THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

IDENTITIES FOR OPPORTUNITIES

A FEASIBILITY STUDY FOR OVERCOMING THE ROHINGYA'S STATELESSNESS CHALLENGES VIA BLOCKCHAIN-BASED DIGITAL SOLUTIONS

RESEARCH FELLOWS

Sneha Indrajit

Jannah McGrath

Matthew Newton

Arica Schuett

Hailey Vandeventer

SENIOR RESEARCH FELLOWS

Allison Anderson

Seth Kane

FACULTY LEAD

Sara Curran

This report is a product of the Applied Research Program in the Henry M. Jackson School of International Studies at the University of Washington. The Applied Research Program matches teams of top-achieving Jackson School students with private and public-sector organizations seeking dynamic, impactful, and internationally-minded analyses to support their strategic and operational objectives.

For more information about the Applied Research Program please contact us at jsisarp@uw.edu or visit our website at http://jsis.uw.edu/arp/

Identities for Opportunities: A Feasibility Study for Overcoming the Rohingya's Statelessness Challenges Via Blockchain Digital Solutions.

Applied Research Program, Jackson School of International Studies

July 2018

Synopsis

This report provides a feasibility assessment for *The Rohingya Project (TRP)* proposal to create self-sovereign digital identities for the stateless Rohingya diaspora, so as to facilitate financial inclusion and other opportunities otherwise unavailable to those without a nation and associated entitlements conferred on citizens of a state. The report first reviews the structural architecture of blockchains to determine the optimal blockchain platform architectural design for TRP objectives and the risks in the application of blockchain based digital identification. Second, it examines the necessary tools in information that are pertinent to the implementation of a blockchain digital ID. This include international laws and regulations that govern identity verification, a study of existing digital ID systems, and a study of TRP's pilot nations, Bangladesh, the Kingdom of Saudi Arabia, and Malaysia. The report concludes with a summary of key findings, recommendations, and areas for further research.

Researchers
Sneha Indrajit
Jannah McGrath
Matthew Newton
Arica Schuett
Hailey Vandeventer

Senior Researchers
Allison Anderson
Seth Kane

Faculty Lead
Professor Sara Curran

Table of Contents

Key Acronyms & Terms

AML - Anti-Money Laundering
CDD - Customer Due Diligence
CTF - Counter Terrorist Financing
FATF - Financial Action Task Force
ID - Identification
KSA - Kingdom of Saudi Arabia
KSI - Keyless Signature Infrastructure
KYC - Know Your Customer
TRP - The Rohingya Project

Executive Summary

This report assesses the key legal, political, social, and technological factors that will influence the adoption of The Rohingya Project's (TRP) blockchain digital ID system. We focus on the TRP's three countries - Bangladesh, Saudi Arabia, Malaysia.

Section 1 - Blockchain: Understanding the Choices and Risks
We have determined that TRP's core objectives for a self-sovereign identity system are decentralization, efficiency, scalability, security, and privacy. Based on our research, we recommend TRP develop a partially-decentralized blockchain with a proof-of-stake consensus mechanism. Using a *distributed ledger technology employing cryptographic methods* will protect user data and avoid the security breaches experienced by Pakistan's and India's highly centralized systems. We recommend that TRP's platform be open-source and platform agnostic (capable of being used across multiple ledgers). Furthermore, TRP should adopt blockchain platforms that allow quantum-proof storage, given emerging security threats. Regarding privacy, especially for vulnerable populations, we recommend *a shred-it-all policy*, where all hardcopy information is shredded after transference to the blockchain, mitigating risks of leaking information through the proposed enrollment system.

Section 2 - International Frameworks: Building TRP's Legitimacy and Reputation
The international Financial Action Task Force (FATF) and its members have developed processes to expand financial access and services to customers lacking traditional identity verifiers, such as a government IDs or employment history. TRP should engage closely with key institutions and organizations, like the United Nations, to both influence ongoing initiatives, as well as explore new and creative ways to accommodate Rohingya needs. We suggest TRP look to non-biometric methods of identity verification, considering the vulnerabilities of the Rohingya diaspora. We encourage TRP to further solidify its reputation through transparent and civic engagement in the process of promoting the potential for using blockchain technologies for the Rohingya diaspora.

Of great value to TRP, ASEAN member states officially recognize digital identification as a mode of legal recognition. This provides a formal institutional basis to justify blockchain IDs as a viable solution for stateless people in ASEAN. Bangladesh offers a feasible context for TRP implementation, but TRP should be aware of a potentially changing policy environment as fears grow that digital forms of identification may encourage long-term settlement in Bangladesh. There is also growing interest in technology-based platforms that encourage financial inclusion, in general, in the Kingdom of Saudi Arabia. Malaysia's laws are relatively amenable to the acceptance of Rohingya digital identification, and recent political developments may harbor an even more hospitable environment for implementing TRP objectives.

Conclusion and Further Research
TRP's objectives will require close monitoring of a rapidly changing technological, regulatory, and legal environment. Global attitudes and various international initiatives are creating new and positive opportunities for TRP. TRP needs to remain knowledgeable about blockchain and associated security innovations. TRP should develop relationships with international organizations and technology firms working in this sector. International Know Your Customer (KYC) standards support the feasibility of TRP. Further research about the risks of inadvertent or nefarious security breaches on blockchain platforms needs to be undertaken to establish TRP credibility. Further research is also required regarding relevant Kingdom of Saudi Arabia

policies and practices, as well as more details regarding a number of Islamic finance systems.

Introduction

The University of Washington's Applied Research Program (ARP) matches teams of undergraduate and graduate student researchers with organizations to develop durable solutions to real-life problems.[1] On behalf of our client, *The Rohingya Project* (TRP), we analyzed the legal, political, social, and technological landscapes in numerous countries to assess the feasibility of a blockchain digital ID system, to support TRP's mission. The Rohingya Project is a non-governmental organization and digital startup based in Malaysia that seeks to alleviate hardships faced by the stateless Rohingya diaspora. Specifically, TRP intends to create a blockchain platform to provide an authenticatable and legitimate proof of identity. Such proof of identity will allow the Rohingya, across multiple countries, to access the regulated financial system and participate in the globalized banking system. TRP believes that enabling financial inclusion for the Rohingya will provide them new, durable opportunities to improve their standard of living. TRP proposes to devise a blockchain solution that protects individuals' privacy and secures their personal information, while at the same time assuring financial institutions of the authenticity of each individual identity and the legitimacy of the platform. In addition, and to demonstrate feasibility, the TRP blockchain platform needs to demonstrate efficiency of its transactions and facilitate a relatively rapid scaling up of individual access to the platform in order to address the immediate and critical needs of this large diaspora of stateless people. We summarize TRPs proposed blockchain platform objectives as decentralization, privacy, security, efficiency and scalability.

Our report begins with an assessment of the technological choices and risks associated with the construction of a blockchain platform that will serve to provide an authenticatable and legitimate self-sovereign identity. In order to build a blockchain that fulfills TRP's core objectives of decentralization, efficiency, scalability, security, and privacy, it is imperative that TRP evaluate and fully assess the various tradeoffs associated with each of these components. This section provides a thorough explanation of each of these core objectives, beginning with decentralization since the level of decentralization has a direct effect on both the efficiency and scalability of the overall platform. In an effort to adhere to these five objectives, we focus specifically on the feasibility of proof-of-stake consensus mechanisms and byzantine fault mechanisms. Since sensitive data will be hosted on this blockchain platform, we provide an overview of the use of Zero Knowledge Proofs and State Channels as a means of safeguarding this data and enhancing the privacy of Rohingya identities.

The second part of the report assesses the international legal frameworks governing the global financial sector in order to understand how the Rohingya will access financial services and as part of our feasibility assessment. The international financial sector is heavily regulated and guided by Know Your Customer (KYC) and other standards, which mandate financial institutions conduct strict due diligence investigations about their clients. These standards, in conjunction with banking systems in the various countries where the Rohingya diaspora predominate, affect which forms of identity verification are necessary to authenticate and legally grant an individual a bank account. Digital ID platforms, either blockchain and non-blockchain, include several key information standards governing the relationship between banks and their clients. We examine digital identification standards throughout Europe and Asia to understand best practices and make recommendations applicable to TRP. Doing so helps TRP prepare their blockchain platform proposal when they approach financial institutions

[1] "Applied Research Program," International Policy Institute, Henry M. Jackson School of International Studies, accessed May 20, 2018, https://jsis.washington.edu/research/ipi/applied-research-projects/.

in each of the countries where there are major populations of Rohingya. At TRP's request, we assessed the feasibility of these practices in the three nations TRP intends for their initial platform launch: Bangladesh, Saudi Arabia, and Malaysia.

This report is a feasibility study of the various legal, political, and social structures that are likely influential in the implementation and adoption of self-sovereign digital identification for the Rohingya diaspora. Our solution involves two systems, blockchain technology and identity authorization, and this report is organized according to these elements. Section 1 assesses choices and risks in constructing blockchain platforms. Section 2 examines the global policy environment for financial inclusion in countries of interest to TRP. In both sections, we employ a Political, Social, Technological, and Legal (PSTL) risk assessment framework to assess and identify potential challenges the TRP can expect. This framework serves to address the competing interests that may present themselves to the TRP.

The table below shows a PSTL analysis of the potential risks to stakeholder engagement:

Political	In maintaining an uncompromised, decentralized blockchain platform, TRP may encounter political pushback from host nations which may demand or require government control over, or access to, personal information as part of the state's regulation of residents and regulation of bank-client information standards.
Social	Diaspora leaders or other international human rights advocates may criticize TRP for encouraging the use of relatively untested technological advances among members of an already vulnerable population.
Technological	Critics may raise concerns over user exploitation by unregulated third-party actors as populations engaging within this platform are unlikely to have prior experience with similar technologies or may not have the smartphones and computers required to access TRP's platform.
Legal	Due to a lack of legal precedent concerning digital IDs and blockchain environments, TRP will need a skilled legal team to assist them in drafting and finalizing a series of legal codes of conduct including but not limited to internal policies, cardholder privacy, interactions, and disclosures with national governments. Failure to provide and establish strong legal footing could severely damage the credibility and functionality of TRP's project.

Figure 1: Stakeholders' PSTL analysis

As a relatively new and untested technology, blockchain carries with it risks that are unknown and difficult to predict. There is a lack of empirical data on the use of blockchain technology for the creation of digital identification generally, and specifically for stateless populations. We have done our best to provide information that assesses these risks since such a project has not yet been undertaken. In addition to discussing the specific risks of using blockchain for stateless population self-sovereign identification, we also explore, general risks associated with various blockchain platforms. We look at the technology's applications involving nation states and international programs utilizing the blockchain's security features and offer recommendations to address potential risks associated with the technology.

Facilitating cooperation and adapting to the needs of numerous governments and stakeholders is vital to the success of any multinational project. As such, this report aims to make clear in what ways TRP can mitigate risks associated with blockchain platforms and develop a digital ID system to streamline Rohingya inclusion into the global financial system and across several pilot countries.

Following Sections 1 and 2 we conclude our report with a set of integrated recommendations for TRP. Finally, we include three appendices with relevant supplementary research. Appendix A examines national identity verification case studies in ten different countries. Appendix B addresses the feasibility of a TRP-conducted survey of displaced Rohingya. Appendix C provides an overview of organizations, with similar objectives as TRP. These organizations might be helpful for TRP and may be willing partners during the next phase of the TRP's efforts.

Section 1: Blockchain – Understanding the Choices and Risks

Questions:

1. What are the broad and specific issues related to personal data privacy and security on a blockchain system that must be addressed for a vulnerable stateless community seeking financial inclusion and other opportunities facilitated through an authenticatable and legitimate digital identification?
2. How are the stateless Rohingya's needs for digital identification limited by the efficiency and scaling constraints presented by a blockchain platform?

Introduction

The purpose of this section is to determine how TRP should design its blockchain platform to best suit its objectives of creating a self-sovereign digital identity on a decentralized blockchain platform to enable the financial inclusion of the Rohingya. This section assesses how the various blockchain platforms conform to TRP's core objectives-- decentralization, efficiency, scalability, privacy, and security. The results show that the extent of decentralization of a blockchain platform is one of the defining features of a blockchain platform that determines its range of capacities and functionality, especially those related to efficiency, privacy, security, and scalability.

Blockchain platforms can be divided into four broad types based on the extent of their decentralization: 1) public blockchains that are fully decentralized, 2) public blockchains that are partially decentralized, 3) private blockchains that are fully centralized, and 4) private blockchains that are partially decentralized. Blockchain platform decentralization is related to the consensus protocol built into their system architecture. Specifically, a consensus protocol determines how a blockchain platform makes decisions and how the platform is run. Consensus protocols are designed to suit different blockchain types and their purpose. For example, one type of system might be best suited for a piloting phase (i.e., a small number of users), whereas scaling up would require a different system. Also, depending on the intended level of privacy (i.e., publicly verifiable information, or encrypted information) or the desired functionality of the system (i.e., financial services, or broader services that include storage) different system architecture might be required. In the analysis that follows we assess the trade-offs associated with The Rohingya Project's core objectives.

In this section, we first provide a discussion of the concept of decentralization within blockchain systems. We explain the key differences between private and public blockchains and the risks of centralization within public blockchains. We then examine trade-offs within the core objectives of efficiency and scalability. Following this assessment, we discuss the consensus protocols that blockchain networks are built upon and provide a comparison of the various protocols. We turn our attention to how blockchains can meet TRP's core objective of privacy. Finally, we conclude with recommendations for the system architecture of TRP's blockchain platform.

Decentralization

One of the key features that distinguish blockchain platforms from traditional identification and transaction databases is that they are decentralized and remove the need for third-party intermediaries. The lack of a centralized database is one of the main appeals of blockchain as

it reduces the risk of confidential and private data being compromised. No central authority controls the system. Instead, the system runs on a trusted distributed network of nodes that store the data and verify its validity.

A node is a computer or hardware device on the network that has a copy of the information within the blockchain.[2] There are full nodes, as well as partial nodes. Full nodes have a full copy of all the information within a blockchain network while a partial node only contains some of the information.[3] Given the amount of space and memory required for a full node, it requires a significant amount of computational power. Nodes are how a blockchain keeps its information decentralized and resilient to security risks such as hacks, power failures, and systemic crashes.[4] What makes decentralization resilient is its reliance on separate components, without sensitive central points that can be easily targeted and attacked, as well as its resistance to collusion amongst nodes which could alter or tamper with information across the network.[5]

Decentralization is at the core of creating the self-sovereign digital identifications that TRP envisions. It allows the individual to control who is given access to their personal information without having to provide that information to a central authority. This helps to mitigate the risk of potentially nefarious or bad actors gaining access to sensitive information, while at the same time enabling the Rohingya to possess a valid piece of digital identification without having to compromise their privacy and security of their identity.

The key benefits of decentralization are immutability and security. Immutability and security increases with the growth in the number of nodes. Importantly, a blockchain needs to have a sufficient number of nodes distributed widely enough so that it is nearly impossible to alter or make changes to the network. Immutability comes with trade-offs, however. The more decentralized a blockchain network, the less control by any authority or manager to make changes needed to improve the blockchain. In other words, striking the right balance between decentralization and executive control is essential to creating a blockchain that meets the needs of TRP.

Consequently, there are three dimensions of decentralization: architectural decentralization, political decentralization, and logical decentralization.[6] Architectural decentralization in a blockchain refers to the number of nodes.[7] Political decentralization refers to the extent of nodal distribution, and how many individuals or organizations control the nodes.[8] Logical decentralization refers to how the system behaves and whether or not it is a singular unit with a common set of rules. Blockchain technology in its purest sense is politically decentralized, architecturally decentralized, and logically centralized.[9] Decisions about these three dimensions of decentralization are crucial for the TRP's ability to meet the needs of a number of different stakeholders as they build their blockchain platform and seek to achieve their core

---

[2] "Blockchain Nodes. What Are Nodes and How Do They Work?" World Crypto Index, accessed May 7, 2018, https://www.worldcryptoindex.com/how-nodes-work/.
[3] Ibid.
[4] Ibid.
[5] Buterin Vitalik, "The Meaning of Decentralization," *Medium*, February 6, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.

objectives.

In simple terms, these three dimensions are frequently summarized as either private and public blockchains. Private blockchains can be fully private and centralized to one organization or partially decentralized – architecturally, politically, and logically centralized. The level of decentralization of a blockchain can be determined by examining the three dimensions of decentralization. Figure 2 offers a schema describing the variance in decentralization across public and private blockchains. The extent of decentralization is represented on a scale of 0-1. In this scale, 0 represents full centralization, 0.5 represents partial decentralization, and 1 represents full decentralization. The private blockchains referenced in this report are partially decentralized as TRP does not intend to use a centralized database.

Key differences between Private and Public Blockchains

Despite the association of blockchain technology with the concept of decentralization, not all blockchain platforms are decentralized. International organizations and financial institutions are increasingly implementing blockchains which are more centralized and private. Private blockchains are only open to a network of known and trusted participants and nodes. Private blockchains are regulated by a central authority which can change rules, revert transactions and modify balances.[10] This allows for greater efficiency but creates a set of risks. A private blockchain is not hack-proof or censorship resistant. Its security is derived by relying on trusted nodes that have been verified by the developer. The extent to which it is immutable depends on the design of the blockchain.

In a public blockchain, however, each transaction is immutable. It would thus be very difficult to commit fraud or alter data given the high degree of computational power required. Altering information within a node requires consensus among more than half of the nodes within the blockchain network. Data can be tampered with only if there is collusion amongst more than half of the nodes within a network.[11] The "51% attack" is much easier to execute in smaller blockchain platforms with a limited number of nodes, or with nodes that are centralized in location.[12]

While decentralization prevents fraud and tampering of data, it does limit an organization's ability to implement changes to the system. If there are system vulnerabilities, and changes need to be instituted, a "hard fork" is required to create a split in the platform and to generate a newly architected system. A public blockchain cannot guarantee that all the users would switch to the upgraded version, however, which would create a division in the platform and compromise security for some nodes.[13] On the other hand, a private, centralized blockchain can fix errors and reverse transactions, providing a greater degree of control over participants and transaction verification.[14] Given this greater control, most institutions choose to implement

---

[10] Jim Donaldson, "Public vs Private Blockchain In A Wide World of Unique Applications," Mojix Inc, August 8, 2017, https://www.mojix.com/private-blockchain/.

[11] Ibid.

[12] Zoran Spirkovski, "Strength in Numbers: A Brief History of 51% Attacks," *CryptoNews*, March 19, 2018, https://www.crypto-news.net/strength-in-numbers-a-brief-history-of-51-attacks/.

[13] Kathleen, Brietman, "Op Ed: Why Ethereum's Hard Fork Will Cause Problems in the Coming Year," *Bitcoin Magazine*, February 3, 2017. https://bitcoinmagazine.com/articles/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year/.

[14] Allison Berke, "How Safe are Blockchains? It depends," *Harvard Business Review*, March 7, 2017, https://hbr.org/2017/03/how-safe-are-blockchains-it-depends.

a private blockchain.

Public Blockchains: Risks of Centralization

While public blockchains are theoretically decentralized, there are still risks of centralization. The risk of centralization here refers to the ease with which the nodes in the system may collude and perform a "51 percent" attack. The extent to which a blockchain platform is decentralized is a function of the number of nodes within the system and how they are distributed. The greater the number of nodes and the more geographically distributed, the more decentralized the platform and the lower the risk of a "51 percent" attack.

Even amongst prominent public blockchains, decentralization does not look the same. Both Ethereum and Bitcoin, for instance, are architecturally and politically decentralized, but Ethereum is more decentralized on both fronts. The Ethereum blockchain platform has the most nodes and is the most architecturally decentralized. Ethereum is also the most distributed regarding latency.[15] Ethereum's nodes are widely distributed across the world and have more homegrown entities, giving it greater political decentralization.[16] In contrast, most of Bitcoin's nodes are in data centers, limiting its decentralization.[17] Ethereum nodes are also primarily operated by individuals while Bitcoin's nodes have a higher percentage of institutions and organizations serving as operators.[18]

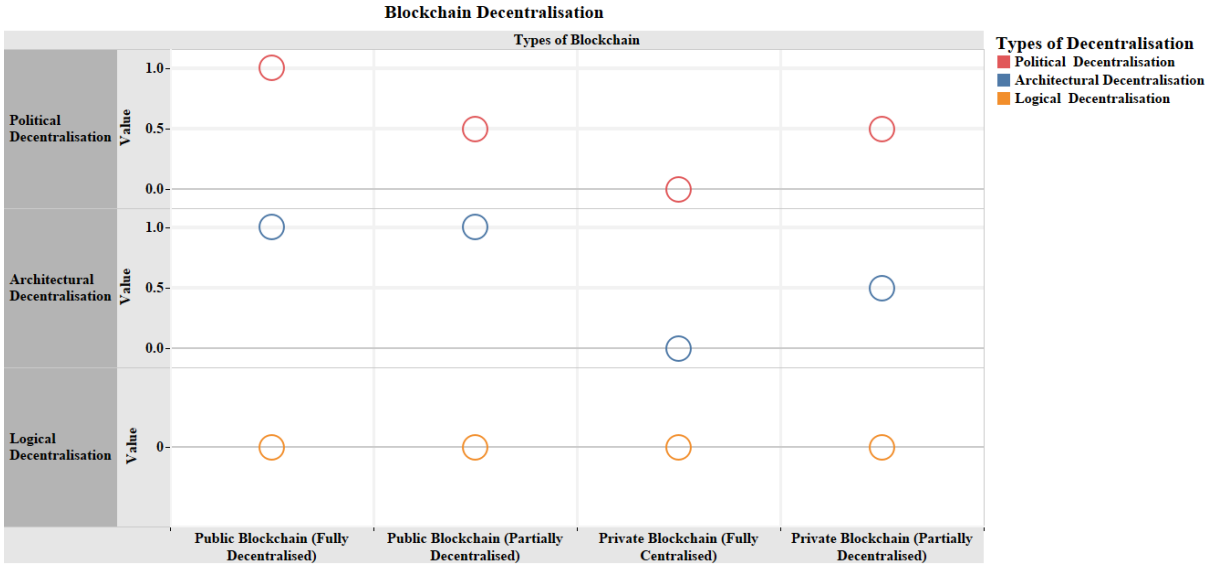

Figure 2: Scale of decentralization

While Figure 2 provides a schema for delineating between private and public blockchains, there are also platforms that straddle both private and public blockchains to serve their intended needs. In the Jupiter Blockchain, data is both stored privately and publicly. Data stored privately on the Jupiter blockchain is stored on the public Waves blockchain as a hash, which

[15] Zane Hintzman, "Comparing Blockchain Implementations," (presentation, 2017 SCTE-ISBE Cable-Tec Expo, Denver, Colorado, October 17, 2017).
[16] Ibid.
[17] Ibid.
[18] Ibid.

is an irreversible form of encryption.[19] This allows for the blockchain to act as both a public and a private blockchain and leverage the benefits of both. Information can be stored privately, but its hashes are still publicly recorded and verifiable on an immutable public blockchain. This grants it greater immutability than a typical private blockchain.

Efficiency

The efficiency of blockchain platforms is inversely related to its decentralization. In a public decentralized blockchain, the verification process to ensure the security of the system limits the number of transactions per second which substantially elevates the amount of computing power required to tamper or alter information. This hampers the efficiency of blockchain platforms such as Ethereum which only manages 20 transactions per second compared to PayPal and Visa which manage 193 and 1667 transactions per second, respectively.[20] The transaction time of a blockchain platform is also tied to its mining power which can lead to reduced cost-efficiency. As more nodes are added, the computational power required increases, which incurs greater costs in maintaining the network.[21] The efficiency of a blockchain platform also depends on its consensus protocol. The Waves blockchain platform is reportedly the fastest and can process up to 190 transactions per second.[22] Waves uses the Bitcoin-NG consensus mechanism for its verification process.[23] It is a form of the proof-of-stake consensus mechanism (See Consensus Protocols).

Scalability

We expect that because TRP will be catering to a relatively small population in its first implementation cycle that scalability is unlikely to be a key concern. As the scope of the project expands, however, scalability is likely to become important, and the TRP will likely encounter the "scalability trilemma." The "scalability trilemma" refers to blockchain's inability to provide decentralization, security, and scalability simultaneously.[24] Given the scalability trilemma, blockchain platforms often sacrifice scalability for decentralization and security.

Thus, while the scalability of the blockchain has been included as one of the key criteria to distinguish these platforms, it is the least likely to be guaranteed. As the scale of the system increases, the amount of data stored within each node also increases.[25] Nodes are thus required to hold larger volumes of data, which require larger storage, bandwidth, and computing power. This could limit the nodes to only being feasible for larger companies and organizations with greater resources, making node distribution more centralized.[26] The only way to ensure decentralization, as well as scalability, would be to distribute information so that each node

---

[19] Frisco D'Anconia, "Is Blockchain Technology Really the Answer to Decentralized Storage?" *Cointelegraph,* May 12, 2018, https://cointelegraph.com/news/is-blockchain-technology-really-the-answer-to-decentralized-storage.

[20] Ibid.

[21] "Is a Blockchain without mining possible?" Medium, last modified December 27, 2017, https://medium.com/@credits/is-a-blockchain-without-mining-possible-9db40edec8b0

[22] Joseph Maurice, "Top 10 Best Blockchain Platforms for ICOs in 2018," *Disruptor Daily,* January 11, 2018, https://www.disruptordaily.com/top-10-best-blockchain-platforms-icos-2018/

[23] "Waves - the fastest ever blockchain", Waves, accessed May 19, 2018, https://waves-ng.wavesplatform.com.

[24] Lotte Schou-Zibell and Nigel Phair, "How Secure Is Blockchain?" *World Economic Forum,* April 20, 2018, https://www.weforum.org/agenda/2018/04/how-secure-is-blockchain/.

[25] Ibid.

[26] Ibid.

does not hold the full volume of data.[27] This would enable the nodes to be more feasibly run by individuals, rather than by large organizations. However, it would also compromise the security of the system, as there would be fewer nodes validating the accuracy of all the data. There are, however, efforts to solve the scalability trilemma, most notably Ethereum's Sharding and Bitcoin's Lighting Network. [28]

Consensus Protocols

The extent of decentralization, efficiency, and scalability of a blockchain platform as well as its architecture is largely determined by its consensus protocol. A consensus protocol is the means by which a blockchain makes decisions without a central authority.[29] It is a group decision making process that attempts to ensure as much agreement as possible, works in favor of the best interests of the group, prioritizes cooperation, egalitarianism, inclusiveness, and participation.[30] It is the method for replicating a shared state across a distributed network to ensure that the state is not lost if one or more nodes crash.[31] This is achieved in a variety of ways, including through the proof-of-work protocol that is used by bitcoin. There are three main objectives that a consensus protocol needs to meet--safety, liveness, and fault tolerance.[32] Safety refers to the probabilistic finality of blocks within a blockchain network.[33] A blockchain network is safe when it does not have two or more competing chains with valid transactions.[34] Liveness refers to the responsiveness of the protocol to validating new transactions. [35] This can be observed when messages broadcast by a node is eventually ordered within the consensus, and messages delivered to one honest node is eventually delivered to all honest nodes.[36] Fault tolerance refers to the ability of a consensus protocol to recover from the failure of a node.[37] Several consensus mechanisms are utilized by blockchain platforms. Some of the key consensus mechanisms are discussed below.

Proof-of-Work (PoW)

The PoW consensus involves miners solving cryptographic puzzles in order to add a block onto the blockchain.[38] Computational power determines one's ability to make decisions on this consensus mechanism. This is because the cryptographic puzzles are designed to be difficult

---

[27] Ibid.

[28] Nick Tomaino, "On the Scalability of Blockchains", *The Control,* March 23, 2018, https://thecontrol.co/on-the-scalability-of-blockchains-ec76ed769405.

[29] "Basic Primer: Blockchain Consensus Protocol," Blockgeeks, accessed April 16, 2018, https://blockgeeks.com/guides/blockchain-consensus/.

[30] Ibid.

[31] Arati Baliga, "Understanding Blockchain Consensus Models," *Persistent Systems,* April 2017, https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf

[32] Ibid.

[33] "Understanding the Basics of a Proof-of-Stake Security Mode," Cosmos, accessed May 1, 2019, https://blog.cosmos.network/understanding-the-basics-of-a-proof-of-stake-security-model-de3b3e160710.

[34] Ibid.

[35] Ibid.

[36] Shehar Bano et al., "SOK: Consensus in the age of Blockchains," Arvix, November 14, 2017, https://arxiv.org/pdf/1711.03936.pdf.

[37] Arati Baliga, "Understanding Blockchain Consensus Models," *Persistent Systems,* April 2017, https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf

[38] Ameer Rosic, "Basic Primer: Blockchain Consensus Protocol," Blockgeeks, January 2018, https://blockgeeks.com/guides/blockchain-consensus/.

and time-consuming to prevent Denial of Service (DOS) attacks.[39] A DOS attack prevents users from accessing information or services.[40] This is prevented by the proof-of-work consensus due to the immense amount of computational power required to execute a DOS on a PoW. Forks are also prevented on the PoW as it is computationally expensive, thus ensuring safety in the PoW consensus.[41] While PoW is safe, transaction finality within the protocol is probabilistic.[42] Transaction finality refers to whether transactions added to the blockchain are final.[43] Transaction finality is probabilistic in the PoW as transactions take time to be confirmed and finalized.[44]

The elements that make the PoW a secure consensus protocol for a distributed network also results in its inefficiency as it consumes an immense amount of power and energy.[45] This also makes it less politically decentralized since most of the mining is concentrated at organizations and institutions with greater computational power. This explains why Bitcoin, which uses the proof-of-work consensus mechanism, is less politically decentralized. This makes the proof-of-work more vulnerable to 51% attacks.

Proof-of-Stake (PoS)

The proof-of-stake consensus mechanism is distinguished from the proof-of-work consensus mechanism in the way in which nodes perform transactions and are incentivized.[46]
Rather than requiring nodes to solve cryptographic puzzles, a proof-of-stake consensus has their network members stake their cryptocurrencies to increase their chances of solving a block and receiving new coins.[47] Staking incentivizes members to work to make the blockchain network succeed since they have a vested financial interest.[48] One's stake in a PoS consensus protocol is directly proportional to the number of transactions that are validated. This means that if you own two percent of Ether, for instance, you would be able to mine two percent of all transactions across Ethereum.[49] One of the concerns with PoS is that power in the network is determined by how rich you are leading to an unequal distribution of power within the network. Like PoW, transaction finality within PoS is probabilistic.[50] However, the transaction

---

[39] Andrew Tar, "Proof-of-Work Explained," Cointelegraph, January 17, 2018, https://cointelegraph.com/explained/proof-of-work-explained.
[40] "Understanding Denial-of-Service Attacks," US Computer Emergency Readiness Team, accessed May 19, 2018, https://www.us-cert.gov/ncas/tips/ST04-015
[41] Shehar Bano, 2017.
[42] Arati Baliga, 2017.
[43] Ibid.
[44] Ibid.
[45] Ameer Rosic, 2018.
[46] Robert Greenfield, "Explaining How Proof of Stake, Proof of Work, Hashing and Blockchain Work Together." *Medium*, July 20, 2017, https://medium.com/@robertgreenfieldiv/explaining-proof-of-stake-f1eae6feb26f.
[47] Jorn Zwanenburg, "Consensus Algorithms Explained: What You Need to Know About Proof-of-Work, Proof-of-Stake and Delegated Proof-of-Stake," *Invest In Blockchain*, May 14, 2018, https://www.investinblockchain.com/consensus-algorithms-explained/.
[48] Ibid.
[49] Jim Manning, "Proof-of Work Vs. Proof-of-Stake Explained," *ETHNews*, November 2, 2016, https://www.ethnews.com/proof-of-work-vs-proof-of-stake-explained.
[50] Tim Kozac, "Consensus Protocols that meet different Business Demands," *IntellectSoft: Blockchain Lab*, March 26, 2018, https://blockchain.intellectsoft.net/blog/consensus-protocols-that-meet-different-business-demands/.

rate of PoS is faster than PoW.[51] The PoS consensus is used by NXT, Tezos, and Ethereum.[52]

Delegated Proof-of-Stake (DPoS)

The DPoS was created to reduce transaction time.[53] It achieves this by delegating the voting and validation procedure to a few participants.[54] Validators of transactions are voted in by coin holders, with the weight of each vote determined by the sum worth of the assets that a voter holds in the network.[55] If a validator fails at their task, voters will vote for a replacement. This allows for the DPoS to function in a decentralized manner as anyone can be a voter if they have a stake in the network, while also allowing for the network to function efficiently. In a DPoS, transactions occur every few seconds.[56] Transaction finality is probabilistic in the DPoS as each transaction still must be confirmed by validators before being finalized.[57] Examples of the DPoS are the EOS and BitShares.[58]

Leased Proof-of-Stake (LPoS)

LPoS works like the PoS, except that it allows for large holders within a blockchain PoS network to lease their coin balances to smaller holders.[59] This allows for smallholders who are relatively poor to have a greater stake in the network and prevents the consolidation of power by a few large nodes. The overall impact of leasing increases user participation in the network.[60] The Waves Blockchain Platform uses the LPoS.[61]

Practical Byzantine Fault Tolerance (PBFT)

In the PBFT consensus protocol, nodes are ordered in sequence with a primary node and backup nodes.[62] The primary node performs a computation when it receives a message and then seeks confirmation from the other nodes within the network.[63] This occurs within a specific time, and the model works under the assumption that the number of malicious nodes in a network cannot simultaneously exceed ⅓ the total number of nodes in a network within a given window of vulnerability.[64] Since the nodes communicate with each other at specific times, consensus can be achieved without the need for confirmation as long as all the nodes approve the proposed transaction.[65] Thus, PBFT allows for immediate transaction finality which improves efficiency.

---

[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] Ibid.
[57] Ibid.
[58] Ibid.
[59] "Blockchain Leasing for Proof of Stake," *Waves Platform*, March 26, 2018, https://blog.wavesplatform.com/blockchain-leasing-for-proof-of-stake-bac5335de049.
[60] Ibid.
[61] Ibid.
[62] Brian Curran, "What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide," *BLOCKONOMI*, May 11, 2018, https://blockonomi.com/practical-byzantine-fault-tolerance/.
[63] Tim Kozac, 2018.
[64] Ibid.
[65] Ibid.

PBFT is used in private blockchains that are more centralized such as Hyperledger and Chain.[66]

Federated Byzantine Fault Tolerance (FBFT)

Unlike the PBFT, FBFT is also designed to be used for permissionless blockchain networks where anyone can join the network.[67] The transactions are verified by a group of validators, thus allowing the FBFT to retain immediate transaction finality.[68] This structure provides partial decentralization while maintaining the efficiency of the network. Examples of FBFT include Stellar and Ripple.[69] The figure below is a table of the various consensus protocols discussed in this report and their properties.

Consensus Protocol	Blockchain Type	Transaction Finality	Transaction Rate	Examples
PoW	Public & Private	Probabilistic	Low	Bitcoin
PoS	Public & Private	Probabilistic	High	Ethereum, NXT, Tezos
DPoS	Public & Private	Probabilistic	High	EOS, BitShares
LPoS	Public & Private	Probabilistic	High	Waves
PBFT	Private	Immediate	High	Hyperledger, Chain
FBFT	Public & Private	Immediate	High	Stellar, Ripple

Figure 3: Consensus protocols

As the figure above shows, the various PoS consensus mechanisms and the FBFT have the greatest amount of flexibility and capacity to fulfill TRP's core objectives. They can be used on both private and public blockchains which allow for TRP to design their desired amount of decentralization. They also have high transaction times which allows for TRP to still prioritize the efficiency of its blockchain platform.

Privacy

One of the primary needs of the TRP with regards to blockchain design is ensuring that personal information is kept private within the context of providing financial inclusion for the Rohingya. For the digital ID to be recognized by financial institutions, it needs to fulfill KYC requirements (See Section 2). A key component of why blockchains are heralded for being secure, however, is that every transaction is publicly verifiable. To bridge this gap while meeting TRP's needs, selective transparency can serve as a solution. There are various modes of ensuring privacy in a blockchain. Some of these include Zero Knowledge Proofs and State Channels.[70]

Zero Knowledge Proof (zk-SNARKS)

Zero Knowledge Proofs are a means of validating the truth of a statement without revealing any specific information.[71] In blockchain technology, Zero Knowledge Proofs allow for the

[66] Ibid.
[67] Ibid.
[68] Ibid.
[69] Ibid.
[70] Michael Smolenski, "Smart Contracts: Privacy vs Confidentiality – Hacker Noon," *Hacker Noon*, October 14, 2017, https://hackernoon.com/smart-contracts-privacy-vs-confidentiality-645b6e9c6e5a.
[71] Lukas Schor, "On Zero Knowledge Proofs in Blockchains," *Medium*, March 23, 2018, https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1.

addresses of the sender and recipient as well as the value amount being transferred to be obscured when the blockchain network verifies transactions. This is achieved using zk-SNARKS which creates challenges deterministically but behaves as if random.[72] This allows it to act as a hash function, so that network validators are not privy to the information within transactions. In this way, it enables privacy in public blockchain platforms.

State Channels

In state channels, sets of transactions between participants are executed and recorded off the chain.[73] Once these transactions are completed, a reference of the transaction is recorded on the blockchain.[74] State channels essentially allow for participants to have two-way discussion channels off the chain.[75] Transactions can be signed and verified off chain through the use of private keys to ensure that the information is true and authorized.[76] State channels allow for greater efficiency because less information is stored on the blockchain and thus less computational power is required for the network to function.[77] This creates higher transaction rates and allows for information to be kept both securely and privately.

Both Zero Knowledge Proofs and State Channels are possible tools that can be added to TRP's blockchain digital ID. The application of zk-SNARKS would be best suited for the purposes of making the exchange of financial services on the blockchain platform private. It would prevent the exchange of finances between the Rohingya to be made public, so as to mitigate the risk of surveillance by bad actors.

The application of State Channels would be best suited to the storage of TRP's personal, private information. One of the concerns of data storage on blockchain platforms is that it reduces efficiency as each node would have to contain massive amounts of information. State Channels enable a blockchain platform to remain efficient since most private information is kept off-chain whilst still allowing for the validity of the private information to be publicly verifiable.

A study into the structural components of blockchains reveals that the design architecture of TRP's blockchain digital ID is likely to need separate chains to meet both its needs of facilitating the exchange of financial services and the storage of private data. To fulfill its core objectives of decentralization, efficiency, scalability, security, and privacy, TRP will need to incorporate a private, partially decentralized blockchain platform with a PoS or FBFT consensus protocol in its architecture. If financially feasible, TRP could model the Jupiter blockchain example and store the private data of the Rohingya as a hash on a public blockchain so as to render the data immutable. Successful implementation of a blockchain digital ID for the Rohingya will require tailoring each component of the blockchain to the five core objectives identified.

---

[72] Gideon Greenspan, "Understanding Zero Knowledge Blockchains," *MultiChain*, November 3, 2016, https://www.multichain.com/blog/2016/11/understanding-zero-knowledge-blockchains/.
[73] Michael Smolenski, 2017.
[74] Ibid.
[75] Stephen Tual, "What are State Channels," *Medium*, January 3, 2017, https://blog.stephantual.com/what-are-state-channels-32a81f7accab.
[76] Antonio Madeira, "What are State Channels," *CryptoCompare*, May 20, 2018, https://www.cryptocompare.com/coins/guides/what-are-state-channels/.
[77] Ibid.

Risks of Blockchain Application for Stateless Rohingya

Certain risks are foreseeable in the application of blockchain based digital identification for stateless people. Since the application would require the Rohingya to have access to a smartphone, there could be financial impediments to accessing digital identification. Much of the Rohingya diaspora are not integrated into the formal economy partly due to their lack of access to documentation that can prove their identity. They are also a vulnerable population susceptible to various abuses including financial predation. It is thus imperative in applying this technology that they have the opportunity and appropriate information to provide affirmative, informed consent. This can be partly facilitated by having the smartphone-based application include the Rohingya language as well as audio (text-to-speech) assistance for the illiterate.

Another set of risks are associated with centralizing collected data before it is transferred to the blockchain. As the information is being collected and verified, there needs to be a protocol in place to destroy that information so that it is not vulnerable to being compromised. A Shred-It-All policy, where all sensitive information documented on paper is shredded after it is transferred to the blockchain, would assist in mitigating these risks. Similarly, digital files should also be removed from any vulnerable database.

Section Conclusion

It is evident through studying the various components of blockchain that designing a blockchain platform requires considering a multitude of tradeoffs. To create a blockchain platform that is effective requires tailoring the architecture of the system to best suit an organization's specific needs. This section has highlighted the key factors that should be considered when deciding how a blockchain platform should be designed. It explores how decentralization, efficiency, privacy, scalability, and security are affected by the type of blockchain platform utilized as well as the type of consensus protocol built into the platform. The technology is currently unable to provide complete solutions that will allow for all TRP's objectives to be met. However, there are architectural designs which make strategic trade-offs in enabling TRP to achieve most of its core objectives.

Section Recommendations

- For the TRP to be able to fulfill its core objectives of decentralization, efficiency, scalability, security, and privacy, we recommend that TRP utilize a partially decentralized blockchain with a proof-of-stake consensus mechanism. The type of proof-of-stake consensus mechanism utilized will depend on which of the core objectives TRP wishes to prioritize.
- Given that this technology is going to be used by a vulnerable population whose information is sensitive, TRP needs to carefully consider how to make its blockchain digital identity private and secure. We recommend that TRP explores the use of State Channels as well as Zero Knowledge Proofs to maintain privacy while still leveraging the benefits of an immutable blockchain platform.

Section 2: International Frameworks: Building TRP's Legitimacy & Reputation

Questions:

1. How can the TRP operate within the global KYC standard with a blockchain platform for stateless Rohingya?
2. What are the best practices regarding digital ID and blockchain identification systems, and how can these be implemented in the target pilot nations of Bangladesh, the Kingdom of Saudi Arabia, and Malaysia?

Introduction

Addressing the financial exclusion of the Rohingya necessitates an understanding of the requirements needed to enter the internationally regulated financial system. Although banking processes may differ around the world, most banks conform to the core regulations prescribed by the Financial Action Task Force (FATF). Following 9-11 and the US Patriot Act, two sets of standards were adopted to improve international capacity to counter money laundering and terrorist financing within the global banking system. Members of the FATF adopted know your customer (KYC) and customer due diligence (CDD) standards that require banks and financial institutions verify banking clients' identities and the legal source and destination of their monies. At the center of these standards was the requirement that a client produce state-sanctioned identification form. Consequently, those people displaced from a nation-state without legal paperwork, those people whose nation-state collapsed, or those people living within a nation-state that does not provide citizenship identification were effectively excluded from international banking systems. Initially, stateless individuals, like the Rohingya, were effectively excluded from global financial systems without recognizable, state-sanctioned identifying verification.

The implementation of KYC and CDD standards throughout the regulated financial system increased the emphasis on individual possession of state-provided and sanctioned identification. Because the KYC and CDD standards were created with state-sanctioned identity at the core of their logic, its use became central to extending financial inclusion. As TRP aims to provide Rohingya with feasible alternatives to the use of state-sanctioned identification, an examination of potential measures and opportunities presented by the current FATF model and its future trajectory can highlight potential points of entry into the global financial sector for those lacking state-backed IDs.

As this platform is launched, TRP can learn some lessons from existing digital identification systems adopted by other nations. Furthermore, by examining current efforts by the UN to push for innovative uses of blockchain technology can help to provide a generalized and acceptable framework for the TRP platform. Various projects by the international community represent interest and support for project growth, as well as additional frameworks for such a development.

By taking lessons from previously launched digital identification systems and blockchain identification systems, TRP can begin to consider the reality of launching their platform in the initial pilot countries of Bangladesh, Saudi Arabia, and Malaysia. The support of digitized IDs in Bangladesh benefits TRP. However, the use of biometrics and labels of the current Rohingya ID system and current repatriation efforts are of concern of TRP. Biometrics are also a concern

in Saudi Arabia, where they are being used for their national ID system. In Malaysia, financial institutions are allowed to determine authenticity at their will, as long as it meets basic FATF and KYC requirements. However, biometrics are presented as an assurance of acceptable identification.

Adoption of Global KYC, CDD & the Modern ID Verification System

The FATF is an intergovernmental body, established in 1989, whose objectives are to create recommendations for evidence-based anti-money laundering and counterterrorist financing (AML/CTF) policies for financial institutions around the world.[78] The FATF regulates and influences banking processes in every associated nation and is comprised of 37 members nations, two observer nations, ten regional organizations of associate members, and 22 observer organizations. The potential TRP pilot nations are participants in the FATF – Malaysia is a member, Saudi Arabia is an observer, and Bangladesh is an associate member via their membership in the Middle East and North Africa regional FATF (MENAFTAF).[79]

In the early 2000s, the US Patriot Act introduced new requirements that all US banks must conform to know your customer (KYC) and customer due diligence (CDD) standards. These additional standards were then adopted by the FATF, creating the contemporary standards for entry into the global financial system. The standards created by the Patriot Act, and then adopted by the FATF, were designed to enhance the previous AML/CTF recommendations with the addition of KYC and CDD standards. The KYC and CDD standards are central to global identity verification.

Under the FATF recommendations KYC standards require that banks: (1) determine the identity of prospective customers; (2) identify the source of funds for customer transactions; (3) determine a customer's "normal and expected" transactions; (4) monitor accounts for transactions that are "not consistent" with such normal and expected transactions; and (5) determine whether such transactions are unusual or suspicious.[80] The latter two recommendations suggest that TRP's blockchain digital ID will need to be private, with a consensus protocol that has a limited number of validators so as to allow for greater executive control to ensure that KYC standards are met.

Customer due diligence (CDD) requires that financial institutions be able to predict the likely financial behavior of their clients. Most commonly this takes the form of gathering information about customer income and work history.[81] Under the FATF recommendations, CDD standards require banks to know and be able to predict the financial behavior of their customers in order to identify criminal activity more readily. Like KYC, this requires financial institutions to acquire and retain additional information about their customers which may assist in the banks' ability to predict their financial habits. Because this is not easily done for customers with limited or alternative ID, financial institutions can mitigate the risk they face by providing clients with various levels of financial services. Although these approaches can vary, the basis of a tiered CDD (customer due diligence) is a gradient of financial services dependent upon

[78] "Who We Are," Financial Action Task Force (FATF), accessed April 16, 2018, http://www.fatf-gafi.org/about/whoweare/.
[79] Ibid.
[80] Paul Stevens and Thomas Bogle, "Patriotic Acts: Financial Institutions, Money Laundering and the War against Terrorism," *Annual Review of Banking Law* 21 (2002): 261–92.
[81] Ibid.

the level of client risk as determined by the bank. Clients who pose an undeterminable risk provided first-tier services granting them access to the most basic account.[82] Such accounts are subject to restrictions, such as transaction and account limits, or the requirement that financial services be conducted in person. The number of tiers, the way they are categorized, and the movement between tiers will vary by circumstance (see appendix A, China).[83] By offering low volume services, the tiered approach simultaneously grants inclusion while reducing the appeal of criminal activity by preventing the movement of large sums of money (see appendix A, Guatemala). As clients develop their reputation and establish their credibility, they can move up the CDD tier.

As a result of FATF's global influence, these recommendations initially produced two unintended consequences: 1) low compliance on the part of financial institutions and 2) the financial exclusion of specific individuals.

In 2014, the FATF responded to low global levels of compliance by making their recommendations more explicit.[84] As a result of this change, compliant banks opted to increase the rigor of current data collection and verification methods. The new collection of data, which included things such as a home address or employer reachable by phone, became commonplace in the identity verification process of banks. To the extent that the disclosure of additional information may enhance crime prevention, the enhanced FATF recommendations also introduced new barriers to the financial inclusion of individuals who lack traditional forms of identity verification.

Although international identity verification practices have expanded to include a range of data, no one component is more essential than national ID. Because national IDs are the core of identity verification across the world, the lack of national identity and statehood has long frustrated the attempts of the Rohingya to access the global regulated financial system.

Recommendation ten of the FATF's AML/CTF processes requires "reliable and independent source documents, data or information" (identification data) to verify customer identity. There are two points at which financial institutions must verify customer identity. The first requires that financial institutions verify customer identity at the time of application. This requires identifying the (future) customer at the point of account set-up, in some cases, no identification is necessary (see Appendix A, China). Conventional means of identifying the customer include the date of birth, gender, the source of income, and address. The second is identity verification. This refers to the verification of customers as they use their accounts. This requires reliable, independent source documentation, data or information that confirms the veracity of the identifying information. The most conventional means of identity verification are traditional identification documents (such as government issued ID), mother's maiden name, PIN, and signature.

The FATF recommendations do not establish any specific requirements regarding how ID data should be collected or verified. As mentioned earlier, this has resulted in a conservative reading of the regulations with a narrow range of conventional adaptations. This has largely been

[82] "FATF Guidance: Anti-money laundering and terrorist financing measures and financial inclusion," Financial Action Task Force, November, 2017, http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf.
[83] Ibid.
[84] Ibid.

influenced by regulators such as the Basel Committee on Banking Supervision and their General Guide to Account Opening and Customer Identification and the FATF itself.

In an effort to broaden financial inclusion the FATF and its members have developed strategies to expand financial access.[85] Given that the strategy for mitigating financial risk is currently based on the ability for banks to identify and predict the financial needs of its customers, the FATF provides two strategies to mitigate financial exclusion while maintaining current standards.[86]

The first strategy aims to expand the identity verification process by permitting the use of non-traditional means of identity verifiers such as referees and biometrics. One of the most well-known forms of alternate verifier is biometric data. Enthusiasm about biometrics has increased as things like fingerprint reading technology have seemed to resolve issues around pins and passwords in mobile devices. Although fingerprint and retina scanners provide access to one form of biometric verifiers, these technologies are expensive, and it should be noted that something as simple as a photograph qualifies as biometric data.

The second form of alternative verifiers is personal referees. Use of a referee, as a measure of verification, would have large impacts on individuals that lack traditional forms of ID. A referee is a person, often a reputable community figure, whose statement is regarded as official testimony in the verification of a person's identity.[87] In practice, referees have included people ranging from indigenous community elders to landlords, teachers.[88] As TRP's processes will include numerous interviews, the current use of referees provides an ideal framework for TRPs objectives. However, there are risks implicit in the use of referees on a vulnerable population (See Section 1, Risks of Blockchain Application for Stateless Rohingya).

Central banks and financial intelligence units have the liberty to choose how and if they perform identity verification when individuals are unable to provide "traditional" identification by preparing guidelines of alternatives. Alternatives may include a voter or tax card (see Appendix A, e.g., Chile), employment card or even, possibly, a "reference letter from a 'suitable reference.'" In some cases, this is a bank designated person such as a current bank customer, in other instances, the government has allowed indigenous community leaders, teachers or landlords, or government employees (see Appendix A, e.g., Fiji or Peru). In several cases, the use of referees provides applicants a means to obtain not only a bank account but a local government ID. In countries which allow this process, the applicant's file may be accompanied by a clarifying memo that their application was verified by a government employee (see Appendix A, e.g., Switzerland or European Union). To mitigate coercion and prevent human trafficking, it may be stipulated that the referee has no financial ties to the applicant (see Appendix A, e.g., New Zealand).[89]

---

[85] Ibid.

[86] Ibid.

[87] "Aboriginal and/or Torres Strait Islander People," Australian Transaction Reports and Analysis Centre (AUSTRAC), Commonwealth of Australia - AUSTRAC 2018, May 4, 2018, www.austrac.gov.au/aboriginal-andor-torres-strait-islander-people.

[88] FATF Guidance, 2017.

[89] "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion," Financial Action Task Force, February, 2013, http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf.

The second strategy encourages banks to provide more opportunities for individuals to access first-tier, limited financial services. In most cases, limited bank services restrict the volume of financial transactions and account balances for bank clients. As these accounts pose a low risk to financial institutions, they can be accessed with limited or unconventional IDs. An unconventional ID is any ID that is not backed by a state or national body.

When considering the practical uses of a TRP built blockchain ID system, the following scenario may occur when using the CDD tiered approach and an initial point of entry. An individual with a TRP, non-state-issued ID may be offered a limited, first-tier account with a banking institution. Initially, this individual may be restricted to a low account balance, e.g., $100-$5,000 USD, and their transactions may be limited to reflect the purchasing power of basic needs, such as daily groceries and monthly housing. However, over time, responsible use (consistent funds, transactions, lack of overdraft) of this account will display a track record of good finances. Working to a similar extent as a credit-score-system, this positive track record may later lead to increased opportunities to access broader financial services. This is due to the fact that with time and use, financial institutions will be able to predict the financial patterns of the individual better using these limited accounts, fulfilling KYC requirements.

Although the CDD tiered approach may appear as an attempt to exclude individuals without traditional ID by limiting the range of available financial tools, it also serves as a point of entry for stateless Rohingya to build credibility within financial institutions without a need for state-backed IDs or employment history. Although the FATF provides these strategies as a means to alleviate financial exclusion, there remain several practical implementation concerns. Further, the unprecedented nature of TRP's project makes it difficult to predict unforeseen risks. These concerns are reflected in the PSTL framework mentioned above. Our PSTL framework anticipates legal hurdles due to lack of legal precedent regarding digital IDs, which may result in financial institutions employing these practices differently, depending on nation and institution. Likewise, the existence of alternative methods (CDD and referees), which substitute for national IDs, may extend the timespan required for applicants to open an account. Lastly, FATF literature repeatedly describes processes as accessible to 'low-risk' applicants but does not provide clear indications or recommendations for how to define 'low-risk.' This ambiguity is likely to result in processes whose effectiveness is determined by the subjective implementation by agents as local as a bank employee. These are risks TRP can interpret as they see fit.

Acknowledging that all IDs are susceptible to potential fraud and abuse, the FATF suggests mitigation measures which include:

- Enhanced monitoring of the business relationships of holders with alternative IDs;
- Background checks on the integrity of "referees" and their relationship to the client;
- Cooperation between financial institutions and national governments to promote flexibility through education, dialogue, and feedback; and
- Increasing awareness that technological solutions can pose challenges such as insufficient connectivity or network strength and expenses for real-time verification.

FATF and Islamic Finance

Given that Islamic financial institutions are concentrated in the Middle East and South Asia, it is important to understand to what extent their policies reflect FATF guidelines.[90] In 2016, the

[90] Kyriakos-Saad et al., "Islamic Finance and Anti-Money Laundering and Combating the Financing of Terrorism

International Monetary Fund reported that relatively little research had been done on the state of AML/CTF risks in Islamic finance.[91] However, Islamic finance practices, such as adherence to Riba, appear not to affect the AML/CTF risk.[92] The current assumption is that criminals target financial institutions based on convenience and opportunity.[93] Lack of Islamic Finance specificity in AML/CTF guidelines and a paucity of oversight may put Islamic Finance at risk.[94] It is possible that these circumstances will engender greater scrutiny from the international community for any unconventional practices relating to identity verification or that fear of such scrutiny may result in more cautious behavior on the part of Islamic Finance institutions.

Two areas which are neglected by the current AML/CTF policies and may pose risks are the nature of the customer relationship and the complexity of Islamic finance products. Rather than an "institution to customer" relationship, Islamic financial institutions employ a "partner" relationship. This may add weaknesses in the monitoring or reporting of suspicious transactions.[95] Additionally, that financial institutions as "partners" may be held in joint liability with the criminal activity of other members may result in more lax or restrictive policies. The complexity of Islamic financial products such as Tawarruq may enable criminal activity not found in conventional financial institutions. Tawarruq allows for commodities to back the transfer of funds and can potentially enable the rapid exchange of funds in a manner conducive to money laundering.[96] However, all these potential risks remain speculative.

The FATF, in response to growing international concern for financial inclusion, has proposed ways to comply with their processes while maintaining the AML/CTF framework.[97] However, there are still many gaps present in the FATF's attempts to increase financial inclusion. Although FATF recommendations are intended to apply to the global financial system, they often are not written in terms conducive to the structures and terminology of Islamic finance.[98] This is noteworthy given the key role of Islamic financial institutions in implementing counterterrorism finance measures. The IMF notes that although many AML/CTF recommendations have been implemented in Islamic financial institutions, there has not been adequate monitoring, evaluation, or follow-up.[99]

Likewise, though the FATF has a current interest in the proportionality of their approaches, there is also increased enthusiasm for the use of biometric data for all populations.[100] Given the potential vulnerabilities for the Rohingya population for using biometric data, the strategies in the following sections reveal methods which can verify and authenticate identities with minimal use of biometric data and that can be incorporated into a blockchain platform.

(AML/CFT)," Social Science Research Network Scholarly Paper, Rochester, NY: February 1, 2016, https://papers.ssrn.com/abstract=2754948.

[91] Ibid. P.4

[92] Ibid.

[93] Ibid. p.8

[94] Ibid. p. 9

[95] Ibid. p. 9

[96] Ibid.

[97] Ibid.

[98] Ibid.

[99] ibid.

[100] Joon Wong, "The UN is using Ethereum's technology to fund food for thousands of refugees", QUARTZ, November 3, 2017, https://qz.com/1118743/world-food-programmes-ethereum-based-blockchain-for-syrian-refugees-in-jordan/.

FATF Subsection Conclusion

More than any other organization in the world the FATF's recommendations shape the regulatory environment governing the policies which permit or prohibit access to the regulated financial system. As a result, it is important to remain aware of the programs they approve or endorse particularly as they continue to show interest and flexibility toward the changes and innovations necessary to expand financial inclusion while remaining within the framework of their recommendations.

Digital ID Systems: Cases & Best Practices

According to the World Bank, some 1.5 billion people lack proof of legal identity.[101] That is why, as part of the UN's sustainable development goals (SDGs), target 16.9 aims to achieve "legal identity for all" by 2030.[102] Although the examined case studies do not solely aim to mitigate the issue of statelessness, their achievements serve as useful guidelines. Here, we examine a number of governmental and non-governmental blockchain ID solutions and note the best practices which can be applied to TRP. We also note multilateral initiatives that aim to solve the issue of statelessness; TRP may benefit from awareness of these projects.

Estonia

Estonia was the first country to herald a blockchain paperless identification option when it offered e-ID cards to members of its "e-Residency" program in December 2014.[103] The intention behind this project was to help streamline international business by providing a "sovereign government-backed identity credential."[104] Today, it is the most advanced government-supported digital identity program in the world. [105] However, it does not count as a form of citizenship or right to travel physically, and E-Residents lack access to all services provided to Estonian citizens. E-residents receive a smart ID card as a form of digital authentication for services. The Estonian government works with some private companies to provide blockchain authentication services.[106]

The particular blockchain technology, developed by Estonian firm Guardtime, is called KSI (Keyless Signature Infrastructure) Blockchain, has been adopted by the US Department of Defense and NATO.[107] The KSI Blockchain is a public blockchain that stores its data as hashes. These hashes are publicly verifiable as signatures with information such as time of entry,

---

[101] "Technical Standards for Digital ID, Draft for Discussion," The World Bank Identification for Development (ID4D) initiative, 2017, http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf.

[102] Sustainable Development Solutions Network, "Indicators and a Monitoring Framework, Launching a Data Revolution for the Sustainable Development Goals," May 15, 2015, http://indicators.report/targets/16-9/.

[103] Clare Sullivan and Eric Burger, "E-residency and Blockchain," *Computer Law & Security Review.* 33, no. 4, (August 2017): 470-481, doi:10.1016/j.clsr.2017.03.016. https://www.sciencedirect.com/science/article/pii/S0267364917300845.

[104] Ibid.

[105] Ibid.

[106] Kaspar Korjus, "Welcome to the Blockchain Nation," *Medium,* July 7, 2017, https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4.

[107] "Estonian Blockchain Technology: Frequently Asked Questions," E-Estonia, accessed May 3, 2018, https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf.

attribution of origin and integrity of the data.[108] The consensus protocol used by KSI blockchain has a limited number of validators which allows for transaction finality and allows for a higher transaction rate. This enables the KSI blockchain to retail all elements of the TRP's core objectives, decentralization, privacy, efficiency, scalability, and security.

The blockchain cryptographic proof of technology is used to protect the integrity of Estonian public services such as e-Banking, e-Law, e-Court systems, e-Police data, and the e-Land registry. The data on the blockchain is theoretically immutable and extremely effective at detecting crime.[109] Other Estonian companies which support public information security include NETgroup, Aktors, (which support the e-Court system), Nortal (involved in data protection), and Rosknet (a secure communications system between governments and businesses).[110]

E-Residents can also access banking services online, transfer funds electronically, and sign documents with digital signatures. One benefit to the Estonian e-Residence system is that the application only requires a scan of a single identity document (such as a passport or national ID card). On the other hand, as mentioned in Section 2, KYC requirements for most financial institutions usually require several forms of identity. According to the Estonian government, "the digital signature and authentication are legally equal to handwritten signatures and face-to-face identification in Estonia and between partners upon agreement anywhere around the world."[111] It should be noted that to access these banking services, banks are obligated to comply with the Estonian banking code of practice and, like most financial institutions, with AML/CTF legislation. New technologies intend to streamline this process. Estonia's largest national bank, LHV, is collaborating with a startup called LeapIn to develop a face-to-face video link system, allowing identity verification to be carried out from anywhere in the world. Cybernetica, a private Estonian R&D and IT company, is exporting the technology behind Estonia's X-road program to several other countries, including Finland, Haiti, and Namibia.[112]

Nongovernmental Perspectives on Blockchain and Digital IDs

The UN has expressed interest in the utilization of blockchain for identification services. Since the UN prioritized universal identification as a Sustainable Development Goal (SDG 16.9), the global community has shown increasing interest in technology innovations, such as digital identification systems or biometric identification systems. International organizations, such as the Association of Southeast Asian Nations (ASEAN) and the United Nations (UN), already view digital IDs as a partial remedy for the resettlement of refugees.[113] These organizations view digital identification systems as an economically efficient, long-term solution to providing identification for the 1.1 billion people who lack it.[114] This section will address

---

[108] "Keyless Signature Infrastructure," Guardtime Federal, accessed June 2, 2018, *https://www.guardtime-federal.com/ksi/*

[109] Ibid.

[110] "KSI Blockchain," E-Estonia, accessed May 3, 2018, https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/.

[111] Clare Sullivan and Eric Burger, 2017.

[112] "Estonian E-solutions Everywhere," E-Estonia, May 2016, https://e-estonia.com/estonian-e-solutions-everywhere/.

[113] "Committed to Improving Lives through Digital Identity," *ID2020 Alliance*, 2017, accessed May 4, 2018, https://static1.squarespace.com/static/578015396a4963f7d4413498/t/596e5d636a49635fe12cf40b/1500405109983/ID2020+Alliance+Governance.

[114] Ibid

possible legal barriers that TRP may encounter. There are several different forms of digital identification, but blockchain is a recently proposed system that may ameliorate issues surrounding statelessness. The use of blockchain for identity is new, and the legal framework for digital IDs and blockchain is undeveloped.

The United Nations has proposed the development of blockchain, digital identification, and identity management as possible solutions for statelessness.[115] Within the Electronic Commerce Working Group, the UN Commission on International Trade Law examined the possible ramifications and considerations that should be put into place within international institutions.[116] Many of their concerns revolve around jurisdiction because in this case of identification they do not respond to a particular nation-state.[117] Were there to be fraudulent activity committed using a blockchain authenticated ID, the lack of a centralized authority will cause confusion. Moreover, the question of who holds jurisdiction of processing this type of criminal activity means that the international community will need to find the proper legal framework to indict. This may present an obstacle for TRP as any identification system aimed at the stateless will need to present a concrete process for assessing criminal activity.

As there lacks precedent for this project, solutions are not yet established for these types of issues, leading to wariness and possible distrust in the system. Distrust among international organizations and states is best addressed through transparency. While wary, international organizations like the UN view blockchain technology as an innovation that will deliver positive returns.[118] This can be referred to in the Ethereum-based project that the UN has used to identify Syrian refugees in Jordan. This can be referred to in the Ethereum-based project that the UN has used to identify Syrian refugees in Jordan. The UN will require transparency from all organizations which offer digital IDs for stateless populations.[119] At this point, laws surrounding blockchain technology for identification are vague and will likely remain so until the technology is further developed.[120] Therefore, it is necessary that TRP continues to observe the international community attitudes towards blockchain technology being used for identity purposes. The UN project in Syrian Refugee camps to distribute aid via a private fork of the Ethereum blockchain reveal that UN's preference for the use of a private blockchain platform. The data on the blockchain is secured through the use of biometrics, which allows the refugees to use their "eyes as wallets" to shop inside the camps and withdraw cash from ATMs.[121] This is likely to indicate international preference which could result in pressure to include biometrics on the blockchain. However, biometrics are not required as an international standard. This loose framework will work to the benefit of TRP as international communities are not likely to push for regulations that counter TRP efforts. By supporting a bond with international organizations, complete with transparency, TRP will experience low-level push back as long as risk remains low.

---

[115] Ibid.

[116] Ibid.

[117] Ibid.

[118] Ibid.

[119]. "Legal Issues Related to Identity Management and Trust Services", United Nations Commission on International Trade Law, Fifty-fifth session, February 20, 2017, https://documents-dds ny.un.org/doc/UNDOC/LTD/V17/010/89/pdf/V1701089.pdf?OpenElement.

[120] Ibid, 2.

[121] Sneha Indrajit, "The Cybersecurity Risks of Using Biometric Data to Issue Refugee Aid," Jackson School of International Studies, July 25, 2017, https://jsis.washington.edu/news/cybersecurity-risks-using-biometric-data-issue-refugee-aid/.

This environment has the potential to encourage innovation from groups, like blockchain ledgers or digital ID platforms like TRP. For stakeholders in TRP, this process should be watched closely and, more importantly, efforts should be made to garner a seat-at-the-table among relevant organizations and processes. As this initiative is in the early stages, along with other blockchain distributed ledger projects, TRP is afforded the opportunity to enter the international community discourse to present what this technology can do for stateless. International organizations will refrain from creating legislation until blockchain is developed further.[122] TRP should advocate for transparency over-regulation which would slow the goals of TRP. The extent to which the international community supports organizations like TRP will be critical in the implementation of digital IDs for stateless people across the world.

One notable project that TRP should be aware of is the ID2020 alliance, a project launched in 2014, which hopes to provide a legal identity for all, including birth registration and supports the same UN SDG Target 16.9 – legal identity for all. The project is supported by public-private partnerships, with Microsoft, Mercy Corps, Hyperledger, and the UN International Computing Center having joined as partners this year. Microsoft donated $1 million to the project, joining Accenture and the Rockefeller Foundation as major donors.[123]

Microsoft, partners in the project, and developers intend to create an "open source, self-sovereign, blockchain identity system," allowing individuals, apps, and services to interoperate across cloud providers, blockchains, and organizations. However, the project seems to be far behind schedule; as of April 30, 2018 (the organization's latest blog post as of May 25), the project is accepting "pilot project proposals," which indicates that the alliance is only in the planning stages.[124]

Non-governmental involvement in TRP is critical and unavoidable. Certain international groups, like the UN, have a significant interest in the cultivation of blockchain technology for multi-purposes, like that of statelessness. Though interested, there is little legal framework oriented towards blockchain technology at this moment. There exist certain legal concerns surrounding jurisdiction towards criminal activity with blockchain technology, but blockchain as a tool for identity exists with little regulation, which will serve to benefit TRP as it innovates and develops. TRP should advocate in the international community for this project and should support transparency in its development over regulations at this stage. TRP should take notice of initiatives like ID2020, which aims to solve worldwide statelessness with the use of blockchain technology. While it is behind schedule, advancements in this objective should be watched.

National Case Studies of Non-blockchain Digital ID Systems

This subsection reviews citizen-focused digital ID frameworks in several nations. As TRP plans to implement a blockchain digital ID system in pilot nations of Bangladesh, Saudi Arabia, and Malaysia, this section will examine the key takeaways of the long-established digital ID programs in Pakistan and India.

---

[122] Soonduck Yoo, "Blockchain Based Financial Case Analysis and its Implications," *Asia Pacific Journal of Innovation and Entrepreneurship* 11, no. 3 (2017), doi:10.1108/APJIE-12-2017-036.

[123] "The ID2020 Alliance Announces New Partners in Digital Identity Initiative," PR Newswire, January 22 2018, accessed May 3, 2018, https://www.prnewswire.com/news-releases/the-id2020-alliance-announces-new-partners-in-digital-identity-initiative-300585991.html.

[124] "ID2020 Accepting Pilot Project Proposals," ID2020, April 30, 2018, https://id2020.org/news/2018/4/30/id2020-accepting-pilot-project-proposals.

The fact that the technical specifications of both Pakistan's and India's digital ID systems conform to ISO (International Organization for Standardization) norms is a relevant takeaway for TRP. Furthermore, the case of India's Aadhaar system demonstrates success in enrolling over a billion people into a digital ID system. Pakistan's program provides a useful example: remote verification of smart identity cards. However, as will be described below, the inherently centralized nature of Pakistan's and India's digital ID systems has rendered them both susceptible to security breaches and leaks of personal data.

Pakistan

In Pakistan, the digitization of citizenship and issuance of electronic identification cards is wide-reaching, with approximately 96% of its 180 million citizens registered in the National Database and Registration Authority (NADRA) system.[125] The government provides two types of identity card documents: Computerized National Identity Cards (CNIS) and the newer Smart National Identity Card (SNIC). Smart National Identity Cards (SNICs) are chip-based identity documents that allow for remote verification of a user's identity and citizenship, in compliance with ISO/IEC 7816, the international standard related to electronic ID cards.[126] SNICs allow cardholders to verify their identity for voting, to receive pensions, and other government services. According to NADRA, SNIC is one of the most secure cards in the world, boasting 36 security features in the card's design. The card itself consists of different layers, which each contain different security features. The older version, the SNIC, only has 16 security features. Remote verification of identification and citizenship is possible using a CNIC or SNIC reader application on mobile phones and are machine-readable.[127]

The SNIC cards include a chip which stores a digital photograph of the owner and four fingerprints on file. When these data are accessed (scanned and matched by a reader), they do not leave the chip itself; the reader system verifies whether it is a match or not. The card is usable as an identity credential in more than 100 airports worldwide because it complies with international standards for machine-readable travel documents (ISAO 9303).[128]

Because not all Pakistanis lived within a close distance of a NADRA center, the institution developed an online web-based platform to issue IDs to overseas Pakistanis. NADRA processes the cards and mails them out to the current address that the user entered in his or her application. However, mailing out physical IDs may be a security risk for TRP. To implement advanced biometric data collection, NADRA partnered with France-based Sagem and US-based Cogent Systems. NADRA collects fingerprint data and facial imagery.[129]

---

[125] Ayesha Siddiqi, "'Disaster Citizenship': An Emerging Framework for Understanding the Depth of Digital Citizenship in Pakistan," *Contemporary South Asia*, November 27, 2017, doi: 10.1080/09584935.2017.1407294 https://www.tandfonline.com/doi/abs/10.1080/09584935.2017.1407294?journalCode=ccsa20

[126] "About Us", National Database and Registration Authority (NADRA), accessed May 3, 2018, https://www.nadra.gov.pk/.

[127] "From an Idea to Reality: Pakistan's Smart Card," *The News CN*, November 11, 2012, https://www.thenews.com.pk/archive/print/395365-from-an-idea-to-reality-pakistan%E2%80%99s-smart-card.

[128] Tariq Malik, "Technology in the Service of Development: The NADRA Story," *Center for Global Development*, November 7, 2014, https://www.cgdev.org/sites/default/files/CGD-Essay-Malik_NADRA-Story_0.pdf

[129] Rabia Garib, "A Database is Born: NADRA in the Early Days," *Network World*, May 14, 2009, https://www.networkworld.com/article/2255157/applications/a-database-is-born--nadra-in-the-early-days.html?page=2.

India

In 2009, the Unique Identification Authority of India (UIDAI) established what is now the world's largest biometric ID system, Aadhaar, with 1.19 billion holders as of 2017. It functions as a physical (ID card) and digital form (PDF) to demonstrate one's identity to access services such as banking, purchasing a phone, and other public services. Aadhaar is built on an open platform, which allows external organizations to re-engineer its application programming interface (API) to create new, connected services. These 'layers' of services, known as the 'India Stack,' the world's largest open API, have enabled a digital infrastructure that can provide presence-less (no need for physical authentication), paperless, and cashless service delivery from anywhere in India. Aadhaar can be leveraged to authenticate new customers for banking services (e-KYC) digitally.[130]

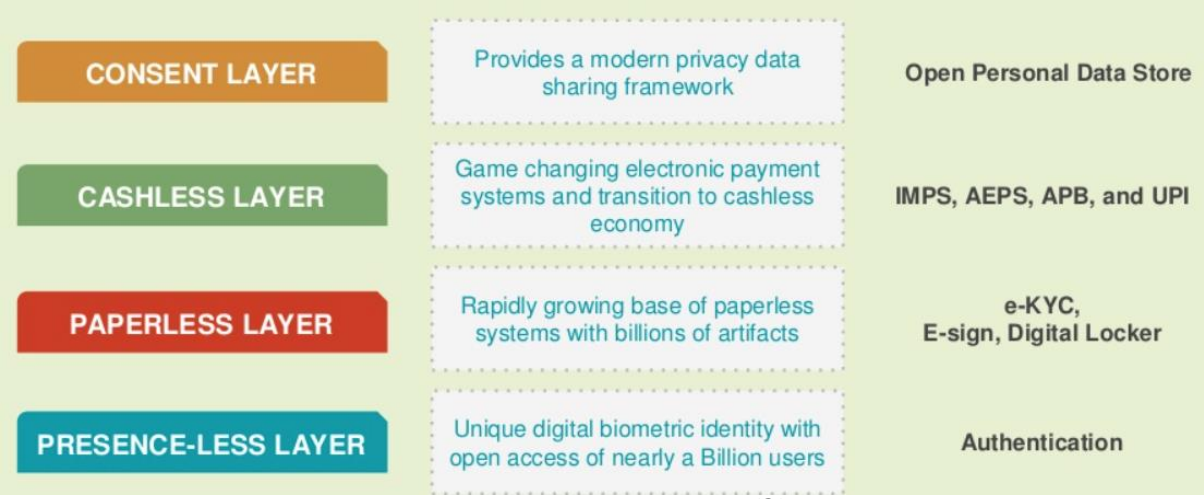

Figure 4: Diagram showing the "layers" of the India Stack.[131]

Aadhaar is an inclusive system because it makes it easy for registered users to help others enroll. Generally, people can submit valid proof of identity and address to enroll, or heads of households can enroll their family members by establishing proof of relationship. In the absence of valid proof of identity or address, an "introducer," someone appointed by the Registrar who has a valid Aadhaar number, can effectively vouch for another person's identity to enroll them. To expedite registration, UIDAI has created comprehensive training materials for registrars and enrollment officers to ensure that they strictly adhere to the official methodology for registering citizens. UIDAI pays Rs 50 ($0.77) for every successful enrollment.[132]

The estimated cost for Aadhaar's roll-out was approximately USD 1.5 billion.[133] One downside to Aadhaar is its high degree of centralization which potentially makes it vulnerable to breaches, leaks, or attacks. According to a study by the Centre for Internet and Society, as many as 135 million Indians may have had their personal information leaked due to this

---

[130] Tanaya Macheel, "Inside Aadhaar, India's Massive Digital Identity Program," *Tearsheet,* August 22, 2017, http://www.tearsheet.co/data/inside-aadhaar-indias-massive-digital-identity-program.

[131] Rahul Balyan, "Startup Goldrush in India," *Reflection, A Marketer's World View,* March 7, 2016, http://www.rahulbalyan.com/2016/03/startup-goldrush-of-india/.

[132] "Aadhaar: Inclusive by Design, A Look at India's National Identity Programme and Its Role in the JAM Trinity," GSMA, March 2017, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/gsma-aadhaar-report-270317.pdf.

[133] Ibid.

vulnerability.[134] Distributed ledger technologies greatly reduce this risk.[135]

TRP and Pilot Nations

The following section aims to assesses each of TRP's potential pilot nations, as well as refer to lessons learned from the cases of Pakistan and India in their pursuit of digital identification. As the Rohingya Project evaluates the feasibility of launching, it is critical to analyze the specifics of the regions and states where there are large populations of the Rohingya and where the current Myanmar government is also situated. By examining the Association of Southeast Asian Nations (ASEAN), TRP can evaluate relevant regional legal trends, as ASEAN countries work to unite and support each other in their goals in order to maintain stability in member countries. The preferred initial launch country of Bangladesh has shown interest in the digital identification, but TRP may face challenges regarding their complicated policy toward the Rohingya. Malaysia presents a strong candidate for the identification platform roll-out but, with recent elections, the new administration's policies are not clear. Additionally, the question of biometrics may present a challenge.

Association of Southeast Asian Nations (ASEAN) and Identification Logistics

Key points:

- It is important that the Rohingya Project be aware of attitudes within ASEAN towards digital identification, as they may indicate the KYC and FATF standards of member states.

ASEAN, established in 1967, consists of ten member states, including Myanmar and Malaysia. By joining together, the group proclaims to cooperate "economic, social, cultural, technical, educational, and other fields" in order to ensure stability in the region and compliance with the UN charter principles, while stating that the association supports on its members to make individualistic choices as long as they comply with ASEAN agreed upon policies.[136]

ASEAN member states have identified digital identification as a potential mode of legal recognition. In the ASEAN Agreement on the Movement of Natural Persons, article 3, section D, the Immigration Formality includes electronic authority as a means of identification within ASEAN States.[137] This makes digital identification a potentially viable option for stateless people within ASEAN. The relative success of projects like NADRA and Aadhaar could encourage further implementation of these types of systems. However, the "member state" stipulation of this agreement may present obstacles for the Rohingya as the use of valid digital IDs refers only to people in possession of member state identification. While it is promising that ASEAN includes the use of digital IDs in their regulations, politics within ASEAN may inhibit the Rohingya from participating.

---

[134] "Aadhaar Numbers and Personal Details of 135 Million Indians May Have Leaked, Says CIS Report," *Outlook*, May 3, 2017, https://www.outlookindia.com/newswire/story/aadhaar-numbers-and-personal-details-of-135-million-indians-may-have-leaked-says-cis-report/968774.

[135] "Distributed Ledger Technologies for Developing Asia," Asian Development Bank, 2017, https://www.adb.org/sites/default/files/publication/388861/ewp-533.pdf.

[136] Ibid.

[137] "ASEAN Agreement on the Movement of Natural Persons," ASEAN, November 19 2012, accessed April 21 2018, http://agreement.asean.org/media/download/20140117162554.pdf, 5.

Bangladesh

Key points:

- The Rohingya diaspora does not consider the current methods by the Bangladesh state to identify acceptable, as it refers to them as a 'Myanmar National' and involves biometric data. Due to the use of biometrics, TRP should be aware that this may signal the desire of the government of Bangladesh to use this level of information for identification.
- Vision 2021 in Bangladesh is important for TRP to be aware of as it indicates a key interest by the state to digitize identification.
- Repatriation efforts in Bangladesh of the Rohingya may affect the launch, as this may represent resistance by the state of opening up financial barriers towards the Rohingya, and may result in shifting populations in the region.

Bangladesh is currently the location of the largest diaspora of Rohingya in the world with about 1 million Rohingya within its borders.[138] They are working with the UN to manage refugee camps that settled long before the crisis, as well as throughout.[139] In Bangladesh, the Rohingya's biometric data is collected by the government, where they are given 'Myanmar National' ID cards.[140] To many Rohingya, this is unacceptable from as using biometric data makes the population vulnerable in the case of hackings, or repatriation and discrimination.[141] The Rohingya are opposed to this 'Myanmar National' ID because it is not accepted in Myanmar, and refers to them as a national of a country where they have been outcast.[142] In Bangladesh, this current method of identifying Rohingya in camps does not meet their needs and requires new technology in Bangladesh.

For Bangladesh, the country has set a goal to increase technological efficiency. Following other countries that have implemented large-scale digital identification systems, Bangladesh aims to digitize citizenship by the year 2021 in a project named Vision 2021.[143] Though this encompasses citizens of Bangladesh, this objective signals the interest by the state to improve identification efficiency. In the coming years, the government aims to digitize identification to identify Bangladeshi citizens more accurately and to deliver services more efficiently.[144] However, reports do not clearly describe how these initiatives will apply to the Rohingya residing in Bangladesh.

Bangladesh has oscillated between welcoming the Rohingya to planning repatriation.[145] Bangladesh will likely continue to follow its current path to digitize the identities of their citizens but have not indicated that this process will include the Rohingya. In the context of

---

[138] Antoni Slodkowski, "Myanmar Not Ready for Return of Rohingya Refugees," *Reuters*, June 2, 2018, https://www.reuters.com/article/us-myanmar-rohingya-un/myanmar-not-ready-for-return-of-rohingya-refugees-un-official-idUSKBN1HF04M.

[139] Ibid.

[140] "Irresponsible Data? The Risks of Registering the Rohingya," *IRIN*, June 2, 2018, http://www.irinnews.org/opinion/2017/10/23/irresponsible-data-risks-registering-rohingya.

[141] Ibid.

[142] Ibid.

[143] Hasanuzzaman Zaman, "Achieving Digital Bangladesh By 2021 and Beyond," *Planning Commission Bangladesh*, 7FYP, February 18, 2015, http://plancomm.gov.bd/wp-content/uploads/2015/02/18_Achieving-Digital-Bangladesh-by-2021-and-Beyond.pdf.

[144] Hasanuzzaman Zaman, 2015, 31.

[145] Hannah Beech, "Will the Rohingya Ever Return Home?", *The New York Times*, February 15 2018, https://www.nytimes.com/2018/02/15/world/asia/rohingya-myanmar-bangladesh.html.

past statements by the government of Bangladesh that they intend to repatriate the Rohingya, it is possible that the government of Bangladesh may not welcome TRP or other forms of official identification for the Rohingya for fear that such measures may encourage long-term settlement in Bangladesh. Further, if much of the diaspora in Bangladesh is to repatriate to Myanmar voluntarily, the Rohingya project will need to consider growing importance of launching the platform in Myanmar. This will be a critical aspect to further research for TRP.

Malaysia

Key points:

- Malaysia's AML/CFT policy represents that it is up to financial institutions to deem an ID authentic or not, which means that digital ID acceptance is up to these institutions, allowing for likely authentication of TRP IDs.
- TRP should be aware that biometrics are included in this policy as a clearer benchmark of authentication than an ID without biometrics.
- Administration changes may further improve the situation in Malaysia for the Rohingya, which paints the importance of being aware of potential policy changes that may affect TRP.

Malaysia's AML/CFT policy aims to address blockchain and cryptocurrency in the Malaysian financial system and ensure transparency in the development and usage of blockchain technology. Though this law is intended to address cryptocurrency, it may also provide a foundation on which to examine the legal feasibility of the use of digital IDs. Under Article 9, Section 3, the AML/CFT policy addresses identification for institutions and accepts authenticated documents, with a photograph of the customer, as a form of identification. Article 9 also offers the stipulation that the financial institution can decide if the document provides the required authenticity.[146]

The policy does not address the authentication of digital IDs but states that reporting institution can be "satisfied with the authenticity of the documents," if it addresses all requisite information.[147] The Malaysian government remains flexible regarding blockchain, and reporting institutions can deem identification satisfactory with or without biometric data. Thus, security risks are a concern following issues with hacking in centralized systems, especially when biometrics are encouraged to be involved.

Mahathir Mohamad, the winner of Malaysia's 2018 election, may be more sympathetic to the Rohingya community.[148] However, whether this will materialize into policies that resolve issues related to Rohingya statelessness is unclear.[149]

Kingdom of Saudi Arabia

Key Points:

- While public and state support for the development of blockchain platforms are

[146] "Malaysia's Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Money Services Business," Bank Negara Malaysia, Central Bank of Malaysia, 2018, http://www.bnm.gov.my/index.php?ch=57&pg=146&ac=197&bb=file

[147] Ibid, 16.

[148] Kirthika Varagur, "Malaysia's Elites Rides the People's Tsunami," *Foreign Policy*, May 11, 2018, http://foreignpolicy.com/2018/05/11/malaysias-elites-ride-the-peoples-tsunami/.

[149] Joshua Kurlantzick, "The Strategic Implications of Malaysia's Election Stunner," *Council on Foreign Relations*, May 16, 2018, https://www.cfr.org/blog/strategic-implications-malaysias-election-stunner.

encouraging, there are outstanding economic factors that may otherwise act as barriers to financial inclusion.

- However, recent changes in the KSA's KYC/AML policies entail increased points of entry (per FATF strategies for further inclusion #2) into the financial services sector for those lacking state-provided IDs through the required fingerprinting.

The Kingdom of Saudi Arabia (KSA) has established clear support for digital identification. Their current national identity card features data storage on a contact chip, which holds data and biometrics such as fingerprints and a photo.[150] The purpose of this section is to build upon the previous assessment of international trends by evaluating and analyzing the political and market climate for new, emergent technologies within the KSA and the greater Middle East and Northern Africa (MENA) region. This assessment will aid TRP in navigating potential roadblocks caused by social, political and market factors when planning to implement the use of digital IDs within the financial services sector.

When assessing the larger MENA region, the dynamic of financial inclusion presents a complicated picture. While only 14% of adults owned a bank account in 2014,[151] there is a rapidly growing "fintech"[152] sector.[153] Saudi authorities have claimed that Fintech is central to its $10 billion investment in a new financial district in Riyadh.[154]

For the most part, MENA industries have been conventional in their approach to fintech, investing mostly in the digitization of their existing services rather than in disruptive technologies. Blockchain is often considered a disruptive technology because of its ability not only to digitize but decentralize transactions and information.[155] Despite this, and to remain globally competitive, the KSA is particularly interested in blockchain and cryptocurrency development. Within the past year, the KSA has hosted multiple-blockchain related events including the nation's first Blockchain Conference.[156] In February 2018, the National Commercial bank partnered with US start-up Ripple to provide "a blockchain-based payment solution to local banks."[157] This serves as a welcome example of platforms outside national systems, interacting with banking services within the KSA.

However, with only 14% of MENA citizens holding a bank account and a high degree of wealth inequality in the KSA, the presence of additional barriers to financial inclusion, separate to those arising from a situation of statelessness, remain prevalent.

---

[150] "The Kingdom of Saudi Arabia National ID Card", HID Global, 2012. https://www.hidglobal.com/sites/default/files/resource_files/hid-gov-id-ksa-cs-en.pdf.

[151] Chloe Domat, "MENA: Dipping into Digital," *Global Finance,* April 11, 2018, accessed May 13, 2018. https://www.gfmag.com/magazine/april-2018/mena-dipping-digital

[152] Fintech denotes an emerging market, formed by the intersection between financial services and technology.

[153] Ibid.

[154] Ibid.

[155] "Blockchain: A Groundbreaking Disruptive Technology or a Passing Fad?", *Protiviti*, 2017, accessed May 19, 2018, https://www.protiviti.com/US-en/insights/blockchain-ground-breaking-disruptive-technology-or-passing-fad.

[156] Nash AE, "Decoding Blockchain KSA", *Fintech Middle East*, April 19, 2018, http://fintechnews.ae/events/decoding-blockchain-ksa/.

[157] "Ripple Blockchain Technology Set to Revolutionize Saudi Arabian Banking Sector." *TechSci Research,* accessed May 15, 2018, https://www.techsciresearch.com/news/2810-ripple-blockchain-technology-set-to-revolutionize-saudi-arabian-banking-sector.html.

Regardless of potential economic barriers, technological progress by way of digital identification Within the KSA has experienced a steady upward slope. In addition to the examples provided by long-established digital ID systems in India and Pakistan, the KSA has developed its own system of digital identification. In December 2007, the National Information Center (NIC), which operates as the IT entity of the KSA's Ministry of Interior, launched an electronic ID initiative.[158] The new ID system is promoted to have enhanced security for citizens, residents, and visitors by matching individuals to their biometric and personal data and is meant to facilitate operability within Gemalto hosts e-ID programs in Bahrain, Belgium, Finland, Oman, Portugal, Qatar, Sweden, Taiwan, and UAE. KSA's national ID is comprised of physical wallet-sized cards paired with an embedded microprocessor which stores the cardholder's digital information.[159] This information includes demographics, facial imaging, and fingerprint scans.

When ensuring the feasibility of a digital ID system of their own, it is suggested that the TRP seek to match the qualifications within present digital ID systems in all three pilot nations and in regard to their respective KYC adaptations. However, the TRP will need to ensure that all data, biometric or otherwise, is consistently updated. This will not only strengthen the relevant uses of TRP's digital ID but also enhance the credibility of the ID itself.

Responding to changes in the KSA's KYC/AML policy, the use of fingerprints for the KSA's national ID card was required in 2005. The inclusion of this biometric data was to reinforce their ID verification system, while concurrently strengthening current AML and Anti-Terrorism measures. Further legislation by the KSA's IT Commission mandates that all Mobile Network Operators must collect finger biometrics of users as of 2016. The biometric data is to be shared with the KSA's National Information Center to verify the identity of sim-card buyers and strengthen national security.[160] This requirement has two distinct impacts on the TRP's project and larger objectives. First, since the KSA requires fingerprint scans to access certain services, conduct sales, and allow for mobility in and out of the state TRP should consider the baseline use of fingerprint scans as a form biometric data hosted within each digital ID. Secondly, the KSA may demand access to information stored on TRP's platform. Thus, TRP will need to consider how it will conform to national laws without breaching the privacy of Rohingya cardholders or compromising the decentralization of TRPs blockchain platform. Furthermore, the use of biometric fingerprinting may increase the credibility of the TRP's ID platform, as is identified by strategy 2 of the FATF's alternative measures for ID verification.

Subsection Conclusion Key Takeaways from Country Cases

After examining the establishment and development of digital ID systems in the countries above, a few lessons relevant to TRP are clear. Pakistan's new SNIC cards, in complying with both ISO/IEC 7816 and ISAO 9303, are embedded with 36 security features to prevent fraud, and they can be used as international travel documents at airports. India's Aadhaar system is built on an open platform, which allows external developers to re-engineer its application programming interface (API) to create new, connected services on it. Furthermore, Aadhaar allows registered users to "vouch for" those lacking proper identity documents to help enroll them. The UIDAI deserves recognition for having over 1.2 billion users registered in Aadhaar,

---

158 "Biometric Technology: Gemalto's solutions and services", *Gemalto*, accessed May 24 2018, https://www.gemalto.com/govt/biometrics.

159 Ibid.

160 Ibid.

which makes Aadhaar the world's biggest digital ID system. One factor that likely led to this success is monetizing enrollment officers by providing them a nominal sum (Rs 50 or $0.77 USD) per each enrollment. Such a method may be of use in implementing The Rohingya Project.

A simple assessment of Saudi Arabia in respect to the implementation of blockchain technology shows positive indicators, while still leaving a key concern. Although there are much public and state support of the use of blockchain technology, the question of state-access to the information that rests on TRP's blockchain remains. Additionally, given the correct KYC/AML standards in the KSA, TRP should consider the inclusion of fingerprinting to enhance the feasibility of Rohingya inclusion into the larger financial sector (per FATF strategies for broadening financial inclusion).

Section Recommendations

- Continue to build and form relationships with potential stakeholders, partners, and affiliated groups. See Appendix C below for a curated list of affiliated groups.
- Enhance the credibility of TRP's project by continuing to engage with the UNHCR in researching the financial situation of Rohingya. JSIS Initial survey details are in Appendix B.
- TRP should consult with a skilled legal team through each stage of the project, in order to ensure that their blockchain platform complies in the pilot nations.
- By following the examples of NADRA and Aadhaar, TRP can use these takeaways in their roll-out of this platform.
- Following the FATF's strategies for broadening financial inclusion and the standardized use of biometrics in the KSA, TRP should consider the inclusion of fingerprint scans as biometric data stored on their blockchain digital ID platform.

Conclusion and Integrated Recommendations

Key points:

- How a blockchain platform fulfills TRP's five core objectives depends on its consensus protocol. Both the proof-of-stake consensus mechanism as well as the federated byzantine fault tolerance consensus mechanism allow for the greatest flexibility in meeting these objectives.
- Privacy is key to protecting the identities of the Rohingya. State Channels, as well as Zero Knowledge Proofs, are both possible tools that can be used to protect the privacy of the Rohingya on a blockchain platform.
- Although not currently paired with blockchain, alternative KYC and CDD approaches exist, which lend credence to the use of interviews and community-based verification in manners similar to TRP's planned objectives.
- Estonia's blockchain digital ID system allows for digital authentication of identity, which streamlines the verification process to access banking services and only requires one form of ID to access banking services.
- International concerns surrounding jurisdiction may present itself as an obstacle for TRP, as the legal framework to process possible criminal activity for blockchain is not yet sufficient.
- Although biometric use in all three TRP pilot nations is varied, their usage can help guide TRP in determining the types of data required in creating a self-sovereign digital ID.

When considering the implementation and construction of a successful blockchain environment, it is integral to assess the feasibility of the project throughout each step of the way. Often, the feasibility of the project is dependent on the overall credibility of TRP, blockchain technology, and financial stakeholders. The JSIS team employed this understanding throughout the report, specifically assessing the potential risks and competing interests as is outlined by our determined PSTL framework.

In the creation of a self-sovereign blockchain based digital identity, there are key trade-offs that TRP must consider. A fully decentralized, blockchain digital identification system may not best suit the needs of the TRP. This report recommends that the TRP pursue a partially decentralized private blockchain platform that uses the proof-of-stake consensus protocol to meet its core objectives of decentralization, scalability, efficiency, and security. Given the sensitive nature of the information being handled, this report also recommends that TRP utilize mechanisms such as Zero Knowledge Proofs and State Channels to fulfill its core objectives of privacy and security.

As is expected, the use of blockchain ecosystems entails several risks. To manage these risks, we recommended that TRP construct and negotiate clear legal codes of conduct throughout all stages of the project. To do this TRP can collaborate with other institutions such as those mentioned in appendix C who have already navigated relevant legal avenues.

The FATF's recommendations shape the regulatory environment governing the policies which permit or prohibit access to the regulated financial system. In attempt to address credibility of financial stakeholders and feasibility of a TRP sponsored digital ID, it is critical to remain aware of the programs they approve or endorse particularly as they continue to show interest and flexibility toward the changes and innovations necessary to expand financial inclusion while remaining within the framework of their recommendations. The frameworks which will

contribute most to the development of TRPs financial platform concern FATF endorsed KYC and CDD standards. KYC standards stipulate that banks must determine the identity of all customers and monitor their financial behavior for suspicious activity. Meanwhile, CDD standards require banks to be able to predict their customers' financial behavior in order to inform their KYC practices. The two sets of standards are complementary, and their structures provide key and non-traditional points of entry, per the FATF's emergent mission to broadening global financial inclusion. However, as TRP officially launches this platform, it is important to be acknowledge that existing frameworks regarding blockchain and other digital solutions are likely to remain loose until this technology is better understood by the international community, which will serve to the benefit of TRP.

By examining the best practices of digital identity projects in Estonia, India, and Pakistan, we conclude that distributed ledger technology should be employed and future advancement in remote identity verification should be integrated. Security risks with the centralized platforms used in India and Pakistan underline the security advantages of decentralized blockchain platforms. Also, quantum-proof blockchains (immune to an attack from quantum computers) will become increasingly important to understand and employ effectively in the short- to mid-future. In effort to appeal to the overall credibility of the project, TRP should join others in advocating for transparency over regulations on blockchain identity and be aware of initiatives, which aim to use blockchain technology and digital IDs to solve identification issues. For example, ID2020 and the government of Bangladesh has an objective to digitize the country by 2021.

Understanding the political viability is key to establish the feasibility of digital IDs and TRP within pre-existing international and regional frameworks. In Malaysia and Bangladesh, the TRP should keep abreast of shifting government policies regarding the Rohingya. Understanding public and political sentiments is also important to ensure the credibility and feasibility of the project. In the Kingdom of Saudi Arabia, TRP should be encouraged by the rapid growth in both fintech and blockchain technologies. However, this positive environment does not eliminate the need for TRP to comply with existing ID standards and national KYC adaptations

Although this report covers a wide breadth of information and serves as an initial assessment of the potential risks that may present themselves TRP, this report does not examine all potential avenues. Acknowledging this, the TRP should consider the following points for further research as they move forward in their project and mission:

- The need to examine how established (whether formal or informal) KYC policies relate to Islamic Finance and Islamic Banking Institutions, including obtaining further details regarding the relationship between Islamic finance and the Basel Committee on Banking Supervision, is critical to TRP.
- Continued research into the uses, concerns, and potential vulnerabilities associated with biometric data is necessary as TRP develops. TRP also should monitor changes to KYC and FATF standards that may affect biometrics.
- TRP should prepare for issues surrounding tradeoffs inherent to blockchain, namely the scalability trilemma, and examine the potential in this being resolved using innovative technologies.
- TRP should continue to seek methods to create different chains on a blockchain platform.

Appendix A: International FATF Case Examples[161]

Canada – Flexible means of customer's identification when prescribed measures cannot be used

- Allows for low-risk individuals who lack AML/CTF compliant ID to hold deposit bank accounts with documents such as non-photo ID issued by a government or certain photo IDs not issued by a government.
- Regulatory amendments of the AML/CFT framework 6/2016

China – Bank account management based on risks

- China's tiered approach illustrates how different measures can be combined to allow a variety of financial services. A Type 1 account must be opened in person and provides a complete assortment of services including the ability to make cash deposits, withdrawals, and transfers.
- Type 2 accounts can be used to purchase financial products, but there are thresholds and limits for transfers and payments. Type 3 accounts allow no cash deposits or withdrawals. Both type 2 and 3 can be opened remotely subject to additional CDD.

European Union – Limited products and services for asylum seekers from high-risk third countries or territories

- The European Union has sought ways in which CDD measures be adapted to facilitate financial inclusion of asylum seekers. The European Banking Authority has determined that AML/CTF risks are unlikely to be lower with asylum seekers certain provisions may adapt to increase access to financial services for asylum seekers within the EU. These include:
    - no provision of credit or overdraft facilities;
    - monthly turnover limits (unless the rationale for larger or unlimited turnover can be explained and justified);
    - limits on the amount of person to person transfers (additional or larger transfers are possible on a case by case basis);
    - limits on the amount of person to person transfers (additional or larger transfers are possible on a case by case basis);
    - limits on the number of transactions to and from third (non-EU) countries (while considering the cumulative effect of frequent smaller value transactions within a set period of time), in particular where these third (non-EU) countries involved are associated with higher AML/CTF risk;
    - limits on the size of deposits and transfers from unidentified third parties, in particular where this is unexpected;
    - prohibiting cash withdrawals from third (non-EU) countries.

Fiji – Letter from a suitable "referee

- Fiji has defined a "referee" as (1) a person who knows the customer (2) whom the financial institution can rely on to confirm that the customer is who he or she claims to be (3) can verify other personal details (occupation, residential address) of the customer. They have stated that for minors the referee may be a teacher, principal, landlords, parent or guardian. For rural individuals, a referee may be a village headman, chief administration officer, provincial administrator or a provincial officer, religious leader, an official from Fiji Sugar corporation or a Fiji government official.

Guatemala – Small account threshold based on an average income analysis

- In 2011 Guatemala conducted a national income analysis which determined the national average median income and remittances per month. They used this information to set an income ceiling to qualify for simplified CDD which was approximately equal to the labor of two working adults receiving remittances.

[161] FATF Guidance, 2017.

New Zealand - Amended identity verification Code of Practice

- 2013 Amended Identity Verification Code of Practice
- low and medium risk customers can be verified through electronic identity verification,
- "referee" cannot have commercial or financial interest in the applicant obtaining ID.

Peru – Simplified CDD measures based on a specific authorization of the supervisor

- Financial Institutions can apply for simplified CDD measures based on authorization granted by the Financial Supervisor of Peru (SBS). Approval for simplified CDD processes permits the financial institution to collect only name and the type and number of the applicant's ID documents which is then verified through the National ID or International ID. They are exempt from collecting info on applicant's ID documents which is then verified through the National ID or International ID. They are exempt from collecting info on nationality, residence, phone number and/or e-mail address, occupation, and the name of employer.

The Philippines – Temporary relaxation of identification requirements following a natural disaster

- The destruction caused by 2013 Typhoon Haiyan impaired government and financial services. The Central Bank of the Philippines (BSP) provided banks relief packages:
    - relaxed ID requirements, such as written certification that clients had lost their IDS
    - transaction thresholds
    - account monitoring requirements

Switzerland – RBA to verify customer's identity in specific situations

- Swiss banks must adhere to a code of conduct which requires the banks prove the identity of the customer, but banks have freedom depending on circumstances. In very exceptional cases such as a customer has no identification documents, the bank can rely on other credentials such as attestations from public authorities. These and other substitute documents must be kept on file with a memo explaining the circumstances.

United States – A risk-sensitive application of the Customer Identification Program

- Banks not required to verify the accuracy of every element of ID only enough that they can form a reasonable belief that the bank knows the true ID of the customer, i.e., the address of a next of kin may be used in place of address or description of the physical location.

Appendix B: Feasibility of a TRP Conducted Survey

This appendix provides a preliminary assessment by the UW JSIS Team on the various research methods and approaches appropriate to TRP's research objectives to uncover information to better understand the financial situation of Rohingya in all three pilot nations. This assessment aims to supply the research tools to answer 1) the extent to which the Rohingya can currently access relevant financial mechanisms, and 2) the range of financial mobility within the Rohingya diaspora and related population data. The planning behind this study under current preparation by TRP with assistance from the UNHCR.

The UW JSIS Team 1) presents recent research projects on key Rohingya populations to locate potential partners and have access to the latest relevant data, and 2) to present first draft questionnaires that TRP might pilot and adapt for their future research initiatives. Key results include that research in Bangladesh should consider the use of Cluster Sampling, whereas research conducted in Malaysia or Saudi Arabia should consider Respondent-Driven Sampling.

Extended Benefit of this Survey to TRP
There is much-added value in surveying the present situation of the Rohingya. Additional surveys can further assist TRP on several accounts including by providing necessary data to create tailored and effective solutions and by addressing international doubts and criticisms on the project itself. Structured surveying can serve as a critical tool for public relations of TRP and building credibility amongst the international community. Noble PR can also facilitate developing partnerships with other groups involved with the Rohingya or other stateless populations. And lastly, measurable data appeals to not only potential partners but also potential investors, strengthening the financial backbone of the Project.

Example Guides
Several organizations and bodies have attempted to measure and survey stateless and minority populations. Many of their reports provide a helpful toolkit and resource for future studies on similar topics. Specifically, the challenges and examples discussed within these guides serve to help us to better outline best practices in data collection and surveying the Rohingya on their financial situation.

Outcomes
The primary outcome of a mapping study, as determined by the UNHCR, is to highlight where protection gaps exist for stateless populations to encourage uniformity about the problem within countries and between regions. The results of a mapping project may also be used to determine the better allocation of resources to deal with statelessness. For example, the financial information collected may aid in determining the type of cryptocurrency best suited for intra-community transactions.

Challenges
As this survey aims to cover the Rohingya in three distinct geographical areas, this presents a unique set of challenges for this study, in comparison to those already conducted. It is important to understand the difference like each survey throughout each respective nation. For example, within each State surveyed, there must be a comprehensive understanding of both the migratory patterns of the Rohingya, as well as the legal opportunities available. These questions are further investigated within the Desk Analysis touched upon within the next section.

Conducting a Desk Review
The JSIS team recommends that the identification of statelessness begin with a 'desk review.' This process would assess the current situation about statelessness in each country by analyzing the sources of data already available. Secondary sources must be reviewed first to see if they can be adapted, reprocessed, or reused before undertaking any of your primary data collection.

A desk review requires assessment of three main sources of secondary data: legislation, research, and statistics. It is primarily utilized to reduce the resources needed for primary research and to prevent duplication. When conducting a desk review, the following four stages must be addressed:

UNHCR[162]
In May 2011, the UNHCR in Geneva published a temporary release *Guidance document on measuring stateless populations.* This Guide was commissioned by the Field of Information and Coordination Support Section (FICSS) and Division of Programme Support and Management (DPSM) and in collaboration with the Statelessness Unit Division of International Protection.

Netherlands Institute for Social Research[163]
This report analyses the Impact of Face-to-Face versus Sequential Mixed-Mode Designs on the Possibility of Nonresponse Bias in Surveys. From the research provided by this group, we suggest that face-to-face survey models would best suit the needs of TRP.

IMISCOE Research[164]
The International Migration, Integration and Social Cohesion in Europe (IMISCOE) Research Network unites researchers from 30 institutes specializing in studies of international migration and social cohesion in Europe. In 2013, IMISCOE Research through Amsterdam University Press released a detailed Guide on *Surveying Ethnic Minorities and Immigrant Populations – Methodological Challenges and Research Strategies.* This guide aims to educate and aid future researchers, policymakers and practitioners, the media, and other interested stakeholders.

Although most of this document focuses on country-specific and regional sampling issues that may arise when surveying minority or immigrant populations, the larger conclusions of this report, including methodological strategies and best practices may be useful to the study of minority ethnic groups worldwide.

The World Bank and OECD
The World Bank drafted a guide to measuring financial capability: Questionnaires and implementation guidance for low- and middle-income countries in 2013. The range of targets within these questionnaires provides a strong example as to how to adapt our questionnaire to the case of the Rohingya taking into consideration the broad spectrum of financial inclusion.[165]

In 2011 the OECD, through their International Network on Financial Education (INFE), produced a guide for surveys which aimed to provide an initial measure of financial literacy "to identify national

---

[162] Lucy Gregg, "Guidance document on measuring stateless populations," Field Information and Coordination Support Section (FICSS), UNHCR Geneva, May 2011, Temporary Release, www.refworld.org/pdfid/4f6887672.pdf.

[163] Joost Kappelhof, "Surveying Ethnic Minorities: the impact of survey design on data quality," Netherlands Institute for Social Research, SCP Publication, The Hague, 2015, https://dspace.library.uu.nl/bitstream/handle/1874/313224/kappelhof.pdf;sequence=1.

[164] "*Surveying Ethnic Minorities and Immigrant Populations,"* IMISCOE Research Group, Eds. Joan Font and Monica Mendez, Amsterdam University Press, 2013, https://www.oapen.org/download?type=document&docid=450851.

[165] "Review of Existing Financial Capability" Guidance Document," World Bank, 2016.

levels of financial literacy and provide a baseline and set benchmarks for national strategies or particular programs."

Example Studies
Within the past two years, there have been two studies conducted by international organizations which have assessed the situation of the Rohingya. Detailed reports and summaries of their studies and findings can be accessed in their online publications (view footnote 114 and 115).

In 2017, Medecins Sans Frontieres (MSF) released a summary of findings from six pooled surveys on the Rohingya situation respective to Myanmar and Bangladesh. MSF is an international association based out of Geneva aimed at assisting populations in distress irrespective of race, religion, creed, or political convictions.[166]

The group XCHANGE conducted a survey from September-October 2017 which was similar to that of MSF. This organization was established to investigate and document human movement in countries of origin, transit, and destination. Their report is aimed at providing information to policymakers, state bodies, NGOs, and the public. The survey collected 1,360 testimonies from Rohingya refugees in Cox's Bazar[167]. Before beginning their study, XCHANGE conducted a desk review. The 2014 census in Myanmar was the first one conducted in Myanmar since 1983 (when the Myanmar government at the time prohibited Rohingya from identifying themselves by their chosen designation). In addition to the History of the Rohingya in Myanmar, the group logs the timeline on the number of 'crackdowns' which have resulted in the mass expulsion of the Rohingya, beginning with the 1970s.

Conclusions from these Studies
The recent exodus of Rohingya peoples from northern Rakhine to Bangladesh in the fall of 2017 catalyzed a wave of research and information on the displaced Rohingya in Bangladesh. Large studies, like the two previously mentioned, have published comprehensive reports on the spread, migratory patterns, incidents, and demographics of Rohingya within Bangladesh. Additionally, there are large, readily available datasets for download on the topic. The Humanitarian Data Exchange (HDX) hosts regularly updates data on the Rohingya within Myanmar and Bangladesh, such as the outline of camps, settlements, and sites in Cox's Bazar.

Best Practices and Recommended Methodology
We recommend that a survey contain both qualitative and quantitative methods. Taking into consideration the challenges of the previous studies, our goal here is to produce a simple yet systematic means of collecting the data determined in the preparation phase. In all locations, surveys should be conducted through person-to-person interviews. These interviews should be recorded both in writing and audio for further analysis.

<u>Bangladesh</u>
Although other groups have used methods such as systematic sampling and simple random sampling, to avoid over-complication, we recommend using Cluster Sampling to determine groups to survey. Under this method, the Rohingya population in Bangladesh is divided into clusters, and a random sample of these clusters is chosen. Cluster sampling is a low-cost means of sampling, significantly reducing the traveling time needed between units. However, it does lack the precision of other means, such as stratified sampling, implying a higher margin of error[168]. Clustered sampling can be easily applied in Bangladesh as the majority of Rohingya reside within various camps in the Cox's Bazar

[166] "Summary of Pooled Findings," Medecins Sans Frontieres, December 9, 2017, http://www.msf.org/en/article/myanmarbangladesh-rohingya-crisis-summary-findings-six-pooled-surveys
[167] "The Rohingya Survey," XCHANGE, Online Report, November 2017, http://xchange.org/reports/TheRohingyaSurvey2017.html
[168] Alice Bloch, "Methodological Challenges for National and Multi-sited Comparative Survey Research," *Journal of Refugee Studies* 20, no. 2, (June 2007): 230–247, https://doi.org/10.1093/jrs/fem002.

District.

Malaysia and Saudi Arabia

As information, data, and reporting on Rohingya populations within these two countries are less easily accessible and known, we recommend surveying through Respondent Driven Sampling Methods. Respondent Driven Sampling Methods is a type of Snowball Sampling which involves asking interviewed members of the relevant population to nominate other individuals who could also be interviewed on the same topic. However, under this method, efforts must, therefore, be made to reduce over-reliance on one network by utilizing multiple independent 'starting sources' (individuals out with cards)[169]. Respondent Driven Sampling starting point individuals would be given numbered cards to hand out to their communities to pass along to those to nominate individuals to come in for the survey. On this card, the reason for the survey, and the location of the survey site must be listed.[170]

An interviewer briefing is designed to ensure that the interviewers know why they are conducting the survey, what the rules and expectations are, and how to deal with any issues that might arise during the survey process. It is therefore important that the briefing is attended by all staff who anticipate working on the survey, and it is imperative that their managers attend as well, so that they fully appreciate the purpose of the survey and hear first-hand any concerns of their staff to properly monitor the survey process to ensure consistency and rigor.[171]

As observed in some of the challenges of previous studies, it is important to consider the skillset of interviewers who will be interacting with Rohingya in each location. Thus, it is wise that in each country listed, interviewers be fluent in the following languages. These languages were determined by geographic dominance, group trends, and lastly to facilitate analysis and international publication.[172]

Bangladesh	English, Rohingya, Bengali
Malaysia	English, Rohingya, Malay (Bahasa)
Saudi Arabia	English, Rohingya, Arabic

Figure 1: Languages in initial launch countries

Core Questionnaire	
Note gender a) Male b) Female	How many children under the age of 18 are in your household? Record number ---
What is your current place of residence? a) "Country, Town/City" b) Don't know c) Declined	How many people (aged 18 and over) are in your household? Record number ---
What is your township of origin? If asked: This is the town from which your Rohingya heritage stems	What is your marital status? a) Married b) Single c) Separated/divorced d) Living with partner

[169] R. Atkinson, and J. Flint, "Accessing Hidden and Hard to Reach Populations: Snowball Research Strategies," Social Research Update, 2001, 33.

[170] Douglas Heckathorn, "Respondent-Driven Sampling: A New Approach to the Study of Hidden Populations," 1997, Social Problems.

[171] Terry Elizabeth Hedrick, Leonard Bickman and Debra J. Rog, *Applied Research Design: A Practical Guide* (Newbury Park, CA: Sage Publications, 1993).

[172] Ibid.

	e) Widowed f) Don't know g) Declined
If any, could you please list the forms of official documentation that you or someone within your household has? a) Citizenship b) Birth or Death certificates c) Work Authorization d) Temporary identification card	Which of these bests describes the community you live in? a) A village or rural area (fewer than 3 people) b) A small town (3,000 to about 15,000 people) c) A town (15,000 to about 100,000 people) d) A city (100,000 to about 1,000,000 people) e) A large city (with over 1,000,000 people) f) Don't know g) Refused *The definitions of village, small town, town, city, and large city are defined by the OECD.

Financial Questionnaire		
Financial Tools	a) Please check if the interviewer has heard of the following financial tools.	b) Check if the interviewer has or has access to the same financial tools.
A pension fund		
An investment account		
A mortgage		
A bank loan secured on property		
An unsecured bank loan		
A credit card		
A current account		
A savings account		
A microfinance loan		
Insurance		
Stocks and shares		
Bonds		
Mobile phone payment account		
Prepaid payment card		
Don't know response given to the question as a whole		
Refused to respond to the question as a whole		

Figure 2: Core questionnaire

Appendix C: Potential Collaborators and Supportive Organizations

Collaboration and networking with key stakeholders has the potential to bring successful strategies, knowledge, and credibility to The Rohingya Project. Over the course of this research we encountered numerous public and private sector stakeholders seeking to pursue solutions to the plight of refugees and stateless people through new and emerging technologies. This appendix can serve as a guide to some of those organizations which appear the most suitable for cooperation with The Rohingya Project. What this selection of companies and organizations reveals is that there is a wide variety of specialties within this sector. This should embolden The Rohingya Project to continue to pursue a platform focused exclusively on the needs of the Rohingya community. Some of the following organizations may serve to be potential partners or sponsors in the development of TRP, but some may simply provide examples or information relevant to the goals of TRP.

Alliance for Financial Inclusion (AFI) www. afi-global.org	AFI is comprised of central banks and financial regulatory institutions from over 90 developing nations. AFI holds conferences, produces white papers, and engages in policy discussion to further the financial inclusion of the poor on multiple fronts. Though not associated with the Rohingya or refugees specifically, they express a desire to utilize technology to address a wide range of financial exclusion issues. In terms of this research, Bangladesh has several members including Bangladesh Bank is a principal member, and the Microcredit Regulatory Authority and the Ministry of Finance of Bangladesh are associate members.
Omidyar Network www.omidyar.com	Pierre Omidyar, the founder of eBay, started Omidyar Network to bring Ebay's spirit of individual enterprise to the developing world. Omidyar Network invests in entrepreneurs pursuing projects in one of six matrices, the first of which is digital identity. Overall Omidyar is an active sponsor of social and tech research and the development of programs that facilitate self-sufficiency in the developing world.
Digi.Me	They have invested in Digi.Me, Identification for Development (ID4D), Indian School of Business, and Learning Machine. Digi.Me has a mission to empower people with better control and access over their personal data. Digi.Me won a City Tech Integrity Award for displaying how their technology can help banks detect fraud, corruption, and help governments and NGOs correctly identify and reach intended aid recipients. This is the diagram used on their website which shows how user data is controlled and stored.
Learning Machine	Learning Machine uses blockchain to anchor records immutably. Their website lists their clients as including The Government of Malta, Massachusetts Institute of

	Technology, and the Federation for State Medical Boards. Their platform verifies blockchain certificates via Blockcerts which they co-developed with MIT. Blockcerts is an open source platform for sharing and storing blockchain certificates. Although data is stored via a phone app, the personal key is created by the user who is then free to access and share their data.
Caribou Digital www.caribou digital.net	Caribou Digital is a consultancy firm which works exclusively with digital solutions for clients in emerging market economies. They have produced an expansive guide on digital identities and have also received sponsorship from Omidyar Network. They have also worked with The Gates Foundation and Mastercard in the research and development of products and services to serve individuals in emerging markets.
World Food Program Building Blocks http://innovation.wfp.org/project/building-blocks	Building Blocks is a blockchain cash transfer program which the world food program is trialing. The program enables cash transfers, through vouchers or pre-paid debit cards, which allow people to purchase their food. Because the use of cash transfers is increasing worldwide blockchain enables the decentralized transfer of funds which has the potential to speed transactions, increase privacy, control financial risks, and improve rapid response in emergencies.
Blockchain Policy Initiative www.blockchainpolicy.org	The Blockchain Policy Initiative is an organization which hopes to contribute to the advocacy for transnational policies which embrace that nature of blockchain for the benefit of humanity. They advocate for the public use of blockchain and the potential it has to improve.
Gemalto https://www.gemalto.com/	Boasting over 200 biometric deployments in 80 countries, Gemalto has become a global leader in providing biometric technology and solutions to enable governments and institutions to solve crimes and protect identities. Amongst their suite of technology products and services includes iris-scanners, facial-recognition, and Gemalto Congent's Automated Biometrics Identification System (ABIS).

Bibliography

"Aadhaar Numbers and Personal Details of 135 Million Indians May Have Leaked, Says CIS Report," *Outlook,* accessed May 3, 2017, https://www.outlookindia.com/newswire/story/aadhaar-numbers-and-personal-details-of-135-million-indians-may-have-leaked-says-cis-report/968774.

AE, Nash. "Decoding Blockchain KSA", *Fintech Middle East*, accessed April 19, 2018, http://fintechnews.ae/events/decoding-blockchain-ksa/.

"A Gentle Introduction to Immutability of Blockchains," Bits on Blocks, accessed February 29, 2016. https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/.

ASEAN. "ASEAN Agreement on the Movement of Natural Persons," November 19, 2012, accessed April 21, 2018, http://agreement.asean.org/media/download/20140117162554.pdf.

"Asia/Pacific Group on Money Laundering (APG)," *FATF*, accessed April 29, 2018, http://www.fatf-gafi.org/pages/asiapacificgrouponmoneylaunderingapg.html.

Asian Development Bank, "Distributed Ledger Technologies for Developing Asia," 2017, https://www.adb.org/sites/default/files/publication/388861/ewp-533.pdf.

awest. "Aboriginal and/or Torres Strait Islander People." Last modified June 29, 2016. /aboriginal-andor-torres-strait-islander-people.

Baliga, Arati, "Understanding Blockchain Consensus Models," *Persistent Systems*, accessed April 2017. https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf.

Bank Negara Malaysia, Central Bank of Malaysia. "Malaysia's Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Money Services Business" http://www.bnm.gov.my/index.php?ch=57&pg=146&ac=197&bb=file.

Balyan, Rahul "Startup Goldrush in India,", *Reflection, A Marketer's World View – Blog by Rahul Balyan,* accessed March 7, 2016, http://www.rahulbalyan.com/2016/03/startup-goldrush-of-india/.

Beech, Hannah. "Will the Rohingya Ever Return Home?", *The New York Times*, Last modified February 15 2018. https://www.nytimes.com/2018/02/15/world/asia/rohingya-myanmar-bangladesh.html.

Berke, Allison, "How Safe are Blockchains? It depends.," *Harvard Business Review*, accessed March 7 2017. https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

"Biometric Technology: Gemalto's solutions and services," *Gemalto*, accessed May 24 2018. https://www.gemalto.com/govt/biometrics.

"Blockchain: A Groundbreaking Disruptive Technology or a Passing Fad?" *Protiviti*, accessed

May 19, 2018. https://www.protiviti.com/US-en/insights/blockchain-ground-breaking-disruptive-technology-or-passing-fad.

“Blockchain and Identity: A Solution without a Problem,” accessed April 17, 2018. https://duwamish.lib.washington.edu/uwnetid/illiad.dll?Action=10&Form=75&Value=1606248.

"Blockchain Nodes. What Are Nodes and How Do They Work?" World Crypto Index. https://www.worldcryptoindex.com/how-nodes-work/.

"Blockchain Leasing for Proof of Stake" *Medium, Waves Platform,* March 26, 2018. https://blog.wavesplatform.com/blockchain-leasing-for-proof-of-stake-bac5335de049

Brazell, Lorna. “Blockchain and Identity: A Solution Without a Problem?”, *Society for Computers and Law*, December/January 2018.

Brietman, Kathleen, “Op Ed: Why Ethereum’s Hard Fork Will Cause Problems in the Coming Year.”, *Bitcoin Magazine,* Last modified February 3, 2017. https://bitcoinmagazine.com/articles/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year/

Buterin, Vitalik. "The Meaning of Decentralization – Vitalik Buterin – Medium." Medium. Last modified February 06, 2017. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

“Committed to Improving Lives through Digital Identity,” *ID2020 Alliance,* 2017, accessed May 4 2018, https://static1.squarespace.com/static/578015396a4963f7d4413498/t/596e5d636a49635fe12cf40b/1500405109983/ID2020+Alliance+Governance.

Curran, Brian. "What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide". *BLOCKONOM,*. Accessed May 11 2018. https://blockonomi.com/practical-byzantine-fault-tolerance/

Domat, Chloe, “MENA: Dipping into Digital” *Global Finance, a*ccessed 13 May 2018. https://www.gfmag.com/magazine/april-2018/mena-dipping-digital

Donaldson, Jim. “Public vs Private Blockchain In A Wide World of Unique Applications.” *Mojix Inc,* August 8, 2017. https://www.mojix.com/private-blockchain/.

D'Anconia, Frisco. "Is Blockchain Technology Really the Answer to Decentralized Storage?" *Cointelegraph.* Accessed May 12, 2018. https://cointelegraph.com/news/is-blockchain-technology-really-the-answer-to-decentralized-storage.

E-Estonia. “Estonian Blockchain Technology: Frequently Asked Questions,” n.d. https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf.

E-Estonia. “KSI Blockchain”, accessed May 3, 2018. https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/.

E-Estonia, “Estonian E-solutions Everywhere,”, May 2016, https://e-estonia.com/estonian-e-solutions-everywhere/.

ET Bureau, “Over 200 Government Sites Reveal Aadhaar Details: No Leakage from UIDAI: Minister,” *Economic Times*, July 20, 2017, https://economictimes.indiatimes.com/news/politics-and-nation/210-government-sites-found-displaying-aadhaar-details-pp-chaudhary/articleshow/59667922.cms.

Evangeline, Ducas, and Alex Wilner. “The Security and Financial Implications of Blockchain Technologies: Regulating Emerging Technologies in Canada.” *International Journal; Toronto* 72, no. 4 (December 2017): 538–62. http://dx.doi.org/10.1177/0020702017741909.

Ferrarini, Benno, Julie Maupin, and Marthe Hinojales. “Distributed Ledger Technologies for Developing Asia.” ADB Economics Working Paper Series. Manila, Philippines: Asian Development Bank, December 2017. https://doi.org/10.22617/WPS179184-2.

Financial Action Task Force. “Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion,”, February 2013, http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf

“"From an Idea to Reality: Pakistan's Smart Card," *The News CN*. November 11, 2012, https://www.thenews.com.pk/archive/print/395365-from-an-idea-to-reality-pakistan%E2%80%99s-smart-card.

Garib, Rabia “A Database is Born: NADRA in the Early Days,” *Network World*, May 14, 2009. https://www.networkworld.com/article/2255157/applications/a-database-is-born--nadra-in-the-early-days.html?page=2

Greenfield, Robert "Explaining How Proof of Stake, Proof of Work, Hashing and Blockchain Work Together." *Medium*, July 20, 2017. https://medium.com/@robertgreenfieldiv/explaining-proof-of-stake-f1eae6feb26f.

Greenspan, Gideon "Understanding Zero Knowledge Blockchains". *MultiChain*, November 3 2016. https://www.multichain.com/blog/2016/11/understanding-zero-knowledge-blockchains/

Grody, Allan D. “What’s Really Holding Back Blockchain in Financial Services.” *American Banker; New York, N.Y.* July 12, 2017. http://search.proquest.com/docview/1917760601/citation/7DA60799D37447C2PQ/1.

GSMA, “Aadhaar: Inclusive by Design, A Look at India’s National Identity Programme and Its Role in the JAM Trinity,” March 2017, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/gsma-aadhaar-report-270317.pdf.

Harwick, Cameron. “Cryptocurrency and the Problem of Intermediation.” *The Independent Review; Oakland* 20, no. 4 (Spring 2016): 569–88.

"Home - Access Blockchain Association Malaysia." Accessed April 21, 2018. https://access-my.org/.

Hintzman, Zane. "Comparing Blockchain Implementations". *EXPO:2017 Fall Technical Forum.* Denver, Colorado. October 17 2017.

ID2020, "ID2020 Accepting Pilot Project Proposals,", April 30, 2018, https://id2020.org/news/2018/4/30/id2020-accepting-pilot-project-proposals

Indrajit, Sneha "The Cybersecurity Risks of Using Biometric Data to Issue Refugee Aid.". *Jackson School of International Studies,* July 25 2017. https://jsis.washington.edu/news/cybersecurity-risks-using-biometric-data-issue-refugee-aid/

"Inside Aadhaar, India's Massive Digital Identity Program." Accessed May 3, 2018. http://www.tearsheet.co/data/inside-aadhaar-indias-massive-digital-identity-program.

"Is a Blockchain without mining possible?" *Medium,* December 27 2017. https://medium.com/@credits/is-a-blockchain-without-mining-possible-9db40edec8b0

Juskalian, Russ, "Inside the Jordanian Refugee Camp that runs on Blockchain". *MIT Technology Review,* April 12 2018. https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/

"Keyless Signature Infrastructure". *Guardtime Federal, accessed June 2 2018. https://www.guardtime-federal.com/ksi/*

Korjus, Kaspar. "Welcome to the Blockchain Nation." *Medium,* July 7, 2017. https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4.

Kozac, Tim. "Consensus Protocols that meet different Business Demands". *IntellectSoft: Blockchain Lab,* March 26 2018. https://blockchain.intellectsoft.net/blog/consensus-protocols-that-meet-different-business-demands/

Kurlantzick, Joshua. "The Strategic Implications of Malaysia's Election Stunner". *Council For Foreign Relations,* May 16 2018. https://www.cfr.org/blog/strategic-implications-malaysias-election-stunner

Kyriakos-Saad, Nadim, Manuel Vasquez, Chady El Khoury, and Arz El Murr. "Islamic Finance and Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, February 1, 2016. https://papers.ssrn.com/abstract=2754948. P. 7

"Legal Issues Related to Identity Management and Trust Services Proposal by the United States of America." Accessed April 21, 2018. https://documents-dds-ny.un.org/doc/UNDOC/LTD/V17/010/89/pdf/V1701089.pdf?OpenElement.

Lewa, Chris and Amal de Chickera. "Trapped in a cycle of Flight: Stateless Rohingya in Malaysia". *The Equal Rights Trust.* London. January 2010.

Macheel, Tanaya "Inside Aadhaar, India's Massive Digital Identity Program," *Tearsheet,* August 22, 2017, http://www.tearsheet.co/data/inside-aadhaar-indias-massive-digital-identity-program.

Madeira, Antonio, "What are State Channels" *CryptoCompare*, May 20 2018. https://www.cryptocompare.com/coins/guides/what-are-state-channels/

Malik, Tariq, "Technology in the Service of Development: The NADRA Story," *Center for Global Development,* November 7, 2014, https://www.cgdev.org/sites/default/files/CGD-Essay-Malik_NADRA-Story_0.pdf

Manning, Jim. "Proof-of Work Vs. Proof-of-Stake Explained." *ETHNews*, November 2 2016. https://www.ethnews.com/proof-of-work-vs-proof-of-stake-explained

Maupin, Julie. "Mapping the Global Legal Landscape of Blockchain and Other Distributed Ledger Technologies," no. 149 (2017): 28.

Maurice, Joseph. "Top 10 Best Blockchain Platforms for ICOs in 2018." *Disruptor.* January 11 2018.
https://www.disruptordaily.com/top-10-best-blockchain-platforms-icos-2018/

"MENAFATF." Accessed April 16, 2018. http://www.fatf-gafi.org/pages/menafatf.html.
Medium. "Is a Blockchain without mining possible?" December 27 2017. https://medium.com/@credits/is-a-blockchain-without-mining-possible-9db40edec8b0

"Modernizing Registration and Identity Management in UNHCR: Introducing PRIMES - UNHCR Blog." Accessed May 3, 2018. http://www.unhcr.org/blogs/modernizing-registration-identity-management-unhcr/.

National Database and Registration Authority (NADRA), "About Us", accessed May 3 2018 https://www.nadra.gov.pk/.

Nagpal, Rohas. "17 Blockchain Platforms — a Brief Introduction." *Blockchain Blog* (blog), April 12, 2017. https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b.

Naylor, Robin Thomas. Wages of crime: Black markets, illegal finance, and the underworld economy. Cornell University Press, 2004.

"Partnering for a Path to Digital Identity." *The Official Microsoft Blog* (blog), January 22, 2018. https://blogs.microsoft.com/blog/2018/01/22/partnering-for-a-path-to-digital-identity/.

Refugees, United Nations High Commissioner for. "Convention and Protocol Relating to the Status of Refugees." UNHCR. Accessed February 8, 2017. http://www.unhcr.org/protection/basic/3b66c2aa10/convention-protocol-relating-status-refugees.html.

"Ripple Blockchain Technology Set to Revolutionize Saudi Arabian Banking Sector." *TechSci Research*, accessed May 15, 2018. https://www.techsciresearch.com/news/2810-ripple-blockchain-technology-set-to-revolutionize-saudi-arabian-banking-sector.html

Rosic, Ameer. "Basic Primer: Blockchain Consensus Protocol." *Blockgeeks*, January 2018. https://blockgeeks.com/guides/blockchain-consensus/.

Russ, Juskalian. "Inside the Jordanian Refugee Camp that runs on Blockchain". April 12 2018. https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/

"Saudi Arabia's Central Bank Signs Blockchain Deal with Ripple." *Reuters*, February 15, 2018. https://www.reuters.com/article/us-saudi-cenbank-currency/saudi-arabias-central-bank-signs-blockchain-deal-with-ripple-idUSKCN1FZ0LD.

Schou-Zibell, Lotte, and Nigel Phair. "How Secure Is Blockchain?" *World Economic Forum.* April 20, 2018. https://www.weforum.org/agenda/2018/04/how-secure-is-blockchain/.

Schor, Lukas. "On Zero Knowledge Proofs in Blockchains". *Medium*, March 23 2018. https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1

Siddiqi, Ayesha. "'Disaster Citizenship': An Emerging Framework for Understanding the Depth of Digital Citizenship in Pakistan," *Contemporary South Asia*, 27 November, 2017, doi: 10.1080/09584935.2017.1407294 https://www.tandfonline.com/doi/abs/10.1080/09584935.2017.1407294?journalCode=ccsa20

Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn and George Danazis. "SOK: Consensus in the age of Blockchains.". The Alan Turing Institute, University College London: United Kingdom. November 14 2017. https://arxiv.org/pdf/1711.03936.pdf

Smolenski, Michael. "Smart Contracts: Privacy vs Confidentiality – Hacker Noon." *Hacker Noon*, October 14, 2017. https://hackernoon.com/smart-contracts-privacy-vs-confidentiality-645b6e9c6e5a.

"Southeast Asia Ready to Embrace Blockchain." Accessed April 27, 2018. https://duwamish.lib.washington.edu/uwnetid/illiad.dll?Action=10&Form=75&Value=1612307.

Stevens, Paul, and Thomas C. Bogle. "Patriotic Acts: Financial Institutions, Money Laundering and the War against Terrorism." *Annual Review of Banking Law*, 21, (2002): 261–92.

Clare Sullivan and Eric Burger, "E-residency and Blockchain," *Computer Law & Security Review*. 33, no. 4, (August 2017) :470-481, doi: 10.1016/j.clsr.2017.03.016. https://www.sciencedirect.com/science/article/pii/S0267364917300845.

Sustainable Development Solutions Network, “Indicators and a Monitoring Framework, Launching a Data Revolution for the Sustainable Development Goals.”, May 15 2015. http://indicators.report/targets/16-9/.

Spirkovski, Zoran. “Strength in Numbers: A Brief History of 51% Attacks”. CryptoNews. March 19, 2018. https://www.crypto-news.net/strength-in-numbers-a-brief-history-of-51-attacks/.

Tar, Andrew. "Proof-of-Work Explained" Cointelegraph. January 17 2018. https://cointelegraph.com/explained/proof-of-work-explained

“Technical Standards for Digital ID, Draft for Discussion” *The World Bank,* 2017. http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf

Tendermint Team. "Understanding the Basics of a Proof-of-Stake Security Model." *Medium*, November 2, 2017. https://blog.cosmos.network/understanding-the-basics-of-a-proof-of-stake-security-model-de3b3e160710.

“The ID2020 Alliance Announces New Partners in Digital Identity Initiative.” *PR Newswire*, January 22 2018, accessed May 3, 2018. https://www.prnewswire.com/news-releases/the-id2020-alliance-announces-new-partners-in-digital-identity-initiative-300585991.html.

Tomaino, Nick. "On the Scalability of Blockchains". *Medium*, March 23 2018. https://thecontrol.co/on-the-scalability-of-blockchains-ec76ed769405

Tual, Stephen, "What are State Channels". *Medium*, January 3 2017. https://blog.stephantual.com/what-are-state-channels-32a81f7accab

HID Global, “The Kingdom of Saudi Arabia National ID Card”, 2012. https://www.hidglobal.com/sites/default/files/resource_files/hid-gov-id-ksa-cs-en.pdf

Tim, Kozak. “Consensus Protocols that meet different Business Demands”. IntellectSoft: Blockchain Lab. March 26 2018. https://blockchain.intellectsoft.net/blog/consensus-protocols-that-meet-different-business-demands/

US -Cert "Understanding Denial-of-Service Attacks"., accessed May 19 2018. https://www.us-cert.gov/ncas/tips/ST04-015

United Nations Commission on International Trade Law, Fifty-fifth session. “Legal Issues Related to Identity Management and Trust Services”, A/CN.9/WG/IV/WP.145, 20 February 2017, https://documents-dds ny.un.org/doc/UNDOC/LTD/V17/010/89/pdf/V1701089.pdf?OpenElement

UNHCR, "Modernizing Registration and Identity Management in UNHCR: Introducing PRIMES”. http://www.unhcr.org/blogs/modernizing-registration-identity-management-unhcr/.

Varagur, Kirthika. “Malaysia’s Elites Rides the People’s Tsunami” *Foreign Policy*. May 11 2018. http://foreignpolicy.com/2018/05/11/malaysias-elites-ride-the-peoples-tsunami/

Waves. "Waves - the fastest ever blockchain", accessed, May 19 2018, https://waves-ng.wavesplatform.com.

"WDR16 Spotlight on Digital Identity." Accessed April 30, 2018. http://pubdocs.worldbank.org/en/959381434483205387/WDR16-Spotlight-on-Digital-ID-May-2015-Mariana-Dahan.pdf.

"Who We Are" *Financial Action Task Force (FATF),* accessed April 16, 2018, http://www.fatf-gafi.org/about/whoweare/.

"Who Are the Rohingya?" Al Jazeera. April 18, 2018. https://www.aljazeera.com/indepth/features/2017/08/rohingya-muslims-170831065142812.html.

Wong, Joon. "The UN is using Ethereum's technology to fund food for thousands of refugees". QUARTZ. November 3 2017. https://qz.com/1118743/world-food-programmes-ethereum-based-blockchain-for-syrian-refugees-in-jordan/

Xu, Xiwei, Weber, Ingo, Staples, Mark, Zhu,Liming, Bosch, Jan, Bass,Len, Pautasso, Cesare, and Paul Rimba. *A Taxonomy of Blockchain Based Systems for Architecture Design.* Sydney: CSIRO, University of New South Wales, Carnegie Mellon University, Lugano:Università della Svizzera italiana, and Switzerland: Chalmers University of Technology, 2017. http://www.pautasso.info/biblio-pdf/blockchain-icsa2017.pdf

Yeoh, Peter. "Regulatory Issues in Blockchain Technology*", Journal of Financial Regulation and Compliance,* 25 no.2 (2016): 201-202, doi:10.1108/JFRC-08-2016-0068.

Yoo, Soonduck. "Blockchain Based Financial Case Analysis and its Implications", *Asia Pacific Journal of Innovation and Entrepreneurship,*11, no.3 (2017), doi:10.1108/APJIE-12-2017-036

Zaman, Hasanuzzaman and Rokonuzzaman. "Achieving Digital Bangladesh By 2021 and Beyond" *Planning Commission Bangladesh*, 7FYP, February 18 2015. http://plancomm.gov.bd/wp-content/uploads/2015/02/18_Achieving-Digital-Bangladesh-by-2021-and-Beyond.pdf

Zulhuda, Sonny. "Whither Policing Cryptocurrency In Malaysia?" 25, no. 2 (2017): 18.

Zwanenburg, Jorn. "Consensus Algorithms Explained: What You Need to Know About Proof-of-Work, Proof-of-Stake and Delegated Proof-of-Stake." *Invest In Blockchain,* May 14 2018. https://www.investinblockchain.com/consensus-algorithms-explained/

Team Bios

Faculty Lead

Sara Curran (scurran@uw.edu): Sara Curran joined the faculty of the University of Washington's Henry M. Jackson School of International Studies and the Daniel J. Evans School of Public Policy & Governance in 2005. She is a Professor of International Studies, Professor of Sociology, and Professor of Public Policy & Governance. She is also an Adjunct Professor of Global Health and affiliate faculty of the Center for Global Studies and the Center for Southeast Asian Studies. Sara holds degrees from the University of Michigan (B.S., Natural Resource Management), North Carolina State University (M.S., Sociology and Economics), and the University of North Carolina at Chapel Hill (Ph.D., Sociology).

Currently, Sara serves as director of the UW's Center for Studies in Demography & Ecology. She researches gender, migration, and environment in developing countries. Current projects include: 1) social change and migration dynamics, 2) climate change, natural disasters, and population change, and 3) several projects related to applied research and training. Her authored work appears in *ANNALS of the American Academy of Political and Social Sciences*, *Demography*, *Population and Development Review*, *Social Science Research*, *Social Forces*, *Teaching Sociology*, *Journal of International Women's Studies*, *Ambio*, *Population & Environment*, and *Journal of Marriage and the Family*.

ARP Program Manager

Allison Anderson (allyja@uw.edu): Allison Anderson is a Ph.D. candidate at the Jackson School of International Studies. Her research interests are centered around gender, development, and information and communications technologies (ICTs) in the Arab world. She is currently studying pathways to women's economic participation in Jordan. Allison came to the Jackson School from the Bill and Melinda Gates Foundation, where she focused on strategic planning and engagement in the Office of the President for Global Health. Previously, she worked at Deloitte Consulting conducting political risk analysis and market research for both public and private sector clients. Allison served two years in the U.S. Peace Corps in Jordan. Allison received her M.A. from Johns Hopkins Paul H. Nitze School of Advanced International Studies (SAIS) where she focused on Strategic Studies and International Economics. She holds a B.A. in Political Science and Arabic & Islamic Studies from the University of Michigan.

Senior Research Fellow

Seth Kane (sethkane@uw.edu): Seth Kane is a Ph.D. student at the Jackson School of International Studies at the University of Washington. His research focuses on the nexus of Myanmar's political transition and peace processes, particularly with regards to the effects of international aid and diplomacy. Seth received his B.A. in Human Biology – Evolution and Ecology from Brown University and his M.A. in Asia Studies and International Economics from the Johns Hopkins School for Advanced International Studies (SAIS). Seth has 11 years' work experience focusing on South and Southeast Asia as a conflict analyst, international politics lecturer, and conflict management project implementer.

Research Fellows

Sneha Indrajit (snehaha@uw.edu): Sneha Indrajit is an International Policy Institute Cybersecurity Research Fellow, and has been so since June 2017. In that time, she has researched the use of biometrics, blockchain technology as well as privacy rights within the U.S. She is a graduating senior pursuing a B.A. in International Studies and an emphasis on foreign policy, diplomacy, peace and security. Her current research interests, besides the

myriad of issues within cybersecurity, include immigration and development. She intends to pursue law in the future. Originally from Singapore, Sneha is fluent in both English and Mandarin. She is also proficient in conversational Tamil. Sneha enjoys writing poetry, public speaking and the company of animals.

Jannah McGrath (mcgraj@uw.edu): Jannah McGrath is an International Policy Institute Research fellow for the Rohingya Project Applied Research Program. She is a graduating senior within the Jackson School pursuing a B.A. in International Studies (Focus: *foreign policy, diplomacy, and peace and security*), with minors in French and Environmental Studies. Throughout the remainder of her undergraduate career and beyond, Jannah hopes to apply a critical understanding of global legal frameworks and a fascination for data analytics to continued engagements which align with the following mission: To have a sustainable and positive impact in the communities she interacts with through critical analysis, technological innovation, cultural understanding and a life of service to the international community focused on finding solutions to social challenges which produce measurable results that disrupt the cycle of poverty and systematic exclusion.

Matthew Newton (mnewton2@uw.edu): Matthew Newton is an International Policy Institute Cybersecurity Research Fellow. Matthew is an M.A. student in the Jackson School's Russian, East European, and Central Asian Studies program. Originally from Los Angeles, Matthew is a 2012 graduate of The Evergreen State College in Olympia, Washington. Before attending the UW, Matthew spent two years in Moscow working as a teacher of English. He has also worked in the digital marketing sphere as a researcher and copywriter. He is a 2016–2018 Foreign Language and Area Studies (FLAS) fellow in Russian. His research interests include Russian politics, international development, and cybersecurity. Matthew additionally enjoys cooking, the outdoors, and cats.

Arica Schuett (aricas@uw.edu): Arica Schuett is an International Policy Institute Research Fellow for the Rohingya Project Applied Research Project. She will graduate in June 2019 with a degree in International Studies (emphasis: International Political Economy) from the Henry M. Jackson School of International Studies. She intends to join her interest in economic and social issues to research and reform aid and funding programs locally and around the world. Currently Arica interns at the Pacific Northwest Economic Region. There she researches economic data and government policy to help the organization facilitate dialogue between industries and governments across the Pacific Northwest and Canada. She enjoys gardening, music, and Seattle's cool, cloudy weather.

Hailey Vandeventer (hailev@uw.edu): Hailey Vandeventer is an International Policy Institute Research Fellow for the Rohingya Project Applied Research Project. She is also a Jackson School Undergrad majoring in Foreign Policy and Diplomacy with a double major in French, and a minor in European Studies. Her research has focused on Europe, migration, and French-Speaking west Africa. She plans to further her career in policy analysis and think tanks.