KINGDOM OF CAMBODIA

NATION | RELIGION | KING

Blockchain Technology Readiness for Cambodia

Ministry of Industry, Science, Technology & Innovation

Ministry of Industry, Science, Technology & Innovation
Phnom Penh, Cambodia
Website: https://www.misti.gov.kh

First eBook Edition: 2023
ISBN: 978-9924-600-21-3

Ministry of Industry, Science, Technology & Innovation address is:
45 Preah Norodom Boulevard, Sangkat Phsar Thmey III, Khan Daun Penh, Phnom Penh, 120203, Cambodia

Foreword

Science, technology, and innovation have played a pivotal role in socio-economic development of most developed nations. Therefore, emerging technologies stand at the forefront of strategic development priorities. As the Minister of the Ministry of Industry, Science, Technology & Innovation and Chair of National Council of Science, Technology & Innovation, I am delighted to see scientists exploring the technological advancements, particularly in the realm of blockchain technologies. I am fully convinced that this scholarly effort in highlighting actual situation of blockchain technologies and its way forward in Cambodia's context are dynamically contributing to the technology development ecosystem in the Kingdom of Cambodia.

Once privacy and security are considered, blockchain technologies became integral to our daily business operations. The adoption of this technology is expected to increase in the coming decade. The discussions with contextual analyses, particularly in the current conditions of developing nations like Cambodia, provide meaningful insights for policymakers, researchers, practitioners, and the private sector. It is timely to bring more understanding to the public since this technology is emerging and its integration to social development significantly relies on scholarly perspectives, including readiness for implementation, weighing advantages against disadvantages, analyzing regional and international trends, understanding the knowledge management and its application, among other relevant factors. In Cambodia, the technology is widely adopted in various sectors including finance and services. Its application is going to expand, and there is a positive shift in social trends toward it.

The diverse academic backgrounds of the authors spur the knowledge within the domain to be more engaging for readers. This group of scholars possess a broad understanding, not just from academic perspective but also from practical experiences in the application of technology. Furthermore, the contribution of authors from the private sector brings more sound innovation to the development of blockchain technologies. Lastly, the insights by policymakers are a shared component in this book entitled "Blockchain Technology Readiness for Cambodia". These collective efforts provide a steppingstone for the blockchain development ecosystem in Cambodia since all aspect of this technological prospects are brought in for the discussion.

Finally, I urge all relevant stakeholders to put your best understanding to streamline your respective endeavor with new trends and future uses of blockchain technologies. I am strongly confident that the thoughtful substances in the book will surely bring innovation cycle for your respective institution. I would like to express my deep appreciation to the authors of the book for having your important ideas in written format. Your valuable contribution is appreciated for future generations.

Phnom Penh, 18 December 2023

Minister

HEM Vanndy

Acknowledgements

This informative document was produced by the General Department of Science, Technology & Innovation (GDSTI) of the Ministry of Industry, Science, Technology & Innovation (MISTI) of Cambodia.

First and foremost, the deepest thanks go to the contributors of each chapter, who have dedicated fruitful efforts in researching and capturing insightful information for this document. Without their commitment, this document would not have been made.

A special thanks to Dr. **Siev Sokly** and Mr. **Thul Rithy** who accepted to be the first consumers of this document, and their feedback has been priceless.

ខ្លឹមសារសង្ខេប

បច្ចេកវិទ្យាប្តូរឆេនបានលេចឡើងជានវានុវត្តន៍បរិវត្តកម្មមួយដែលមានសក្តានុពលខ្លាំងក្នុងបដិវត្តកម្មនៃវិស័យទាំងឡាយ ជាអាទិ៍៖ ហិរញ្ញវត្ថុ, ខ្សែច្រវាក់ផ្គត់ផ្គង់, កម្មន្តសាល, សុខាភិបាល, និងអភិបាលកិច្ច។ ចំណុចស្នូលរបស់ប្តូរឆេនគឺលក្ខណៈវិមជ្ឈការ សន្តិសុខ និងសក្តានុពលសម្រាប់ទំនាក់ទំនងឆ្លាតវៃ។ ប្រទេសមួយចំនួនដូចជា ចក្រភពអង់គ្លេស, អេមីរ៉ាតអារ៉ាប់រួម, សាធារណរដ្ឋប្រជាមានិតចិន, ហូឡង់, សិង្ហបុរី, អូស្ត្រាលី, និងម៉ាឡេស៊ី បានលើកទឹកចិត្តខ្លាំងដល់ឧស្សាហកម្មក្នុងការប្រើប្រាស់បច្ចេកវិទ្យាប្តូរឆេន ដែលការណ៍នេះអាចជាមូលដ្ឋានក្នុងការអនុវត្តសម្រាប់ប្រទេសកម្ពុជា។

ឯកសារនេះបង្ហាញពីការវាយតម្លៃគ្រប់ជ្រុងជ្រោយក្នុងការត្រៀមខ្លួនរបស់កម្ពុជា សម្រាប់ការចាប់យកបច្ចេកវិទ្យាប្តូរឆេន។ ឯកសារនេះ បកស្រាយស៊ីជម្រៅពីទិដ្ឋភាពបច្ចេកទេសរបស់ប្តូរឆេន, រុករកថែមទៀតពីករណីប្រើប្រាស់ផ្សេងៗ, កំណត់យុទ្ធសាស្ត្រសម្រាប់ការអនុវត្តឱ្យបានជោគជ័យ, វិលេចពីបញ្ហាប្រឈមផ្សេងៗដែលពាក់ព័ន្ធនឹងការចាប់យកបច្ចេកវិទ្យាប្តូរឆេន និងផ្តល់អនុសាសន៍ដល់អ្នកធ្វើគោលនយោបាយ ក៏ដូចជាអ្នកពាក់ព័ន្ធទាំងឡាយ។

រាជរដ្ឋាភិបាលកម្ពុជាបានកំណត់នូវបេសកកម្មប្រកបដោយមហិច្ឆតាចំនួនពីរ រួមាន៖ ១) ការឈានទៅជាប្រទេសដែលមានចំណូលមធ្យមកម្រិតខ្ពស់នៅឆ្នាំ២០៣០ និង២) ការឈានទៅជាប្រទេសដែលមានចំណូលខ្ពស់នៅឆ្នាំ២០៥០។ ចាំបាច់ណាស់ កម្ពុជាបានធ្វើពិពិតកម្មការអភិវឌ្ឍសេដ្ឋកិច្ចរបស់ខ្លួនដើម្បីបន្សុំទៅនឹងចក្ខុវិស័យនេះ ដោយផ្តោតជាពិសេសលើវិទ្យាសាស្ត្រ បច្ចេកវិទ្យា និងនវានុវត្តន៍ (**វ.ប.ន.**) ក្នុងការឆ្លើយតបនឹងបញ្ហាប្រឈមថ្មីៗនេះ ជាអាទិ៍៖ ផលជះនៃជំងឺរាតត្បាតកូវីដ-១៩ និងជម្លោះអន្តរជាតិផ្សេងៗដែលកំពុងកើតមាន។ ដើម្បីជ្រោមជ្រែងដល់ចក្ខុវិស័យនេះ ឧបករណ៍គោលនយោបាយមួយចំនួនបានរៀបចំឡើង មានដូចជា៖ ផែនទីបង្ហាញផ្លូវ **វ.ប.ន.** កម្ពុជា២០៣០, របៀបវារៈស្រាវជ្រាវជាតិ ឆ្នាំ២០២៥, ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថល កម្ពុជា ២០២១-២០៣៥, និងគោលនយោបាយពាក់ព័ន្ធផ្សេងទៀត។ ដូច្នេះ ការចាប់យកបច្ចេកវិទ្យាប្តូរឆេន អាចមានបរិស្ថានសមប្រកបមួយក្នុងបរិបទកម្ពុជា។

បច្ចេកវិទ្យាប្តូរឆេនត្រូវបានគេមើលឃើញថាផ្តល់នូវដំណោះស្រាយសម្រាប់ការងារជាក់ស្តែងជាច្រើនតាមរយៈការទាញយកប្រយោជន៍ជាអតិបរិមាពីបណ្តាញវិមជ្ឈការ និងអាល់ហ្គោរីតកំបាំង កូដ។ នវានុវត្តន៍នេះធានាថាសមាជិកទាំងអស់ក្នុងបណ្តាញអាចទាញយកបាននូវព័ត៌មានដូចគ្នា ដោយមិនចាំបាច់មានអន្តរការី និងដោះស្រាយនូវហានិភ័យពីការក្លែងបន្លំនិងការរំខាន។ លក្ខណៈពិសេសនេះជាមូលដ្ឋាននៃក្តីសង្ឃឹមដ៏អស្ចារ្យមួយសម្រាប់វិស័យជាច្រើនដូចជា៖ ហិរញ្ញវត្ថុ, ការគ្រប់គ្រង់ខ្សែច្រវាក់ផ្គត់ផ្គង់, សុខាភិបាល, សេវាកម្មសាធារណៈ, និងវិស័យជាច្រើនផ្សេងទៀត។ ក្នុងវិស័យហិរញ្ញវត្ថុ គម្រោងអនុវត្តន៍ដ៏លេចធ្លោចំនួនពីរបាននិងកំពុងបោះដំហានទៅមុខ។ គម្រោងទី១ «**បាគង**» ដែលផ្តួចផ្តើមដោយធនាគារជាតិនៃកម្ពុជា មានគោលដៅជំរុញកម្ពុជាជា

សង្គមដែលមិនប្រើក្រដាស់ប្រាក់ និងពង្រីកបរិយាបន្នហិរញ្ញវត្ថុ តាមរយៈការធ្វើសមាហរណកម្មអ្នកផ្តល់សេវាកម្មហិរញ្ញវត្ថុទាំងឡាយទៅក្នុងប្រព័ន្ធរួមមួយដោយមានផ្ទៃកម្មវិធីចំហ (API)។ គម្រោងទី២ «**ប្តូរផេ**» ជាវិធីដោយប្រើប្តូរឆេនជាមូលដ្ឋានសម្រាប់ការផ្ទេរប្រាក់ឆ្លងដែន។ ក្នុងការគ្រប់គ្រងខ្សែច្រវាក់ផ្គត់ផ្គង់ ការប្រើប្រាស់ចំនួនពីរត្រូវបានលើកឡើង។ ករណីទី១ «**ឧស្សាហកម្មគ្រឿងបន្លាស់ស្វ័យប្រវត្តិ**» យកម៉ូដែលនៃការគ្រប់គ្រងខ្សែច្រវាក់ផ្គត់ផ្គង់ដែលមានមូលដ្ឋានប្តូរឆេន ដើម្បីបើកការកំណត់អត្តសញ្ញាណ និងស្វែងរកគ្រឿងបន្លាស់ស្វ័យប្រវត្តិ, ធ្វើឱ្យប្រសើរដំណើរការខ្សែច្រវាក់ផ្គត់ផ្គង់ និងបង្កឱ្យមាននវានុវត្តន៍សម្រាប់ម៉ូដែលធុរកិច្ច។ ករណីទី២ «**ឧស្សាហកម្មវាយនកណ្ឌ**» ប្រើប្រាស់បច្ចេកវិទ្យានេះនៅទីក្រុងដាក្កា នៃប្រទេសបង់ក្លាដែស។ សម្រាប់វិស័យសុខាភិបាល ករណីគួរឱ្យកត់សម្គាល់ចម្បងមួយគឺការប្រើប្រាស់បច្ចេកវិទ្យាប្តូរឆេនក្នុងប្រព័ន្ធគ្រប់គ្រងវ៉ាក់សាំងនៅប្រទេសម៉ាឡេស៊ី។ ការអនុវត្តនេះធ្វើឱ្យប្រសើរឡើងនូវកិច្ចខិតខំប្រឹងប្រែងរបស់រដ្ឋាភិបាលក្នុងការប្រយុទ្ធប្រឆាំងនឹងជំងឺកូវីដ-១៩ ដោយជួយសម្រួលដល់ការចែកចាយគ្រឿងឧបករណ៍សុខាភិបាល និងអំណោយសប្បុរសធម៌ផ្សេងៗ, ពង្រឹងការតាមដាន និងសន្តិសុខទាំងវ៉ាក់សាំងនិងអ្នកទទួលវ៉ាក់សាំង, និងស្តុក និងរៀបចំឱ្យមានព័ត៌មានពីវ៉ាក់សាំងពេលឆ្លងដែន។ ករណីចុងក្រោយគឺទស្សនាទានស្តីពី «ការរៀបចំរដ្ឋាភិបាលឌីជីថលដោយប្រើប្តូរឆេន» ដែលប្រើក្នុងវិស័យសេវាកម្មសាធារណៈ។ បច្ចេកវិទ្យាប្តូរឆេន ត្រូវបានប្រើដើម្បីធានាសន្តិសុខការស្តុកទិន្នន័យរបស់ធុរកិច្ច ប្រជាជន និងរដ្ឋាភិបាល, សម្រួលដំណើរការជាលក្ខណៈអតិពលកម្ម, កាត់បន្ថយឱកាសដែលអាចមានអំពើពុករលួយ និងការរំលោភបំពានផ្សេងៗ, និងពង្រីកទំនុកចិត្តក្នុងកិច្ចការរដ្ឋាភិបាល និងប្រព័ន្ធរបស់រដ្ឋ។

ការធ្វើសមាហរណកម្មដោយជោគជ័យនៃបច្ចេកវិទ្យាប្តូរឆេនអាស្រ័យជាចម្បងលើប្រសិទ្ធភាពនៃយុទ្ធសាស្ត្រអនុវត្តន៍។ ដោយមើលឃើញពីធម្មជាតិថ្មីថ្មោងនៃបច្ចេកវិទ្យាប្តូរឆេន តម្រូវការចាំបាច់នោះគឺការបណ្តុះកម្លាំងការងារមួយដែលស្ទាត់ជំនាញ តាមរយៈកម្មវិធីបណ្តុះបណ្តាល និងអប់រំគ្រប់ជ្រុងជ្រោយ។ ទន្ទឹមគ្នានេះដែរ កិច្ចខិតខំប្រឹងប្រែងគប្បីផ្តោតចម្បងលើការយល់ដឹងរបស់សាធារណជន, ជំរុញការចូលរួមឱ្យបានសកម្ម, និងបង្កើតប្រព័ន្ធអេកូឡូស៊ីដែលភ្ញាស់ឱ្យមាននវានុវត្តជន និងធុរកិច្ចថ្មីក្នុងស្រុក។ ការបាត់បង់នូវការស្គាល់នៃប្តូរឆេន និងសក្តានុពលរបស់បច្ចេកវិទ្យានេះ អាចជាឧបសគ្គដល់ឧស្សាហកម្ម និងអ្នកធ្វើគោលនយោបាយ ក្នុងការទាញយកឱ្យអស់លទ្ធភាពពីសក្តានុពលនៃបច្ចេកវិទ្យានេះ។ ជាងនេះទៅទៀត ការបង្កើតឱ្យមានក្របខណ្ឌគតិយុត្តដឹងមាំមួយជាកិច្ចការចាំបាច់ ដែលម្យ៉ាងគឺបណ្តុះនវានុវត្តន៍សម្រាប់បច្ចេកវិទ្យាប្តូរឆេន និងម្យ៉ាងទៀតគឺការពារផលប្រយោជន៍របស់អ្នកប្រើប្រាស់ និងវិនិយោគិន។ បើប្រព័ន្ធអេកូឡូស៊ីនេះមានតុល្យភាពល្អហើយ មូលដ្ឋានគ្រឹះនៃការបញ្ចូលបច្ចេកវិទ្យាប្តូរឆេននឹងកើតមានឡើងដោយជោគជ័យក្នុងវិស័យផ្សេងៗ និងឧស្សាហកម្ម។

ការចាប់យកបច្ចេកវិទ្យាប្តូរឆេនដែលមានបញ្ហាប្រឈមជាច្រើនក្នុងក្របខណ្ឌអនុវត្តន៍ ផ្តល់នូវអត្ថប្រយោជន៍ដ៏ច្រើន។ បញ្ហាប្រឈមទាំងឡាយអាចត្រូវបានដោះស្រាយ លុះត្រាតែមានមូលដ្ឋាននៃប្រព័ន្ធអ៊ីនធឺណិតល្បឿនលឿន, ការផ្គត់ផ្គង់ថាមពលថេរមួយ, និងការចំណាយថ្លៃដើមច្រើនសម្រាប់អនុវត្ត។ ជាងនេះទៅទៀត កង្វះអ្នកជំនាញយល់ច្បាស់ពីបច្ចេកវិទ្យាប្តូរឆេននៅតែជាឧបសគ្គក្នុងការចាប់យកឱ្យបានទូលំទូលាយ

សម្រាប់ប្រទេសជាតិ។ ម្យ៉ាងទៀត ក្តីបារម្មណ៍អាចកើតមានលើកម្រិតនៃបណ្តាញប្តូកឆេន, គម្លាតយេនឌ័រនៅតែមានក្នុងការចាប់យកបច្ចេកវិទ្យា, បញ្ហាកើតមានពីបរិយាបន្នហិរញ្ញវត្ថុ និងភាពទុកចិត្តបាននៃកិច្ចសន្យាឆ្លាតវៃ។ លើសពីនេះទៅទៀត សន្តិសុខ និងក្តីបារម្មណ៍លើឯកជនភាព នៅតែជាបញ្ហាប្រឈមមួយ ដែលទាមទារឱ្យមានដំណោះស្រាយគ្រប់ជ្រុងជ្រោយក្នុងគោលដៅចាប់យកឱ្យអស់លទ្ធភាពនូវសក្តានុពលនៃបច្ចេកវិទ្យា ក៏ដូចជាកាត់បន្ថយហានិភ័យផ្សេងៗ។

ទស្សនាទាន និងការវិភាគដែលបានរៀបចំឡើងដោយអ្នកជំនាញចង្អុរបង្ហាញឱ្យឃើញថា ប្រទេសកម្ពុជាត្រូវតែរៀបចំប្រព័ន្ធអេកូឡូស៊ីគាំទ្រមួយ ដែលរួមមានការរៀបចំឱ្យមានយុទ្ធសាស្ត្រជាតិ, ការធ្វើឱ្យប្រសើរឡើងនូវកិច្ចសហប្រតិបត្តិការ, និងហេដ្ឋារចនាសម្ព័ន្ធដ៏ប្រសើរមួយ។ ជាងនេះទៅទៀត ក្រសួងឧស្សាហកម្ម វិទ្យាសាស្ត្រ បច្ចេកវិទ្យា និងនវានុវត្តន៍ ត្រូវរៀបចំឱ្យមានក្របខណ្ឌគតិយុត្តដើម្បីធានាឱ្យមានផលជះជាវិជ្ជមាននិងបរិយាបន្ននៃបច្ចេកវិទ្យាប្តូកឆេនក្នុងកម្រិតមួយដែលអាចគ្រប់គ្រងបាន។ ជាងនេះទៅទៀត ក្រុមប្រឹក្សាជាតិវិទ្យាសាស្ត្រ បច្ចេកវិទ្យា និងនវានុវត្តន៍ ជាស្ថាប័នសមស្របមួយដើម្បីឆ្លើយតបនឹងបញ្ហាប្រទាក់ក្រឡារបស់បច្ចេកវិទ្យាប្តូកឆេន។ ជាចុងបញ្ចប់ រាជរដ្ឋាភិបាលកម្ពុជាត្រូវមានគម្រោងរៀបចំកម្លាំង និងក្រុមការងារជាបន្ទាន់មួយដើម្បីឆ្លើយតបនឹងតម្រូវការខ្លាំងរបស់អ្នកជំនាញបច្ចេកវិទ្យាប្តូកឆេន។ ការណ៍នេះទាមទារ ការរៀបចំក្រុមការងារថ្នាក់ជាតិដែលដឹកនាំសម្របសម្រួលដោយក្រុមប្រឹក្សាជាតិវិទ្យាសាស្ត្រ បច្ចេកវិទ្យា និងនវានុវត្តន៍ ដើម្បីត្រួតពិនិត្យវឌ្ឍនភាពនៃបច្ចេកវិទ្យាប្តូកឆេន។ ក្នុងពេលជាមួយគ្នានេះដែរ រាជរដ្ឋាភិបាលគួរផ្តោតយុទ្ធសាស្ត្រលើការរៀបចំឱ្យមានការអភិវឌ្ឍមូលធនមនុស្ស ដែលជាមូលដ្ឋានសម្រាប់ស្ថាប័នឧត្តមសិក្សាក្នុងវិស័យ **វ.ប.ន.** ដើម្បីត្រៀមខ្លួនគ្រប់គ្រាន់សម្រាប់ការស្រាវជ្រាវ និងអភិវឌ្ឍន៍ប្រកបដោយសមត្ថភាព។

Executive Summary

Blockchain technology has emerged as a transformative innovation with the potential to revolutionize various sectors, including finance, supply chain, manufacturing, healthcare, and governance. Blockchain, at its core, is a decentralized, secure transaction ledger technology that ensures data integrity and immutability through cryptographic mechanisms. It offers transparency, decentralization, security, and the potential for smart contracts. Several nations such as the UK, the UAE, China, the Netherlands, Singapore, Australia, and Malaysia have followed a broad approach to encouraging industry to trial blockchain – an approach which could be applicable in Cambodia.

This document presents a comprehensive readiness assessment of Cambodia for the adoption of blockchain technology. It delves into the technical aspects of blockchain, explores its divers use cases, outlines strategies for successful implementation, highlights challenges associated with blockchain adoption and provides recommendations for policymakers and stakeholders.

The Royal Government of Cambodia has set two ambitious missions: becoming 1) an upper-middle-income country by 2030, and 2) a high-income country by 2050. Aligning with this vision, Cambodia is diversifying her economic development, particularly focusing on science, technology, and innovation (STI), in response to recent challenges, notably the impact of the COVID-19 pandemic and the recent international conflicts. Numerous policy instruments have been established including Cambodia's STI Roadmap 2030, National Research Agenda 2025, Cambodia Digital Economy, Society Policy Framework 2020-2035, and other related policies. Hence, the context of Cambodia is favorable for blockchain technology adoption.

Blockchain technology offers an appealing solution for a wide range of applications by leveraging a decentralized network and cryptographic algorithms. This innovation ensures that all participants within the network can access identical information, consequently negating the necessity for intermediaries and mitigating the risk of fraud or tampering. This inherent characteristic holds immense promise in various sectors, such as finance, supply chain management, healthcare, public services and more. In financial sector, two notable cases come to fore: firstly, the "Bakong project" initiative by the National Bank of Cambodia, which advocates for a cashless society and bolsters financial inclusion by integrating multiple financial service providers into a unified system through an open API. Secondly, "Blockpay", a blockchain-based remittance model streamlining cross-border money transfers. For supply chain management (SCM), two use cases are highlighted: the first, a case study in the auto parts industry, wherein a blockchain-based SCM model is proposed to enable the identification and tracking of automotive spare parts, optimize supply chain process and instigate business model innovations. The second instance unfolds in textile industry in Dhaka of Bangladesh. For healthcare sector, a noteworthy case study details the deployment of blockchain technology in the Vaccine Management System in Malaysia. This application enhances the government effort in combating COVID-19 by facilitating the distribution of medical supplies and charitable donations, bolstering traceability and security for both the vaccines and their recipients, and storing and generating vaccination information for cross-border travel. Lastly, an illustrative case study delves into the concept of "Building a Digital Government Powered by Blockchain" within the public service sector. The blockchain technology is harnessed to secure storage of government, citizen, and business data, streamline labor-intensive processes, reduce the likelihood of corruption and abuse, and amplify trust in government and online civic systems.

Successful integration of blockchain technology relies on the effectiveness of implementation strategies. Given the relatively nascent nature of blockchain, there is a need to cultivate a proficient workforce through comprehensive educational and training programs. Simultaneously, efforts should be dedicated toward raising public awareness, fostering active engagement, and creating an ecosystem conducive for local startups and innovators. The dearth of familiarity with blockchain and its potential can constraint the involvement of both industry and policymaker in harnessing the technology's full potential. Furthermore, the establishment of a robust regulatory framework is paramount; one that not only nurtures blockchain innovation but also safeguards the interests of consumers and investors. In this delicate balance, the foundation for blockchain's successful assimilation into various sectors and industries is laid.

The adoption of blockchain technology, while offering a spectrum of advantages, does not come without its share of challenges. These challenges encompass prerequisites such as high-speed Internet connectivity, a consistent power supply, and substantial implementation costs. Moreover, the shortage of experts well-versed in blockchain technology in Cambodia poses a hurdle to its widespread adoption. Additionally, concerns arise regarding the scalability of blockchain networks, the persisting gender disparities in technology adoption, issues of financial inclusion, and the reliability of smart contracts. Furthermore, security and privacy concerns remain at the forefront, demanding comprehensive solutions harness the full potential of blockchain while mitigating associated risks.

Insights gained and analyses conducted by experts indicate that to rapidly advance positive socio-economic development through the integration of blockchain, Cambodia must establish a supportive ecosystem, including the adoption of a national strategy, enhanced collaboration, and improved infrastructure. Moreover, the Ministry of Industry, Science, Technology & Innovation needs to enact a comprehensive legal framework to ensure positive and inclusive impacts of blockchain at a manageable scale. Additionally, the National Council of Science, Technology & Innovation is identified as a suitable governmental entity to address cross-cutting issues related to blockchain. Finally, to cope with the growing demand for blockchain technology experts, Cambodia needs to swiftly implement task force and workforce planning. This involves creating a national-level task force, led by the National Council of Science, Technology & Innovation, to monitor blockchain technology development. Simultaneously, the government should strategically focus on human capital development, laying the foundation for higher education institutions in science, technology, and innovation to be well-prepared for research and development competence.

Contents

Editorial Team

CHHEM Kieth Rethy, MD, PhD (edu), PhD (his)	Senior Editor-in-Chief
HUL Seingheng, Ph.D.	Senior Editor
KHUN Kimang, Ph.D.	Editor

Contributors

1. Introduction

TEP Sovan, MSc.

2. Understanding the Context

HUL Seingheng, Ph.D.

3. Foundational components

KHUN Kimang, Ph.D.

4. Use Cases and Potential Applications in Cambodia

Liew Voon Kiong, Ph.D.

5. Implementation Strategies for Cambodia

SENG Molika, MSc.

CHEN Sovann, Ph.D.

6. Challenges for Cambodia

CHHEM Siriwat, MSc.

YONG Monyoudom, MSc.

SOK Kimheng, MSc.

7. Concluding remarks and Recommendation

CHHEM Kieth Rethy, MD, Ph.D. (edu), Ph.D. (his)

Publisher

Ministry of Industry, Science, Technology & Innovation

List of Tables

List of Figures

List of Abbreviations

1. Introduction

It has been more than 20 years since the blockchain technology was proposed from the concept to real applications. In early 1992, Stuart Haber and W. Scott Stornetta developed a system for timestamping digital documents (Sarmah, 2018). This system is designed in a way that makes it difficult to tamper with. In 2008, the first blockchain technology concept was introduced by Satoshi Nakamoto in his paper "Bitcoin: A Peer-to-Peer Electronic Cash Systems," (Nakamoto, 2008). The idea of Peer-to-Peer electronic cash system is to enable direct online payment from one source to another in the network without having to rely on any third-party. Since then, many works on blockchain concept have been done to produce a cryptocurrency network called the Bitcoin (Rathee, 2020). The success of Bitcoin led to the development of many other blockchain-based cryptocurrencies such as Ethereum, Litecoin and Ripple (Vujičić et al., 2018). In recent years, blockchain technology has gained popularity in other industries such as supply chain management, healthcare, and real estate (Mohamed & Al-Jaroodi, 2019; Bodkhe, et al., 2020; Hölbl, Kompara, Kamišalić, & Zlatolas, 2018; Saari, Vimpari, & Junnila, 2022). As the technology continues to evolve, we expect to see more innovative uses of blockchain in the future.

This chapter undertakes an overview of blockchain technology, from the perspective of providing solutions for real-world problems. Section 1.1 provides non-technical description and explanation of blockchain technology applications in different sectors. Section 1.2 focuses on the benefits that blockchain technology offers for Cambodia's development. The organization of this document is given in Section 1.3.

1.1. Overview of blockchain technology

Blockchain, as the name suggests, is an ordered chain of blocks, each is a group of transactions issued by peer, making change of the information in the network. Blockchain follows the concept of decentralized databases, where multiple computers in the network maintain a copy of the same ordered chain. Every user in the network has access to the copy of ordered chain and exchanges information with each other directly based on the identical copied chains. This is different from the cloud technology, in which only the admin has access to the whole database and validates transactions between users (Saghiri, 2020).

The procedure of a block being created and added into the chain can be broken down as following (Toorajipour et al., 2022):

- Initially, when a block is created, it is broadcasted to everyone in this peer-to-peer network.
- After everyone receiving the new block, it is their work to verifies the block to make sure that it has not been tampered with. This step ensures no other invalid modified of information on this network.
- Once the new block is checked and verified, everyone in the network adds this new verified block into their own blockchain.
- The consensus of the network is then created to agree about the validation of the new block.
- All the added blocks cannot be modified. In case that a block is found to be tampered with, it will be rejected from the network and block cannot be added.

For many years, blockchain has been a very popular and widely used topic. It has been adopted in many sectors not only in the financial sector, but also it is proved to be used in other sectors as well such as industrial IoT, agriculture, supply chain management, health, etc.

(Borah et al., 2020) proposes a novel project called FARMAR which leverages blockchain technology to tackle the inefficiency and inconsistency in supply chain management (SCM) in the agricultural sector in India. They find out that the current common problems in the agricultural supply chain are the following:

- Corruption among middlemen is rampant.
- Lack of transparency throughout the chain as goods transit through the chain.
- Lack of accountability by all relevant stakeholders.

So, blockchain technology is proposed due to the benefit of storing the information that can be distributed to farmer, middleman, and all relevance stakeholders with accountability, transparency, and security. With these features in place, it can be used to manage the entire agricultural supply chain while enforcing high standards of security and transparency.

Another application of Blockchain is proposed in logistics transportation in food sector due to its features of traceability and transparency. As the global food market grows (Statista, 2022a), the challenges also rise such as data reliability, trustworthiness of the supply chain, the delivery standard for temperature and humidity during transportation, and the food storage. This information needs to be tracked, traced, and monitored correctly to ensure the quality and safety of product (Nasir et al., 2014). As such, blockchain technology has emerged as an effective form of support for food traceability, safety, and transparency (Centobelli et al., 2022). For instance, the study of (Kamble et al., 2019) suggests that encryption of messages and absence of central admin may enhance trust and security in the food industry while the study of (Acciarini et al., 2023) concludes that the adoption of Blockchain technology has positively influences purchase intention in the food sector. Concretely, from the company's perspective, there is positiveness in adopting blockchain technology as all information produced along supply chains is auditable with details in real-time would increase the trustworthiness and the credibility of the company. On the other hand, the consumer can have full information of the products in this supply chain of agri-food.

In healthcare industry, many applications of blockchain technology have been emerged. The major problem in the healthcare industry is to deal with the sensitive data of the patient. Generally, the medical record of the patient is digitized into electronic medical record (EMR) and is usually distributed in many systems from place to place. These multiple systems can be owned and operated by more than one healthcare service provider. There are many challenges in sharing EMRs among healthcare providers due to numerous problems including security and privacy issues, vulnerability to cyber-attack, which cause the data loss or destruction, and inaccuracy of data entry from paper to computer. Within these issues, blockchain technology can be used to secure the interchange of EMR among many stakeholders (clinics, hospitals, doctors, and patient himself/herself). One of the U.S. startups, Gem (G. Prisco, 2016), has developed a healthcare application called *Gem Health* network using the Ethereum blockchain technology. With the use of this shared network infrastructure, different healthcare specialists can access the same information, which can improve patient care and address operational inefficiency issues. It also helps limit medical negligence and prevent health issues in an early stage, which can lead to extensive savings in medical costs. It also allows medical experts to track the interactions between a patient and all their previous physicians, which provides a transparent view of a patient's entire treatment history and can help to build trust between all the stakeholders involved in their care (Mettler,

2016). The benefits of utilizing blockchain technology in healthcare domain can be the following (Jaroodi, 2019; Bell et al., 2018):

- Enable controlled sharing of EMRs among multiple healthcare stakeholders. The healthcare providers can interchange EMRs in a secure and controlled way. This would ensure that patients receive the best possible care, as their healthcare providers all have the same information.
- Facilitate patients' ownership of their EMRs, while inhibiting their ability to alter them. The patients will have the right to access and control their own EMRs. However, they will not be able to alter or delete any of the information in their EMRs. This is important to protect the integrity of the data and to ensure that patients receive accurate and up-to-date information.
- Allow patients to control and securely share their health data while maintaining their privacy. The patients will be able to share their health data with others, such as family members, care providers, or researchers, while maintaining their privacy. This can be done by using secure and encrypted methods for sharing data.
- Enhance pharmaceutical supply chain management processes. The sharing of EMRs can be used to improve the efficiency and effectiveness of pharmaceutical supply chain management. This can be done by tracking the movement of medications through the supply chain and by identifying potential counterfeit or expired medications.
- Facilitate fine-grain analysis of patients' data, medical innovations, and research results. The sharing of EMRs can be used to conduct fine-grained analyses of patients' data. This can help to identify new medical innovations and research results.

The manufacturing sector is another major industry that has adopted blockchain technology. Blockchain is a cutting-edge information technology that has the potential to revolutionize sustainability in businesses and industries. A great deal of research has been conducted on how blockchain can be used to enable sustainable manufacturing in Industry 4.0, from technical, commercial, organizational, and operational perspectives (Leng et al., 2020). One key area in manufacturing where blockchain can be used is in logistics management as discuss earlier. Logistics management is essential for any manufacturer to ensure fair pricing and timely delivery of raw materials and supplies for production. Additionally, it helps ensure efficient and timely product delivery to customers. Blockchain can be used to improve logistics management in numerous ways (Jaroodi, 2019), including:

- Reducing time delays in the logistics process by providing a single, immutable source of truth for all data related to shipments. This can help eliminate the need for manual reconciliation of data, which can often cause delays.
- Reducing management costs by automating many of the tasks involved in logistics management. For example, blockchain can be used to automatically track the status of shipments and to generate reports on logistics performance.
- Reducing human errors in the logistics process by providing a secure and transparent way to track data. This can help prevent errors such as mislabeled shipments or incorrect delivery addresses.

In another aspect, Blockchain can be used to enable social manufacturing networks (SMNs) among manufacturing enterprises. SMNs are a new way of manufacturing that allows enterprises to share and utilize their resources more effectively, fairly, and securely (Ding et al., 2016). This can help enterprises to build more personalized products and individualized services for customers, and to enhance their competitive capabilities. Overall, adopting blockchain in manufacturing sector can help (Leng et al., 2020):

- manage the logistics and supply chain of the company more effectively thanks to data transparency of the entire chain process including supply of raw materials, delivery to customers, inventory management, business planning and production floor operation.
- reduce the cost of manufacturing by enabling enterprises to share resources therefore having fair pricing and effective expense.
- improve the quality of manufacturing by ensuring that the right resources are used to produce the right products in the production operation.
- speed up the manufacturing process by providing a secure and efficient way to track the sharing of resources and monitoring the entire process.
- Increase more personalized products and individualized services with multi-companies vertical and horizontal collaboration through data transparency and traceability.

1.2. Benefits of blockchain technology for Cambodia's development

According to Cambodia Industrial Development Policy and Plan 2015-2025, the Royal Government of Cambodia (RGC)'s vision is to transform and modernize Cambodia's industrial structure from labor-intensive to skill-driven by 2025 by connecting regional and global value chains to develop regional production networks and interconnected production clusters, which enhances domestic industry competition power and productivity, and moving towards the development of technology-driven, knowledge-based modern industries. There are five priority sectors including:

- A new industry or manufacturing enterprise with high value-added product, creativity, and strong competitiveness, focusing not only on consumer goods, but also on production equipment such as machinery assembly, mechanical/electronic/electrical equipment assembly, transportation assembly, and natural resource processing.
- Small and medium-sized enterprises in various industries, especially those involved in drugs and medical equipment, construction, packaging, furniture manufacturing, and industrial equipment.
- Agro-industrial production for export and domestic markets
- Supporting industries for agriculture, tourism, textile, regional production chains linked to the provision of raw materials, especially for the garment sector, and production of spare parts and semi-finished products.
- Industries supporting regional production lines of information, communication, and technology (ICT), energy, heavy industries, cultural and traditional handicraft, and green technology.

Technologies will play a very important role in supporting and fostering the strategic development of Cambodia in these priority sectors, and science and technology areas. Blockchain technology provides secure, transparent, and tamper-proof database, which can be used as a decentralized platform for building a strong foundation of administration infrastructure, and management systems supporting cross sectors development such as education, health, agriculture, industrial manufacturing, etc. This enables trust and accountability in government and private businesses in Cambodia.

The first pentagon of "Pentagonal Strategy – Phase I" (PS-I) is about Human Resource Development. It is the foundation for improving general education, vocational and competence skills, entrepreneurship, creativity and innovation, and a healthy lifestyle. In Side 1 "Enhancement of quality of Education, Science and Technology", RGC aims at strengthening comprehensive inspection of school management to ensure full time teaching as required by the curriculum and to improve the school

governance by preparing school monitoring system to ensure effective and timely response from the nation level. In addition, EduTech roadmap has mentioned about building next-generation technology-enhanced learning ecosystem, which focus on improving innovation and entrepreneurship skills. The primary objective is to rapidly integrate technologies into teaching at home and in schools to support students in acquiring skills and knowledge they need to succeed in life and careers in the modern workplace and society. This will result in building student's capacity for STEM majors at university as well as encouraging multidisciplinary and multi-stakeholder collaboration between the government, industries, academia, and community. According to EduTech, management systems such as LMS, SMS, EMIS, and HRMS are introduced with a purpose to digitalize schools enabling the paperless institutions and to facilitate the interaction between students and teachers. This will give a bold benefit to education sector in terms of monitoring and managing of the school systems to produce human capital corresponding to industrial needs. Regarding technology, Blockchain is very suitable for developing management systems and digital learning platforms. Due to its potential features of transparency, decentralization, and security, blockchain can support educational sector in Cambodia as the following:

- Secured and transparent student records: Blockchain can be used to create a secure and transparent record of student academic records preventing fraud and ensuring that students have access to their accurate records.
- Distributed learning platforms: Blockchain can be used to create distributed learning platforms allowing students to learn from anywhere in the world and would also help to reduce the cost of education.
- Digital badges and micro-credentials: Blockchain can be used to issue digital badges and micro-credentials helping students to track their learning progress and employers to assess the skills of job applicants.
- Increased access to education: Blockchain could be used to create a more decentralized education system improving the accessibility to education for people in rural areas.
- Improved learning outcomes: Blockchain could be used to personalize learning and provide students with more feedback.

Moreover, HealthTech Roadmap of MISTI in 2022 points out three inter-related and reinforcing visions: 1) An Integrated One Health Approach, 2) Multidisciplinary Policy and Governance for Health Technology, and 3) Strengthened Research and Knowledge Sharing Capacity. Blockchain plays an important role with the target development of electronic medical record, advanced telemedicine infrastructure, and personal healthcare application. The potential benefits of blockchain in health sector could be:

- Improved Patient Care: Blockchain can improve patient care by providing doctors with more accurate and up-to-date patient information.
- Increased efficiency: Blockchain can help improve the efficiency of the healthcare system by facilitating information sharing and care coordination.
- Healthcare Supply Chain: Blockchain can be used to track healthcare supply chains ensuring that medical supplies are authentic and not tampered with.
- Healthcare Payments: Blockchain can be used to pay for healthcare services, which helps reduce fraud and facilitate patient payment.
- Tracking the spread of disease: Blockchain can track the spread of disease by recording the movement of people and goods. This helps identify outbreaks of disease and prevent its spread.

The other main features of blockchain are traceability and reliability of the information to be shared with related stakeholders. This feature is important in agricultural sector. As mentioned in AgriTech

Roadmap (MISTI, 2022), blockchain is one key technology that reduces inefficiencies and waste, fights food fraud, and improves food safety. To be more specific, the use of blockchain technology will give numerous advantages in agricultural sector including:

- Track the movement of goods: By tracking the movement of goods from farm to market, it helps to ensure that products are delivered on time and in good condition.
- Reduce food waste: Blockchain can be used to track the movement of food, which can help reduce food waste.
- Improved crop yields: Blockchain can be used to collect crop yields and other agricultural data. This data can then be analyzed to identify trends and patterns, which can be used to improve crop yields and agricultural practices.
- Enhancing resilience: The resilience of agricultural sector can be enhanced by tracking weather patterns and other data which give a predictable outcome and help farmers adapt to changing climate conditions.
- Transparency: The record of all transactions in agricultural supply chain will be transparent and this will help build trust between farmers, suppliers, and consumers regarding pricing, safety, and quality of goods.

Finally, to strengthen manufacturing sector, RGC has embraced four strategies (Cambodia Industrial Development Policy and Plan 2015-2025): 1) Attract foreign investment and private domestic investments with a focus on large industries, 2) Develop and modernize small and medium enterprises (SMEs) ensuring the technology transfer and industrial linkages, 3) Strengthen the country competitiveness by disseminating market information and reducing informal fees, and 4) Coordinating supporting policies (development of human resource, technical training, improvement of industrial relations, development of support infrastructure such as transportation/logistics, and information and communication technology (ICT), supply of electricity and clean water, and public, social and financial services). Correspondingly, blockchain can play a crucial role in assisting, modernizing, and accelerating these strategic activities. The details benefit of blockchain contributing to manufacturing sector can be explored as follow:

- Increased collaboration efficiency: Blockchain can help increase efficiency in manufacturing by facilitating information sharing with partners in coordinating the production process.
- Traceability in the supply chain: The flow of goods and services from suppliers to customers will be better planned, organized, and controlled. Additionally, it will result in improving efficiency, reducing cost, and ensuring the product or goods are delivered on time and in good condition.
- Track the manufacturing process: The movement of products throughout the manufacturing process can be tracked from sourcing raw materials to delivering the finished goods. This would give accurate production floor, stock inventory management, and demand forecasting and planning.
- Track the use of resources: Blockchain could be used to track the use of resources such as water and energy. This could help reduce environmental impacts and manufacturing waste and ensure that resources are used efficiently.
- Transparency: Blockchain can be used to create a transparent record of all transactions in the manufacturing supply chain. This would help to build trust between manufacturers, suppliers, and customers.

1.3. Organization of this document

This document is structured into seven chapters, each serving a specific purpose in the overall narrative. This first chapter lays the groundwork by providing an initial overview of blockchain technology and its benefits for Cambodia. Moving forward, Chapter 2 delves deeper into the socio-economic factors and existing technological infrastructures in Cambodia, providing valuable insights to understand Cambodia's context. Chapter 3 explores the fundamental building blocks and components of blockchain technology and identity management systems. Chapter 4 shifts the focus towards practicality, discussing real-world applications and scenarios where blockchain technology can be effectively utilized. Implementation is at the forefront in Chapter 5 where strategies and approaches for successfully implementing the blockchain technology are thoroughly examined. Chapter 6 covers the potential hurdles and obstacles that may arise during the implementation. These obstacles are classified into three categories: 1) technological, 2) socio-economic, and 3) security and privacy challenges. Finally, Chapter 7 brings the document to a close, summarizing the key findings, insights, and takeaways while offering potential recommendations for future actions to adopt blockchain technology successfully.

2. Understanding the Context

2.1. Socio-Economic Factors of Cambodia

Cambodia is experiencing economic stability thanks to her strategic policies, but recent challenges, especially those due to COVID-19 pandemic, have prompted Cambodia to diversify her economic developments with an emphasis on science, technology, and innovation as a strategic driver for long-term growth. Cambodia has been relying on some important sectors including industry, tourism, agriculture, and construction. Lately, the service sector has been negatively affected due to COVID-19 pandemic, the uncertainty in supply chain caused by Russia-Ukraine conflict, and various environmental issues. Even though the service sector, especially tourism, is heavily affected by the pandemic, Cambodia continues to display good signs of economic stability. This is because the supply chain in agricultural and industrial sectors are not severely interrupted. Moreover, the service in the financial sector seems to be growing well due to various government policy interventions, notably Cambodia Digital Economy and Society Policy Framework 2020-2035 (RGC, 2020). After the pandemic, the country regains her composure and catches up with more diverse forms of economic development from the traditional economic pillars. In addition to policy intervention for recovery, the country has valued the significant role of science, technology, and innovation (STI) as a strategic sector for long-term growth. For instance, the Ministry of Industry, Science, Technology & Innovation (MISTI) was established during the pandemic in 2020. This structural transformation could add up more to transform the socio-economic development from conventional paradigm to skill-based economy.

Cambodia's Gross Domestic Product (GDP) sectoral distribution has remained relatively stable over a ten-year period (see Figure 2.1), with the service sector consistently above 30%, a slight growth in industry, and a slight decline in agriculture leading Cambodia to boost local food production. The economic share from industry is seen to be contributed mainly from labor intensive activities viz garment and footwear industries. On the other hand, agricultural activities are responsible in general as primary producers. The processed agricultural products have less business to serve local and oversea markets as seen in the research ecosystem report jointly made by MISTI and UNESCAP (MISTI and ESCAP, 2022). For this reason, one of the national research priority agenda among the eight fields is agricultural food processing, which is "Local food: 70 percent of Cambodia food consumption is produced locally". It is noted in the eight-priority agenda include (MISTI, 2022):

- 'Local food': 70 percent of Cambodia food consumption is produced locally.
- 'Reliable Energy Supply': 90 percent of energy consumption is generated locally.
- 'Quality Education': Education meets international quality standards.
- 'Electronic and mechanical spare parts': Cambodia exports 70 percent of the electronic and mechanical spare parts produced in the country.
- 'Cloud-based services': Cambodia's cloud-based services development is on par with ASEAN.
- 'Electricity and potable water': All Cambodians have access to reliable electricity and safe potable water.
- 'Carbon neutrality': Cambodia becomes a carbon neutral country.
- 'Digitally-enhanced health': All Cambodians have access to digitally-enhanced health services.

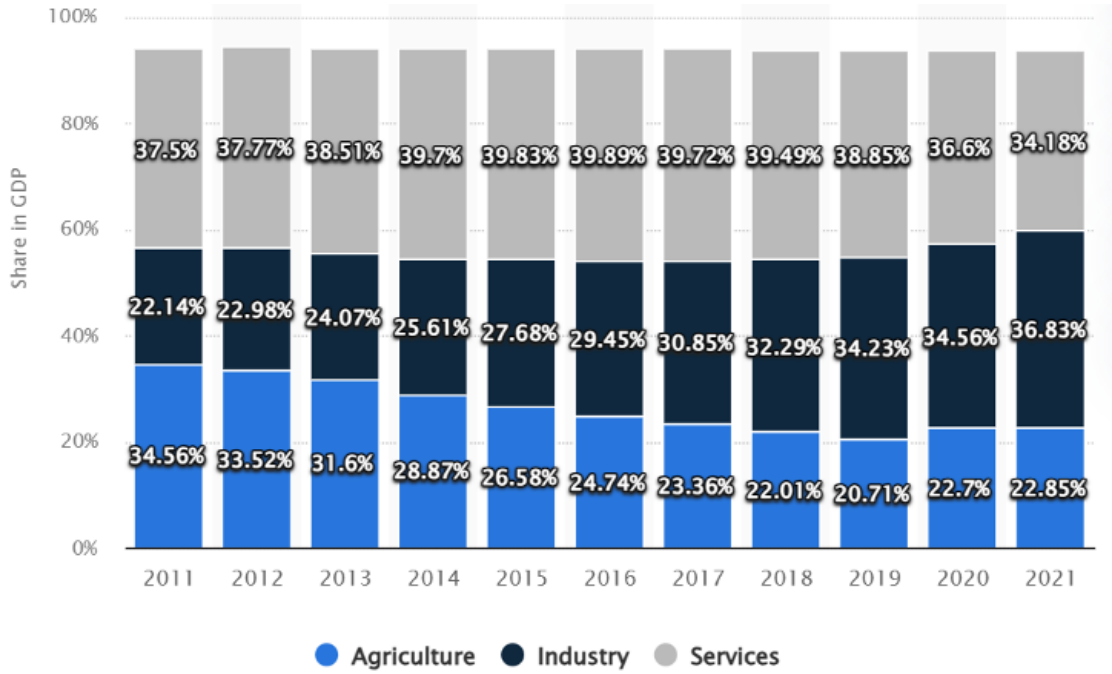


Figure 2.1. Share in Gross Domestic Product (GDP) by major sectors from 2011 to 2021 (Statista, 2023). This chart shows that the GDP sectoral distribution is relatively stable over a ten-year period.

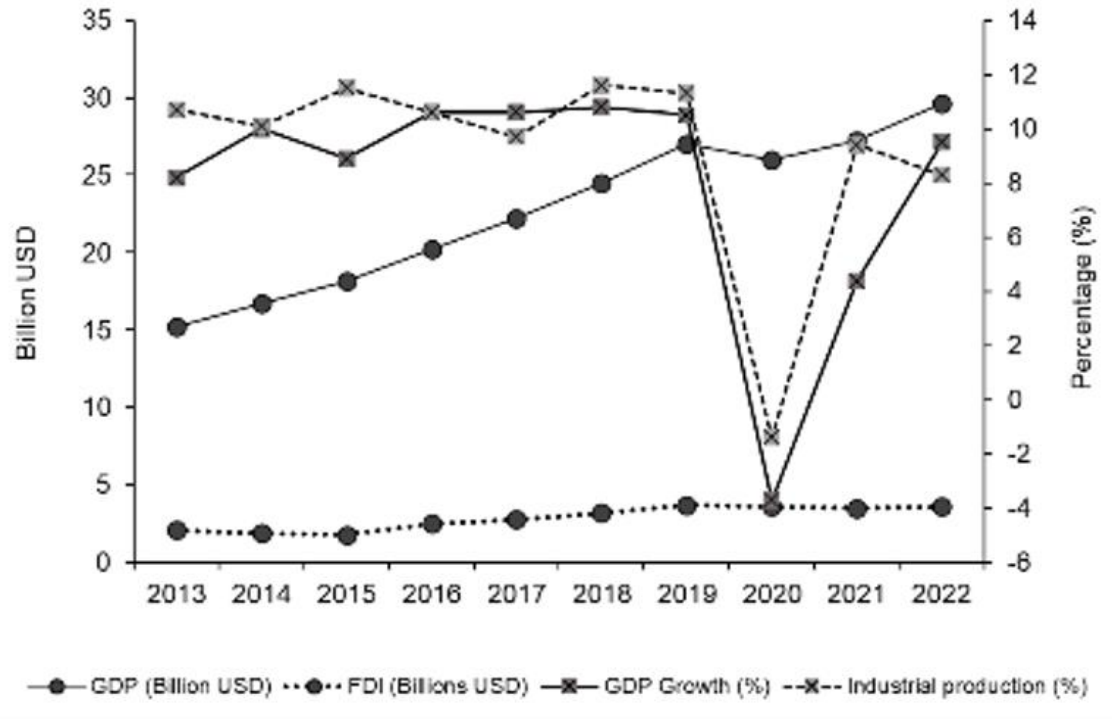


Figure 2.2. Cambodia Economic Growth from 2013 to 2022 (https://www.focus-economics.com/countries/cambodia). GDP and FDI stand for Gross Domestic Product and Foreign Direct Investment respectively. This figure shows that GDP and FDI dropped drastically in 2020 due to COVID-19 pandemic.

The vision of RGC to become an upper-middle-income country by 2030 and high-income country by 2050 is evidence that all policies and further structural transformation are supporting this national

endeavor. The launching of industrial policy 2015-2025 is obvious that the industry is to be shifted from intensive-based labor to skill-based labor (RGC, 2015). Other important policy instruments have been established to compliment the vision, which includes National Policy on STI 2020-3030, Cambodia's STI Roadmap 2030, National Research Agenda 2025, Automotive and Electronic Roadmap, and many other related policies. The above policies are intervened to address challenges and ensure resilience growth. From 2021, Cambodian economy starts growing again after the pandemic. It is known that before COVID-19 pandemic, Cambodian economic growth rose to more than 7% for almost ten years as seen in Figure 2.2. The percentage of people in poverty has reduced significantly from 2009 to 2019. It was estimated that about 2 million people escaped from the poverty line per assessment by the Ministry of Planning (MoP, 2021). The stability of macroeconomics and the openness to foreign trade and investment are the major factors attributing to the growth in the last decade (World Bank, 2022).

RGC has implemented policy initiatives to leverage economic conditions and support growth, focusing on recovery from the pandemic and long-term economic resilience, but unpredictable global challenges pose uncertainties that lead to RGC's steps for structural transformation, including economic diversification and digital transformation for long-term growth. The industrial production was hit hard by the pandemic as seen in Figure 2.2. This decline in 2020 caused a significant decrease of GDP in the same year. The situation has some improvement in 2021 and 2022 for the overall GDP. However, the industrial production went down again for 2022. The GDP remains increasing, which explains that the other sectors such as agriculture or services shared more value in the overall economy. To elevate the economic situation and maintain economic growth, the government has launched many important operational policy initiatives. One of the major policy interventions in action is the Strategic Framework and Programs for Economic Recovery in the Context of Living with COVID-19 in a New Normal 2021-2023 (RGC, 2021). The main objective of the policy is to put Cambodia's economic growth in the near-and-medium terms, back on path to its potential growth and strengthen resiliency for sustainable and inclusive socio-economic development in the long term. It is important to note that this policy intervention addressed mainly the challenges due to the pandemic, while the new uncertain circumstances such as Russia-Ukraine conflict and instability in the financial sector in the United States has not been accounted for in the policy. Additionally, the new trading regulation due to Environmental Social Governance could pose another challenge in the trading ecosystem. For these reasons, the government has placed some significant steps for structural transformation for long term growth, which include economic diversification model and digital transformation.

Cambodia aims to address slow growth in foreign direct investment (FDI) and industrial production's share of GDP by attracting FDI in high-value-added sectors, developing local human capital, and promoting technology-based manufacturing among local small and medium enterprises for inclusivity and resilience. The growth in billion dollars of FDI has been increasing slowly, while the share of industrial production to GDP is also not significantly increasing during this last ten years as seen in Figure 2.2. Thus, the vibrant ecosystem of attracting FDI in the high-value-added sectors is the forefront endeavor for Cambodia. At the same time, the development of human capital for the industrial priority sectors needs to be made to ensure that knowledge/technologies are transferable to the local. After some period, the locals will be capable to domesticate the knowledge/technologies once the FDI is relocated to another sectors. On the other hand, mobilizing local resources for investment in technology-based manufacturing could be timely since FDI is always moving from one sector to another. Thus, promoting or upgrading local small and medium enterprises are indispensable for inclusivity and resilience purposes.

Demographically, Cambodia has a population dominated by the young age of between 10 to 40 years old. The population pyramids show this group of labor force got shrunk a little in 2019 per data from the general population census of Cambodia (GPCC) in 2019. In general, the tendency is getting smaller in the future per overall observation on demographic development mode of many countries around the world. This demographic change correlates strongly to the socio-economic development. As shown in Figure 2.3, the demographic dividend of Cambodia could have about more than ten years.

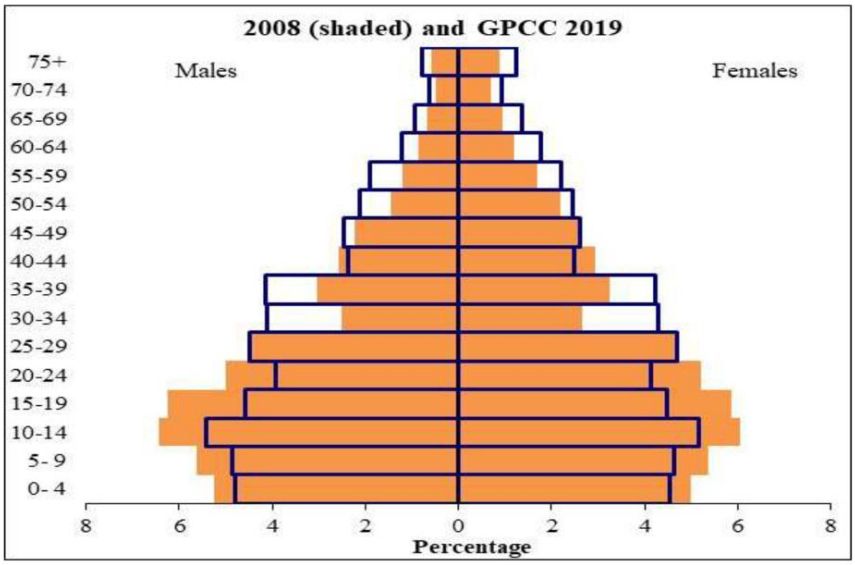


Figure 2.3. Population pyramid of Cambodia in 2008 (shaded) and 2019 (MoP, 2021).

2.2. Existing Technological Infrastructures in Cambodia

Blockchain applications rely strongly on the existing soft and hard infrastructures. Soft infrastructure refers to policy and operational instruments allowing this technology to be deployed officially and legally. Hard infrastructure refers in general to the technical competences and physical systems. Technological advancement of blockchain technology has been growing promisingly in private sectors, especially the financial transaction. In principle, the internet of things is fundamental in node networking of blockchain technology. This basic infrastructure is required for both physical systems and software management. At the same time, cybersecurity in physical and virtual space is undeniably needed to deploy blockchain technology.

Blockchain infrastructure requirements are necessary for both software and hardware. These infrastructures are the general foundation for successful deployment of blockchain in the public and business sectors. The software requirements include 1) Solidity which is common languages built upon C++, Python, and JavaScript, 2) Geth (go-ethereum) – This is the gateway to the implementation of decentralized system – 3) Mist – This is made by developers, which required exceptionally memory capacity of at least 1TB – 4) Solc (Solidity Compiler) is outputs byte code as results from application solidity, which is used in smart contact development, 5) Remix IDE is a tool used for designing, testing, debugging, and deploying the smart contract system. On the other hand, the hardware requirement for blockchain implementation has seen to be diverse, which depends on application types, either public or private organizations. However, some common grounds of hardware infrastructure for blockchain could be 1) Central Processing Unit (CPU): It is known that high performance of processors is always fundamental in deployment of computational tasks. Thus, central processing unit is one of the major tools to be primarily assessed, 2) Blockchain and Graphic Processing Units: this is the supporting unit

to CPUs, mainly in the calculation performance, 3) Nodes and Clients: the computer as nodes for authenticating of transaction, recording, storing, or network governance, while the clients are the required computer programs, and 4) Cluster: this refers to failover protection, load balancers, container services, and monitoring and alerting services. Finally, the other most important factor is secure infrastructures. There are at least four aspects to implement the blockchain smoothly and successfully. They include 1) Infrastructure as a service, 2) Platform as a service, 3) Optimize participation: Hardware, nodes, and solution, and 4) Enterprise-Grade Security and Technical Support (ServerMania, 2023).

3. Foundational components

Blockchain is a relatively new technology that possesses properties of transparency, immutability, traceability, and decentralization necessary for various applications (Wang & Jiang, 2020). Basically, it allows a community of users to record transactions on a shared ledger within the community, such that under normal operation of the blockchain network no transaction can be altered once published. This characteristic can be utilized to create identity management solutions that allow the user to take control over his/her own identity (*i.e.*, self-sovereign identity). This chapter provides a high-level technical overview of blockchain technology and blockchain-based identity management systems.

3.1. Blockchain Infrastructure

Blockchain technology is a decentralized and distributed digital ledger system that securely records and stores transactions across a network of computers, ensuring transparency, immutability, and trust without the need for a central authority. In 2008, the concept of blockchain was integrated with various technologies and computing principles to enable modern cryptocurrencies. These digital currencies are secured by cryptographic methods instead of relying on a central repository or authority.

In this section, we will first briefly describe the background of blockchain technology. Then, we will cover the foundational components of blockchain technology. Finally, we will portray smart contract technology.

3.1.1. Background on Blockchain Technology

The fundamental concepts underpinning blockchain technology first arose in the late 1980s and early 1990s. During this period, seminal work was done and laid the groundwork for what would later become blockchain. In 1989, Leslie Lamport formulated an early consensus protocol called Paxos, which dealt with how to reach agreement between computers in an untrustable network, and submitted the paper *The Part-Time Parliament* (Lamport, 1998) to *ACM Transactions on Computer Systems* in 1990. Additionally, in 1991, cryptographically linking information in a chain to form a tamper-evident log of document signatures was explored (Narayanan et al., 2016). These pioneering innovations established core techniques like decentralized consensus, cryptographic audit trails and fault tolerance that blockchain later built upon. In 2008, the combination of these concepts enabled the first modern electronic cash that is described in Satoshi Nakamoto's whitepaper, *Bitcoin: A Peer Electronic Cash System* (Nakamoto, 2008). Later in 2009 the Bitcoin cryptocurrency blockchain network was established.

The success of Bitcoin fostered broader appreciation of blockchain technology. Before the creation of Bitcoin, various electronic cash systems (*e.g.*, eCash and NetCash) had been developed but failed to gain widespread adoption. Bitcoin was the first successful electronic cash system built using blockchain technology. It is implemented in a distributed fashion such that no single user managed the electronic cash and no single point of failure existed. Its primary advantage was to allow direct transactions between users without the need for a trusted third party. It also has an incentive structure such that the users who manage to publish new blocks and maintain copies of the ledger are incentivized with issuance of new cryptocurrency in a defined manner. Bitcoin's novel approach of combining

cryptography, a distributed public ledger, and an incentive structure fueled its rapid growth and popularized blockchain technology.
Blockchain technology facilitates trust between untrustable parties without relying on trusted intermediaries. Such an outstanding feature is enabled by four fundamental attributes of blockchain system:

1. **Ledger** - The blockchain uses an *append-only* ledger that provides a full record of transactions. Unlike traditional databases, the record cannot be overridden.
2. **Secure** - Cryptographic techniques ensure the ledger's data is tamper-resistant and verifiable. Users can trust that the ledger contents have not been altered.
3. **Shared** - The distributed ledger is shared among the network of users, enabling transparency.
4. **Distributed** - The decentralized architecture distributes trust across the network. This diversity makes the blockchain resilient against localized attacks.

3.1.2. Blockchain Classification

Blockchain networks fall into two broad categories based on their permission model - permissionless or permissioned. The permission model refers to who is allowed to participate in core blockchain maintenance activities like publishing new blocks. In permissionless blockchains, anyone can take part with no authorization needed. These open participation networks allow any user to read data, submit transactions, and publish blocks. By contrast, permissioned blockchains restrict these privileges to approved entities. Only authorized entities can participate in consensus activities like block validation and creation. So permissionless ledgers are fully decentralized and open, while permissioned ledgers have some centralized control over access permissions. This distinction is a key differentiator between blockchain types with major architectural implications. It also affects factors like trust assumptions, security requirements and performance tradeoffs.

Permissionless

Permissionless blockchains allow free, open participation without any central oversight. Anyone can join the network anonymously and immediately begin reading data, submitting transactions, and publishing new blocks. There are no gatekeepers restricting access or vetting participants. All users operate with equal permissions in a fully decentralized manner. The lack of accounts and identity in permissionless systems enhances privacy and censorship resistance. However, it necessitates technical anti-abuse mechanisms or "consensus" systems like Proof-of-Work and Proof-of-Stake (see Section 3.1.4) to avoid the greater threats from unidentified participants. The consensus systems in permissionless cryptocurrency networks usually incentivize non-malicious behavior with the native cryptocurrency.

Permissioned

Permissioned blockchains place restrictions on who can participate in critical consensus activities like publishing new blocks. Participants in permissioned blockchains cannot unilaterally modify ledger state. The improved oversight curbs misbehavior and mitigates threats like Sybil[1] attacks that are concerned in open networks. However, gatekeeping introduces some level of centralized trust and control. Permissioned systems trade off decentralization for efficiency gains in performance and resource usage by operating within a bounded, vetted set of semi-trusted participants.

[1] A Sybil attack is a type of attack on a computer network service in which an attacker subverts the service's reputation system by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence.

Permissioned blockchains can retain core technical advantages of permissionless networks like asset traceability and resilient data storage through distribution. Albeit permissioned, approved participants still replicate an authoritative ledger that transparently tracks ownership histories and state changes. Transactions remain visible to authorized parties, if not fully public. And decentralized storage spreads trust while eliminating centralized data silos. Permissioning acts as an access control layer surrounding a distributed ledger backend that may mirror permissionless designs. So, attributes like provenance tracking, redundancy, and auditability still derive from the blockchain architecture itself in permissioned systems.

Some institutions may opt for permissioned blockchains to exert stronger supervision over their ledger use cases. By restricting participation, permissioned systems offer more safeguards for sensitive applications. Organizations can more selectively dictate who operates nodes, accesses data, and publishes blocks based on their security and control preferences. Permissioning provides insulation from external threats when internal trust is sufficient. Healthcare, finance, and other highly regulated industries tend to favor permissioned control to better govern membership, visibility, and modifications. The oversight curbs risks associated with public openness while still utilizing a blockchain backend. When full decentralization is unnecessary, permissioning strikes a pragmatic balance between trust distribution and organizational oversight over blockchain networks.

3.1.3. Components of Blockchain Technology

At a high-level, blockchain leverages established computing mechanisms like cryptography tools (e.g., cryptographic hash functions, digital signatures, asymmetric-key cryptography) along with record-keeping concepts like append-only ledgers. This section discusses the main components of blockchain in detail, including cryptographic hash functions, transactions, asymmetric-key cryptography, addresses, ledgers, blocks, the chaining process that connects blocks together, and smart contract.

Cryptographic Hash Functions

One key component that enables secured ledger's data is the use of cryptographic hash functions for many transactions. **Hashing** refers to the process of converting any data (e.g., a file, text, or image), regardless of its size, into a fixed-length value, called a **message digest** or simply **digest**. The digest is unique to the input data, meaning that hashing an input several times gives the same digest. In general, even the slightest modification to the input produces an entirely different output digest. Simple examples shown in Table 3.1 are inspired by (Yaga et al., 2019).

Cryptographic hash functions have these important security features:

1. They are **preimage resistant**: Given some digest value, it is computationally infeasible to infer the correct input value. That is, given a digest 'z', it is computationally infeasible to find 'x' such that '$hash(x) = z$'. This means that they are one-way functions.
2. They are **second preimage resistant**. This means that given a specific input it is computationally infeasible to find a second input which produces the same digest. That is, given 'x', it is computationally infeasible to find 'y' such that '$hash(x) = hash(y)$'. This property is also referred to as *weak collision resistance*.
3. They are **collision resistant**. It is computationally infeasible to find two different inputs that produce the same output. That is, it is computationally infeasible to find a pair '(x, y)' such that '$hash(x) = hash(y)$'. This property is sometimes referred to as *strong collision resistance*.

One cryptographic hash function that is widely used in blockchain systems is SHA-256 (NIST, 2015). SHA-256 stands for Secure Hash Algorithm 256, where 256 denotes the length of the output in bits. Its speed, simplicity, and hardware implementation support have led to its adoption by many major blockchains including Bitcoin and Ethereum, which are two of the most popular cryptocurrencies.

SHA-256 algorithm satisfies the three important features above. It generates a 32-byte hash value (1 byte = 8 bits, 32 bytes = 256 bits) that is typically rendered as a 64-character hexadecimal string (see Table 3.1 below). So, there are $2^{256} \approx 10^{77}$, or
115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936
possible digest values. Consequently, even though the collisions (i.e., two different input values produce the same digest, $\exists x \neq y$ such that $hash(x) = hash(y)$) are theoretically possible, the probability of these events is extremely low. SHA-256 is considered as collision resistant because to find a collision in SHA-256, one would need to run the algorithm, on average, about 2^{128} times. To put it into perspective, it would take roughly 2.004×10^{10} years for the entire Bitcoin network with the maximal hash rate of 538.05 ExaHash/second (*Bitcoin Hashrate Chart - BTC Hashrate 409.55 EH/s*, n.d.) to generate a collision (note that the universe is estimated to be 1.37×10^{10} years old). So, SHA-256 is a promising cryptographic hash function.

Table 3.1. Examples of input text and corresponding SHA-256 Digest Values (Yaga et al., 2019)

Input Text	SHA-256 Digest Value
1	`0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b`
2	`0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35`
Hello, World!	`0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f`

Cryptographic hash functions play a crucial role in a blockchain network. Their utilities are multiple:

- Deriving address – discussed in Section 3.1.3.
- Create unique identifiers.
- Safeguarding the block data – a publishing node will hash the block data, generating a digest that will be stored within the block header.
- Safeguarding the block header – in Proof-of-Work based blockchains (see Section 3.1.4) a publishing node will hash the block header with different nonce values (see Section 3.1.3) until the puzzle requirements have been accomplished.

While SHA-256 is a popular choice, there are many different cryptographic hash algorithms employed in various blockchain platforms. For example, Ethereum uses a function called Keccak-256 function, which was chosen by the National Institute of Standards and Technology (NIST) as the winner of a cryptographic competition to establish the SHA-3 hashing standard (Dworkin, 2015). Another cryptographic hash function known as RIPEMD-160 (Dworkin, 2015) is also common in blockchain applications.

Cryptographic Nonce

A cryptographic nonce is a random number that is intended to be used once. In the Proof-of-Work consensus model (see Section 3.1.4), a cryptographic nonce is combined with data to produce different hash digests per nonce:

$$hash(data + nonce) = digest.$$

The nonce gives fine-grained control over the resulting hash to enable finding solutions that meet the requirements of the consensus puzzle. We will see how cryptographic nonce is used in Section 3.1.4.

Transactions

In the context of blockchain, a **transaction** refers to an exchange or interaction occurring between two or more parties on the network. Transactions encapsulate some action taking place, such as transferring funds or assets between users, executing a contract, or recording an event. Each transaction formally registers the specifics like participants, amounts transferred, and time. Figure 3.1 shows a simple example of a cryptocurrency transaction. By bundling interactions between parties into transactions, blockchains can record a verified, ordered log of all activity on the network.

While the specific data included in transactions can vary across different blockchain platforms, the overall transaction process works similarly in most implementations. At a high level, a user on the blockchain network initiates a transaction by submitting relevant details like sender, receiver, amount, digital signatures, etc. The transaction request is propagated to nodes on the network for validation. Valid transactions are bundled into blocks and added to the distributed ledger.

For a basic cryptocurrency transaction on a blockchain, there are some standard pieces of information that are typically required:

- **Inputs** - The input section typically provides a record of the digital assets being transferred. For the case of new digital assets, the input section documents the origin event. For a cryptocurrency transaction, the inputs would list which prior transactions are providing the funds, and the amounts involved. This links back to the assets' origins on the blockchain. The inputs essentially cite the supporting documentation justifying the sender's ownership of the assets in question. By referencing past transactions as inputs, a provable trail of custody for the funds is maintained on the blockchain ledger. Specifying verifiable inputs is crucial to proving the transaction's validity and conformance with the rules of the system.
- **Outputs** - The output section defines who will receive the transferred digital assets and in what amounts. For a cryptocurrency transaction, the outputs designate the recipient addresses and the quantity of coins each will get. This allows the funds to be divided up and sent to multiple parties in a single transaction. By explicitly specifying the receiving accounts and amounts, the transaction outputs provide critical information to enable the network to correctly process the transfer and maintain an auditable record of where the assets went. Defining unambiguous outputs is essential for accurate execution of transactions.

Although commonly utilized to exchange digital assets like cryptocurrency, blockchain transactions have the flexibility to transfer arbitrary data beyond just financial transactions. The same transaction mechanisms can also convey information between parties, enable interactions with smart contracts (see Section 3.1.6), and record documents on the blockchain. For instance, users can leverage transactions for tracking supplies, registering property, filing records, triggering an automated action, identity authentication, etc. Any process that benefits from permanent, transparent documentation on the blockchain can likely be modeled through transactions. Their versatility makes transactions a

fundamental medium for communication between users as well as tools for accomplishing objectives within the blockchain ecosystem.

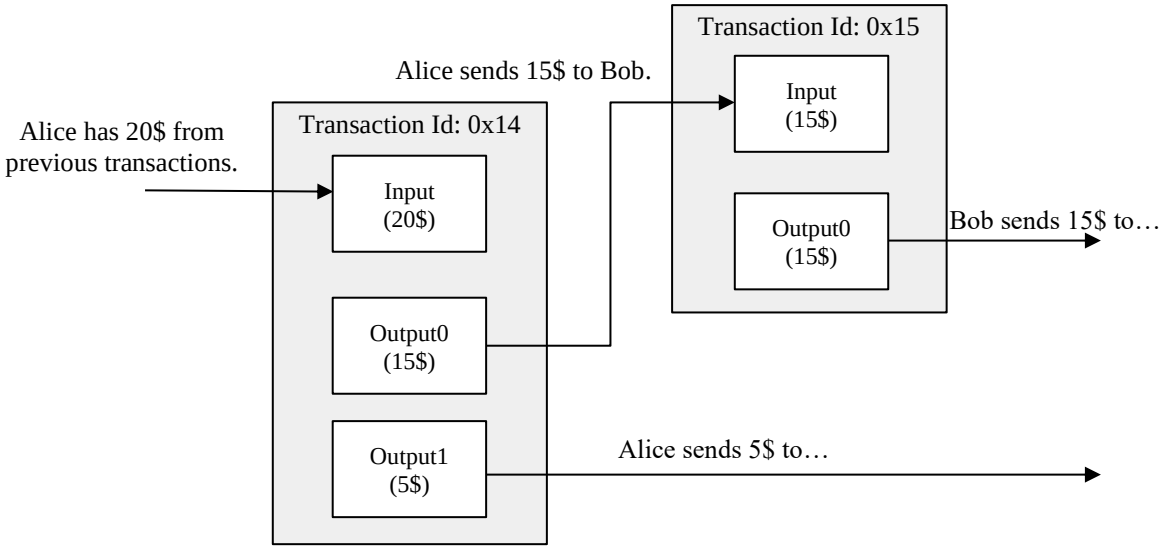


Figure 3.1. An example of a cryptocurrency transaction. Alice has $20 in her account, and she transfers $15 to Bob.

No matter how transaction data is generated or transmitted in a particular blockchain implementation, verifying the validity and authenticity of transactions is crucial. Validity means ensuring each transaction adheres to the blockchain's protocols and requirements before adding it to the ledger. Authenticity means guaranteeing the transaction was truly authorized by the sender through digital signature verification. Rigorously checking both validity and authenticity is essential to maintain the accuracy and security of the blockchain. Invalid or fraudulent transactions could corrupt the ledger if not properly filtered out. By thoroughly scrutinizing every transaction, blockchains can engender trust and transparency between participants without centralized control.

Asymmetric-key Cryptography

Blockchains use asymmetric cryptography, also known as public-key cryptography. This involves using a mathematically linked pair of keys - a private key and a public key. The private key is kept secret, while the public key can be widely shared. Data encrypted with the private key can only be decrypted by the corresponding public key. Alternatively, data can be encrypted with the public key and decrypted only by the corresponding private key. The security of asymmetric cryptography stems from the computational infeasibility of deducing the private key from the public key or vice versa. So, the public-key cryptography enables identification and verification without compromising secrecy.

A crucial benefit of asymmetric-key cryptography is to enable trust between unfamiliar users in a blockchain network. Complete strangers can execute transactions without relying on a trusted intermediary. This works because the math underlying public-private key pairs allows users to independently verify transaction integrity and authenticity, even if they do not personally know the sender. Concretely, a transaction can be encrypted with a private key such that anyone with the public key can decrypt it. Since the public key is openly available, encrypting the transaction with the private key ensures that the signer of the transaction has access to the private key. Alternatively, one can encrypt data with a user's public key such that only the users having the private key can decrypt it. A drawback

is that asymmetric-key cryptography requires heavy computation which slows down the authentication process.

Symmetric-key cryptography differs from asymmetric-key cryptography in that it uses a single shared key for both encryption and decryption. The sender encrypts with the secret key and the recipient decrypts with the same secret key. This contrasts with the public-private key pair model used in asymmetric cryptography. The main advantage of symmetric-key cryptography is its faster performance compared to asymmetric-key cryptography. However, it requires users to securely exchange a shared key out-of-band first before sending encrypted data. A "trick" to get a competitive speed while avoiding key distribution issues is to encrypt the data with symmetric-key cryptography and then encrypt the symmetric-key with asymmetric-key cryptography.

Here is a summary of the use of asymmetric-key cryptography in many blockchain networks:

- Private keys are used to digitally sign transactions.
- Public keys are used to derive addresses.
- Public keys are used to verify signatures generated with private keys.
- Asymmetric-key cryptography provides the ability to verify that the user transferring value to another user is in possession of the private key capable of signing the transaction.

In some permissioned blockchains, it is possible to leverage business's existing public key infrastructure for asymmetric-key cryptography to provide user credentials. Rather than each user generating and managing their own key pairs, the blockchain network can interface with the business's established directory services such as identity, certificate, and key data to authenticate the user on the blockchain. This avoids users from redundant key management, boosting efficiency and convenience compared to standalone key creation strictly for the blockchain.

Addresses and Address Derivation

Some blockchains utilize addresses to identify users on the network. An address is generated by applying a hash function to a user's public key and adding extra metadata like version info and error checking codes. This produces a short alphanumeric identifier that does not actually reveal the public key. Using addresses rather than transmitting public keys directly provides a layer of indirectness that enhances privacy. Addresses also shorten the length of identification strings for compact representation.

To generate addresses from public keys, each blockchain essentially defines its own address derivation algorithm, utilizing choices like hash function, metadata, encoding, checksums, etc. While the algorithms differ in detail, they generally follow the same basic template of hashing keys then adding extra information. An address is usually converted into a QR code (Quick Response code, a 2-dimensional bar code which can contain arbitrary data) to facilitate the use with mobile devices. Allowing custom address schemes permits blockchains to optimize for attributes like length, human readability, error checking, and versioning. Standardizing at the blockchain level also ensures uniform addresses across users for consistency. So, address derivation is an area where blockchain protocols can diverge to suit different design goals.

Private-Key Storage

In some blockchain implementations, particularly permissionless networks, users are responsible for managing and safeguarding their private keys. To avoid manual recording, they often use software to securely store their keys. This software is usually called a **wallet**. The wallet can store private keys,

public keys, and associated addresses. Some wallets can also compute the total number of digital assets a user may have.

One significant risk with users controlling their own private keys is that losing a private key essentially destroys access to any associated digital assets forever. Private keys are generated using secure random number generation algorithms that make regenerating the exact same key practically impossible. Users cannot simply reset lost keys like forgotten passwords. So, losing a private key permanently cuts off access to funds or assets secured by that key, with no feasible way to get them back. This is why users may use special secure hardware to store their private keys offline; alternatively, users may take advantage of an emerging industry of private key escrow services. These key escrow services can also satisfy Know-Your-Customer (KYC) laws in addition to storing private keys as users must provide proof of their identity when creating an account.

Ledgers

In blockchain contexts, the term ledger refers to the complete record of all the transactions that have occurred on the network. The ledger permanently captures an ordered chronological sequence of transactions from the genesis block onwards. It serves as the authoritative dataset powering the shared reality of the blockchain network. The ledger grows over time as new blocks of transactions are appended to it according to the consensus protocol. Access to this universally accepted ledger history allows decentralized parties to coordinate and audit past activity without centralized control.

There is growing interest in exploring distributed ownership of the ledger. The shift from centralized ledgers to shared, distributed ledgers is an exciting frontier enabled by blockchain's innovations. Table 3.2 provides exhaustive advantages of blockchain ledgers over centralized ledgers.

Table 3.2. Comparison between centralized ledgers and blockchain ledger (Yaga et al., 2019)

Centralized ledgers	Blockchain Network
Centralized ledgers are vulnerable to loss or destruction, as they are controlled by a single entity. Users of these ledgers must trust that the owner has properly backed up the system, or they risk losing their data.	A core attribute of any blockchain network is distribution across many peers rather than centralization. This distributed topology intrinsically creates redundant copies of the ledger replicated on nodes across the network. All participants maintain up-to-date duplicates that are continually synchronized as transactions occur. This duplication eliminates single points of failure and provides resilience. If any node drops off the network, there are many duplicates persisting on other nodes. The decentralized nature also makes it virtually impossible to shut down, corrupt or censor the ledger. Attackers must compromise every decentralized node to alter records.
Centrally owned ledgers are often homogeneous, meaning that all the software, hardware, and network infrastructure is the same. This can make the system vulnerable to attack, as an attack on one part of the network can spread to other parts of the network.	Blockchain networks are inherently heterogeneous, meaning that the components like software, hardware, and network infrastructure vary across different nodes. Attacking one node provides no guarantee that the same attack will succeed on other nodes that likely have completely different configurations. Compromising heterogeneous systems requires crafting distinct

	targeted attacks for the diversity of devices and setups. Their decentralized nature also means blockchains have no central bottleneck to target.
A risk with centralized ledger systems is geographic consolidation in single regions. When all servers and infrastructure reside in one physical area, regional disruptions can make the entire ledger globally inaccessible. That is, network failures, power outages, and natural disasters in the region could knock the central servers offline and bring the system down worldwide.	An advantage of blockchain networks is their geographic dispersal across peer nodes globally. That is, nodes exist in diverse physical locations across countries and continents. This intrinsically provides disaster tolerance and failover: If nodes in one region go down, the network continues functioning with nodes in other areas. The global scattering of nodes essentially makes blockchains immune to geographic contingencies that threaten traditional centralized designs.
Transactions on a centrally owned ledger are not transparent, meaning that users cannot see all the transactions that are taking place. This can make it difficult to verify the validity of transactions, and users must trust that the owner of the ledger is validating each transaction correctly.	Blockchain networks have a mechanism in place to ensure that all transactions are valid. If a malicious node were to transmit invalid transactions, other nodes in the network would detect and ignore them, preventing the invalid transactions from spreading throughout the network.
The transaction list on a centrally owned ledger may not be complete, meaning that there may be valid transactions that have not been recorded. This can be a problem because users must trust that the owner of the ledger is including all valid transactions that have been received.	Blockchain networks store all accepted transactions in a distributed ledger. When a new block is created, it must reference the previous block (more on this in following section). This is how the blocks are chained together, forming a chronological record of all transactions. If a node tries to create a new block without referencing the previous block, it will be rejected by the network.
Transaction data on a centrally owned ledger may have been tampered with, meaning that it is possible for the owner of the ledger to change or delete past transactions. This can be a problem because users must trust that the owner of the ledger is not altering the data.	Blockchain networks use cryptographic frameworks such as digital signatures and cryptographic hash functions to ensure that their ledgers are tamper-evident and tamper-resistant. This means that it is very difficult to modify or delete data in a blockchain ledger, even when having access to the ledger.
A centrally owned system may be insecure because users must trust that the associated computer systems and networks are receiving critical security patches and have implemented best practices for security. If the system is not properly secured, it may be breached and has personal information stolen.	Blockchain networks are distributed systems, which means that there is no single point of failure or attack. The data in a blockchain network is also publicly viewable, so there is nothing to steal by attacking the network itself. To attack the network users, an attacker would need to individually target them. However, the honest nodes in the network would resist any attack on the blockchain itself. If an individual node is not patched, it would only affect that node, not the system overall.

Blocks

New transactions are permanently recorded on the blockchain through publishing nodes bundling them into blocks. Each block consists of two components - (1) block header containing metadata, and (2) block data containing the batch of validated and authentic transactions. The validity and authenticity are guaranteed by verifying that the transaction is correctly formatted and that the providers of digital assets in each transaction (listed in the transaction's "input" values) have each cryptographically signed the transactions. This verification ensures that the providers of digital assets for a transaction had access to the private key which could sign over the available digital assets. The other full nodes will check the validity and authenticity of all transactions in a published block and will not accept a block if it contains invalid transactions.

While data fields may vary over blockchain implementations, most of implementation use data fields as the following:

- Block Header:
    - The block number, also called "block height" in some blockchain networks.
    - The hash value of the previous block header.
    - A hash representation of the block data (various methods can be adopted to accomplish this, such as generating a Merkle Tree, and storing the root hash, or by utilizing a hash of all the combined block data).
    - A timestamp.
    - The size of the block.
    - The nonce value. For blockchain networks which utilize mining, this is a number which is manipulated by the publishing node to solve the hash puzzle. Other networks may or may not include it or use it for another purpose other than solving a hash puzzle.
- Block Data
    - A list of transactions and ledger events included within the block.
    - Other data may be present.

Figure 3.2 shows a simple example of block architecture in which Merkle Tree is used in the block header (Liu et al., 2020).

Merkle Tree

Merkle trees provide an efficient cryptographic data structure to summarize large amounts of transaction data into compact digests for block headers. The tree hashes pairs of transactions recursively until a single root digest summarizes the entire set (see Figure 3.2). This Merkle root compactly represents the full tree of hashes in only 32 bytes. Storing just the root in block headers instead of all transactions drastically shrinks storage needs. The elegant structure enables distributed peers to verify if transactions match the header digest without transmitting entire blocks. The arboreal hashing pattern allows efficiently proving transaction inclusion and absence. Merkle trees lend succinctness and verification to the massive transaction volumes in blockchains. Their succinct digest roots lend efficiency while retaining integral transaction security properties.

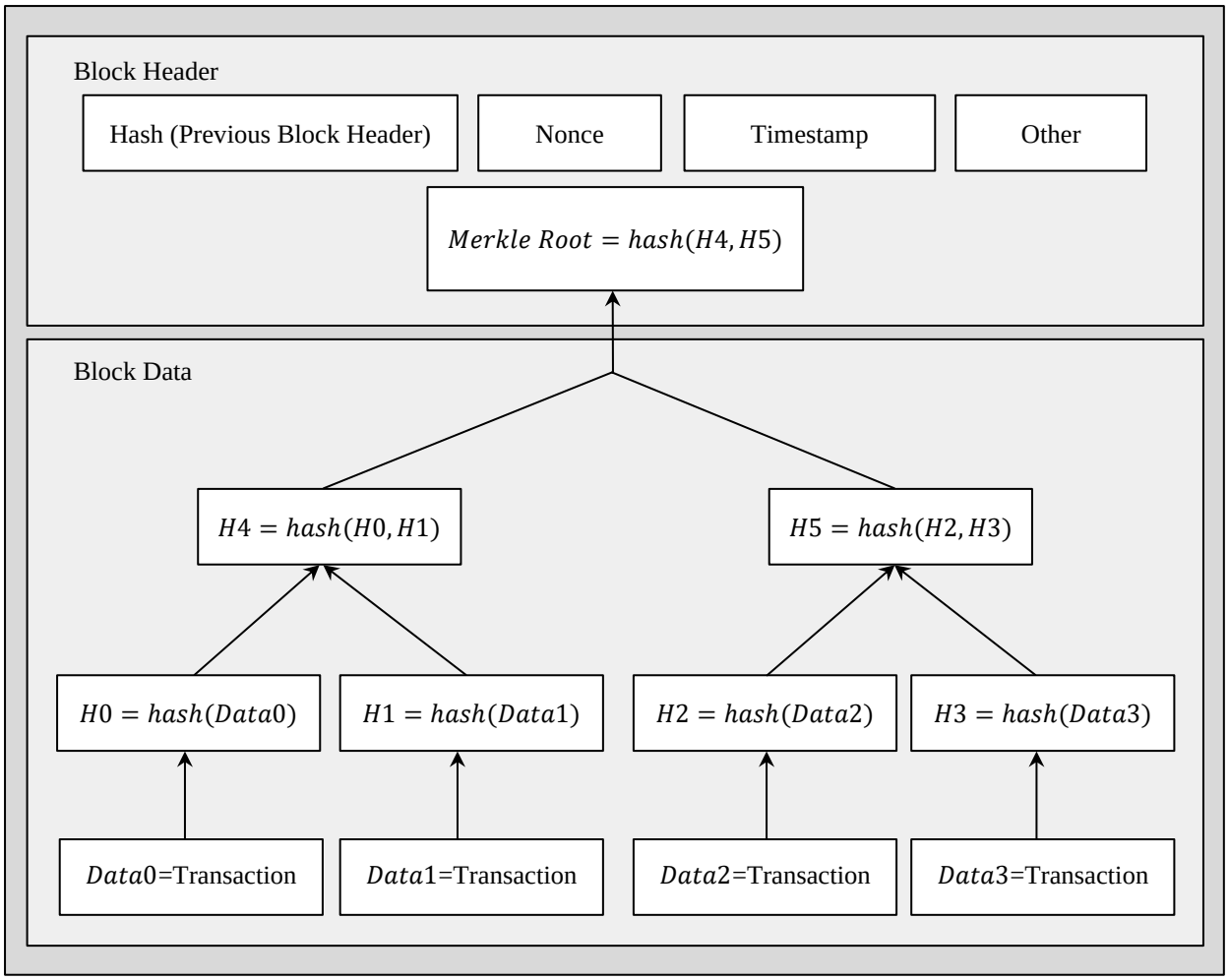


Figure 3.2. An overview of block architecture in which Merkle tree is used in the block header. The block head contains the hash value of the previous block header, nonce value, timestamp, other information, and Merkle tree root hash value. The block data contains 4 transaction data which are stored in the leaves of the Merkle tree. Each of Data0, Data1, Data2, and Data3 is hashed into H0, H1, H2, and H3 respectively. Then, H0 and H1 are hashed together creating H4, and H2 and H3 are hashed together creating H5. Finally, H4 and H5 are hashed together creating the Merkle tree root hash value.

Chaining Blocks

The defining technique that underlies the blockchain architecture is chaining blocks together by including hash pointers. Each new block header contains a cryptographic hash digest of the previous block's header. This links the new block to the prior block in a way that forms a chronological chain. Each new hash extends the chain by certifying the history that came before it. This continuity provides an immutable sequence and tamper evidence. Modifying any earlier block would cause a cascade of invalid hashes propagating forward. This innovation allows decentralized ledgers to transparently grow in a historically verifiable, tamper-resistant manner with no centralized coordination needed. Figure 3.3 represents a generic chain of blocks.

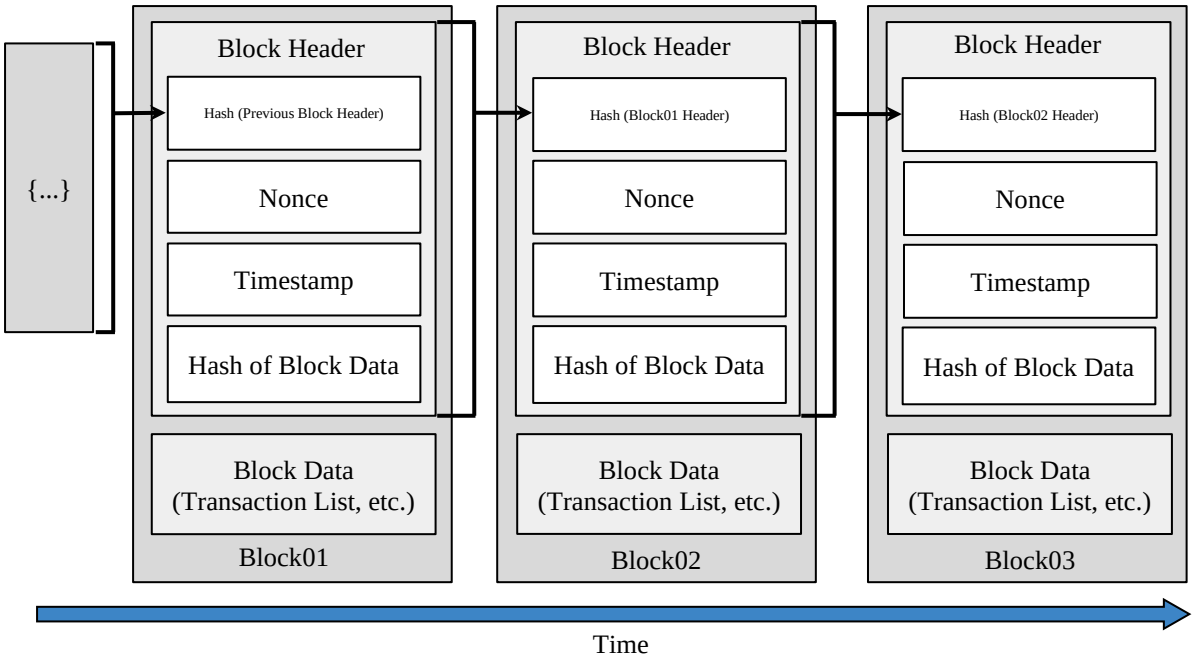


Figure 3.3. Generic chain of blocks. When created, Block01 contains the hash of previous block header. Block02 is created after Block01 and contains the hash of Block01's header. Block03 is created after Block02 and contains the hash of Block02's header. This structure makes it impossible to overwrite data in the block. Concretely, overwrite data in Block03 requires modifications on Block02, Block01, and other blocks that were created before Block01.

3.1.4. Consensus Models

One key characteristic of blockchain technology is deciding which node will add the next block to the chain. In permissionless networks, many publishing nodes compete to publish the next block. The node that manages to do so receives some incentives and/or transaction fees. So, each publishing node participate in maintaining the network by a desire for financial gains, not the well-being of the network.

Since there is no intermediary to decide which node can publish the next block, blockchain technology uses **consensus models** to enable a group of mutually distrusting users to work together. Consensus models are protocols that preserve the well-being of the networks, and the network users must accept them upon entering the network.

Upon joining a blockchain network, all users implicitly accept the initial state of the system. This is encoded in the only pre-configured block, the **genesis block**. Every blockchain network has a published genesis block and every block must be appended to the blockchain after it, based on the consensus model. Regardless of such model, each block must be valid and thus can be validated independently by each network user. The combination of the initial state and the ability to verify each block since then allows users to agree upon the current state of the blockchain. Note that in case of conflicts where there are two valid chains, the default mechanism in the majority of blockchain networks is to adopt the 'longer' chain because it has the most amount of work put into it. More detail about conflict resolution will be given in the following sections.

A defining attribute of blockchains is the elimination of reliance on trusted third parties to validate system state. Blockchain technology enables participants to verify integrity independently and securely

through peer-to-peer consensus. To add a new block to the blockchain, all nodes must come to a common agreement over time; however, some temporary disagreement is allowed. For permissionless blockchain networks, the consensus model must work even in the presence of possibly malicious users since these users might attempt to disrupt or take over the blockchain. For permissioned blockchain networks, legal remedies may be used if a user acts maliciously.

Some permissioned blockchains involve approved publishing nodes that may have established trust. So, a resource intensive (like computation time, investment, etc.) consensus model to decide which node publishes the next block may not be necessary. Generally, the higher the level of trust is, the lower the need for resource usage as a measure of generating trust is.

In the following sections, several popular consensus models are discussed.

Proof of Work Consensus Model

In Proof-of-Work (PoW) blockchains, publishing rights are earned by solving a mathematical puzzle that requires substantial computation. Whoever first finds a solution meeting the difficulty criteria wins the privilege of adding the next block. The solution to a puzzle is the "proof" of expending work to deter cheating. The computational difficulty makes discovering solutions highly arduous. However, the puzzles are constructed such that verifying a solution's validity is relatively trivial. This asymmetry between puzzle solving and solution checking underpins PoW security. It discourages Sybil[1] attacks by limiting block publishing to those willing to repeatedly expend real computing resources in hopes of finding valid puzzles.

A typical puzzle method is to require a block header hash digest be less than a target value. To find solutions, publishing nodes repeatedly tweak their candidate block header in hopes of generating a satisfactory hash digest. This involves iteratively making minor modifications, like incrementing a nonce value, to vary the input data. This brute force strategy is computationally expensive. The target value may be changed over time to adjust the difficulty (up and down) to influence how often blocks are being published. A few simple examples can be found in (Section 4.1, Yaga et al., 2019).

A key property of PoW puzzles is that exerting effort on one puzzle does not improve chances of solving subsequent puzzles. The mathematical problems posed in each round are completely independent and with random solutions. So, past computation provides no advantage in finding future answers. This prevents runaway monopolization by early lucky solvers. Participation stays equitable because solutions require brute force guessing rather than cumulative progress. The independence also incentivizes sharing solutions once found since keeping them secret provides no benefit. PoW puzzles thus stay perpetually difficult while encouraging collaboration through detached randomness rather than compounding gains. Work is its own reward detached from impacting future outcomes.

Proof of Stake Consensus Model

Proof-of-Stake (PoS) consensus relies on the principle that users invested in the system will be motivated to uphold its security. Stake refers to putting at risk cryptocurrency or other holdings tied to blockchain integrity. Those with larger stakes have more financial incentive to maintain the network's proper functioning rather than undermine it. Their chance to validate blocks correlates to share of

[1] Recall that a Sybil attack is a type of attack on a computer network service in which an attacker subverts the service's reputation system by creating many pseudonymous identities and uses them to gain a disproportionately large influence.

holdings, aligning publishing power with vested interest in preserving system value. Unlike PoW, PoS leverages "skin in the game" rather than pure computing power to determine influence. The collateral at stake discourages malicious behavior that might devalue the currency backing the investment. PoS thus leverages financial buy-in for decentralization among partially identified participants.

PoS consensus does not require publishers to perform demanding computational mining puzzles. So, expensive specialized hardware and enormous electricity consumption become unnecessary. The absence of intensive calculations makes PoS more energy-efficient and eco-friendly.

There are various techniques used in PoS systems to algorithmically select block publishers based on stakes:

- Random selection - Publishers are chosen randomly weighted by the amount of staked holdings. So, if a user had 42 % of the entire blockchain network stake they would be chosen 42 % of the time; those with 1 % would be chosen 1 % of the time.
- Voting - Staked users repeatedly vote to elect a changing subset of publishers (also known as **Byzantine fault tolerance proof of stake** (Jean-Paul et al., 2015)).
- Coin aging - Coins must be staked for a period before they can improve publication odds.
- Delegation - Users vote to select delegates who then manage publication but can be revoked.

So staked users may randomly win proportionally to stakes, directly vote on publishers, have stakes mature over time, or elect delegated representatives.

Some PoS designs face a vulnerability called the "nothing at stake" problem. This refers to stakers having little disincentive against signing multiple conflicting blockchains to maximize rewards when forks happen. Unlike PoW mining, there is minimal resource cost to validating many chains simultaneously. Stakers can double sign forks with no downside (this causes ledger conflict as discussed in the following sections). This undermines the finality of transactions until one fork definitively wins out. The indiscriminate cross-signing diminishes network security and consensus finality. It enables denial-of-service attacks and saps confirmation confidence. Various mechanisms like locking stakes, slashing and governance limits help mitigate nothing at stake risks. But it remains a technical issue stemming from staking's intrinsic cost asymmetry compared to mining's concrete resource burns. The lack of real expenditure makes stakers' commitments weaker.

Proof of Authority/Proof of Identity Consensus Model

Proof-of-Authority (PoA) consensus leverages the established real-world identities of publishing nodes to inspire trust. Unlike anonymous systems, publishing nodes must undergo an identification process linking their blockchain keys to proven entities (Liew, 2020). Documents asserting their identities get formally verified and registered on-chain. The need to transparently stake identifiable reputations discourages malicious actions. Identified publishers are incentivized to sustain trustworthiness tied to their brands because their publishing rights derive from users' faith in their approved personas rather than opaque technical factors. This consensus model is not suited to permissionless blockchain networks due to low levels of trust. Proof-of-authority substitutes traditional legitimacy for pure cryptography in semi-trusted settings where relationships pre-exist. Section 4.4.1 will cover an application of blockchain network in which PoA model is used.

Round Robin Consensus Model

In the round robin consensus method used by some permissioned blockchains, publishing rights rotate sequentially between approved nodes in a circular order. The permissioned whitelist provides a finite

list of nodes for deterministic cycling such that nodes take turns creating blocks one after another. This evenly distributes block creation duties using a simple fair scheduling policy. No complex cryptographic puzzles or stakes are necessary with vetted nodes. The revolving turns prevent any one node from dominating. A lapse just moves on to the next node for efficiency. The predictable publisher sequence enables reliable throughput without unnecessary competition between trusted nodes.

Proof of Elapsed Time Consensus Model

Proof-of-elapsed-time consensus relies on trusted execution environments in hardware to impart delays before publishing. Publishing nodes request timeout durations from their computer system. The secured hardware generates random wait times and hands them to the publishing node software. Nodes must idle for their assigned intervals before attempting to publish. The first node emerging from waiting publishes the next block, and the entire process starts over again. The randomness in wait time discourages malicious nodes because they cannot predict the minimum wait time to dominate the system. Most current computer systems (such as Intel's Software Guard Extensions, or AMD's Platform Security Processor, or ARM's TrustZone) can generate random times as required by this consensus model.

Ledger Conflicts and Resolutions

As mentioned previously, multiple blocks can be published at approximately the same time. This leads to differing versions of a blockchain, which is called **conflict**. Conflicts produce inconsistency in the blockchain network. So, they are usually resolved quickly. Typically, the "longest" chain with the most work or endorsements wins out, with discarded blocks' transactions re-queued in the pending transaction pool. That is, the more blocks that have been built on top of a published block, the more likely it is that the initial block will be the "official" published block.

3.1.5. Forking

Modifying blockchain networks poses complex coordination challenges, especially for open permissionless systems with global decentralized users governing through consensus. Protocol upgrades or data structure modifications are called **forks**. They are classified into two categories: **soft forks** and **hard forks**.

Note that in the previous section, we use the term 'fork' to refer to temporary ledger conflicts. Forks in the ledger are temporary and not due to a software update.

Soft Fork

A soft fork refers to a change made to a blockchain protocol that retains compatibility with older software versions. Nodes that did not install the update can still fully interact with updated nodes and process new blocks. Only participants adopting the change will apply the new rules. If very few nodes upgrade, the new rules may not take effect since old nodes remain dominant.

A toy example of a soft fork would be that a blockchain decided to reduce the block's size, say from 2MB to 1MB. Updated nodes would change the block size and continue to transact normally; non-updated nodes would see these new blocks as valid because the change made does not violate their rules (i.e., the block size is under the maximum allowed). However, if a non-updated node were to publish a block with a size greater than 1MB, updated nodes would reject it as invalid.

Hard Fork

Unlike soft forks, hard forks introduce non-backwards-compatible rule changes. At a preset time, all nodes must upgrade to new rules or be permanently forked off the main chain. Hard forks necessitate unanimous adoption to avoid permanent network splits because otherwise non-upgraded nodes will reject new blocks that follow the changes. For permissioned blockchain networks, this risk network fracturing can be mitigated by requiring the "known" publishing nodes to adopt the changes.

A well-known example of a hard fork is from Ethereum. In 2016, a smart contract called the Decentralized Autonomous Organization (DAO) was constructed on Ethereum. Due to errors in the smart contract construction, an attacker extracted Ether, the cryptocurrency used by Ethereum, resulting in $50 million theft (Wong & Kar, 2016). A hard proposal was voted on by Ether holders, and the majority of users agreed to adopt the changes creating a new version of the blockchain, without the errors, and also returning the stolen funds. The old fork was then renamed Ethereum Classic and continued operating.

Cryptographic Changes and Forks

Major cryptographic vulnerabilities may necessitate blockchain hard forks. If core algorithms like hashing or digital signatures are compromised, there could be a fork requiring all future clients to use a stronger mechanism. This could pose a significant practical problem as it could invalidate all existing specialized mining hardware. This hardware invalidation risks miner resistance, as their investments become obsolete. It exemplifies the challenge of coordinating indispensable changes across decentralized users with divergent incentives.

Suppose that SHA-256 is discovered to have a flaw (this is possible but with extremely low probability as explained in Section 3.1.3). Then, blockchain networks that use SHA-256 will need a hard fork to migrate to a new hashing algorithm. The nodes with updated hash algorithm would "lock" all the previous blocks into SHA-256 (for verification) and publish new blocks with the new hashing algorithm. There are many cryptographic hash algorithms, and blockchain networks can choose whichever suits their requirements. For instance, while Bitcoin uses SHA-256, Ethereum uses Keccak-256 (Dworkin, 2015) as mentioned in Section 3.1.3.

With the arrival of quantum computing systems, the vulnerabilities of cryptographic features are taking shape. This will require blockchain networks to adopt a hard fork to change ineffective cryptographic algorithms, and research for more effective cryptographic algorithms. There have been many studies on the impact of quantum computing on cryptographic mechanisms such as *Report on Post-Quantum Cryptography* (Chen et al., 2016) of NIST. Table 3.3 replicates a table that can be found in (Chen et al., 2016) and describes the impact of quantum computing on common cryptographic algorithms.

In consequence, the arrival of quantum computers also threatens the use of asymmetric-key pairs. This is because quantum computing is likely to break algorithms that rely on the computational complexity of integer factorization (such as RSA) or work on solving discrete logarithms (such as DSA and Diffie-Helman).

Table 3.3. Impact of Quantum Computing on common cryptographic algorithms (Table 2, Yaga et al., 2019).

Cryptographic Algorithm	Type	Purpose	Impact from Large-Scale Quantum Computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	N/A	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

3.1.6. Smart Contracts

Dated 1994, Nick Szabo defined the term **smart contract** as "a computerized transaction protocol that executes the term of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries." (Szabo, 1994).

Smart contracts are built on blockchain technology. A smart contract consists of code and data (also known as functions and state) that gets deployed on a blockchain network through cryptographically signed transactions, like Ethereum's smart contracts or Hyperledger Fabric's chaincode. The smart contract is run by nodes on the blockchain network. All executing nodes must get the same execution results, which are then recorded on the blockchain. For most blockchain networks, the publishing nodes execute the smart contract code simultaneously when publishing new blocks. However, there are blockchain networks such that the publishing nodes do not execute smart contract code but validate the execution results of the nodes that do.

For smart contract enabled permissionless blockchain networks (such as Ethereum), the user who issues a transaction to a smart contract will have to pay for the cost of code execution. So, there is a limit on execution time that can be consumed by a call to a smart contract, varying in complexity of the code. If this limit is violated, the execution stops, and the transaction is discarded. This process not only incentivizes the publishers for executing the smart contract code, but also avoids malicious users from using then accessing smart contracts that will perform a denial of service on publishing nodes by consuming all resources (e.g., using infinite loops).

For smart contract enabled permissioned blockchain networks, such as those relying on Hyperledger Fabric's chaincode, the payment for smart contract code execution may not be required because these networks are built around having identified participants, and other methods for preventing bad behaviors can be employed (e.g., revoking access).

3.2. Digital Identity Systems

In today's digital world, digital identities are becoming more and more significant. Most people now have multiple digital identities that are tied to different aspects of their lives - like work, personal relationships, and professional affiliations. As society relies more heavily on technology and online interactions, having clearly defined digital identities allows us to navigate these spaces and platforms securely and efficiently. So, managing our digital footprints thoughtfully has become an important part of life.

In this section, we will first define what identity management is, especially the criteria that an identity management system should respect. Secondly, we provide a few examples of blockchain-based identity management systems. Finally, we discuss some challenges for blockchain-based identity management systems.

3.2.1. Identity Management

Identity management (IdM) is also referred to as identity and access management in the literature. In general, IdM refers to the policies, procedures, and technologies organizations use to make sure only approved users can access the relevant resources within that organization (Manohar & Briggs, 2018). It provides a structure for controlling access to sensitive systems and data, by verifying identities and granting the correct permissions. Identity management (IdM) is a well-established field, as evidenced by the large number of standards and frameworks such as Security Assertion Markup Language (SAML) (Hughes et al., 2005), the Web Services Federation (WS-Fed) (Goodner & Nadalin, 2009), the Identity Federation Framework (ID-FF) (Cantor et al., 2003), and the Identity Web Services Framework (ID-WSF) (Cahill et al., 2007). Examples of IdM criteria include the CoSign Protocol[1], the Open Authentication (OAuth) (Parecki, n.d.), and the OpenID Connect[2] (OIDC). With proper identity management in place, organizations can regulate who can view, utilize, or change resources, ensuring security and compliance.

However, as our world becomes more digital and interconnected, the number and diversity of systems and identities that need to be managed has increased significantly. This means we need to re-examine traditional identity management paradigms. For instance, some have tried to utilize blockchain's inherent features like decentralization, transparency, trust, and security to come up with next-generation identity management models (Dunphy & Petitcolas, 2018; Zambrano et al., 2018; Wadhwa, 2019).

System Components

Consider the following scenario - a user wants to get a service but needs to do an identification. She/He asks an identity provider for proof of her/his identity, and the provider responds with a token. The user utilizes the token to get the service. This involves an exchange of information between the two parties (the user and the identity provider). If the service provider is a separate third-party entity, this becomes a three-party identity management model - consisting of the user, identity provider and identity dependent. In this model, the user's identity credentials are stored only with the identity provider. The identity dependent, usually the service provider, can only verify the user's identity by checking with the provider. Besides providing credentials, the identity provider should also handle identity management, resetting identities, revoking identities and other related functions. Having a centralized third-party

[1] https://cosignweblogin.github.io/
[2] https://openid.net/developers/how-connect-works/

identity provider allows for streamlined identity verification and access control across multiple relying parties. But it also means the provider has significant control over user identities and activities. To sum up, there are three entities involved:

- **User**: Users are the primary enablers of the system, and they benefit from the services provided by the service provider and identity provider. However, not all users have the same privileges.
- **Service Provider**: Service provider is an important part of the system and is mainly responsible for providing services for users (once they are successfully authenticated).
- **Identity Provider**: Identity provider, the core of the system, is responsible for providing users with identity services (e.g., registration, authentication, and management). This entity also provides user authentication.

To resume, to enjoy a desired service, a user must request for the service from the service provider, and the latter requests for identity information from the user. The user receives the request and replies with the corresponding information. The service provider requests the identity provider to validate the user's identity. The identity provider returns the authentication results, and the service provider provides service based on the received validation. A workflow of a typical IdM solution is represented in Figure 3.4.

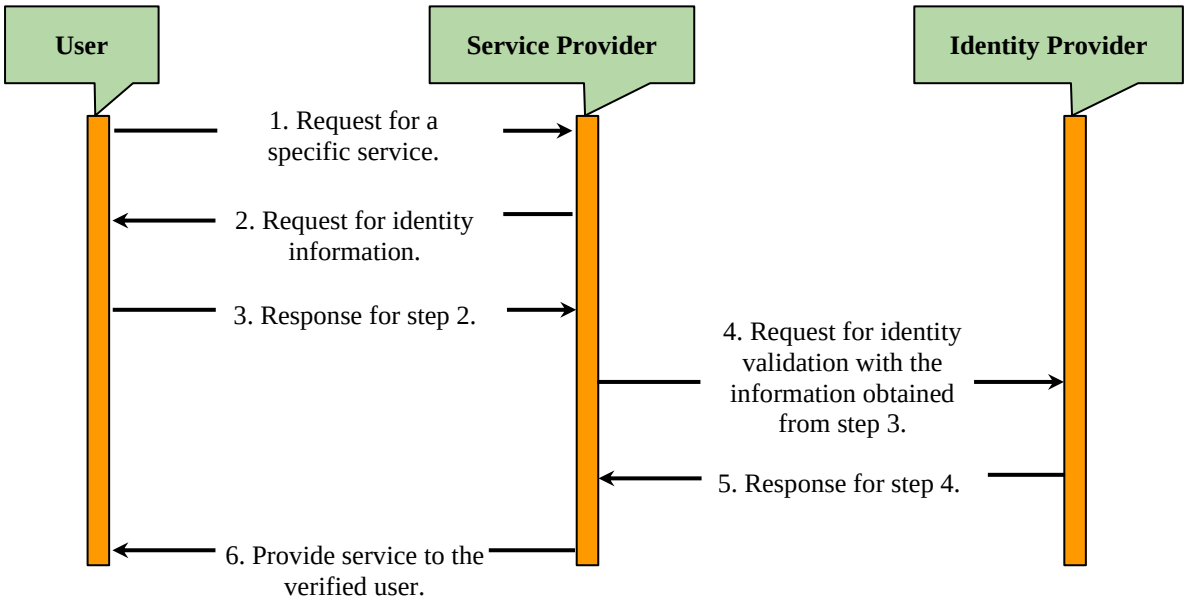


Figure 3.4. Workflow diagram of a typical IdM solution.

Classification of Identity Management Systems

There is a wide variety of identity management systems and architectures that have been proposed and implemented (Mohamad et al., 2016; Rowden, 2004; Caldwell, 2016; Martinez et al., 2016; Pavalanathan & De Choudhury, 2015). The Identity Management Architecture (IdMA) can be categorized into three classes: Independent IdMA, Federated IdMA, and Centralized IdMA.

- **Independent IdMA**: In this type of architecture, each service provider maintains its own separate user identity data (see Figure 3.5a). That means the identities managed by different providers are not interoperable. While this structure is simple, it does not scale well as the number of service providers increases, since each one must store identities. It is also impractical

for users to remember separate credentials (e.g., usernames, passwords) for every individual service provider without reusing passwords. Lack of identity portability also creates friction and barriers for users trying to access multiple platforms. Thus, isolated identity silos may be simple to implement but lead to substantial challenges as the digital ecosystem expands.

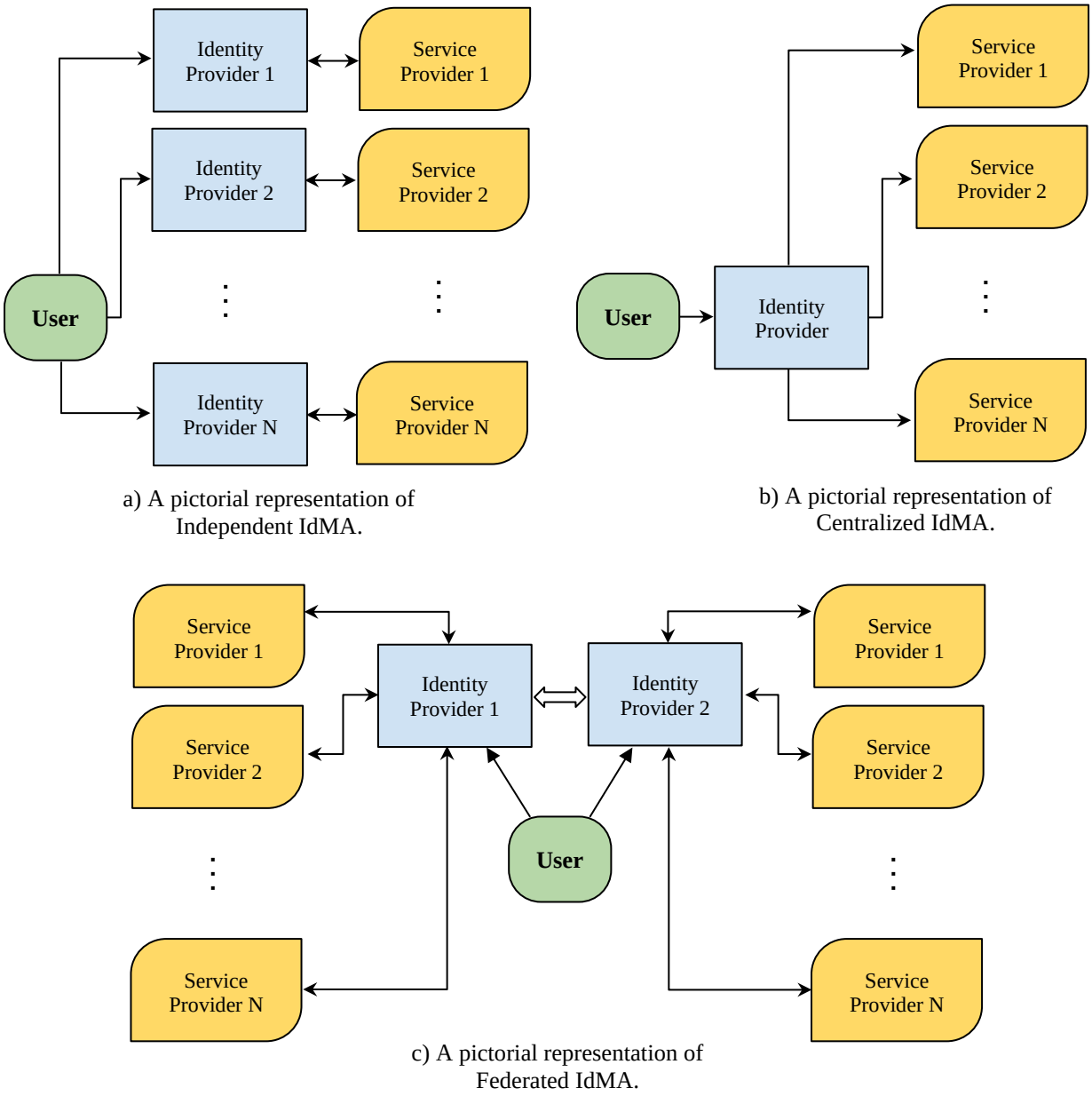
- **Centralized IdMA**: The centralized identity management architecture has only one identifier and identity provider within a trusted domain (see Figure 3.5b). Users can use the same credentials to access all connected systems and services in the ecosystem. This reduces redundancy and saves users from managing multiple identities. However, it also concentrates control and risk in one identity provider. If that system is compromised, it could impact many different service providers at once. So, a robust, reliable identifier and identity provider are crucial for centralized IdMA security.
- **Federated IdMA**: The federated identity management architecture establishes a trusted domain with multiple identity providers in a federation. A trusted domain includes several service providers that accept, and trust user identities issued by other providers in the federation (see Figure 3.5c). This allows for identity portability across the ecosystem's members without centralized control. Users can leverage existing identities and credentials to access different systems seamlessly. Federated architecture balances portable digital identity with distributed control through partnerships between identity providers in a domain.

Laws of Identity

We will now revisit Cameron's law of identity (Cameron, 2005), which is frequently used in the literature to evaluate IdM systems. By (Cameron, 2005), there are 7 laws that technical identity systems must conform:

- **User Control and Consent**: Technical identity systems must acquire a user's approval before revealing information identifying her/him. This guarantees the user' control on her/his identity information.
- **Minimal Disclosure for a Constrained Use**: The solution which discloses the least amount of identifying information and best limits its use is the most stable long-term solution. This guarantees the use of identity information on demand.
- **Justifiable Parties**: Digital identity systems should be designed in a way that limits the disclosure of identifying information to only those parties who have a legitimate need to know. This guarantees that the third parties would not access more identity information than needed.
- **Directed Identity**: A universal identity system must be able to support both "omnidirectional" identifiers, which can be used by anyone, and "unidirectional" identifiers, which can only be used by specific entities. This will allow for the discovery of individuals while preventing the unnecessary release of information that could be used to track them.
- **Pluralism of Operators and Technologies**: A universal identity system must be able to connect and facilitate the interaction of multiple identity technologies that are run by multiple identity providers. This law provides convenience for both developer and cooperator and guarantees the system's scalability.
- **Human Integration**: The universal identity metasystem must define the human user as a component of the distributed system, integrated through clear human-machine communication mechanisms that offer protection against identity attacks. This law provides some prestored hints like guides and emergency manuals for all users.
- **Consistent Experience Across Contexts**: The unifying identity metasystem must guarantee its users a simple and consistent experience across different contexts and operators, while

enabling the separation of contexts through multiple technologies. This law guarantees a certain quality of experience for the users.



a) A pictorial representation of Independent IdMA.

b) A pictorial representation of Centralized IdMA.

c) A pictorial representation of Federated IdMA.

Figure 3.5. Pictorial representation of a) Independent IdMA, b) Centralized IdMA, and c) Federated IdMA.

Cameron's law of identity plays a crucial role in the implementation of IdM systems by regulating the behavior of IdM systems. Several works such as (Dunphy & Petitcolas, 2018; El Haddouti & El Kettani, 2019) analyze different IdM solutions based on Cameron's seven laws of identity.

3.2.2. Blockchain-based Identity Management Solutions

Blockchain-based data structure has emerged as a new paradigm for digital IdMs, as it aims to enable decentralization, transparency, privacy, and control to the users. By (Dunphy & Petitcolas, 2018; Čučko

& Turkanović, 2021), all blockchain-based identity management proposals fell into one of two categories:

- **Self-Sovereign Identity** (SSI) gives individuals full ownership and control over their digital identities, without needing centralized identity providers. Users get to choose what personal data is shared, who to share it with, and when to stop sharing. SSI enables trusted interactions to access identity information while still preserving privacy. This is enabled through an ecosystem that facilitates collecting and recording user attributes, while spreading trust between different digital identities. (Ferdous et al., 2019) presents a fundamental taxonomic outline of an SSI ecosystem by mathematically formalizing various properties of an SSI.
- **Decentralized Trusted Identity** (DTI) models are similar to traditional digital identity management solutions which rely on existing trusted public credentials like government Id cards, passports, etc. First, a proprietary service performs identity proofing to validate these credentials. Then, it stores identity verification proofs on a blockchain for later validation by third parties (e.g., service providers...). This decentralizes identity data while still leveraging familiar trusted credentials.

Both SSI and DTI IdM solutions can be implemented on either permissioned or permissionless blockchains. However, the kind of blockchain used to develop the solution directly impacts the properties of IdM solutions (Panait et al., 2020).

In the following, two blockchain-based IdM solutions are discussed. The first solution is **uPort** (Lundkvist et al., 2017) which is the first existing identity solution that enables SSI. The second one is **ShoCard** which belongs to DTI models. These two solutions are commonly and globally reviewed in the literature (Seyam & Habbal, 2023; Ahmed et al., 2022; Liu et al., 2020). An extensive and comprehensive survey can be found in (Ahmed et al., 2022).

uPort (Lundkvist et al., 2017)

uPort (Lundkvist et al., 2017) was an open source decentralized identity framework that aimed to give users control over their identity using blockchain (Dunphy & Petitcolas, 2018). It utilized public permissionless Ethereum blockchain and smart contracts to implement SSI. The uPort system consisted of a mobile app, Ethereum contracts, and a registry for uPort IDs. It allowed users to securely share credentials, sign transactions, and manage keys and data. Figure 3.6 illustrates how a transaction occurs in uPort. The original uPort project has now been divided into two new initiatives - Veramo[1] and Serto[2]. Both continue the goal of user-controlled identity. Veramo is a JavaScript framework for building apps that use cryptographically verified data. Serto helps organizations adopt decentralized identifiers and verifiable credentials using W3C standards. The original uPort mobile apps, libraries and services are now deprecated. Though uPort itself is discontinued, its ethos lives on through Veramo and Serto - demonstrating the evolving landscape of blockchain-based identity management.

In the uPort system, users have potential control over their own data to read/write to their registry, which could be harmful as they are able to remove negative attributes from their records. uPort provides discreet services, but there is no search directory to find Ids and connect with others. In addition to these limitations, uPort has two major disadvantages. First, a government could control its citizens while facilitating digital transactions by leveraging identity systems. Secondly, on one hand, if an attacker gains access to a user's private key, their confidential information could be stolen. On the other hand,

[1] https://veramo.io/
[2] https://www.serto.id/

the recovery delegates for different uPort users are visible on the blockchain, making them prime targets for attackers looking to exploit users' identities. Also, confidential data temporarily stored on the Chasqui server is not encrypted, which could lead to compromised data.

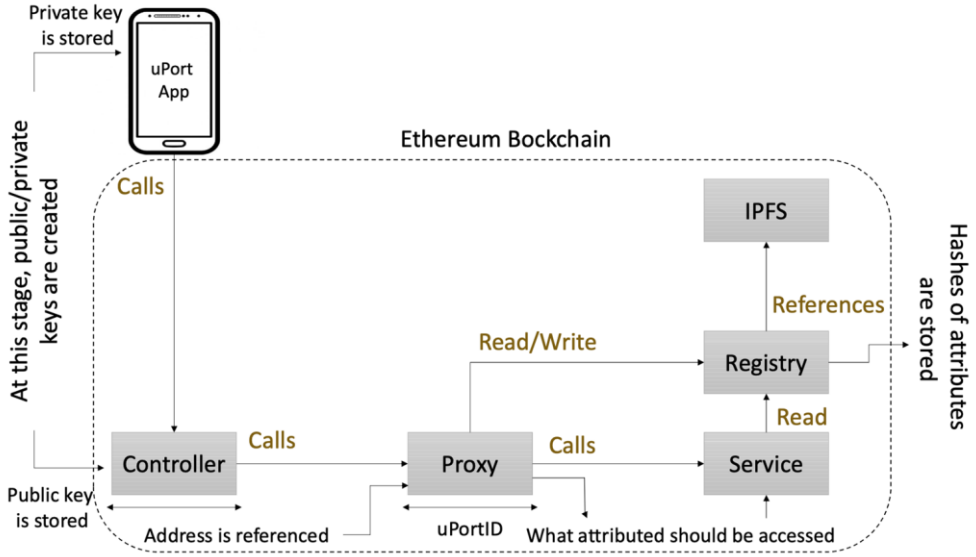


Figure 3.6. The general architecture of uPort (Alsayed Kassem et al., 2019). IPFS, InterPlanetary File System.

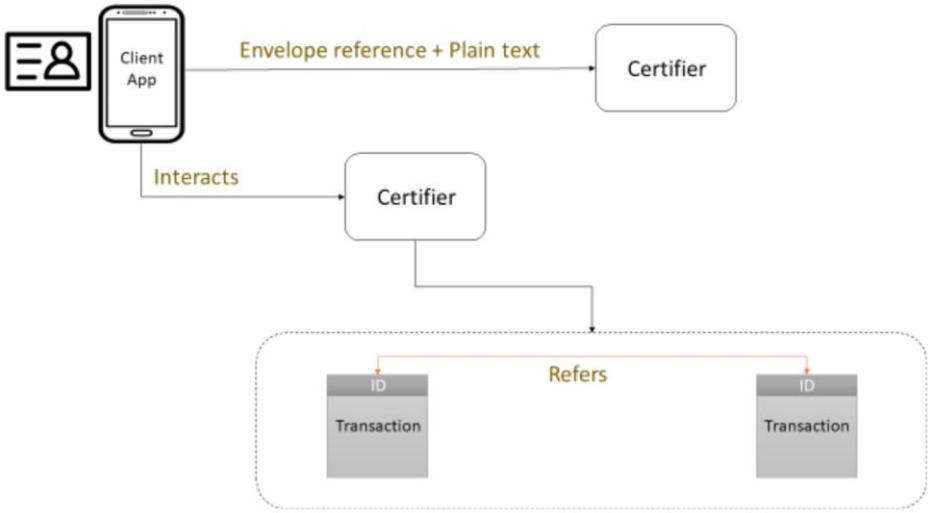


Figure 3.7. The architecture of ShoCard (Alsayed Kassem et al., 2019).

ShoCard (ShoCard, 2016)

ShoCard (ShoCard, 2016) is a digital identity and authentication service built on the Bitcoin blockchain. It allows individuals and businesses to identify each other securely and verifiably, enabling fast and seamless transactions. ShoCard identities are stored in the Bitcoin blockchain using public/private key pairs - users hold the private keys while services use the public key to authenticate via ShoCard (Figure 3.7 shows how the transactions occur in a ShoCard network). Although built on a public blockchain, ShoCard's architecture is engineered to be scalable. ShoCard does not minimize shared data (Gilani et al., 2020), though some (e.g., Van Bokkem et al., 2019) argue that it provides data minimization.

The ShoCard server functions as an intermediary that manages the certification exchanged between users and service providers. However, the design is more centralized than relying on the distributed ledger technology. This implies that if a company ceases to exist, then identities are unusable. Users are required to upload credentials, demanding more information than needed; for instance, a scanned copy of a passport must be uploaded. In addition, even though the data is encrypted on the ShoCard server, it can be associated with both ShoCardIds and relying parties, which compromises privacy.

3.2.3. Discussion

While blockchain-based IdM has been extensively researched and recognized for its potential in areas like IoT, healthcare, and cloud computing, there are still many limitations and challenges like scalability, key management, regulation, and sustainability. There are open questions around optimal architecture, standards, and integration with legacy systems. Continued analysis of these challenges and real-world performance are needed to fully unlock its capabilities and maximize benefits.

Scalability

Scalability refers to a blockchain's ability to efficiently process increasing transactions without slowdowns or bloating. Blockchains store transaction backups across blocks for transparency and availability. But as transactions grow, block size and quantity increase, impacting performance. Supporting more transactions while optimizing speed is complex. Research on effective load balancing and scaling techniques is always needed. Ideal blockchains provide availability and transparency while expanding storage and processing capabilities as required. By design, blockchain-based IdM is distributed, decentralized, and fault tolerant, reducing deployment and maintenance costs. However, scalability is a key barrier to public blockchain adoption. Many blockchain identity solutions are now frameworks, prototypes or schemes anticipating future scalability research. With continued advancement, blockchain-based identity solutions can potentially scale efficiently while retaining decentralization benefits.

Exclusion of Intermediaries

Blockchain-based identity management systems provide decentralized solutions without centralized authority control. However, most still rely on central servers or intermediaries for data storage and key revocation. Removing certificate authorities entirely could jeopardize identity functions like lookups, as noted in (Gilani et al., 2020). It is true that permissionless blockchains like Bitcoin eliminate intermediary needs for processes like auditing, but many sectors will likely remain reliant on third parties, like national registries, voting, and trade platforms. While blockchain technology can significantly reduce intermediary roles and alter trust relationships, complete elimination is improbable. (Tseng & Shang, 2021) discusses sustaining necessary intermediary functions for identity management, supply chains, agriculture and more. The disintermediation concept in blockchain business models is also examined (Tan et al., 2021). Blockchain evolution will likely transform rather than fully eliminate trusted third-party roles.

Leakage of Personal Information

When users provide personal data to relying parties, it may be shared with unauthorized third parties outside the identity management context. This data sharing risk exists in any system that discloses user details. Minimizing data exposure helps mitigate this. Many researchers use zero-knowledge proofs to share the minimum necessary data with verifiers. Systems that store less on-chain data may also enhance privacy generally, depending on the architecture and data type.

Identity Revocation

Blockchains are immutable, so changing or deleting identity data is challenging. Identity revocation refers to rescinding credentials. This is difficult in decentralized identity systems without central revocation servers. Some identity solutions avoid storing credentials or keys on-chain, relying on user on-device storage. However, this risks loss from device failures or user errors, especially for non-technical users. Systems like ShoCard lack identity revocation capabilities. uPort has basic key recovery but needs more development. Academic research explores revocation for blockchain identity management in healthcare, IoT and mobile networks. Using multiple blockchains could also help address revocation and key recovery. Overall, blockchain-based IdMs need robust identity and credential revocation techniques for recovery from loss, theft, and other issues.

Key Leakage

Public and private keys aim to ensure blockchain privacy. Similar to what mentioned in Section 3.1.3, if private keys are lost, resetting digital identity is extremely difficult. Proper key management is critical for decentralized identity adoption. Research identifies two types of key leakage - explicit leakage from open-source platforms, and implicit leakage from user cryptographic misuse. Solutions like multi-party signing protocols are suggested to strengthen key control. Overall, resilient key management is essential for robust identity privacy in blockchain systems. Secure key generation, storage, recovery, and revocation mechanisms need greater focus, along with user education to avoid leakage.

Overlooking the Conditional Traceability, Accountability, and Control Features

Current decentralized identity efforts often overlook user access control, accountability, and conditional traceability. Privacy protections allow anonymous payments, enabling criminal blockchain uses. Also, decentralization increases adversarial opportunities, making the privacy-accountability balance harder. So, anonymity should be conditional, with transparency and traceability possible under defined circumstances. Access controls, auditing, and selective disclosure mechanisms that uphold both privacy and accountability warrant more research. Overall, decentralized identity solutions must evolve to not only protect but responsibly manage privacy. Preserving user rights while retaining social protections is critical as blockchain-based IdM matures.

Speed and Consumption Issues of Consensus Protocol

As mentioned in Section 3.1.4, the consensus mechanisms used for trust and validation impact the speed, scalability, and service agreements between parties on a blockchain network. Before any transactions are accepted, all nodes must reach consensus, which increases messages and slows systems as they grow. Efficient, flexible consensus protocols are needed to quickly validate identities without reducing network speed. Most current blockchain-based IdM solutions use PoW, PoS or Practical Byzantine Fault Tolerance (PBFT) consensus, each with drawbacks: PoW is energy intensive and enables attacks through race conditions, PoS risks centralization and unfairness, and PBFT is vulnerable to Sybil attacks that disrupt consensus. Hybrid consensus switches between protocols to balance risks and quality. Ongoing research explores proofs of entitlement, activity, reputation, authorization, etc. to optimize blockchain consensus for identity. The goal is an adaptive framework balancing security, scalability, and efficiency for identity systems. Advancing tailored, versatile consensus protocols will empower blockchain identity solutions to scale sustainably.

4. Use Cases and Potential Applications in Cambodia

In the past decade, blockchain has emerged as one of the most talked-about technologies, often surrounded by hype and speculation. While it is true that blockchain has been somewhat overhyped, it cannot be denied that this technology has the potential to revolutionize numerous industries. Entities spanning diverse sectors, ranging from startups to multinational corporations, governments, and non-profit organizations, have unequivocally acknowledged the immense value of blockchain. As a result, they are actively spearheading the development and successful implementation of blockchain-based applications (Liew, 2020). Thus, it has become crucial for individuals, business owners, enterprises, and governments alike to closely monitor and embrace this emerging trend.

Blockchain technology offers several advantages that make it an attractive solution for a wide range of applications. One of its key strengths is its ability to provide transparency and immutability in data transactions. By utilizing a decentralized network and cryptographic algorithms, blockchain ensures that all participants have access to the same information, eliminating the need for intermediaries and reducing the risk of fraud or tampering. This feature has immense potential in various sectors, such as supply chain management, finance, healthcare, public services and more. Furthermore, blockchain technology facilitates secure and streamlined peer-to-peer transactions, removing the necessity for conventional intermediaries such as banks or payment processors. This not only reduces costs but also accelerates transaction speed, making it an appealing option for businesses and individuals alike. Given these transformative capabilities, it is evident that blockchain technology is here to stay and warrants the attention and exploration of all stakeholders.

4.1. Financial Inclusion

Financial services such as payments, savings, credit, and others are essential components of our daily lives, empowering us to efficiently handle a wide range of expenses and investments, including necessities like food, housing, transportation, health, education, and beyond. While banks and financial institutions offer most of these services, it is concerning that the World Bank estimates nearly 1.7 billion adults, equivalent to 31% of the global population, lack access to banking services (Chapiro, 2021). In developing countries, the figure can be as high as 61%. Furthermore, women face even greater disadvantages, with approximately 55% of them lacking access to essential banking services.

Improving financial inclusiveness is a primary objective within the United Nations Sustainable Development Goals (UNCDF, n.d.). Through this initiative, we can foster more stable financial systems and economies, mobilize domestic resources via national savings, and ultimately bolster government revenue, thereby enhancing the well-being of populations in less developed countries.

4.1.1. What is Financial Inclusion?

According to the World Bank, financial inclusion refers to the provision of accessible and affordable financial products and services that cater to the needs of individuals and businesses. This encompasses various aspects such as transactions, payments, savings, credit, and insurance, all delivered responsibly and in a sustainable manner (David, 2023).

The World Bank Group acknowledges the significant role of financial inclusion in combating extreme poverty and fostering shared prosperity (Mhlanga, 2023). The initial stride towards achieving broader financial inclusion is facilitated by access to a transaction account, enabling individuals to securely hold and conduct various monetary transactions such as sending and receiving payments. In addition, individuals will have the opportunity to establish financial security through various means, including saving money, investing in financial products to meet their children's education and retirement needs, and adequately preparing for potential financial challenges (Lichtfous et al., n.d.).

4.1.2. Digital Financial Inclusion

To promote financial inclusion, the World Bank is actively involved in the digitization of financial services, aiming to enhance accessibility and cost-effectiveness for underserved and unbanked populations. The President of the World Bank, Mr. Jim Yong Kim, is renowned for his impactful statement: "Universal access to financial services is within reach—thanks to new technologies, transformative business models and ambitious reforms. As early as 2020, such instruments as e-money accounts, along with debit cards and low-cost regular bank accounts, can significantly increase financial access for those who are now excluded."

Digital financial inclusion means utilizing cost-effective digital methods to extend access to formal financial services, catering specifically to financially excluded and underserved populations (The World Bank, n.d.). These services are designed to meet their unique requirements and are delivered responsibly at an affordable cost to customers, ensuring sustainability for providers.

Providing services to currently unbanked or underserved populations necessitates the utilization of cost-effective and efficient digital tools. These tools typically include a digital transactional platform, a network of retail agents, and the widespread use of mobile phones by both customers and agents to facilitate transactions on the platform. These three fundamental components form the basis of any digital financial service (David, 2023).

The encouraging development is that digital financial services, particularly those accessible through mobile phones, have experienced remarkable expansion in more than 80 countries in recent years, leading to substantial rates of adoption (The World Bank, n.d.). Consequently, a significant number of individuals who were previously marginalized or lacked access to financial services can now transition from relying solely on cash transactions to utilizing formal financial services. These comprehensive services encompass payments, transfers, savings, credit, insurance, and even securities, conveniently accessible via mobile phones and other digital technologies.

4.1.3. Driving Financial Inclusion with Blockchain

Since their inception, blockchain technologies have demonstrated tremendous potential in promoting financial inclusion and streamlining the formalization of remittances (Rella, 2019). Blockchain technology presents an array of possibilities, encompassing faster, cost-effective, and highly secure payment processing. Furthermore, its distributed ledger capability instills enhanced trust among participants. Originally conceived as a foundation for virtual currencies, blockchain has now found extensive utilization across various industries, notably in the realm of payments (David, 2023).

Furthermore, blockchain technology facilitates global payment processing and various other transactions through encrypted distributed ledgers, ensuring dependable real-time transaction

verification. Consequently, intermediaries such as clearing houses and correspondent banks are rendered unnecessary. In addition, blockchain applications have gained significant appeal for remittances, particularly for transferring small amounts of money, thanks to their instantaneous, affordable, and traceable transactions that support multiple currencies across domestic and international mobile networks. Moreover, these applications can effectively store a variety of currencies within diverse mobile networks, highlighting the potential of blockchain-based systems.

After conducting comprehensive analysis of relevant prior research, it is evident that blockchain technology possesses the potential to facilitate digital financial inclusion across various domains. This technology finds application in diverse areas such as financial transactions, savings optimization, credit extension, and insurance provision (David, 2023). In short, sustainable development can be achieved through various avenues, and one promising approach is leveraging blockchain technology to enhance financial inclusion. Governments, particularly those in developing economies, must prioritize serious consideration of blockchain investments to foster greater financial inclusion.

Let us delve into two fascinating use cases that demonstrate the transformative power of blockchain technology in fostering financial inclusion. The first use case revolves around providing secure and transparent financial services to the unbanked populations in developing countries such as Cambodia. By leveraging blockchain's decentralized nature, individuals without access to traditional banking systems can now participate in the global economy, opening doors to economic empowerment and growth. The second use case is a proposed model that illustrates how blockchain technology enables seamless cross-border remittances, eliminating intermediaries and reducing transaction costs for migrant workers, thereby facilitating faster and more affordable money transfers. Through these real-world applications, blockchain technology is ushering in a new era of financial inclusion, revolutionizing the way people access and utilize financial services worldwide.

4.1.4. Case 1: Project Bakong

Financial Inclusion is the top priority for the National Bank of Cambodia (NBC), and promoting a cashless society is a key strategy to achieve this goal. Ensuring accessible and affordable digital transactions, along with mobile banking and money transfers, is an effective way to enhance financial inclusion. To address this, the NBC has introduced Project Bakong, which brings together all participants into a unified system. Through their Bakong accounts, created via the Bakong App installed on their smartphones, individuals can easily access and spread financial services across the country (National Bank of Cambodia & Soramitsu, 2020).

Bakong, a cutting-edge Real-Time Gross Payments System, is the result of a successful partnership between SORAMITSU Co., Ltd (a technology company based in Japan) and the National Bank of Cambodia. This innovative platform prioritizes financial inclusion by providing a user-friendly yet robust iOS and Android app (Soramitsu, n.d.). Project Bakong aims to explore alternative technology platforms and develop a cutting-edge payment system that prioritizes financial inclusion, enhances interoperability among stakeholders, and facilitates seamless local currency transactions, all while ensuring utmost safety and efficiency (National Bank of Cambodia & Soramitsu, 2020).

Despite the gradual development of current payment systems over the past decade, achieving interoperability in retail payments between banks and Payment Service Institutions (PSIs) remains a significant challenge. Presently, there is no Real-Time Gross Settlement (RTGS) mechanism in place for banks, except for end-users, and interbank clearings and settlements occur only twice daily (National

Bank of Cambodia & Soramitsu, 2020). The integration of Distributed Ledger Technology[1] (DLT) in Cambodia's payment systems presents a remarkable opportunity to revolutionize the way all participants are interconnected and tackle multiple challenges simultaneously. Bakong revolutionizes the payment industry by integrating multiple service providers into a unified system through an open API. This empowers users to engage in seamless, secure, and real-time peer-to-peer transactions without incurring any transaction fees.

To fully harness the benefits of technological innovation, the NBC is enthusiastically embracing blockchain technology as an integral component of its national payment system, aiming to (National Bank of Cambodia & Soramitsu, 2020):

- Address the issue of interconnectivity and interoperability across platforms of payment operators.
- Enhance the efficiency of payment systems by achieving lower costs, faster speeds, and enhanced security.
- Promote financial inclusion.
- Ease KHR (Khmer Riel) cash payment.

To achieve these objectives and enhance the current payment systems, the NBC embarked on an exploration of various alternative technologies, such as DLT and blockchain, in 2017. These endeavors present the NBC and the financial sector with an exceptional chance to delve into novel payment and operational technologies that offer enhanced security and resilience. This initiative, known as Bakong, has adopted Hyperledger Iroha as the DLT platform, and the pilot testing of the project has been underway since July 2019.

Project Bakong is a pioneering payment system platform that harnesses Distributed Ledger Technology (DLT) to significantly improve the efficiency, cost, speed, and security of transactions. The core nodes of Project Bakong are strategically deployed within closed-loop infrastructures situated at the NBC, allowing participants to access them through the payment gateway. To ensure security and integrity, only registered individuals are permitted to engage in business transactions within the system. The consensus mechanism employed by Project Bakong involves a robust (2n+1) out of (3n+1) node validation process, with "n" representing the total number of nodes.

The implementation of Bakong revolutionized the financial landscape by seamlessly connecting all financial institutions and payment service providers through a single, cutting-edge payment platform. This transformative system enables real-time fund transfers without relying on a centralized clearing house. Furthermore, institutions currently utilizing FAST can seamlessly integrate with Bakong without the need to modify their existing infrastructure.

Bakong not only offers an extensive feature (P2P) but also empowers end-users to conduct real-time retail fund transfers effortlessly through its all-in-one mobile payment and banking application. This application facilitates seamless fund transfers by enabling users to scan QR codes, input phone numbers, or simply select recipients from their contact list. Additionally, it allows convenient deposits into any accounts within Bakong's network of participating banks.

[1] Distributed ledger technology (DLT) encompasses the technological infrastructure and protocols facilitating simultaneous access, validation, and record updating across a networked database. It serves as the foundation for creating blockchains, enabling users to observe changes and their respective authors, minimizing the necessity for data auditing, ensuring data reliability, and granting access solely to relevant individuals (Frankenfield, 2023).

In a nutshell, Bakong serves as a catalyst for promoting cashless payments in the digital economy. This payment system greatly facilitates the adoption of cashless transactions among the unbanked population, offering them a more convenient financial access through the Bakong platform compared to the current payment methods. With its innovative technology, Bakong presents an opportunity for financial institutions to invest in Project Bakong at a low cost, allowing them to expand their payment services via smart devices and further promote financial inclusion among the unbanked population.

4.1.5. Case 2: Blockchain-based Remittance Model

Remittances represent a steady supply of foreign funds for many low- and middle-income countries and play a vital role in lowering the level of poverty (Digital Financial Services Working Group, 2018). Remittances support demand for local consumption and complement the volatile flows of other types of international funds, such as foreign direct investment and aid. At the household level, remittances are associated with increased spending on housing, education, and income-generating activities. Thus, remittances play an important role in the economic growth of low- and middle-income countries such as Cambodia.

However, the involvement of numerous intermediaries significantly inflates the cost of cross-border remittances, making it exorbitantly expensive. The average commission rate per remitter reaches an astonishingly high 7.68% due to the excessive number of intermediate links (as shown in Figure 4.1). In addition, the remittance cycle is long, from a few days to weeks or even months. Moreover, existing cross-border remittances also suffer from other issues such as fraud, exchange rate losses, counterparty risk, red tape and more. On top of that, an estimated 1.7 billion people are unbanked and therefore excluded from existing global financial services, including cross-border money transfer. As a result, a large proportion of remittances are still sent through informal channels, which lack consumer protection mechanisms (Digital Financial Services, 2018). In short, transferring money across international borders is still complicated, time consuming and expensive. Therefore, a crucial measure to bolster financial inclusion entails enhancing the remittance system.

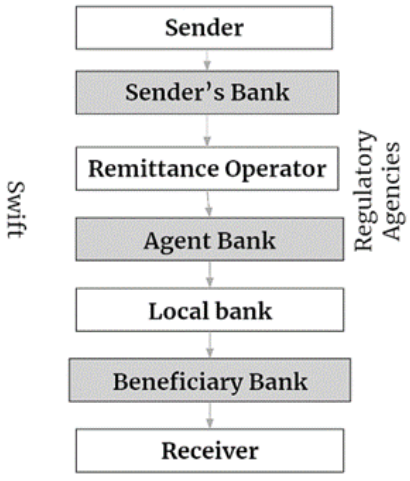


Figure 4.1. The process of Cross-Border Money Transfer (Liew, 2020).

Fortunately, the proliferation of innovative digital technologies is rapidly transforming the remittance landscape. Innovative technology-based remittance models are slowly replacing incumbent, clunky and

costly models. These new models help to reduce transfer costs and time and improve access at both the sending and receiving ends. Let us examine several emerging business models for cross-border money transfer, as described in Table 4.1.

Table 4.1. Emerging Models for Cross-Border Remittance.

Remittance Model	Description
Mobile Money	Cross-border remittances are sent through mobile money or e-wallet accounts. The transfer can happen between: - Providers owned by the same group holding company. - Different providers working in cooperation. - Multiple providers connected through a "hub" operated by a third party. - Mobile money/e-wallet accounts can be used by the senders and the receivers.
Online	Users transfer money through an online remittance platform. The transfer can be made through the provider's mobile phone app or website. Senders can use their online banking account, debit card, credit card and more to link to the platform to send money. Receivers can receive funds in several ways, such as mobile money, bank account deposit, airtime top-up or cash pick-up.
Peer-to-Peer	This is a fully online model as no cash is accepted or sent out. Transactions can happen only through a bank account, card or closed loop wallet offered by the provider. As the cross-border movement of money is low, the cost of remittances is also relatively low.
Blockchain	This blockchain-based model enables money transfer in the form of cryptocurrencies like Bitcoin, Ethereum and more. Funds are sent and received in the respective local fiat currency, but the cross-border transfer of funds happens through blockchain in the form of digital cryptocurrency. For example, platforms such as Ripple and Ethereum enable cross-border payment services through their own cryptocurrencies (XRP and Ether, respectively) or through their platforms based on blockchain technology. Blockchain provides a decentralized ledger of transactions (blocks) distributed among all members of the network (chain). The ledger is updated every time a transaction takes place once verified and approved by the nodes in the blockchain network.

The Blockchain Remittance Model: Blockpay

Since their emergence, blockchain technologies have demonstrated significant potential in facilitating financial inclusion and enhancing the formalization of remittances (Rella, 2019). The Blockpay model will utilize blockchain technology as its foundation. The primary objective is to develop a remittance model that operates on the blockchain, enabling unbanked individuals and migrant workers to send money quickly and affordably to their home countries. Additionally, we aim to democratize the digital asset market, particularly for those who are unbanked and underserved in society.

Blockchain can solve the pain points of high cost and delay of cross-border remittance. Indeed, blockchain-based remittance can simplify the entire process, removing unnecessary intermediaries and other barriers. The idea is to provide frictionless and near instant payment solutions. Unlike traditional

services, a blockchain network need not rely on a slow and tedious process of approving transactions, which usually goes through several banks and intermediaries.

A blockchain remittance system can perform worldwide financial transactions based on a distributed network of computing devices known as nodes. This means that several nodes participate in the process of verifying and validating transactions which can be done in a decentralized and secure way. The encryption feature of blockchain provides security and an easily verifiable public audit trail. Enhanced security results in a reduction of the widespread fraud observed in traditional banking. Overall, blockchain technology can provide faster and more reliable payment solutions at a much lower cost.

The Blockpay Platform and Wallet

Blockpay is a blockchain digital platform that features a web app and mobile wallet that can be funded with crypto and fiat currencies. It will also allow auto conversion of crypto to fiat currency and vice versa. Therefore, users can not only send money but are also able to trade and invest in crypto assets as well. Moreover, Blockpay is also a full-fledged DeFi[1] platform that allows peer-to-peer lending where borrowers can have access to instant loans and lenders can earn interest with their digital assets.

Additionally, Blockpay mobile wallets offer the convenience of being funded by a wide range of cryptocurrencies, including Bitcoin, Ether, Litecoin, Dot, CBDC and more, ensuring high liquidity. What sets it apart is that users can also deposit fiat currencies directly within the same mobile application. By seamlessly integrating e-wallets within the Blockpay platform, all crypto-to-fiat conversions are executed in real-time, utilizing live exchange rates. This feature enables smooth cross-border money transfers at significantly reduced costs compared to traditional remittance methods. As a result, mainstream users can confidently embrace cryptocurrencies for remittance and payment, knowing that conversions reflect instantly in their Blockpay wallets.

Blockpay Prepaid Card

Blockpay will also issue prepaid cards by establishing strategic partnership with a globally renowned card issuing company. The prepaid cards can store fiat as well as cryptocurrencies. By integrating the Blockpay wallet app (iOS and Android versions) with Blockpay Cards, the unbanked and the underserved will have easy access to financial services which were unreachable before. This inclusion allows the masses to participate in the crypto world with a network of clients and with a Blockpay Card that has million points of acceptance globally, including ATM withdrawals.

With Blockpay wallet and prepaid cards, we can help to propel the unbanked to the forefront of currency freedom with the ease of exchanging fiat money into cryptocurrencies and vice versa. Therefore, the wallet and prepaid cards allow financial inclusion to a huge population that otherwise would be left behind in the push to a cashless society. The wallet and prepaid card can be loaded with cryptocurrencies like Bitcoin, Ethereum, USDT, USDC, CBDC and other cryptocurrencies.

The prepaid cards will enable users to spend the money on merchant outlets or online shopping malls in a cashless manner. The card can be linked to the mobile wallet and funds can be topped up using debit card, prepaid card, credit card, bank transfer, kiosks, or merchants. Users who are unbanked or

[1] Decentralized Finance

underbanked can use channels like kiosks and cash deposit machines to load their Blockpay Wallet which can be transferred to their Blockpay Cards. In addition, Blockpay also offers virtual cards.

To send money across borders, the fiat currency is converted by Blockpay wallet into a cryptocurrency and transferred via Blockpay blockchain network to the receiver's wallet. The cryptocurrency will be converted into fiat currency and transferred into the prepaid card. The receiver then cashes out the money with a Blockpay card at an ATM. An unbanked sender or receiver can interface with a cash point such as a convenience store chain, telco top-up card, Bitcoin ATM, and even traditional ATMs. Recipients use codes which allow them to withdraw cash without a card and even without a bank account. The remittance flow is as shown in Figure 4.2.

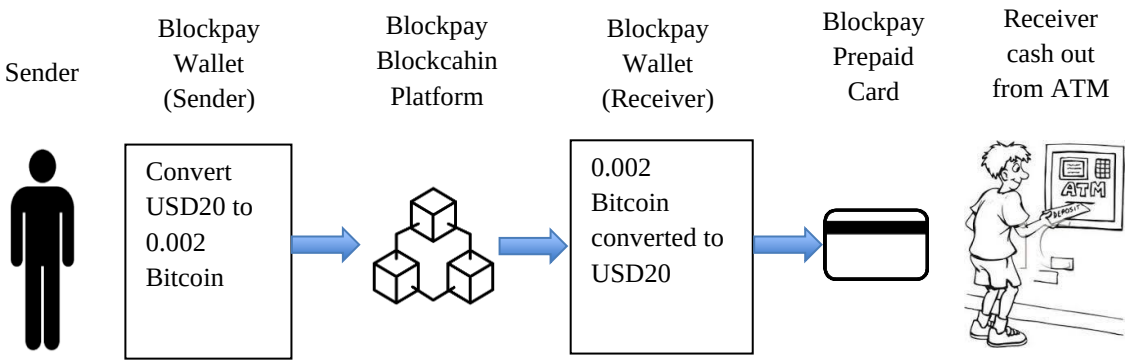


Figure 4.2. The remittance flows.

*Other than Bitcoin, the digital currency can be Ethereum, USDT, CBDC and more. The conversion will be based on the crypto to fiat exchange rates.

This innovative blockchain-based remittance model has the potential to revolutionize the financial landscape in Cambodia. With its secure and transparent nature, this model can provide a seamless and efficient way for individuals to send and receive money across borders. By leveraging the power of blockchain technology, Cambodia's remittance industry can witness enhanced speed, reduced costs, and increased accessibility, ultimately benefiting both the senders and recipients of funds. Embracing this adaptable and forward-thinking solution could pave the way for a more inclusive and technologically advanced financial ecosystem in Cambodia.

4.2. Supply Chain Management (SCM)

Traditional supply chain management faces various challenges that impact the efficiency and cost-effectiveness of operations. One significant challenge is the difficulty in tracking and tracing products throughout the supply chain. This lack of transparency leads to delays, inefficiencies, and increased costs. Additionally, counterfeiting and fraud are pervasive issues, causing substantial financial losses and reputational damage to companies (Bowman, 2018).

Blockchain enables recording of transactional data throughout the supply chain, creating an immutable record of origin and enabling full traceability of products. This transparency optimizes supply-and-demand management, enhances resilience, and promotes sustainable production, logistics, and consumption. Various applications address environmental challenges and corporations face increasing pressure to address supply chain risks, such as corruption, human rights violations, and environmental

degradation. Many companies are making public commitments, but implementing and showcasing achievements is difficult without improved supply chain visibility. Blockchain-based solutions offer transparency and traceability, fostering confidence, exposing illegal activities, reducing costs, improving monitoring and reporting, and potentially preventing litigation. As these solutions become mainstream, companies can demonstrate responsible and ethical operations efficiently, benefiting investors and asset managers. increased transparency builds trust and helps eliminate counterfeit products from the supply chain (World Economic Forum, 2018).

Another benefit of blockchain technology in supply chain management is its potential to combat theft and reduce inefficiencies. Traditional supply chains often suffer from information gaps and delays due to manual processes and disparate systems. Blockchain-based platforms can facilitate the sharing of real-time information among relevant stakeholders, improving collaboration and decision-making. For example, in a case study by IBM, a blockchain platform was used to track and authenticate diamonds across the supply chain (Henderson, 2020). The system reduced the time required for verification, eliminated paperwork, and minimized the risk of theft and fraud. Such efficiencies not only lead to cost savings but also enhance the overall security and integrity of the supply chain.

In short, traditional supply chain management faces significant challenges such as tracking and tracing difficulties, counterfeit products, fraud, and theft. However, blockchain technology offers solutions to address these pain points. By providing transparency, traceability, and real-time information sharing, blockchain can improve the efficiency, security, and cost-effectiveness of supply chains (Bowman, 2018).

Let us delve into the realm of blockchain technology and its potential applications in the supply chain management domain. We will delve into two hypothetical use cases that show promise for adaptation and potential implementation in the Cambodian context. Harnessing the power of blockchain, these innovative solutions have the capacity to revolutionize SCM practices, enhancing transparency, traceability, and efficiency in the country's supply chains. By examining these use cases, we aim to uncover the transformative possibilities that lie ahead for Cambodia's SCM ecosystem.

4.2.1. Blockchain-Powered Smart SCM: Case 1 - Auto Parts Business Case Study

This case study was conducted by Dr. Liew Voon Kiong for Tan Chong Motor Holdings Berhad, the franchise holder and exclusive distributor of Nissan passenger and light commercial vehicles, as well as Renault vehicles in Malaysia.

The automotive supply chain is an overly complex and broad ecosystem, involving a wide range of participants such as parts suppliers, manufacturers, sellers, and aftermarket suppliers. Counterfeit products are a significant issue for automotive manufacturers and suppliers. The counterfeit spare parts market is currently estimated at several billion dollars (Crypto AG, n.d.).

Automotive Supply Chain Issues

Parts supply and management is key to an auto parts business. However, current auto parts supply chain faces many issues including difficulty in tracking of parts, theft of parts, data fraud, counterfeit products.

Ensuring consistent accuracy and error-free processes is of utmost importance for automotive suppliers, as it guarantees the prompt delivery of correct parts to their intended destinations.

Counterfeit products pose a significant challenge for automotive manufacturers and suppliers, with the illicit market for counterfeit spare parts estimated to be worth several billion dollars. These fraudulent components, being of inferior quality, are prone to failure, resulting in dissatisfied customers and a detrimental impact on brand trust. This issue is particularly critical in the realm of vintage cars, as a counterfeit spare part can substantially diminish the overall value of the vehicle (Liew, 2020).

Confronted with thousands of spare parts, numerous parameters, and manufacturers distributed across regions or globally, the supply chain management team must contend with an immense volume of data. Two most common challenges are:

- The need to keep inventories well-stocked but not overstock.
- The need to deal with the sheer number of recalls.

To address the aforementioned challenges, we propose implementing blockchain technology. Blockchain technology offers enhanced transparency throughout the supply chain, leading to substantial cost reductions and simplified business operations with multiple parties. Automakers and suppliers can derive unique advantages from blockchain technology, including safeguarding their brands against counterfeit products and improving the brand experience by implementing customer-centric business models.

Benefits of blockchain-powered SCM in the auto parts industry

Identification and Tracking of Automotive Spare Parts

Counterfeit Protection – Verifying Authenticity and Origin

Counterfeit products pose a significant challenge for automotive manufacturers and suppliers, with the counterfeit spare parts market currently valued at several billion dollars. These counterfeit spare parts are typically of inferior quality, making them more prone to failure. Consequently, this not only disappoints customers but also erodes trust in the brand.

A collaborative partnership can be established between the parties, ensuring the strict confidentiality of sensitive business information. This confidentiality is achieved through the utilization of blockchain cryptographic methods, protecting against not only internal manipulators within the business network but also external attackers. A spare parts service center, for example, can effectively verify the authenticity of a part during replacement by leveraging the immutability of blockchain. This tamper-proof solution ensures a single source of truth, leading to fewer disruptions for customers and enhancing the trust relationship with the manufacturer.

Protection of Aftermarket Business

The global aftermarket business was valued at over 800 billion USD in 2018 and is projected to exceed a trillion USD within the next decade. Vehicle spare parts account for over 50% of this market, with the business divided between OEM (Original Equipment Manufacturer) and IAM (Independent Aftermarket) Suppliers. With each product or part having a unique representation on the blockchain, this technology enables the enforcement of business terms pertaining to precise production volume and

timing. Moreover, this level of enforcement can be extended to manufacturers employing a dual sourcing strategy with multiple suppliers.

Spare Parts Liability Resolution

To expedite the process of replacing a failed spare part and establish liability, it is crucial to trace the part back to its manufacturer. By leveraging blockchain technology to digitally represent and identify parts, an accurate and transparent method for tracing their origin can be achieved. Consequently, all parties involved in the blockchain have clear visibility into liability, enabling faster resolution of any disputes and allowing resources to be directed towards customer engagement.

Vehicle Recall Optimization

Numerous recalls are associated with potentially life-threatening product defects, posing a huge liability for automakers. By leveraging blockchain technology, both the vehicle and its individual components can be meticulously recorded on the blockchain. If automakers possess precise information regarding the installation of defective parts in specific cars, they can execute recalls with utmost accuracy. Consequently, this implementation would lead to substantial cost savings for manufacturers.

Optimizing the Supply Chain Process

Inbound Logistics and Smart Manufacturing

Efficient planning of production capacity necessitates seamless coordination among multi-tier suppliers, third-party logistics, and transportation companies within the manufacturing plant. The complex and error-prone task of tracking and tracing individual parts across the inbound supply chain is further compounded by the lack of accurate, real-time information, which is scattered across disparate databases.

By utilizing a distributed and immutable blockchain ledger shared among all involved parties, a comprehensive and precise record of the status, quantity, and whereabouts of each component can be established. This meticulous transparency has the potential to enhance real-time logistics and optimize plant production capacity.

Outbound Logistics Planning

The outbound supply chain in the automotive sector consists of an intricate network that includes manufacturers, distributors, importers, and dealers. Similar to the inbound supply chain, participants in the outbound supply chain lack a common data sharing model. Having a shared blockchain-based system across the different participants will offer transparency and visibility. This will ensure faster transactions by lowering settlement periods.

Business Model Innovation

Car Personalization and Customer Engagement

Driver profile along with car customization preferences can be saved in a personal blockchain wallet. Shared or leased cars will authenticate the driver using the wallet and the car settings are personalized based on the driver profile. Besides that, automakers and mobility operators can thus create new business models focusing on individual preferences.

Dynamic Pricing Models in Automotive Insurance and Leasing

A driver profile, encompassing miles driven, efficient vehicle usage, and accident history, is securely stored on the blockchain. Users can share this data with insurance and leasing providers who offer personalized products based on their driving profile. The key advantage of utilizing blockchain technology in this context is the immutable storage of the driver profile and historical events, ensuring a reliable and trustworthy source of information. Providers can rely on this single source of truth for offering personalized products with dynamic pricing, while users have access to better priced products and get incentivized for good driving behavior.

Digital Car Wallet

The ownership history, maintenance, and repairs of a vehicle can be securely stored in a blockchain-based car wallet, ensuring transparency and verifiability. This enables the establishment of a reliable ownership record and fair price assessment for second-hand cars, expediting the transfer of ownership process.

By leveraging the unique identification of vehicles on the blockchain, stolen cars can be effortlessly tracked and traced, enhancing security measures. Additionally, the transfer of ownership becomes significantly smoother, reducing both trust issues and business friction. Moreover, when repairs and parts replacements are accurately tracked on the blockchain, warranty claims become transparent to all parties involved, fostering a more efficient and reliable process.

Car-to-Infrastructure Transactions

Blockchain technology offers a unique way to automate transactions between machines and enable the future of M2M (machine to machine) commerce. Cars in the future will be equipped with blockchain-based wallets, and transactions with toll booths, park stations and electric charging outlets will be automated without manual intervention.

The Proposed Blockchain SCM Model

The current auto parts SCM model is complex and inefficient as the channel members work in silos and do not have access to shared databases, as shown in Figure 4.3.

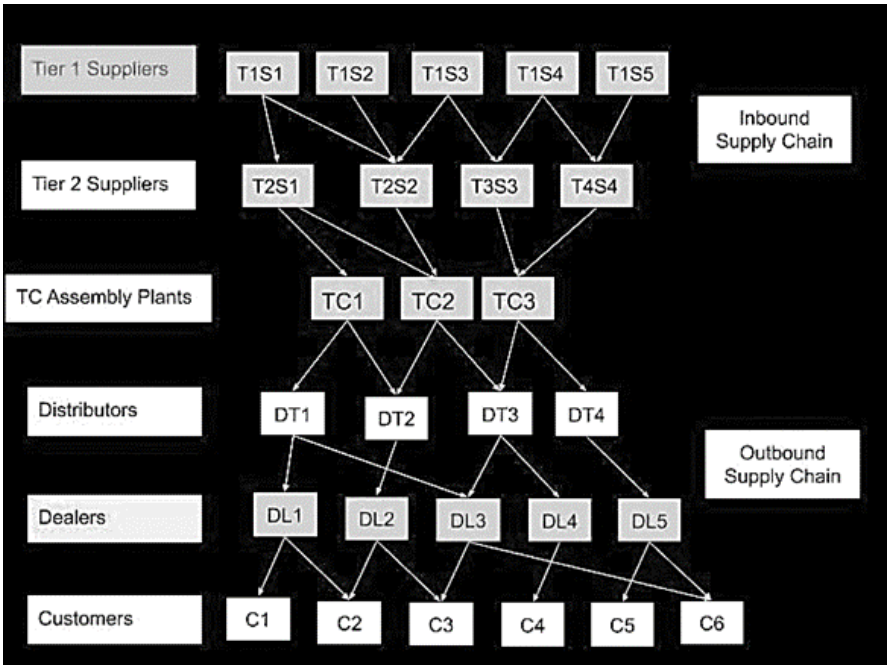


Figure 4.3. The current auto parts supply chain management model. The shortcuts in the figure are: T1S1-Tier1 Supplier, T2S1-Tier2 Supplier, TC-Tan Chong (Name of Tan Chong Motors), DT-Distributor, DL-Dealer, C-Customer.

The proposed blockchain smart supply chain model is based on the Hyperledger Fabric Framework. The channel members will be more interconnected and have better access to shared common ledger. The model is illustrated in Figure 4.4.

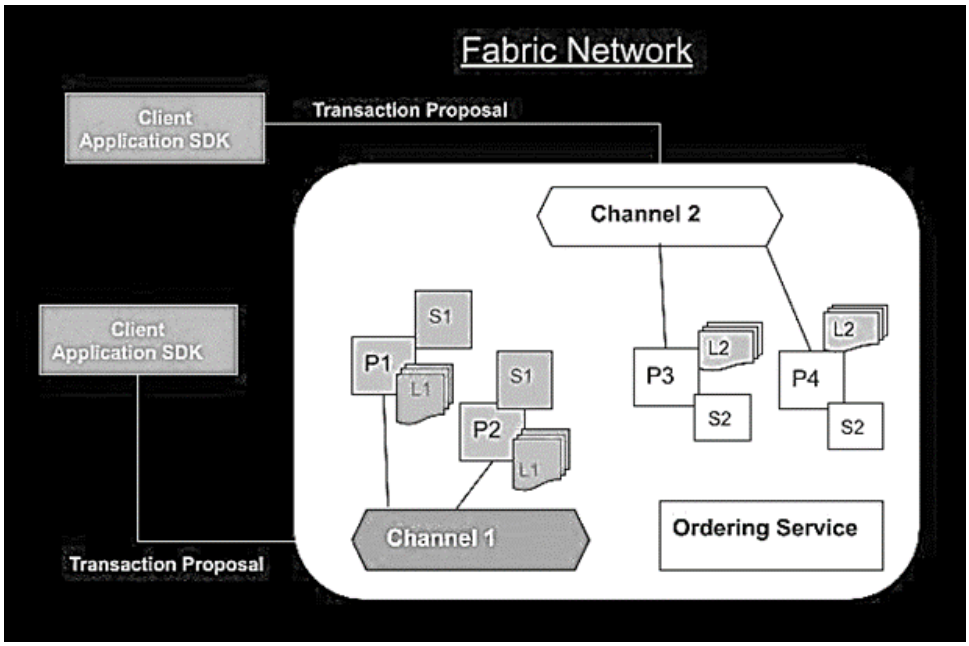


Figure 4.4. Fabric Network.

Figure 4.4 shows two channels, channel 1 and channel 2. Each channel has its own application, peers, ledger, and smart contract (chaincode). In this example, channel 1 has two peers, P1 and P2 and channel 2 also has two peers, P3 and P4. Ordering service is the same across any network and channel.

Application 1 will send transaction proposals to channel 1. P1 and P2 will then simulate and commit transactions to ledger L1 based on chaincode S1. On the other hand, Application 2 will send transaction proposals to channel 2. P3 and P4 will simulate and commit transactions to ledger L2 based on chaincode S2. Further illustration of channels can be found in Figure 4.5.

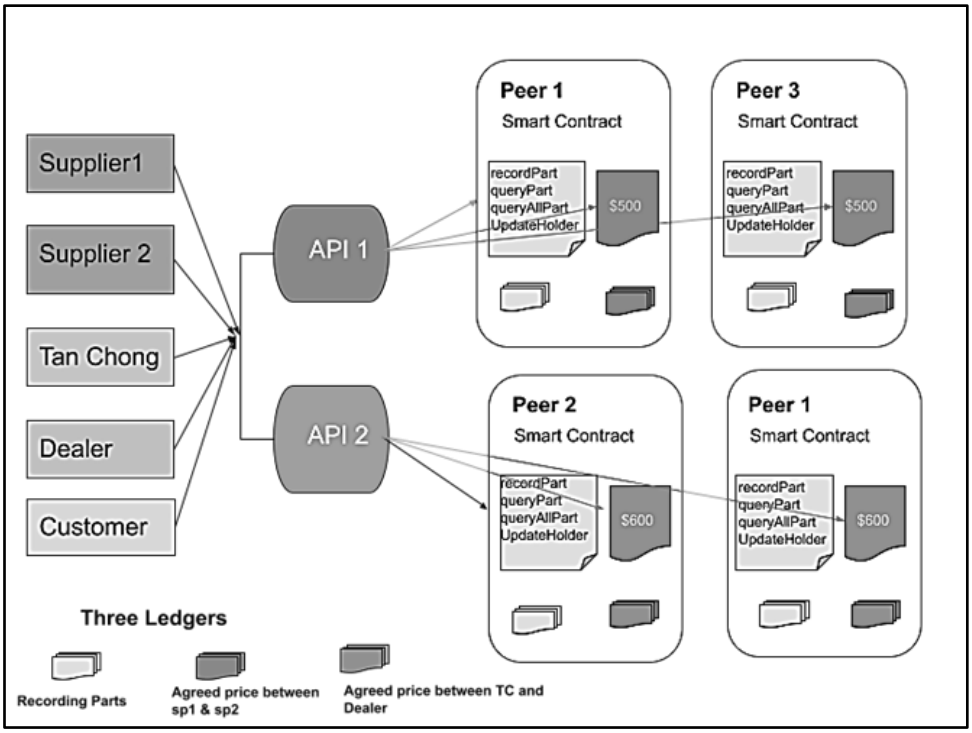


Figure 4.5. Blockchain Powered SCM. *Tan Chong is a fictitious name of a car assembler.

The SCM blockchain network can be hosted on a secure server like AWS, as illustrated in Figure 4.6.

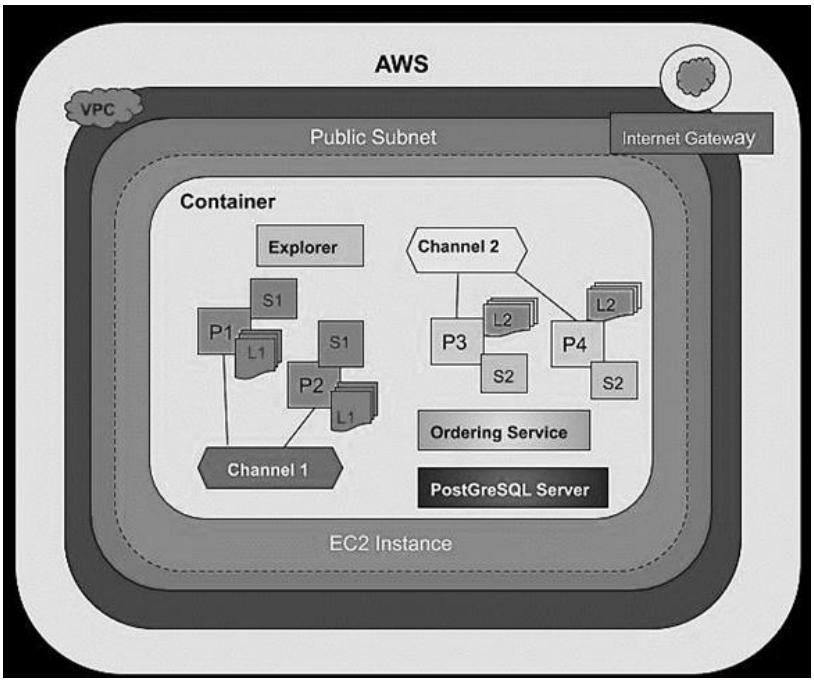


Figure 4.6. An example in which Amazon Web Service (AWS) hosts a SCM blockchain network.

4.2.2. Blockchain-Powered Smart SCM: Case 2 - Textile Industry

This case study was done for a company based in Dhaka. It examined the issues faced by the Bangladesh textile industry and provides a possible solution based on blockchain. Figure 4.7 outlines the complexity of the textile supply chain in Bangladesh.

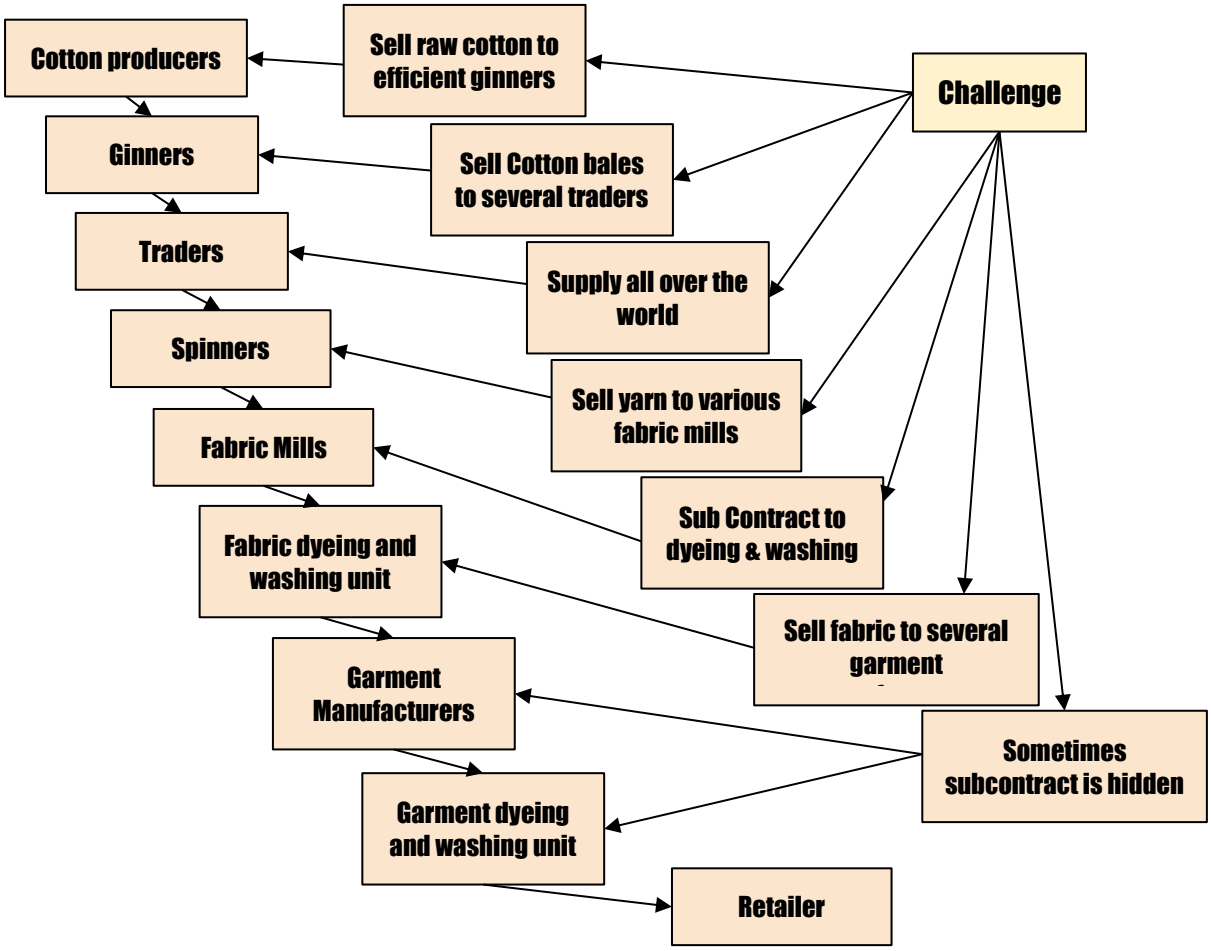


Figure 4.7. Textile Supply Chain Challenges in Bangladesh.

The supply chain demonstrates the traceability of cotton, starting from the firm holder and extending to the retailer. Cotton serves as a crucial input in the apparel industry. To produce a single T-shirt using conventional cotton, a staggering 2700 liters of water are required. In today's context, sustainability has emerged as a vital consideration, and apparel brands face the challenge of insufficient time and resources to oversee every aspect of the supply chain, including crop production and retail. However, a major obstacle they encounter is the lack of knowledge regarding the origin of the cotton they utilize (Liew, 2020).

The textile supply chain, from the raw product to the retailer trade, remains excessively complex, making it nearly impossible to trace a textile back to its place of origin due to secretive supply structures within the textile and clothing industry. However, to promote sustainability, cotton traceability is gaining significance. By leveraging technology for traceability, it becomes feasible to track each production step at every level of the production chain.

- **Cotton Producers:** Small firm holders cultivate and harvests the cotton crops, which are delivered to ginners. For traceability, cotton producers can give a unique code or tag to their raw cotton.
- **Ginners:** Cotton bales are classified according to fiber strength, length, color, non-fiber content and fineness. Ginners sell cotton bales to various cotton traders.
- **Traders:** Traders usually buy cotton bale from various sources and sell it to spinning mills all over the world. So, traceability is difficult for the textile industry. For traceability, cotton bales need a bar code or tag.
- **Spinners:** Spinning mills buy cotton bales from several traders. Using a traceability system, they can get information about their cotton bales.
- **Fabric Mills:** Fabric mills buy yarn from various sources. Sometimes, it can come from foreign spinning mills. So, traceability can be more complex.
- **Dyeing & Washing Unit:** Sometimes fulfills fabric demand. Fabric mills may have a subcontract with another unit or engage in outsourcing.
- **Garment Manufacturers:** Every garment manufacturer buys fabric from various sources. And sometimes they have a hidden subcontract with other units.
- **Retailers:** Retailers are the final sellers to consumers. Due to sustainability issues, they want to trace their whole supply chain. Every product could have a unique code or barcode that gives customers all the information about that product, from cotton production to retailer.

The traditional SCM is excessively intricate due to channel members operating in isolation and lacking access to shared databases. This can be visualized in Figure 4.8, illustrating the SCM model.

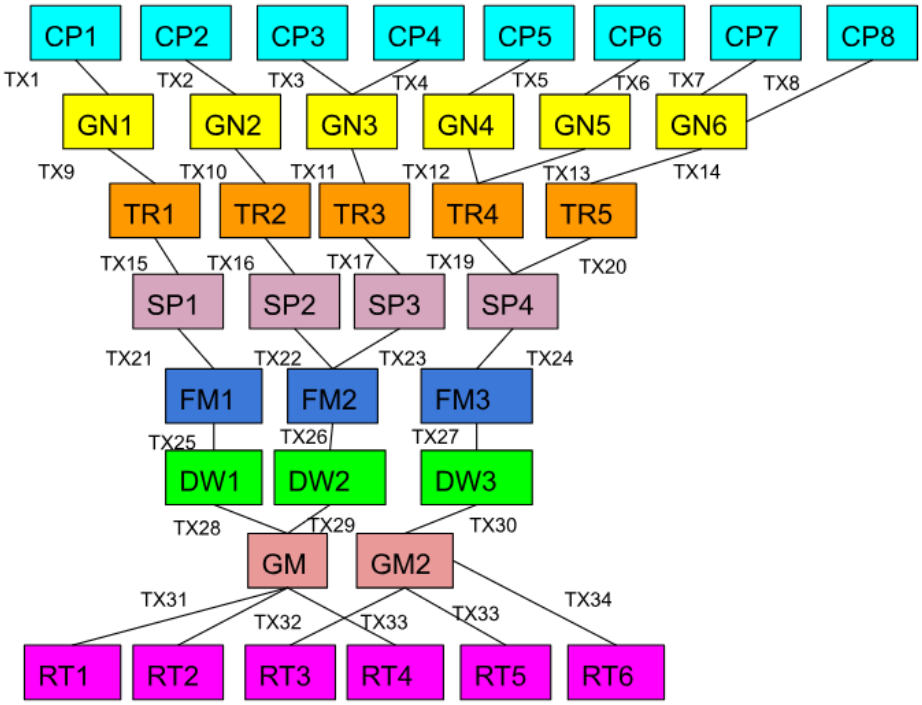


Figure 4.8. Transaction Flow of Traditional SCM. The shortcuts in the figure are CP-Cotton Producer, GN-Ginner, TR-Trader, SP-Spinner, FM-Fabric Mill, DW-Dyeing & Washing, GM-Garment Manufacturer, RT-Retailer.

The Blockchain Solution

An effective solution entails the creation of a textile blockchain network, which would be hosted on a cloud server, as depicted in Figure 4.9. The architecture of this blockchain network follows the Hyperledger Fabric Framework. Channel APIs will facilitate the recording of transactions among channel members, with peer nodes responsible for submitting the data to a blockchain platform hosted on a cloud server. Validator nodes will then validate and permanently record the transactions on the blockchain, while smart contracts (chaincode) execute the necessary functions. The updated blockchain will be broadcasted across the entire Textile Blockchain Network, enabling every channel member to trace and track their product ID. This can be done by scanning a QR code connected to the network via a UI linked to the channel APIs. The transaction details are saved in the world state as a key/value pair based on the specifications of a chaincode contract, allowing Ali's API to effectively create a transaction on the ledger. This solution will ensure trust, transparency, traceability and trackability in textile supply chain management.

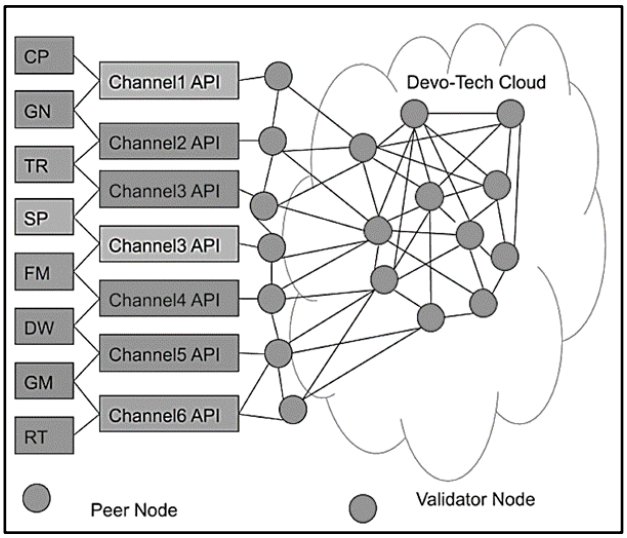


Figure 4.9. Architecture of textile blockchain network solution that is hosted in Devo-Tech Cloud server. The shortcuts are CP – Cotton Producer, TX – Transaction, GN – Ginners, TR – Traders, SP – Spinners, FM – Fabrics Mills, DW – Dyeing and Washing, GM – Garment Manufacturers, RT – Retailers. Devo-Tech is the name of a technology park in Dhaka.

4.3. Healthcare and Public Services

4.3.1. Blockchain in Healthcare

Blockchain technology has the transformative potential to revolutionize the healthcare industry by prioritizing the patient as the focal point of the healthcare ecosystem, while simultaneously enhancing the security, privacy, and interoperability of health data. Through the utilization of this technology, electronic medical records can become more efficient, disintermediated, and secure, offering a promising alternative model for health information exchanges (HIE). Although it is not a universal solution, this rapidly evolving field presents abundant opportunities for experimentation, investment, and proof-of-concept testing (Deloitte, n.d.).

The assurance of authenticity in medical goods holds great importance within the healthcare sector, and the challenge can be effectively addressed through the utilization of blockchain technology. Blockchain in healthcare has proven to be valuable for supply chain management of medical goods, as it guarantees the provenance of medical goods, thereby confirming their authenticity. (STL Partners, n.d.). MediLedger stands out as a prominent blockchain protocol that empowers companies throughout the prescription drug supply chain to authenticate medicines, along with verifying crucial details such as expiry dates and other significant information.

Another potential use case of blockchain in the healthcare sector involves the efficient management of electronic medical records (EMR) to tackle the problem of data silos. In the conventional approach, medical records are possessed by individual clinics and hospitals operating in silos, hindering data sharing, and leading to treatment delays. Data silos pose a significant challenge for healthcare systems worldwide, as they result in fragmented medical histories, limiting patients and healthcare providers from accessing comprehensive information. In 2016, research published by Johns Hopkins University revealed that the third most common cause of death in the United States was medical errors arising from inadequately coordinated care, including unfulfilled planned actions or omissions in patient records (STL Partners, n.d.).

The blockchain-based system for medical records can integrate with existing electronic medical record software and serve as a comprehensive, unified view of a patient's record. It is important to highlight that the actual patient data is not stored on the blockchain. Instead, each new record added to the blockchain, such as a physician's note, a prescription, or a lab result, is converted into a distinct hash function. Each hash function is unique and can only be deciphered with the patient's consent, ensuring protection against data breaches, and ensuring privacy. Each time a patient record is amended, or a patient agrees to share a portion of their medical record, it is recorded as a transaction on the blockchain. Medicalchain stands as a prominent company collaborating with healthcare providers to incorporate blockchain-enabled EMRs (STL Partners, n.d.).

The main advantages of blockchain based EMR are as follows:

- Establish a comprehensive and reliable single source of truth for a patient's medical records, resulting in an enhanced experience for both patients and healthcare providers.
- Patients have the ability to track every update made to their medical records and provide explicit consent whenever they are shared with healthcare providers or any other parties. Additionally, patients can choose to share their medical records, or specific parts of them, with researchers and set time limitations on how long third parties can access their medical information.
- Medical insurers can promptly receive validated confirmation of healthcare services directly from patients, eliminating the need for intermediaries and reducing both time and costs involved.

The following section explores a blockchain-based healthcare case study that holds immense promise for implementation in Cambodia.

4.3.2. Case Study: Vaccine Management System (VMS)

The coronavirus pandemic has drawn attention to various uses of blockchain technology, one of which is the suggestion to utilize blockchain as the most efficient method for distributing the stimulus package in the United States. Additionally, the Chinese government has integrated blockchain technology into multiple applications to enhance their efforts in combating COVID-19. They employ distributed ledger

technology (DLT) to monitor the transmission of the virus, manage medical records, and facilitate the distribution of medical supplies and charitable donations. To combat the outbreak, the World Health Organization (WHO) has initiated the implementation of a DLT platform for sharing COVID-19 pandemic data. Furthermore, numerous companies and non-profit organizations have also introduced blockchain-based projects to address the COVID-19 outbreak (Liew, 2020).

The Malaysian Government has developed and implemented a system to combat the COVID-19 virus, known as the Vaccine Management System (VMS), as shown in Figure 4.10. VMS is a pilot project under the National Blockchain Roadmap and has been developed by MIMOS. It utilizes Hyperledger Fabric blockchain technology and effectively governs the management of COVID-19 vaccines, offering valuable support to the COVID-19 National Immunization Program (Program Imunisasi Covid-19 Kebangsaan or PICK) (Malaysian Government, n.d.).

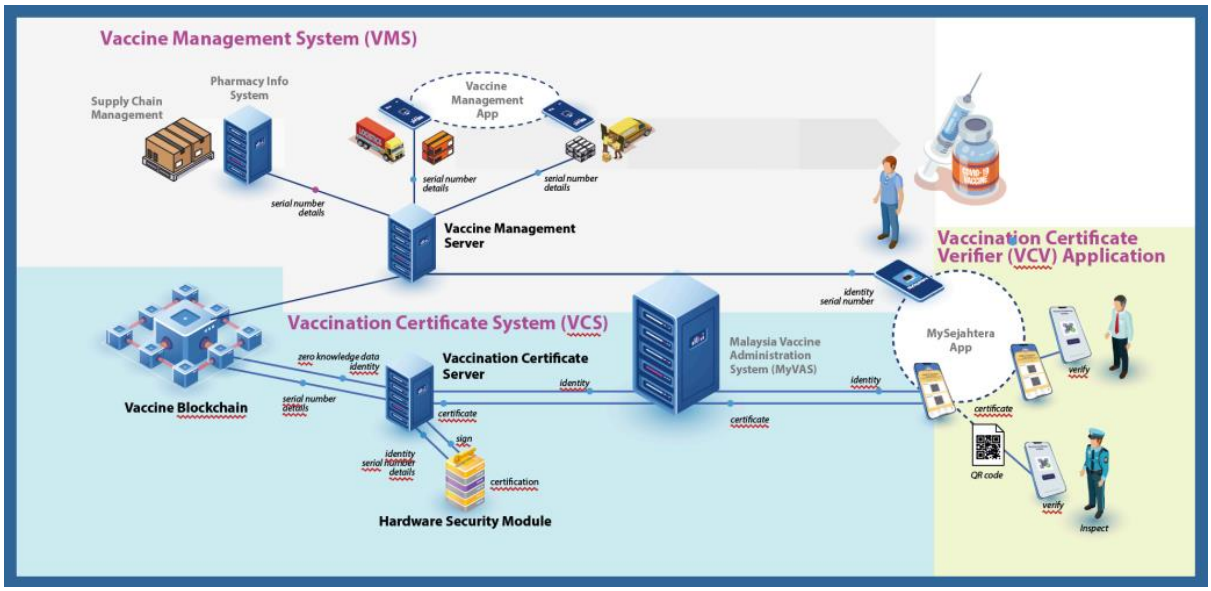


Figure 4.10. Vaccine Management System (Ministry of Science, Technology & Innovation, 2022).

It is designed to prevent counterfeit vaccines and generate digital vaccination certificates. This system ensures visibility of the Covid-19 vaccine throughout the entire supply chain, from the manufacturer to individuals at the Pusat Pemberian Vaksin (PPV). Additionally, this initiative enhances traceability and security for both the vaccines and their recipients, while also storing and generating vaccination information for cross-border travel. The system has the potential for future expansion to include other types of drugs and vaccines. The COVID-19 vaccination program received full support from the Ministry of Health (MOH), the authorized governing body of the project.

VMS enables the tracking of vaccine movements throughout the supply chain process until they are received by recipients, providing traceability based on the serialized number to identify the vaccine receiver. It also provides a Digital Health Certificate to the authority when necessary, indicating the vaccination status. Additionally, VMS helps prevent counterfeit vaccines and allows for checking the vaccination status for subsequent doses. Furthermore, patients can provide feedback through MySejahtera regarding any symptoms experienced as a result of the vaccination (Malaysian Government, n.d.).

The implementation of VMS contributes to the achievement of Sustainable Development Goal (SDG) initiatives, specifically SDG 8, which focuses on promoting decent work and economic growth, and SDG 9, which aims to build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation.

The Vaccine Management System (VMS) comprises two components: Vaccine Logistic Tracking (VLT) and Post Vaccination & Proof of Vaccination (PoV), as depicted in Figure 4.11 and Figure 4.12. VLT is utilized by the Division of Pharmacy Services Program (Bahagian Program Perkhidmatan Farmasi or PPF) and is integrated with the Pharmacy Information System (PhIS) and Clinic Pharmacy Information System (CPS). On the other hand, PoV is implemented through MySejahtera[1].

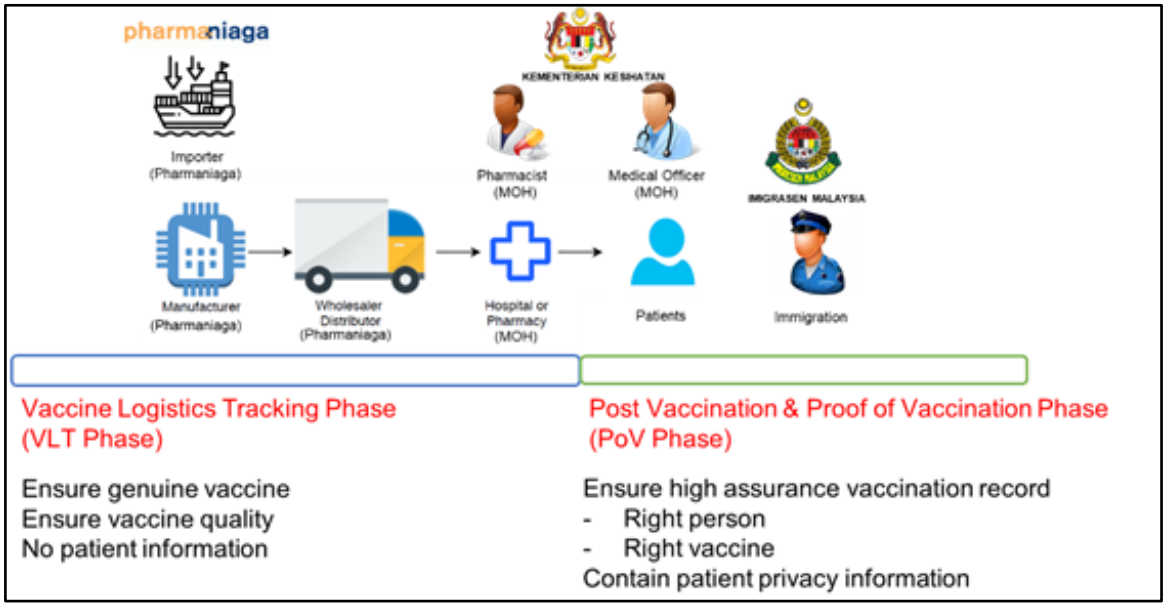


Figure 4.11. VLT and PoV components in VMS (Malaysian Government, n.d.).

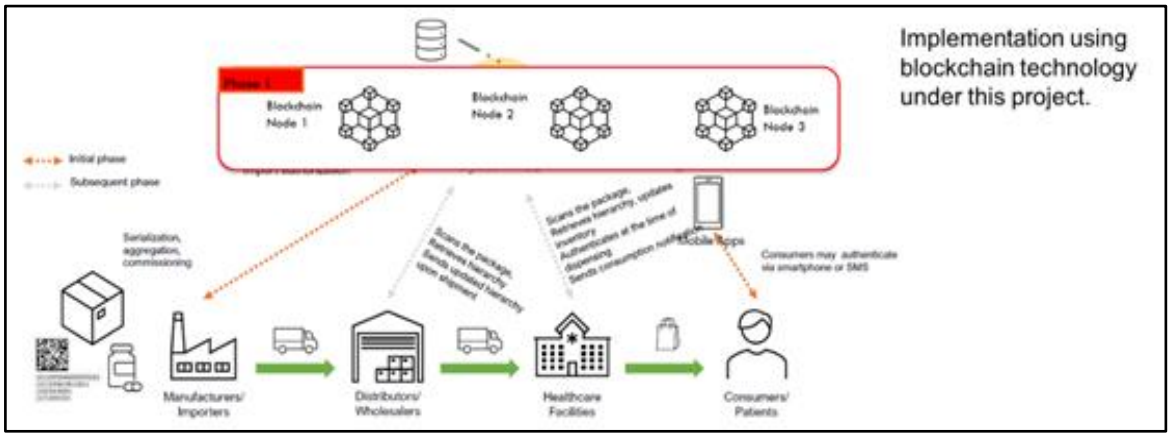


Figure 4.12. Track and Trace (VLT) execution model (Malaysian Government, n.d.).

Figure 4.13 depicts the process of an individual receiving a vaccine at PPV. The individual scans the GS1 code using the MySejahtera app, and the data is then transmitted to the VMS server through

[1] MySejahtera is an application which was developed to assist the Government in managing the COVID-19 outbreak in Malaysia.

MyVAS. The transmitted data includes information such as the individual's name, identification card number, PPV location, and the name of the medical officer (MO).

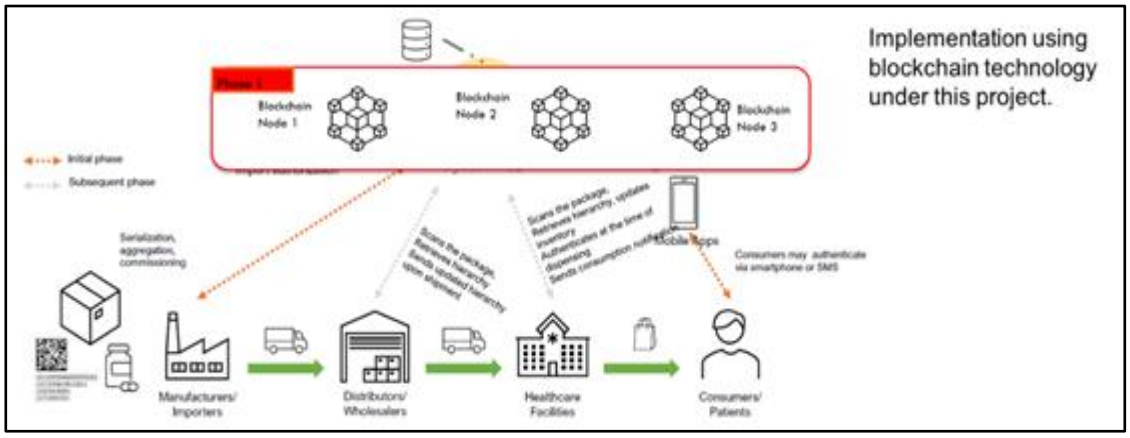


Figure 4.13. PoV execution model (Malaysian Government, n.d.).

4.4. Blockchain in Public Services

Governments and public sector organizations are increasingly adopting blockchain technology as a solution to replace siloed and inefficient centralized systems. Traditional systems are inherently insecure and costly, whereas blockchain networks provide enhanced security, agility, and cost-effectiveness, making them a compelling alternative (Consensys, n.d.).

A blockchain-powered digital government offers a range of benefits, including enhanced data protection, streamlined processes, and reduced instances of fraud, waste, and abuse. By adopting a blockchain-based government model, individuals, businesses, and governments can collaborate and share resources through a secure distributed ledger protected by cryptography. This decentralized structure eliminates the risk of a single point of failure, ensuring the safeguarding of sensitive citizen and government data while promoting trust and accountability (Consensys, n.d.).

Now, we delve into a potential application that revolves around a blockchain-powered digital government. This innovative solution holds immense potential and paves the way for its adaptation and implementation within the borders of Cambodia.

4.4.1. Case Study: Building a Digital Government Powered by Blockchain

This case study was conducted for Datasonic Group Berhad, a prominent security-based ICT solutions provider in Malaysia. It was also presented in a regional blockchain conference.

Digital government represents a cutting-edge approach in public administration science, surpassing the e-government paradigm. Unlike its predecessor, which merely involved digitizing public administration, digital government encompasses the development of novel public services and service delivery models that capitalize on digital technologies, governmental assets, and citizen information. This emerging paradigm prioritizes the provision of user-centric, agile, and innovative public services. Considering its potential, blockchain stands out as a highly innovative digital technology that demands attention within the new framework of governmental policymaking and service delivery (Liew, 2020).

A digital government based on blockchain can safeguard data, streamline processes, and minimize instances of fraud, waste, and abuse, all while enhancing trust and accountability. In a government

model built on blockchain technology, individuals, businesses, and governments collaborate and exchange resources through a decentralized ledger system secured with cryptography. This framework eradicates the risks associated with a central point of failure and inherently safeguards confidential citizen and government information (Consensys, n.d.).

A government built on blockchain technology holds the potential to address long-standing pain points and unlock the following benefits:

- The secure storage of government, citizen, and business data
- Streamlining labor-intensive processes.
- Reducing the excessive costs associated with accountability management.
- Decreased likelihood of corruption and abuse
- Enhanced trust in government and online civic systems.

Estonia embarked on testing blockchain technology as early as 2008, preceding the publication of the Bitcoin whitepaper that introduced the term "blockchain." Since 2012, Estonia has actively employed blockchain in its operations, safeguarding national data, e-services, and smart devices across public and private sectors. The country has notably established the X-Road, a decentralized network system. (Liew, 2020), as shown in Figure 4.14.

Figure 4.14. X-Road, The decentralized public internet (source: https://e-estonia.com/).

The X-Road Public Internet facilitates secure storage and communication of information in a distributed manner, leveraging a robust data exchange layer. Furthermore, this system guarantees interoperability, confidentiality, and integrity across various institutions and platforms. The exchange authentication incorporates multi-level authorization and meticulously maintains processing logs. Furthermore, not only is all the data encrypted and signed, but also all the involved parties are clearly and securely identifiable.

The Dubai Blockchain strategy, on the other hand, aims to fulfill H. H. Sheikh Mohammed bin Rashid Al Maktoum's vision of making Dubai the world's first city fully powered by Blockchain by 2020 and the happiest city on earth. This comprehensive strategy rests on three strategic pillars: Government Efficiency, Industry Creation, and International Leadership, ensuring its success (Liew, 2020).

To establish a digital government, the initial step involves establishing a National Digital Id Blockchain Network. Our proposition is to create a National Digital Id Blockchain Network, employing Ethereum Parity's Proof of Authority (PoA) Consensus Protocol, which will be hosted on the secure cloud server of the National Registration Department (NRD). It is imperative that this blockchain operates as a private permissioned network (see Section 3.1.2 for its definition). Proof of Authority (PoA) is an innovative consensus algorithm family that offers exceptional performance and fault tolerance, making it particularly suitable for blockchain networks, especially private ones. Coined by Gavin Wood, co-founder, and former CTO of Ethereum, PoA introduces a practical and efficient solution. Under the PoA framework, nodes are granted the privilege to generate new blocks based on their demonstrated authority. To obtain this authority and the corresponding right to generate new blocks, a node must successfully undergo a preliminary authentication process (see Section 3.1.4 for more detail).

The PoA consensus protocol offers the following advantages:

- High-performance hardware is not necessary. Unlike PoW consensus (see Section 3.1.4), PoA consensus eliminates the need for nodes to allocate computational resources to solve complex mathematical tasks.
- The generation of new blocks follows a predictable time interval, although this duration may vary for PoW and PoS consensuses (see Section 3.1.4).
- A high transaction rate is achieved by generating blocks in a sequential manner at regular intervals by authorized network nodes. This enhances the speed at which transactions are validated.
- If at least 51% of nodes remain uncompromised, PoA incorporates a ban mechanism for nodes and provides methods to revoke their block generation rights, thereby enhancing resilience against compromised and malicious nodes.

To begin constructing the National Digital Id Blockchain Network, the initial task entails carefully selecting the Notary Nodes (Validator Nodes). These nodes should be individuals of unquestionable trustworthiness and possess a distinguished reputation. Prominent candidates may include esteemed public servants such as the chief judge, minister, lawyer, central bank governor, and NGO president, among others.

A notary node is a self-reliant individual who stakes their identity and assumes the responsibility of maintaining a network node. This node serves the purpose of validating transactions and incorporating new blocks into the blockchain. In the context of the National Digital Id Blockchain Network, their primary role involves validating data submitted to them, which is then sent back to the registration nodes to finalize the application process and issue identification documents such as Id cards, birth certificates, and other pertinent records. A notary node (validator) has both technical and social responsibilities, both of which are important for the health, performance, and security of the network:

- Technical Responsibilities:
    - Ensure node is secure by practicing safe key management.
    - Maintain node requisite software version.
    - Monitor node to ensure its availability and participation in consensus.
    - Monitor network in general and communicate with other validators and network entities if problems arise.

- Social Responsibilities:
    - Participate in on-chain governance of the network.

- Adding new validators.
- Removing validators, *i.e.*, for compromising security of network, malicious behavior, non-participation in governance.
- Monitor node to ensure its availability and participation in consensus.
- Changing the approve ballot threshold.
- Changing consensus contract.

In addition to the notary nodes, we need to establish registration nodes that consist of directors from branches of the National Registration Department across the country. These registration nodes play a crucial role in receiving and processing various documents and applications such as national Ids, passports, birth certificates, and more. However, their authority is limited to submitting the data to the National Digital Id Blockchain Net for validation by the notary nodes.

To enhance connectivity, the National Digital Id Blockchain Network should establish connections with all ministries, government departments, local councils, government agencies, and institutions. These entities should be granted authorized access to specific data on the shared database, such as tax records, health data, criminal records, and financial status, eliminating the need for paperwork and enabling the creation of a paperless and environmentally friendly e-government system.

Storing biometric data on a blockchain is discouraged. Instead, it is recommended to store any personally identifiable information in off-chain storage as a verifiable claim. This claim should include a cryptographic reference to the data placed on a blockchain, ensuring integrity and provenance. Citizen data is securely stored in the Blockchain as key/value pairs, organized according to document types, as exemplified in the following JSON file:

$ var IC = { id: ‘0001’, name: ‘Ali’, date_of_birth: ‘20070928’, address: { No: ‘108’, street: ‘Avenue 10’, city: ‘New York City’, district: ‘Manhattan’, state: ‘New York’}, date: ‘20190610’, time: ‘1235’, place: ‘PJ01’, biometric_ref: ‘0012abvned’ }.

The National Id Blockchain Net is illustrated in Figure 4.15.

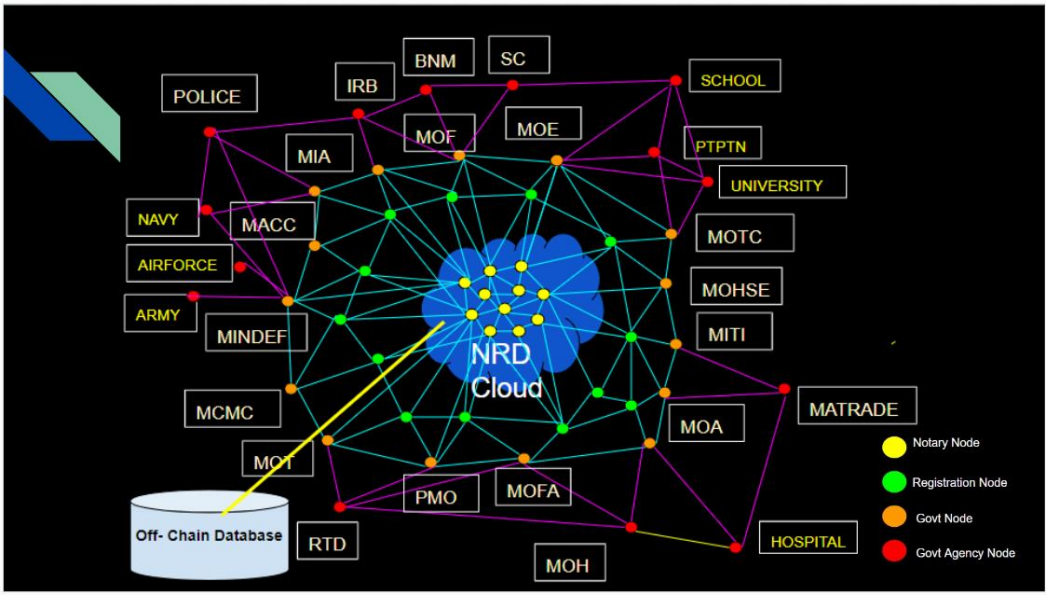


Figure 4.15. National Digital Id Blockchain Net. NRD stands for National Registration Department.

5. Implementation Strategies for Cambodia

The dawn of blockchain technology has arrived, ushering in a new era of transformation and promise for Cambodia. The immense potential to revolutionize various sectors of the country's economy and society is nothing short of extraordinary. Blockchain offers the tantalizing prospect of heightened efficiency, unrivaled transparency, and fortified trust in the nation's systems, propelling it towards a digital frontier of unprecedented possibilities.

However, this untapped potential demands a prudent and strategic approach. Realizing the full benefits of blockchain necessitates a well-calibrated implementation plan, one that is painstakingly tailored to the distinct needs and challenges faced by Cambodia. As the nation embarks on this ground-breaking journey, it is essential to lay the groundwork for a seamless integration of this transformative technology.

5.1. Capacity Building in Cambodia

In the pursuit of transforming itself into a leading player in the adoption of blockchain technology, Cambodia recognizes that its most asset lies in its people. The nation's visionary approach emphasizes the strategy of capacity building, aiming to empower its workforce with the knowledge and skills required to navigate the intricacies of blockchain and harness its revolutionary potential.

At the heart of this transformative journey lies the National Science, Technology & Innovation Policy 2020-2030, meticulously crafted to strengthen Cambodia's STI foundation and induce a surge in human resources dedicated to science and technology, research and development. Moreover, the policy endeavors to enhance the STI ecosystem, encompassing regulatory frameworks, relevant laws, and fostering synergy among organizations, all geared towards creating an innovation-enabling environment for sustainable and inclusive development. To concretely achieve the objectives of the National STI Policy, Cambodia has charted a path through the Cambodia’s STI Roadmap 2030. This roadmap serves as a guiding beacon for government ministries and relevant institutions, setting clear objectives and defining key actions to be taken in the short and medium terms, all aimed at realizing specific targets by 2030. Education stands tall as one of the pivotal pillars of this roadmap, highlighting the pressing need to build and nurture human capital in the STI fields. By cultivating a culture of scientific, digital, and entrepreneurship literacy from early stages of basic education, Cambodia aims to breed a new generation of brilliant minds, budding scientists, and visionary innovators. Furthermore, the roadmap advocates for the adoption of Science, Technology, Engineering, and Mathematics (STEM) education in higher education, empowering the youth with technological readiness and a profound understanding of these disciplines. This strategic investment ensures that Cambodia remains well-positioned in the ever-evolving landscape of innovation. As a significant consequence of this capacity-building effort, Cambodia's workforce will be increasingly proficient in handling cutting-edge technologies. The nation's growing expertise in science and technology will naturally spark curiosity and exploration of emerging technologies like blockchain. This newfound technological readiness and proficiency create an environment conducive to the widespread adoption of blockchain solutions across diverse sectors. Recognizing the importance of collaboration with the private sector, the roadmap proposes strengthening partnerships with technical and vocational education and training (TVET) institutions. This alliance will equip the workforce with industry-relevant skills, ensuring seamless integration with the fast-paced, tech-driven world.

Cambodia firmly believes that strategic development of human resources is the bedrock upon which the promotion of STI thrives. Through an unwavering commitment to capacity building, the nation aspires to carve its place in the forefront of the blockchain revolution. By fostering a highly skilled and innovative workforce, Cambodia sets the stage for embracing blockchain technology across sectors and shaping a prosperous future driven by technology and innovation. By investing in capacity building, Cambodia can foster innovation, entrepreneurship, and a robust ecosystem that attracts both local and foreign blockchain-related investments. Furthermore, a well-prepared workforce can lead the charge in adopting blockchain technology across sectors such as finance, agriculture, healthcare, supply chain, and governance, propelling Cambodia towards greater efficiency and transparency.

Building a Skilled Workforce:
Capacity building begins with education and training programs targeted at various levels of expertise. For students and young professionals, introducing blockchain-related courses and certifications in universities and vocational institutions can lay the groundwork for a skilled future workforce. Government-sponsored scholarships and grants can encourage students to pursue specialized blockchain education both domestically and abroad.

Workshops and Training for Professionals:
For those already in the workforce, organizing workshops, seminars, and training sessions on blockchain's technical aspects and real-world applications can be highly beneficial. By bringing in experts and practitioners, these sessions can foster a deeper understanding of the technology and inspire professionals to explore innovative blockchain solutions for Cambodia's unique challenges.

Public Awareness and Engagement:
Public awareness and engagement are crucial components of capacity building. The government, in collaboration with relevant stakeholders, can launch public campaigns, webinars, and public forums to educate citizens about blockchain technology. By fostering a better understanding of blockchain's potential and dispelling misconceptions, the public can become more receptive to its implementation in various sectors of society.

Establishing Centers of Excellence:
Creating centers of excellence for blockchain research and development can serve as hubs for cutting-edge knowledge and expertise. Collaborations between universities, research institutions, and private enterprises can facilitate knowledge sharing, spur innovation, and attract international partnerships.

Supporting Local Startups and Innovators:
Encouraging and supporting local startups and innovators working on blockchain projects is essential. Establishing innovation funds, incubators, and accelerators dedicated to blockchain can provide much-needed financial and mentoring support to entrepreneurs with groundbreaking ideas. In addition, organizing blockchain hackathons and competitions can nurture a vibrant ecosystem of homegrown talent.

Government-led Training Initiatives:
The government can take a leadership role in capacity building by organizing targeted training initiatives for public officials. Empowering policymakers, regulators, and government employees with blockchain expertise will facilitate informed decision-making, fostering an environment conducive to blockchain adoption.

Long-term Perspective:
Capacity building is a continuous process that requires a long-term perspective. The government, academia, and private sector must collaborate to develop a sustainable ecosystem for blockchain education and skill development. A roadmap outlining the nation's vision for blockchain capacity building can serve as a guiding framework for strategic planning and resource allocation.

As Cambodia invests in capacity building, it will pave the way for a skilled and competent workforce capable of harnessing the full potential of blockchain technology. A well-informed and capable workforce will not only drive the adoption of blockchain solutions across industries but also spur innovation and entrepreneurship, positioning Cambodia as a regional leader in the ever-evolving blockchain landscape. By unlocking the potential of blockchain expertise within its people, Cambodia can build a solid foundation for its digital transformation and secure its place in the forefront of the global technological revolution.

5.2. Public-Private Partnerships in Cambodia

Public-private partnerships (PPPs) can be a valuable tool for the implementation of blockchain technology in Cambodia. The Law on Public-Private Partnerships was enacted in November 2021. The law provides the legal framework for PPPs in Cambodia. It defines PPPs as "a contractual arrangement between the Government and a private party, whereby the private party agrees to finance, design, build, operate, maintain or transfer a public asset or a public service in return for a specified return."

The law sets out the different types of PPPs that can be undertaken in Cambodia, as well as the procedures for establishing and managing PPP projects (MEF, Law on Public-Private Partnership, 2021). It also establishes a General Department of Public-Private Partnerships (GDPPP) to act as the secretariat for the Ministry of Economic and Finance (MEF) and oversee the implementation of PPPs.

The law is seen as an important step in promoting PPPs in Cambodia. It provides a clear and transparent legal framework for PPPs, which will help to attract private investment in these projects. The law also provides for the establishment of the GDPPP, which will help to ensure that PPP projects are implemented effectively and efficiently.

Government also has recognized the importance of PPPs for the development of science, technology, and innovation (STI), the digital government, and the digital economy and society. This is evident in several policy and framework documents, such as the Cambodia STI Roadmap 2030, the Cambodia Digital Government Policy, and the Cambodia Digital Economy and Society Policy Framework 2021-2035. These documents all identify PPPs as a strategic or policy direction for the development of STI, digital government, and the digital economy and society in Cambodia (MISTI, 2021; MPTC, 2022; MEF, 2021). There are several benefits to PPPs for blockchain technology in Cambodia.

The use of PPPs for blockchain technology in Cambodia has the potential to bring several benefits. These benefits include:

- Reduced costs of development and implementation
- Increased speed and efficiency of development
- Increased innovation and creativity
- Increased trust and cooperation between the public and private sectors
- Increased social and economic impact.

The Need for PPPs

There are several reasons why PPPs are important for the development and adoption of blockchain technology in Cambodia.

First, blockchain technology is a complex and expensive technology to develop and implement. This means that it is often beyond the resources of a single organization. PPPs can help to pool resources from both the public and private sectors, which can help to reduce the costs of development and implementation.

Second, blockchain technology is often used in conjunction with other technologies, such as artificial intelligence and machine learning. This means that it requires a wide range of expertise that may not be available within a single organization. PPPs can help to bring together different organizations with different areas of expertise, which can help to ensure that blockchain projects are successful.

Third, blockchain technology is still in its early stages of development. This means that there is a need for collaboration and cooperation between different organizations in order to share knowledge and resources. PPPs can help to facilitate this collaboration and cooperation, which can help to accelerate the development and adoption of blockchain technology in Cambodia.

A Comprehensive Strategy for PPPs in Blockchain Technology

The way forward for public-private partnerships (PPPs) for blockchain technology in Cambodia is to develop a comprehensive strategy that addresses the challenges and takes advantage of the opportunities. This strategy should include the following elements:

- **The development of a clear and transparent regulatory framework for PPPs**: This framework should provide guidance on the roles and responsibilities of the public and private sectors, as well as the terms and conditions of these partnerships.
- **The development of capacity building programs for the public and private sectors**: This includes training government officials and private companies on the principles of blockchain technology, as well as the legal and regulatory framework governing its use.
- **The promotion of trust and cooperation between the public and private sectors**: This is essential for ensuring that these partnerships are successful and that the benefits of blockchain technology are realized.

By taking these steps, Cambodia can reap the benefits of this cutting-edge technology. Some specific examples of PPPs that could be undertaken in Cambodia include:

- The Royal Government of Cambodia (RGC) could partner with a private company to develop a national blockchain infrastructure.
- The RGC could partner with a private company to develop blockchain-based applications for government services.
- The RGC could partner with a private company to provide blockchain training and education programs.

With these initiatives, the RGC can help to ensure that the country has the infrastructure, applications, and workforce necessary to support the development and adoption of blockchain technology.

5.3. Regulatory Framework in Cambodia

The regulatory framework for blockchain in Cambodia is still in its early stages of development. It is very important to create a regulatory environment that is supportive of blockchain innovation, while also protecting consumers and investors.

In 2017 the National Bank of Cambodia (NBC) issued a statement that did not explicitly ban cryptocurrencies but did state that they were not legal tender and that any transactions involving them would be subject to prior business licensing (NBC, Cambodia to ban the trading of Crypto currency such as Bitcoin, 2017). In 2018, the NBC, the Securities and Exchange Regulator of Cambodia (SERC), and the General-Commissariat of the National Police issued a joint statement that reiterated the position that cryptocurrencies were not legal tender and that any unlicensed activity involving them was prohibited. However, the statement also acknowledged the potential benefits of blockchain technology and indicated that the authorities were open to discussing the development of a regulatory framework for its use (NBC, SERC & NP, Joint statement between NBC, SERC, and the General Commissariat of the National Police, 2018).

In 2022, the SERC and Binance, a leading cryptocurrency exchange, signed a memorandum of understanding (MoU) to collaborate on the development of a regulatory framework and bolstering the digital asset businesses in Cambodia (SERC, 2022; Binance, 2022). Under the MoU, Binance will provide technical advice and training to the SERC, and the two organizations will work together to develop a pilot trading platform for digital assets.

The development of a regulatory framework for blockchain in Cambodia is still ongoing, but the RGC's recent actions suggest that it is open to the potential benefits of this technology. The MoU with Binance is a positive step, and it is likely that the authorities will continue to develop a regulatory framework that will allow Cambodia to benefit from blockchain technology while minimizing the risks associated with it.

Here are some recommendations for the regulatory framework which will require harmonizing existing laws and creating new laws that govern blockchain technology in Cambodia:

- The framework should be clear and comprehensive, providing guidance on the legal status of cryptocurrencies, the licensing requirements for blockchain businesses, and the taxation of digital assets.
- The framework should be flexible enough to accommodate the evolving nature of blockchain technology.
- The framework should be designed to promote innovation and growth in the blockchain industry.

These regulatory frameworks will need to address the following issues:

- The legal status of cryptocurrencies
- The licensing requirements for blockchain businesses
- The taxation of digital assets
- The protection of consumers and investors
- The prevention of fraud and money laundering

To safeguard citizens' privacy, organizations of all sizes, including academia, should adopt a privacy-by-design approach to developing blockchain applications/algorithms. The multi-ministries committee

should also oversee the proper incorporation of ethics and privacy measures in blockchain development to ensure compliance with best practices. This regulatory framework will help to ensure that blockchain technology is used in a safe and responsible manner, while also maximizing its potential benefits for Cambodia.

Well-designed regulatory framework for blockchain in Cambodia could help to attract investment and talent to the country, and it could also help to position Cambodia as a leader in the regional and global blockchain industry.

6. Challenges for Cambodia

Blockchain technology has gained global attention for its potential to revolutionize various industries by providing transparency, security, and efficiency in data management. However, for countries like Cambodia, adopting blockchain presents a unique set of challenges. This chapter explores the obstacles that Cambodia faces in its journey towards blockchain readiness.

6.1. Technological Challenges in Cambodia

Infrastructure Challenges

Internet Connectivity

Cambodia's technological infrastructure, particularly its internet connectivity, plays a pivotal role in enabling blockchain adoption. Blockchain networks rely on robust internet connections to maintain the distributed ledger and validate transactions. Unfortunately, Cambodia's internet infrastructure may not be sufficiently developed, particularly in rural areas. This digital divide could hinder the widespread use of blockchain technology. In 2021, Cambodia initiated projects to expand internet access to rural communities, but challenges like limited resources and geographical barriers persisted (Chea, 2023). These issues might still be impacting blockchain adoption in these regions.

Power Supply

A reliable power supply is equally crucial for uninterrupted blockchain operations. Blockchain nodes, which validate and record transactions, must operate continuously. Frequent power outages or fluctuations can disrupt these nodes, compromising the network's stability (Khmer Times, 2023). In 2023, Cambodia planned power outages for maintenance work. While these measures were necessary, it highlights the vulnerability of the power supply and its potential impact on blockchain infrastructure.

Shortage of Blockchain Experts

Building and maintaining blockchain solutions requires a specialized skill set. Cambodia faces a shortage of qualified blockchain developers, engineers, and experts who can design and implement blockchain projects effectively. This skill gap could slow down the development of local blockchain solutions. Cambodia’s universities have stated offering blockchain course, but it takes time to produce a workforce with the necessary expertise. Organizations may need to seek international collaboration to fill this talent gap.

Decentralization versus Regulation

Blockchain’s decentralized nature challenges traditional regulatory frameworks. Cambodia needs to develop clear and comprehensive regulations to address issues such as data privacy, security, and smart contract legality. Striking a balance between fostering innovation and ensuring compliance is a delicate task. In 2021, Cambodia’s Ministry of Economy and Finance issued a digital currency proposal, highlighting the government’s recognition of the importance of blockchain technology. However, achieving a regulatory framework that encourages innovation while safeguarding against misuse remains a challenge.

Cross-Platform Interaction

Interoperability refers to the ability of different blockchain platforms and applications to seamlessly interact with each other. Cambodia might face challenges in ensuring that various blockchain ecosystems can communicate effectively. This is crucial for promoting cross-industry collaboration and data sharing. The Royal Government of Cambodia (RGC) may seek to implement blockchain in healthcare and supply chain management. Ensuring that these systems can exchange data securely and efficiently requires addressing interoperability challenges.

Handling Increased Transactions

As more users and applications join the blockchain network, scalability becomes a concern. Ensuring that the blockchain infrastructure can handle a growing number of transactions without compromising performance is vital. This challenge is not unique to Cambodia but is a fundamental aspect of blockchain technology (also mentioned in Section 3.2.3). Cambodia's emerging fintech sector could see increased adoption of blockchain-based payment systems, already on the move with the National Bank of Cambodia (NBC) Bakong blockchain-based infrastructure. To support this, the country must invest in solutions that enhances the scalability of its blockchain networks.

Cambodia's journey towards blockchain readiness involves overcoming various technological challenges. The development of infrastructure, cultivation of technical expertise, establishment of a balanced regulatory framework, solving interoperability issues, and addressing scalability concerns are all critical components of this transformation. While these challenges are formidable, Cambodia has shown commitment to embracing blockchain technology, and with concerted efforts and strategic planning, it can position itself as a significance player in the global blockchain ecosystem.

6.2. Economic and Social Challenges in Cambodia

Cambodia is a country experiencing rapid economic growth, which has slowed down due to the negative impacts of the COVID-19 pandemic. To ensure a solidified economic recovery and successful transition to become a richer country by 2030 and 2050 as nationally envisioned, the RGC recognizes the potential of blockchain technology to enhance transparency, efficiency, and security across various sectors. The formulations of a wide array of relevant policy and regulatory frameworks along with the gradual adoption of blockchain technology can reaffirm such a strategic move. However, adopting blockchain technology comes with its own socio-economic challenges that require careful consideration as follows:

High cost of implementation

Integrating blockchain systems can be expensive, particularly for Cambodia's small and medium-sized enterprises. Although the cost varies according to the types of blockchain technology used and the number of users in the network, it is known that the development of a simple blockchain application can cost from $15,000 up to $130,000 for a complex project (Bhagat, 2022). For Bitcoin, the estimated total cost to record the transaction can reach more than $600 million annually (Khadka, 2020). High initial costs and ongoing maintenance can deter businesses from harnessing the benefits of blockchain.

High energy consumption

As mentioned above, reliable power supply is crucial for proper operation of blockchain. Traditional blockchain systems, like Proof-of-Work (see Section 3.1.4 for its definition), can be energy-intensive and thus raise environmental concerns. For example, the Bitcoin blockchain uses as much electricity as the whole of Ireland, that is, an estimated 3 Gigawatts (Ganne, 2018), and it produces approximately

22 megatons of carbon dioxide (Khadka, 2020). In a country with a developing energy infrastructure like Cambodia, energy consumption can hinder the widespread adoption of such technologies.

Limited digital literacy

Cambodian youth (UNDP Cambodia, 2020) and small businesses (The Asia Foundation, 2023) alike still lack adequate digital literacy, which impedes their ability to utilize blockchain applications effectively. Bridging this knowledge gap is crucial to ensure equal participation in the blockchain-driven economy.

Gender disparities

Women in Cambodia often face barriers to accessing education and technical training (USAID Cambodia, 2020). This gender gap in digital literacy can exacerbate existing socio-economic disparities when adopting blockchain technology.

Financial inclusion

While blockchain can offer solutions for financial inclusion, reaching the unbanked and underbanked populations in Cambodia requires concerted efforts. Creating user-friendly and accessible blockchain applications is vital to achieving inclusive economic growth.

Regulatory uncertainty for businesses and investors

Cambodia's legal framework is still developing concerning blockchain technology. The ambiguity surrounding regulations can create uncertainty for businesses and investors, hindering innovation and investment in the sector.

Smart contract reliability

Smart contracts, though touted for their trustworthiness, are not immune to coding errors and vulnerabilities. Ensuring the reliability and safety of smart contracts is crucial for their adoption in various sectors, such as finance and supply chain.

Blockchain technology offers immense potential for Cambodia's socio-economic development, but its adoption is not without challenges. Addressing socio-economic hurdles associated with blockchain technology is necessary for harnessing its transformative power effectively. Collaborative efforts between the government, private sector, and civil society can pave the way for a more inclusive and sustainable blockchain ecosystem in Cambodia. By addressing these challenges, Cambodia can maximize the benefits of blockchain technology while mitigating potential risks.

6.3. Security and Privacy Concerns in Cambodia

Blockchain technology offers numerous benefits and is considered a foundational technology of the fourth industrial revolution and has applications in various sectors such as healthcare, supply chain, education, and insurance (Tan, 2020). However, its application and implication in Cambodia necessitates a closer examination of the unique challenges or risks that Cambodia could face and sets the foundation for the further analysis before adopting this technology.

The six common security properties of blockchain technology identified in previous literature (Le, 2021), are namely integrity, transparency, traceability, accountability, anonymity, and unforgeability while the privacy properties include confidentiality and privacy. Therefore, it is indeed true that

achieving all these properties (*i.e.*, security versus privacy) simultaneously can be challenging due to conflicts of interest between different stakeholders and the nature of different blockchain types.

For instance, public blockchains (Nakamoto, 2008) may prioritize anonymity, while private, consortium or government-run blockchains (Pahlajani, 2019, Dib, 2018, Alkhateeb, 2022) may require user identification for regulatory compliance. The openness of public blockchain networks allows for the participation of potentially malicious nodes that can disrupt the network, compromise transactions, or manipulate data. In terms of private, consortium or government-run blockchains, the governance and consensus mechanisms are necessary for decision-making in blockchain networks, but flawed processes or centralized control can compromise security and integrity.

Moreover, in blockchain networks that use a Proof-of-Work (PoW) consensus algorithm (see Section 3.1.4 for its definition), a 51% attack (Ye, 2018) where a single entity or group controls over 50% of the network's computing power, enabling them to manipulate the blockchain technology. Other attacks are vulnerable to security include DdoS attack (Abhishta, 2019), selfish mining attack (Chicarino, 2020), and Sybil attack (Zhang, 2019). In addition, smart contracts can have vulnerabilities, leading to financial losses or unintended consequences if exploited. Private key security is crucial as compromising or stealing private keys grants unauthorized access to digital assets.

While blockchain offers transparency, privacy concerns arise in certain use cases or applications. Public blockchains may expose sensitive information, posing challenges for industries where privacy is essential. Additionally, blockchain's cross-jurisdictional nature presents legal and regulatory complexities, especially regarding compliance with data protection and anti-money laundering regulations. To mitigate these challenges, type of blockchain, governance framework, and privacy policy, drawing insights from the General Data Protection Regulation (GDPR) (Regulation, 2018) shall be consider, especially in the context of Cambodia.

Despite the aforementioned challenges, risks, and vulnerabilities between security and privacy, there are some cryptographic techniques and mechanisms that play crucial roles in ensuring the security, privacy, and integrity of blockchain systems and related applications that Cambodia could further explore, namely, hash function (Gilbert, 2003), encryption scheme (Acar, 2018), digital signature (Goldwasser, 1988), secret sharing scheme (Shamir, 1979), multi-party computation (Zhong, 2019), zero-knowledge proof (Sun, 2021), distributed key management (Ma, 2019), self-sovereign identity (Ferdous, 2019), access control mechanism (Sok, 2022). The provide foundation for building secure decentralized systems and protecting sensitive data in various contexts, especially in the context of Cambodia.

In short, by understanding the potential risks and vulnerabilities, organizations, and policymakers can make informed decisions and develop robust strategies to mitigate these concerns. It underscores the need for a balanced approach that considers both the advantages and potential drawbacks of blockchain technology, ensuring that security and privacy are appropriately addressed in the Cambodian context.

7. Concluding remarks and Recommendation

Technological advancement has fostered significant development to many developing regions. Yet, the positive impacts and potential downsides of emerging technologies continue to be actively debated among practitioners, policymakers, and researchers. Cambodia values technological progress and is convinced that the integration of science, technology, and innovation in all sectors is a constant endeavor to achieve the goal of reaching upper-middle income status by 2030 and high-income status by 2050. Lessons learned and desk analyses by experts point out that:

- Blockchain technology has emerged as a transformative tool in an environment where transparency, decentralization, security, and the potential for smart contracts are essential. Building a favorable ecosystem for the adoption and adaptation of technology *viz* blockchain national strategy, improving collaboration and infrastructure support are necessary for Cambodia to quickly pioneer positive impacts on socio-economic development through the assimilation of blockchain.
- Policy instruments on science, technology, and innovation are important driving forces to realize the potential of blockchain technology. The Ministry of Industry, Science, Technology & Innovation must take significant actions to establish a legal framework ensuring that the technology incurs positive impacts with inclusivity and a controllable scale. Moreover, the National Council of Science, Technology & Innovation is a suitable existing governmental structure to coordinate or act for some cross-cutting issue of blockchain.
- Dominated by a young population and with a rapid penetration of internet users, as well as the widespread use of smart devices, Cambodia is in a favorable position to adopt blockchain technology. Cambodia must harness these strengths by immediately integrating this technology into public services and private investment.
- The initiative of Bakong project by the National Bank of Cambodia is the government's first significant step in introducing blockchain technology in Cambodian society. The successful implementation of blockchain technology in the country must be broadly communicated to the public to inspire users, while good and bad practices must be discussed to find improvement in Cambodian context.
- The lack of familiarity with blockchain technology can hamper the implementation strategies, resulting in the underutilization of this potential technology, particularly in the public and private sectors. Public awareness through formal education in higher education, improving research and development, talent grants, mobility, and technology transfer in the form of institutional-level training are necessary.
- Task force and workforce planning have not been in place to address the demand for blockchain technology experts. Cambodia must take quick action to have a sufficient workforce for the demand in both the public and private sectors. A task force at the national level, coordinated by the National Council of Science, Technology & Innovation, must be established to oversee the development of blockchain technology. Meanwhile, the government must strategize the foundation spirit of human capital development for the workforce. This lays the groundwork for science, technology, and Innovation higher education institutions to have readiness in research and development competence.

Bibliography

Abhishta, A., Joosten, R., Dragomiretskiy, S., & Nieuwenhuis, L. J. (2019, February). Impact of successful ddos attacks on a major crypto-currency exchange. In *2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)* (pp. 379-384). IEEE.

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur)*, *51*(4), 1-35.

Acciarini, C., Cappa, F., Di Costanzo, G., Prisco, M., Sardo, F., Stazzone, A., & Stoto, C. (2023). Blockchain technology to protect label information: The effects on purchase intentions in the food industry. *Computers & Industrial Engineering*, *180*, 109276.

Adoption in Tourism MSMEs in Cambodia. Phnom Penh: TAF.

Ahmed, M. R., Islam, A. M., Shatabda, S., & Islam, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *IEEE Access*, *10*, 113436-113481.

Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. *IEEE Access*, *7*, 36500-36515.

Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. *Sensors*, *22*(4), 1304.

Alsayed Kassem, J., Sayeed, S., Marco-Gisbert, H., Pervez, Z., & Dahal, K. (2019). DNS-IdM: A blockchain identity management system to secure personal data sharing in a network. *Applied Sciences*, *9*(15), 2953.

Aslihan Nasir, V., & Karakaya, F. (2014). Consumer segments in organic foods market. *Journal of consumer marketing*, *31*(4), 263-277.

Bell, L., Buchanan, W. J., Cameron, J., & Lo, O. (2018). Applications of Blockchain Within Healthcare. *Blockchain in healthcare today*.

Bhagat, V. (2022, November 25). Blockchain Development Cost – Blockchain Pricing. Retrieved from PixelCrayons: https://www.pixelcrayons.com/blog/blockchain-development-cost/

Binance. (2022, June 30). *Binance Signs MoU with The Securities and Exchange Regulator of Cambodia*. Retrieved from Binance: https://www.binance.com/

Bitcoin Hashrate Chart - BTC Hashrate 409.55 EH/s. (n.d.). CoinWarz. Retrieved August 3, 2023, from https://www.coinwarz.com/mining/bitcoin/hashrate-chart

Borah, M. D., Naik, V. B., Patgiri, R., Bhargav, A., Phukan, B., & Basani, S. G. (2020). Supply chain management in agriculture using blockchain and IoT. *Advanced applications of blockchain technology*, 227-242.

Bowman, R. J. (2018, November 21). *Q&A | The Challenges of Automotive Supply Chains*. https://www.supplychainbrain.com/articles/29021-the-challenges-of-automotive-supply-chains

Cahill, C. P., Whitehead, G., & Yang, H. (2007). Liberty ID-WSF Provisioning Service Specification. *CA, USA: Liberty Alliance Project, Intel Corp*.

Caldwell, J. D. (2016). *Emotional Labor and Identity Management Among HIV Counselors and Testers*. Doctoral Dissertation, University of Central Florida.

Cambodian Youth. Phnom Penh: UNDP Cambodia.

Cameron, K. (2005). The laws of identity. *Microsoft Corp*, *12*, 8-11.

Cantor, S., Hodges, J., Kemp, J., & Thompson, P. (2003). Liberty id-ff architecture overview. *Wason, Thomas (Herausgeber): Liberty Alliance Project Version*, *1*.

Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., & Secundo, G. (2022). Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Information & Management*, *59*(7), 103508.

Chapiro, C. (2021, November 24). *Working Toward Financial Inclusion With Blockchain*. Retrieved July 4, 2023, from https://ssir.org/articles/entry/working_toward_financial_inclusion_with_blockchain24

Chea, V. (2023, March 30). Mobile, internet services in provinces to be strengthened - khmer times. Khmer Times - Insight into Cambodia. Retrieved October 3, 2023, from https://www.khmertimeskh.com/501264700/mobile-internet-services-in-provinces-to-be-strengthened/

Chicarino, V., Albuquerque, C., Jesus, E., & Rocha, A. (2020). On the detection of selfish mining and stalker attacks in blockchain networks. *Annals of Telecommunications*, *75*, 143-152.

Consensys. (n.d.). *Blockchain in Government and the Public Sector*. Retrieved July 5, 2023, from https://consensys.net/blockchain-use-cases/government-and-the-public-sector/

Crypto AG. (n.d.). www.cryptotec.com

Čučko, Š., & Turkanović, M. (2021). Decentralized and self-sovereign identity: Systematic mapping study. *IEEE Access*, *9*, 139009-139027.

Daley, S. (2023, February 16). *Blockchain in Healthcare: 17 Examples to Know*. https://builtin.com/blockchain/blockchain-healthcare-applications-companies

David, M. (2023, February 6). Block chain technology for digital financial inclusion in the industry 4.0, towards sustainable development? *Frontiers in Blockchain*, 13. 10.3389/fbloc.2023.1035405

Deloitte. (n.d.). *Blockchain: Opportunities for health care*. Retrieved July 5, 2023, from https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html

Di Pierro, M. (2017). What is the blockchain?. *Computing in Science & Engineering*, *19*(5), 92-95.

Dib, O., Brousmiche, K. L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun*, *11*(1), 51-64.

Digital Financial Services Working Group. (2018, August). *Innovative Cross-Border Remittance Services: Experiences From Afi Member Countries*. https://www.afi-global.org/sites/default/files/publications/2018-09/AFI_DFS_cross%20border_AW_digital.pdf

Ding, K., Jiang, P., Leng, J., & Cao, W. (2016). Modeling and analyzing of an enterprise relationship network in the context of social manufacturing. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, *230*(4), 752-769.

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE security & privacy*, *16*(4), 20-29.

Dworkin, M. J. (2015, August). SHA-3 Standard: Permutation- Based Hash and Extendable-Output Functions. *Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.FIPS.202

El Haddouti, S., & El Kettani, M. D. E.-C. (2019). Analysis of identity management systems using blockchain technology. In *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)* (pp. 1-7). IEEE.

Elkhoury, N. (2016, July 12). *https://inspirage.com/2016/07/supply-chain-challenges-automotive-industry/*.

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE access*, *7*, 103059-103079.

Frankenfield, J. (2023, May 31). *Distributed Ledger Technology (DLT): Definition and How It Works*. https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp

G. Prisco, “The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab,” BitCoin Magazine, April 2016. URL: https://bitcoinmagazine.com/articles/the- blockchain-for-heathcare-gem-launches-gem-health-network-with-philips- blockchain-lab-1461674938/ Accessed Aug. 2023.

Ganne, E. (2018). Can Blockchain Revolutionize International Trade? Geneva: WTO.

Gilani, K., Bertin, E., Hatin, J., & Crespi, N. (2020). A survey on blockchain-based identity management and decentralized privacy for personal data. In *2020 2nd Conference on Blockchain Research \& Applications for Innovative Networks and Services (BRAINS)* (pp. 97-101). IEEE.

Gilbert, H., & Handschuh, H. (2003, August). Security analysis of SHA-256 and sisters. In *International workshop on selected areas in cryptography* (pp. 175-193). Berlin, Heidelberg: Springer Berlin Heidelberg.

Goldwasser, S., Micali, S., & Rivest, R. L. (1988). A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on computing*, *17*(2), 281-308.

Goodner, M., & Nadalin, A. (2009). Web Services Federation Language (WS-Federation) Version 1.2. *OASIS Web Services Federation (WSFED) TC*.

Hackius,, N., & Petersen, M. (2017, October). *Blockchain in Logistics and Supply Chain: Trick or Treat?* (Issue 23). Hamburg International Conference of Logistics (HICL).

Henderson, J. (2020, May 18). *IBM establishes blockchain platform to track jewellery supply chain*. https://supplychaindigital.com/technology/ibm-establishes-blockchain-platform-track-jewellery-supply-chain

How OpenID Connect Works. (n.d.). OpenID. Retrieved July 29, 2023, from https://openid.net/developers/how-connect-works/

Hughes, J., Cantor, S., Hodges, J., Hirsch, F., Mishra, P., Philpott, R., & Maler, E. (2005). Profiles for the oasis security assertion markup language (saml) v2. 0. *OASIS standard*, *200503*.

Jean-Paul, B., Rachid, G., & Ali, S. (2015). Making BFT protocols really adaptive. In *2015 IEEE International Parallel and Distributed Processing Symposium* (904--913). IEEE. https://doi.org/10.1109/IPDPS.2015.21

Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the Blockchain technology adoption in supply chains-Indian context. *International Journal of Production Research*, *57*(7), 2009-2033.

Khadka, R. (2020). The Impact of Blockchain Technology in Banking: How Can Blockchain Revolutionize the Banking Industry? Kokkola: Centria University.

Khmer Times. (2023, June 23). Cambodia: Planned power outages to continue in parts of Phnom Penh and Kandal Province through June 25 - Khmer Times. Khmer Times - Insight into Cambodia. Retrieved October 3, 2023, from https://www.khmertimeskh.com/501313202/cambodia-planned-power-outages-to-continue-in-parts-of-phnom-penh-and-kandal-province-through-june-25/

Lamport, L. (1998, May). The Part-Time Parliament. *ACM Transactions on Computer Systems*, *16*(2), 133-169. https://dl.acm.org/citation.cfm?doid=279227.279229

Le, T. V., & Hsu, C. L. (2021). A systematic literature review of blockchain technology: Security properties, applications and challenges. Journal of Internet Technology, 22(4), 789-802.

Leng, J., Ruan, G., Jiang, P., Xu, K., Liu, Q., Zhou, X., & Liu, C. (2020). Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey. *Renewable and sustainable energy reviews*, *132*, 110112.

Lichtfous, M., Yadav, V., & Fratino, V. (n.d.). *Can Blockchain Accelerate Financial Inclusion Globally?* Retrieved July 4, 2023, from https://theblockchaintest.com/uploads/resources/file-36385816098.pdf

Liew, V. K. (2020, April 2). *Fighting COVID-19 with Blockchain*. https://www.blockchainguide.biz/fighting-covid-19-with-blockchain/

Liew, V. K. (2020). *Blockchain and Cryptocurrency: A Blockchain and Cryptocurrency Guidebook for Everyone*. Amazon.com.

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Blockchain-based identity management systems: A review. *Journal of network and computer applications*, *166*, 102731.

Lundkvist, C., Heck, R., Torstensson, J. a. M., Mitton, Z., & Sena, M. (2017). Uport: A platform for self-sovereign identity. *URL: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf*.

Ma, M., Shi, G., & Li, F. (2019). Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. *IEEE access*, *7*, 34045-34059.

Malaysian Government. (n.d.). *Vaccine Management System (VMS)*. Retrieved July 5, 2023, from https://www.malaysia.gov.my/portal/content/31246

Manohar, A., & Briggs, J. (2018). Identity management in the age of blockchain 3.0.

Martinez, L. V., Ting-Toomey, S., & Dorjee, T. (2016). Identity management and relational culture in interfaith marital communication in a United States context: A qualitative study. *Journal of Intercultural Communication Research*, *45*(6), 503-525.

MEF. (2021). *Cambodia Digital Economy and Society Framework 2021-2035.* Phnom Penh: MEF.

MEF. (2021). *Law on Public-Private Partnership.* Phnom Penh: MEF.

Mettler, M. (2016, September). Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)* (pp. 1-3). IEEE.

Ministry of Science, Technology & Innovation (MISTI). (2022).

MISTI & ESCAP, 2022. The Research Ecosystem of Cambodia, *Joined Study Report between MISTI and UNESCAP*.

MISTI, 2022. National Research Agenda 20225, *Government Policy*.

MISTI. (2021). *Cambodia's STI Roadmap 2030.* Phnom Penh: MISTI.

Mohamad, B., Bakar, H. A., Ismail, A. R., Halim, H., & Bidin, R. (2016). Corporate identity management (cim) in malaysian higher education sector: Developing a conceptual model. *International Review of Management and Marketing*, *6*(7), 175-180.

MoP, 2021. The profile of demographic and gender dividend of Cambodia, General Secretariat for population Development.

MPTC. (2022). *Cambodia Digital Government Policy 2022-2035.* Phnom Penh: MPTC.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.

National Bank of Cambodia & Soramitsu. (2020, June). *Project Bakong-Next Generation Payment System*. https://soramitsu.co.jp/bakong/whitepaper

National Institute of Standards and Technology. (2015, August). Secure Hash Standard (SHS). *Federal Information Processing Standards (FIPS) Publication 180-4*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

Ministry of Science, Technology, and Innovation (MOSTI) of Malaysia. (2022, August). National Blockchain Roadmap 2021-2025. https://www.mosti.gov.my/wp-content/uploads/2022/08/National-Blockchain-Roadmap-2021-2025.pdf

NBC, SERC, & NP. (2018, May 11). Joint statement between NBC, SERC, and the General Commissariat of the National Police. Phnom Penh.

NBC. (2017, Dec 05). Cambodia to ban the trading of Crypto currency such as Bitcoin. Phnom Penh, Cambodian.

Overseas Development Institute (ODI). (2020). Fostering an Inclusive Digital

Pahlajani, S., Kshirsagar, A., & Pachghare, V. (2019, April). Survey on private blockchain consensus algorithms. In *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)* (pp. 1-6). IEEE.

Panait, A.-E., Olimid, R. F., & Stefanescu, A. (2020). Identity Management on Blockchain--Privacy and Security Aspects. *arXiv preprint arXiv:2004.13107*.

Parecki, A. (n.d.). *OAuth 2.0 — OAuth*. OAuth. Retrieved July 29, 2023, from https://oauth.net/2/

Pavalanathan, U., & De Choudhury, M. (2015). Identity management and mental health discourse in social media. In *Proceedings of the 24th international conference on world wide web* (pp. 315-321).

Rathee, P. (2020). Introduction to blockchain and IoT. *Advanced applications of blockchain technology*, 1-14.

Regulation, General Data Protection. "General data protection regulation (GDPR)." *Intersoft Consulting, Accessed in October* 24, no. 1 (2018).

Rella, L. (2019, October 17). Blockchain Technologies and Remittances: From Financial Inclusion to Correspondent Banking. *Frontiers in Blockchain*. doi: 10.3389/fbloc.2019.00014

RGC, 2015. Industrial Development Policy 2015-2025, Government Policy.

RGC, 2020. Cambodia Digital Economy and Society Policy Framework 2020-2035, *Government Policy*.

RGC, 2021. The Strategic Framework and Programs for Economic Recovery in the Context of Living with COVID-19 in a New Normal 2021-2023, Government Policy.

Rowden, M. (2004). *Identity: Transforming performance through integrated identity management*. Gower Publishing, Ltd.

Saghiri, A. M. (2020). Blockchain architecture. *Advanced applications of blockchain technology*, 161-176.

Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, *8*(2), 23-29.

SERC. (2022, June 30). Market Info. (SERC) Retrieved from https://www.serc.gov.kh/

ServerMania, 2023. Blockchain Infrastructure and Hardware Requirements Explained,

Seyam, H., & Habbal, A. (2023). A Systematic Review of Blockchain-based Identity Management Solutions. In *International Conference on Recent Academic Studies* (Vol. 1, pp. 246-253).

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612-613.

ShoCard, S.I.T.A. (2016). Travel identity of the future-white paper. *Book Travel Identity of the Future--White Paper, edn*.

Sok, K., Colin, J. N., & Po, K. (2022, May). Multi-authority Decentralized Attribute-Based Authorization Framework. In *International Conference on Advanced Information Systems Engineering* (pp. 18-30). Cham: Springer International Publishing.

Soramitsu. (n.d.). *SORAMITSU — Designing a Better World Through Decentralized Technologies*. Retrieved July 5, 2023, from https://soramitsu.co.jp/#projects

Statista. (2023). Cambodia: Share of economic sectors in the gross domestic product (GDP) from 2011 to 2021, Economic and Politic. Retrieved July 31, 2023, from https://www.statista.com/statistics/438728/share-of-economic-sectors-in-the-gdp-in-cambodia

Statista. (2022a), "Revenue of the food market 2012-2025 | Statista". Retrieved March 1, 2022, from https://www.statista.com/forecasts/1243605/revenue-food-market-worldwide

STL Partners. (n.d.). *5 blockchain healthcare use cases in digital health*. Retrieved July 6, 2023, from https://stlpartners.com/articles/digital-health/5-blockchain-healthcare-use-cases/

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE network*, *35*(4), 198-205.

Tan Monivisal (2020). Blockchain Technology: More Than Just Bitcoin. CD-Center, Vol 2, Issue 6.

Tan, T. M., Salo, J., Petri, A., Veikko, S., & Sandner, P. (2021). Revealing the disintermediation concept of blockchain technology: How intermediaries gain from blockchain adoption in a new business model. In *Impact of globalization and advanced technologies on online business models* (pp. 88-102). IGI Global.

The Asia Foundation (TAF). (2023). The Current State and Role of Digital Technology

The World Bank. (n.d.). *Digital Financial Inclusion*. Retrieved July 4, 2023, from https://www.worldbank.org/en/topic/financialinclusion/publication/digital-financial-inclusion

Toorajipour, R., Oghazi, P., Sohrabpour, V., Patel, P. C., & Mostaghel, R. (2022). Block by block: A blockchain-based peer-to-peer business transaction for international trade. *Technological Forecasting and Social Change*, *180*, 121714.

Transformation in Cambodia. London: ODI.

Tribis, Y., El Bouchti, A., & Bouayad, H. (2018). Supply chain management based on blockchain: A systematic mapping study. In *MATEC Web of Conferences* (Vol. 200, p. 00020). EDP Sciences.

Tseng, C.-T., & Shang, S. S. (2021). Exploring the sustainability of the intermediary role in blockchain. *Sustainability*, *13*(13), 1936.

UNCDF. (n.d.). *Sustainable Development Goals*. Retrieved July 4, 2023, from https://www.uncdf.org/sdgs#ide

UNDP Cambodia. (2020). Digital Literacy for Employability and Entrepreneurship among

United Nations Educational, Scientific and Cultural Organization. TVET country profile: Cambodia. 2020.

USAID Cambodia. (2020). Gender and Inclusive Development Analysis. Phnom Penh: USAID Cambodia.

Van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-sovereign identity solutions: The necessity of blockchain technology. *arXiv preprint arXiv:1904.12816*.

Vujičić, D., Jagodić, D., & Ranđić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)* (pp. 1-6). IEEE.

Wadhwa, S. (2019). *Decentralized digital identity management using blockchain and its implication on public sector*. Doctoral dissertation, Dublin Business School.

Wang, H., & Jiang, Y. (2020). A novel blockchain identity authentication scheme implemented in fog computing. *Wireless Communications and Mobile Computing*, *2020*, 1-7.

World Bank, 2022. Cambodia Poverty Assessment: Toward a more inclusive and Resilient Cambodia, Executive Summary.

World Economic Forum. (2019, January). Innovation with a Purpose: Improving Traceability in Food Value Chains through Technology Innovations. https://www3.weforum.org/docs/WEF_Traceability_in_food_value_chains_Digital.pdf

World Economic Forurm. (2018, September). Building Block(chain)s for a Better Planet. https://www3.weforum.org/docs/WEF_Building-Blockchains.pdf.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018, September). Analysis of security in blockchain: Case study in 51%-attack detecting. In *2018 5th International conference on dependable systems and their applications (DSA)* (pp. 15-24). IEEE.

Zambrano, R., Young, A., & Verhulst, S. (2018). Connecting refugees to aid through blockchain-enabled ID management: world food programme's building blocks. *GovLab October*.

Zhang, S., & Lee, J. H. (2019). Double-spending with a sybil attack in the bitcoin decentralized network. *IEEE transactions on Industrial Informatics*, *15*(10), 5715-5722.

Zhong, H., Sang, Y., Zhang, Y., & Xi, Z. (2020). Secure multi-party computation on blockchain: An overview. In *Parallel Architectures, Algorithms and Programming: 10th International Symposium, PAAP 2019, Guangzhou, China, December 12–14, 2019, Revised Selected Papers 10* (pp. 452-460). Springer Singapore.


ក្រសួងឧស្សាហកម្ម វិទ្យាសាស្ត្រ បច្ចេកវិទ្យា និងនវានុវត្តន៍
MINISTRY OF INDUSTRY, SCIENCE, TECHNOLOGY & INNOVATION