act as a springboard and open the door for further multi-disciplinary research, collaborating with other schools and departments of XMU, on the application of BCoT such as in supply chain, grid energy, HR management, industrial engineering, securities settlement (stock market), legal domains, FinTech etc. Thus, the research will also initiate the possibility of a wide range of research that will contribute to the economic and societal development.  On a different note: one undergraduate junior student will be formally recruited to work on the project for a year. Furthermore, FYP and/or other enthusiastic students will have the opportunity to join the group voluntarily. These students will be trained and supervised as required. Thus, these XMUM students will be directly benefitting from the project by gaining knowledge and experience in research and product development and/or financial inventive. This will bridge the gap between academic knowledge and industrial experience and therefore, will increase their chances of employability.  (C) Comment on the status of similar or related research in Malaysia and abroad, and state how is your proposed research project different from them:  To date, there are few studies that have investigated the association between Blockchain and IoT and their fused application in various healthcare networks and applications – amongst them the important ones have been included in the above literature review. In fact, there is little published data on such research in Malaysia. However, through personal intricate network, the principal investigator of this project proposal is aware of a similar research project being currently conducted at the Institute of Sustainable Energy, Universiti Tenaga Nasional. The focus of their research is integrating IoT and Blockchain for facilitating solar energy grid systems. On the contrary, the focus of this research will be developing a light-weight BCoT architecture strengthening the security measures of BCoT and enhancing its performance for Health Level Seven (HL7) IoT networks. The model developed will be transferable to other industrial sectors that need to both scale and preserve security and integrity of their networked distributed application.  (D) Past research experience/publications related to the proposed research project:  I have completed my post-doctoral research, at the Chinese University of Hong Kong (CUHK), in Financial Technologies (FinTech), including blockchain and smart contracts. Although, the currently proposed research is slightly different than what I have been doing at CUHK, it is still in the domain of blockchain technologies. I also have previous experience in working on IoT. The following is a list of my publications/presentations in the domain of IoT and Blockchain:  **Keynote and Invited Speech:**   * “[Restoring Direct Holdings and Unified Pricing to Securities Markets with Distributed Ledger Technology](http://finance.zuel.edu.cn/2019/1106/c1093a227772/page.htm)”, invited Research Lecture, Wenlan Finance Forum, School of Finance, Zhongnan University of Economics and Finance, Wuhan, China. * “Chaining the Bubbles in the Blocks”, INET Young Scholars Initiative (YSI) Workshop, part of WINIR ’18 Conference, The Chinese University of Hong Kong, Hong Kong SAR, 14-16 September 2018. * “Anatomy of Blockchain Technologies”, International Conference on Emerging Technologies in Computing 2018 (iCETiC '18), London Metropolitan University, London, UK, 23-24 August 2018.   **Journal Papers and Lecture Notes:**   * **Mahdi H. Miraz** and Maaruf Ali, “Integration of Blockchain and IoT: An Enhanced Security Perspective”, Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 52-63, Vol. 4, No. 4, 1st October 2020, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2020.04.006, Available: <http://aetic.theiaer.org/archive/v4/v4n4/p6.html>. **[Scopus Indexed].** * David C. Donald and **\*Mahdi H. Miraz**, “Multilateral Transparency for Securities Markets through DLT”, [Fordham Journal of Corporate & Financial Law](https://news.law.fordham.edu/jcfl/about/)*,* Vol. XXV, Issue 1, January 2020, pp. 97-153, Available: <https://ir.lawnet.fordham.edu/jcfl/vol25/iss1/2/>. **[Fordham Journal of Corporate & Financial Law is the #1 most-cited specialty journal in banking and finance].** * **Mahdi H. Miraz** and Maaruf Ali, “Blockchain Enabled Smart Contract Based Applications: Deficiencies with the Software Development Life Cycle Models”, [Baltica Journal](http://www.balticajournal.com/index.html), Vol. 33, Issue 1, 20th January 2020, ISSN: 0067-3064, pp. 101-116, published by Lithuanian Academy of Sciences, Available: <http://balticajournal.com/baltica/journals/published/1578108946_IL1qQ.pdf>.**[ISI SCIE Impact Factor 0.5 (Q4); Scopus/SCImago 2019: CiteScore 0.9, SNIP 0.522, SJR 0.218 (Q3)].** * Md Mehedi Hassan Onik and **\*Mahdi H. Miraz**, “Performance Analytical Comparison of Blockchain-as-a-Service (BaaS) Platforms”, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 285, Online ISBN: 978-3-030-23942-8, Print ISBN: 978-3-030-23943-5, Series Print ISSN: 1867-8211, Series Online ISSN: 1867-822X, DOI: 10.1007/978-3-030-23943-5\_1, pp. 3-18, August 2019,Published by Springer-Verlag, Available: <https://link.springer.com/chapter/10.1007/978-3-030-23943-5_1>. [**WoS/ISI ESCI Indexed, Scopus 2019: CiteScore 0.5 and SNIP 0.211; SJR 2019: 0.151 (Q4)**]. * Junaid Chaudhry, Uvais Qidwai and **\*Mahdi H. Miraz**, “Securing Big Data from Eavesdropping Attacks in SCADA/ICS Network Data Streams through Impulsive Statistical Fingerprinting”, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 285, Online ISBN: 978-3-030-23942-8, Print ISBN: 978-3-030-23943-5, Series Print ISSN: 1867-8211, Series Online ISSN: 1867-822X, DOI: 10.1007/978-3-030-23943-5\_1, pp. 3-18, August 2019,Published by Springer-Verlag, Available: <https://link.springer.com/chapter/10.1007/978-3-030-23943-5_6>. [**WoS/ISI ESCI Indexed, Scopus 2019: CiteScore 0.5 and SNIP 0.211; SJR 2019: 0.151 (Q4)**]. * **Mahdi H. Miraz** and David C. Donald “Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities”, Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 11-18, Vol. 3, No. 1, 1st January 2019, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2019.01.005, Available: <http://aetic.theiaer.org/archive/v3/v3n1/p5.html>. [**Scopus Indexed]** * Zainab Alansari, Nor Badrul Anuar, Amirrudin Kamsin, Safeeullah Soomro, Mohammad Riyaz Belgaum, **Mahdi H. Miraz** and Jawdat Alshaer, “Challenges of Internet of Things and Big Data Integration”, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 200, Online ISBN: 978-3-319-95450-9, Print ISBN: 978-3-319-95449-3, Series Print ISSN: 1867-8211, Series Online ISSN: 1867-822X, DOI: 10.1007/978-3-319-95450-9\_4, pp. 47-55,Published by Springer-Verlag, Available: <https://link.springer.com/chapter/10.1007/978-3-319-95450-9_4>. [**WoS/ISI ESCI Indexed, Scopus 2019: CiteScore 0.5 and SNIP 0.211; SJR 2019: 0.151 (Q4)**]. * **\*Mahdi H. Miraz** and Maaruf Ali, “Blockchain Enabled Enhanced IoT Ecosystem Security”, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 200, Online ISBN: 978-3-319-95450-9, Print ISBN: 978-3-319-95449-3, Series Print ISSN: 1867-8211, Series Online ISSN: 1867-822X, DOI: 10.1007/978-3-319-95450-9\_3, pp. 38-46, Published by Springer-Verlag, available: [https://link.springer.com/chapter/ 10.1007/978-3-319-95450-9\_3](https://link.springer.com/chapter/10.1007/978-3-319-95450-9_3). [**WoS/ISI ESCI Indexed, Scopus 2018: CiteScore 0.5 and SNIP 0.211; SJR 2019: 0.151 (Q4)**]. * **\*Mahdi H. Miraz**, Maaruf Ali, Peter S. Excell and Rich Picking, “Internet of Nano-Things, Things and Everything: Future Growth Trends”, (Invited Paper) in [*Future Internet*](http://www.mdpi.com/journal/futureinternet)*,* ISSN: 1999-5903, Volume 10*, Issue 8, Paper No. 68,* Published by MDPI. DOI: 10.3390/fi10080068, 27 July 2018*.* Available: <http://www.mdpi.com/1999-5903/10/8/68>.[**Scopus/SCImago 2019: CiteScore 2.8, SNIP 1.046, SJR 0.387 (Q2); ISI and DBLP Indexed]** * \***Mahdi H. Miraz** and Maaruf Ali, "Applications of Blockchain Technology beyond Cryptocurrency” [*Annals of Emerging Technologies in Computing (AETiC)*](http://www.aetic.theiaer.org/), pp. 1-6, Vo2. 1, No. 1, 1st January 2018, Published by International Association of Educators and Researchers (IAER), Print ISSN: 2516-0281, Online ISSN: 2516-029X, DOI: 10.33166/AETiC.2018.01.001, Available: <http://aetic.theiaer.org/archive/v2n1/p1.pdf>. [**Scopus Indexed]**   **Book Chapters:**   * **\*Mahdi H. Miraz**, “Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies”, In: “Advanced Applications of Blockchain Technology”, Studies in Big Data, Vol. 60, pp 141-159, Published by Springer Nature, 25 September 2019, DOI: 10.1007/978-981-13-8775-3\_7, Print ISBN: 978-981-13-8774-6, Online ISBN: 978-981-13-8775-3, Available: <https://link.springer.com/chapter/10.1007%2F978-981-13-8775-3_7>.   **Conference papers:**   * **\*Mahdi H. Miraz** and David C. Donald, “LApps: Technological, Legal and Market Potentials of Blockchain Lightning Network Applications”, proceedings of the 3rd International Conference on Information System and Data Mining (ICISDM2019)*,* 6th – 8th April 2019, University of Houston, USA, proceedings to bepublished by ACM in May 2019, Available: <https://dl.acm.org/citation.cfm?id=3325942>. * **\*Mahdi H. Miraz** and David C. Donald, “Application of Blockchain in Booking and Registration Systems of Securities Exchanges”, in the proceedings of the [IEEE International Conference on Computing, Electronics & Communications Engineering 2018 (IEEE iCCECE '18)](http://www.iccece18.theiaer.org), 16-17 August 2018, at University of Essex, Southend, UK, Online ISBN: 978-1-5386-4904-6, E-ISBN:978-1-5386-4903-9,DOI: 10.1109/iCCECOME.2018.8658726, pp. 35-40, Published by IEEE, Available: <https://ieeexplore.ieee.org/document/8658726>. [**WoS/ISI ESCI and Scopus Indexed**]. * Zainab Alansari, Nor Badrul Anuar, Amirrudin Kamsin, Mohammad Riyaz Belgaum, Jawdat Alshaer, Safeeullah Soomro and **Mahdi H. Miraz**, “Internet of Things: Infrastructure, Architecture, Security and Privacy”, in the proceedings of the [IEEE International Conference on Computing, Electronics & Communications Engineering 2018 (IEEE iCCECE '18)](http://www.iccece18.theiaer.org), 16-17 August 2018, at University of Essex, Southend, UK, Online ISBN: 978-1-5386-4904-6, E-ISBN:978-1-5386-4903-9, DOI: 10.1109/iCCECOME.2018.8658516, pp. 150-155, Published by IEEE, Available: <https://ieeexplore.ieee.org/document/8658516/>. [**WoS/ISI ESCI and Scopus Indexed**]. * Md Mehedi Hassan Onik, \***Mahdi H. Miraz**, Chul-Soo Kim, “A Recruitment and Human Resource Management Technique Using Blockchain Technology for Industry 4.0” in the proceedings of the IET 2018 Smart Cities Symposium (SCS ’18), held at University of Bahrain, Bahrain between 22-23 April 2018, pp. 11-16, Published by IET, DOI: 10.1049/cp.2018.1371, Available: https://ieeexplore.ieee.org/document/8643177. * Safeeullah Soomro, \***Mahdi H. Miraz**, Anupama Prasanth and Mirza Abdulla, “Artificial Intelligence Enabled IoT: Traffic Congestion Reduction in Smart Cities” in the proceedings of the IET 2018 Smart Cities Symposium (SCS ’18), held at University of Bahrain, Bahrain between 22-23 April 2018, pp. 81-86, Published by IET, DOI: 10.1049/cp.2018.1381, Available: https://ieeexplore.ieee.org/document/8643187. * **\*Mahdi H. Miraz**, Maaruf Ali, Peter Excell and Rich Picking, “A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)”, in the proceedings of the fifth international IEEE conference on Internet Technologies and Applications (ITA 15) held at Creative and Applied Research for the Digital Society (CARDS), Glyndŵ﻿r University in Wrexham, North East Wales, UK, DOI: 10.1109/ITechA.2015.7317398, Print ISBN: 978-1-4799-8036-9, pp 219-224, 8-11 September 2015, Published by IEEE, Available: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7317398>. **[Scopus and ISI/WoS Indexed]**   (E) In the past five years, were you a Principal Researcher or Co-researcher of any research projects that were already completed? **YES** (Delete one of them) If **YES**, please give details:   1. Title of research project – Application of Blockchain in Booking and Registration Systems of Securities Exchanges 2. Role –Co-researcher 3. Source of research fund (Fund name) – As part of postdoctoral assignment 4. Period of the research project – from May 2018 to April 2019 5. Where was the fund held – The Chinese University of Hong Kong (CUHK), Hong Kong SAR 6. Amount of fund– More than 280,000 RM 7. Title of research project – Contracts made ‘smart’ 8. Role –Co-researcher 9. Source of research fund (Fund name) – As part of postdoctoral assignment 10. Period of the research project – from April 2019 to August 2020 11. Where was the fund held – The Chinese University of Hong Kong (CUHK), Hong Kong SAR 12. Amount – More than 205,000 RM   **NOTE**: For more than one, please copy and paste the aforementioned i to vi in the space immediately below and complete the details.  (F) Currently, are you a Principal Researcher or Co-researcher of any **existing** research project? **NO** If **YES**, please give details:   1. Role – Principal Researcher / Co-researcher (Delete one of them) 2. Title of research project – 3. Period of the research project – from to 4. Source of research fund (Fund name) – 5. Where is the fund held – 6. Amount – RM   **NOTE**: For more than one, please copy and paste the aforementioned i to vi in the space immediately below and complete the details.  (G) In the current cycle of XMUMRF application, are you a Co-researcher of any other **proposed** research project? **NO** If **YES**, please give details:   1. Role – Principal Researcher / Co-researcher (Delete one of them) 2. Title of research project – 3. Amount applied for – RM   **NOTE**: For more than one, please copy and paste the aforementioned i to iii in the space immediately below and complete the details. | | | | | | | | | | | | | | | | | | | |
| **PROJECT SCHEDULE/GANTT CHART OF RESEARCH ACTIVITIES** | | | | | | | | | | | | | | | | | | | |
| **Activity** | | | **Year 1** | | | | | | | | | | | | | | | | |
|  | | | **J** | **A** | | **S** | | **O** | **N** | | **D** | | **J** | **F** | | **M** | **A** | **M** | **J** | | |
| **Systematic Literature Review** | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
| **Derive, develop and evaluate a suitable smart-contract enabled BCoT consensus method** | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
|  | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
|  | | | **Year 2** | | | | | | | | | | | | | | | | |
|  | | | **J** | **A** | | **S** | | **O** | **N** | | **D** | | **J** | **F** | | **M** | **A** | **M** | **J** | | |
| **Derive, develop and evaluate a suitable smart-contract enabled BCoT consensus method (Continued)** | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
| **Design and codify the blockchain-enabled smart contracts** | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
| **Finalise and evaluate the Proof-of-Concept (PoC) Prototype** | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
|  | | | **Year 3** | | | | | | | | | | | | | | | | |
|  | | | **J** | **A** | | **S** | | **O** | **N** | | **D** | | **J** | **F** | | **M** | **A** | **M** | **J** | | |
| **Finalise and evaluate the Proof-of-Concept (PoC) Prototype (Continued)** | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
| **Analyse the evaluation results** | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
| **Patent Application (if any)** | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
|  | | |  |  | |  | |  |  | |  | |  |  | |  |  |  |  | | |
| **PROJECT MILESTONES** | | | | | | | | | | | | | | | | | | | |
| **Milestone** | | | | | | | **Key deliverable(s)** | | | | | | | | **Completion date** | | | | |
| **Completion of the Systematic Literature Review** | | | | | | | **1. Publication of a review article** | | | | | | | | **June 2022** | | | | |
| **Derive, develop and evaluate a suitable smart-contract enabled BCoT consensus method** | | | | | | | **1. An Algorithm or system to strengthen BCoT security aspects** | | | | | | | | **December 2022** | | | | |
| **Design and codify the blockchain-enabled smart contracts** | | | | | | | **1. A Proof-of-concept prototype**  **2. Presentation at a conference** | | | | | | | | **December 2023** | | | | |
| **Testing and verification followed by write-up** | | | | | | | **1. A complete report**  **2. Presentation at a conference**  **3. Publication of a research article** | | | | | | | | **June 2024** | | | | |
| **Prepare and submit patent application (if any)** | | | | | | | **1. Patent** | | | | | | | | **June 2024** | | | | |
|  | | | | | | |  | | | | | | | |  | | | | |
| **ACCESS TO EQUIPMENT AND MATERIAL** | | | | | | | | | | | | | | | | | | | |
| **Equipment** | | | | **Existing** | | | | | | | | | | | | | | | |
| **XMUM** | | | | **External (Please specify)** | | | | | | | | | | | |
|  | | | | Matlab License | | | | Solidity and Ethereum Platform for overall development of the Blockchain application;  Ganache can be used for storing smart contracts, which is part of the Truffle suite of Ethereum development tools;  For the test environment, Rinkeby can be utilised, which is an Ethereum testnet for tests and prototypes. | | | | | | | | | | | |
|  | | | | E-library Access | | | | Hardware such as Arduino/Raspberry Pi, high-performance PC with dual monitor etc. | | | | | | | | | | | |
|  | | | |  | | | |  | | | | | | | | | | | |
|  | | | |  | | | |  | | | | | | | | | | | |
| **BUDGET**  *(Please indicate estimated budget for this research proposal)* | | | | | | | | | | | | | | | | | | | |
| Total amount of research fund applied: | | | | | | | | | | | | | | | | | | | |
| NOTE: In principle, the amount requested for each expenditure category should not exceed 50% of the total amount of research fund applied; however, it is subject to justification presented to the Research Management Center, and will be judged on a case-by-case basis. | | | | | | | | | | | | | | | | | | | |
| **Vote** | | **Expenditure Category** | | | **Item/Detail and amount (RM)** | | | | | **Justification** | | | | | **Total amount (RM)** | | | | | |
| 11000 | | Allowance for assistant: | | |  | | | | |  | | | | |  | | | | | |
| 21000 | | Travel and subsistence | | |  | | | | |  | | | | |  | | | | | |
| 24000 | | Rentals | | |  | | | | |  | | | | |  | | | | | |
| 27000 | | Research supplies and materials | | |  | | | | |  | | | | |  | | | | | |
| 28000 | | Minor modifications and repairs | | |  | | | | |  | | | | |  | | | | | |
| 29000 | | Special services | | |  | | | | |  | | | | |  | | | | | |
| 35000 | | Equipment and accessories | | |  | | | | |  | | | | |  | | | | | |
|  | | **Total amount**: **RM** | | | | | | | | | | | | |  | | | | | |
| **LIST OF JOURNAL PUBLICATIONS WITH XMUM AFFILIATION** | | | | | | | | | | | | | | | | | | | |
| **No.** | **Title of publication** | | | | | | | **Year published** | | | | **Quartile** | | | **No. of Citations** | | | | |
| 1 | \*Mahdi H. Miraz, Maaruf Ali and Peter Excell, “Adaptive User Interfaces and Universal Usability through Plasticity of User Interface Design”, Computer Science Review, 40 (May 2021), pp. 100363-100388, ISSN: 1574-0137, E-ISSN:1557-7341, DOI: 10.1016/j.cosrev.2021.100363 URL: https://www.sciencedirect.com/science/article/pii/S1574013721000034. | | | | | | | 2021 | | | | WoS Q1 | | | 2 | | | | |
| 2 | \*Mahdi H. Miraz, Maaruf Ali, Peter S. Excell and Sajid Khan “AI-based Culture Independent Pervasive M-Learning Prototype Using UI Plasticity Design”, Computers, Materials & Continua, ISSN:1546-2218, E-ISSN:1546-2226, 2021, Published by World Scientific, Vol.68, No.1, 2021, pp.1021-1039, 22 March 2021, DOI:10.32604/cmc.2021.015405, Available: https://www.techscience.com/cmc/v68n1/41814. | | | | | | | 2021 | | | | WoS Q1 | | | 2 | | | | |
| 3 | \*Mahdi H. Miraz, Peter S. Excell and Maaruf Ali, “Culturally inclusive adaptive user interface (CIAUI) framework: Exploration of plasticity of user interface design”, International Journal of Information Technology & Decision Making (IJITDM), ISSN: 0219-6220, E-ISSN: 1793-6845, Vol. 20, No. 1, pp. 1-26, Published by World Scientific, DOI: 10.1142/S0219622020500455, 20 January 2021, Available: https://www.worldscientific.com/doi/10.1142/S0219622020500455. | | | | | | | 2021 | | | | WoS Q2 | | | 2 | | | | |
| 4 | Mahdi H. Miraz and Maaruf Ali, “Integration of Blockchain and IoT: An Enhanced Security Perspective”, Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 52-63, Vol. 4, No. 4,  Published by IAER, DOI: 10.33166/AETiC.2020.04.006, Available:  <http://aetic.theiaer.org/archive/v4/v4n4/p6.html>. | | | | | | | 1st October 2020 | | | | Scopus | | | 1 | | | | |
|  |  | | | | | | |  | | | |  | | |  | | | | |
|  |  | | | | | | |  | | | |  | | |  | | | | |
| **PATENT SEARCH**  *(describe how your research output shall produce an innovative idea or technology that has the potential to be a solution for stakeholders (community, industry, government etc.) and offers a unique proposition)* | | | | | | | | | | | | | | | | | | | |
| *To identify if the researcher is able to coherently present a compelling argument for his/her proposal in light of the IP landscape and factors identified in the (Yes/No) Section. The answer would reflect an understanding of the applicant's research advantage and limitations and the prospect of moving the completed research beyond this stage of funding.*  *A patent search was conducted using the string “( Healthcare OR COVID-19 ) AND ( ( Health ( Level Seven ) ) AND ( Blockchain AND ( ( Smart Contract ) AND ( Light-weight Consensus ) ) ) )” through LENS.ORG. The search produced a result demonstrating 193 published patents. The search result exhibits an upward trend in patent application in this domain. This is a positive indicator for our project. The COVID-19 pandemic most likely has an impact on the slightly lower number of patents in the year 2020.* | | | | | | | | | | | | | | | | | | | |
| **DECLARATION AND APPLICANT’S SIGNATURE** | | | | | | | | | | | | | | | | | | | |
| I hereby declare that:  ( √ ) All information given in this form is true and accurate. XMUM has the right to reject or cancel the application/offer without prior notice if any information is found to be inaccurate.  ( ) This research proposal is also or has been presented to other research fund(s).  Fund’s name:  Total amount:  Application period:  **Name: Signature:**  **Date:** | | | | | | | | | | | | | | | | | | | |
| **RECOMMENDATION BY SCHOOL / DEPARTMENT** | | | | | | | | | | | | | | | | | | | |
| **Comments:** | | | | | | | | | | | | | | | | | | | |
| **Name:**  **Signature:**    **Date:** | | | | | | | | | | | | | | | | | | | |

**Note: All applications submitted will be treated in full confidence and the decision of the evaluation committee is final.**

**XMUMRF APPLICATION**

**APPLICANT’S CHECKLIST**

|  |  |  |
| --- | --- | --- |
| √ |  | Applicant’s brief CV with a list of related publications |
| √ |  | Each co-researcher’s brief CV with a list of related publications |
| √ |  | List of applicant’s three representative refereed journal papers related to this application with full text (pdf) |
| X |  | List of applicant’s previous research grant(s), together with the grant award letter(s). [These were part of postdoctoral research. Therefore, I do not have any formal grant award letters] |
| √ |  | Research flowchart |
| √ |  | Simplified patent search report |