

# Self-Sovereign Identity on a Blockchain

Abraham Ross

Honor's Capstone

## **Problem Statement**

Imagine a life a world away. 1995 Peru, the Tupac Amaru Revolutionary Movement is in full swing and engaged in a bloody insurgency to the Shining Path, fifty to seventy thousand deaths and counting by the end of the conflict. You and your family, like many others, decide to flee the country in hopes of better worlds and safety away from the conflict, however, in the rush, you leave behind most of your possessions, including your ID. When you arrive in a new country to set up your life without an ID or civil records that were all destroyed in the conflict, you and millions of others are unable to have access to social or financial services, or even enroll yourselves or kids in school. This is exactly what happened to millions of Peruvian citizens fleeing the country during the insurgency that took place throughout the 1990's and still something that occurs all over the world in suppressed nations to this day. Growing up in a secured and developed country such as the United States, the issues of IDs never really cross most people's minds as they are easily able to access passports and driver's licenses or social security cards. However, this is a real issue in other nations across the world. The examples above are merely the tip of the iceberg when it comes to issues surrounding identification around the world. The inability of citizens in impoverished nations to own their own identity leads to issues with simple financial aspects such as opening a bank account or being able to own their own assets without the government seizing them. But it also opens up more serious issues such as ease of crime like human trafficking, and how these citizens are unable to own their accomplishments like degrees or have the ability to enroll in school, vote, or apply for jobs. This Honors Capstone paper explores how running self-sovereign identities on blockchain may minimize the vulnerability that millions of people currently face. This paper explores the viability of this technology and its challenges with implementation. It argues that digital

identities should be implemented across all impoverished nations so these citizens can attain a self-sovereign identity, but that steps taken towards the use and deployment of these identities needs to be well thought out and planned in advance.

For years companies and people are the world have been developing blockchain technology for institutional purposes. However, in recent years the concept of a blockchain and the common words such as NFT's and Cryptocurrency that it is associated with burst onto the scene of popularity to the point where the entire world was made aware of them. The limited understanding of the actual technology behind these concepts and blockchain's (but more specifically bitcoin's) sketchy past has led to a controversial divide in how people feel about the topic. My point is not whether blockchain technology is evil or good, I plan to explore it's uses to provide security in identity to underdeveloped nations, however, there is a certain level of understanding that needs to be developed before I dive into that material. An important point to distinguish off the bat is blockchain can exist without cryptocurrency. Many people think they only go together, so when discussing business applications of the technology, the question "so when does bitcoin come in" always comes up at the end of conversations. The best way to think about it is: blockchain is to bitcoin as the internet is email, email is simply a function of the internet, but couldn't exist without it. Blockchain is the technology that bitcoin and other cryptocurrencies or NFT's operate on but has many other business applications that have nothing to do with those two.

### **What is Blockchain?**

Blockchain is referred to as a distributed ledger technology, the simple understanding of this is that blockchain is a cohesive data base with encrypted and verified entries. Each entry is immutable but shared for anyone in the blockchain to see. Blockchains can be public or private.

If a blockchain is public, anyone can see the transactions or data entries going on in the chain, if it is private though, only certain people have access to the entries on the blockchain. Typically, institutions with security concerns such as banks that use blockchain for remittance payments, will use a private blockchain. Before an entry can be added to the blockchain, the transaction information must be confirmed by fifty one percent of users or “computers” who have a copy of the record history and are part of the network. This is not simply the people who can see the transactions, this is everyone who has stake in the network or company with access the chain. The computers make sure every detail of the transaction is authorized and legitimate before deciding on approval to pass the entry onto the blockchain. Once the data entry is added, it cannot be changed. The entry must perfectly match every other entry in the blockchain. This verification process is why blockchain’s history cannot be edited. This stops any attempts at hacking because if a person wanted to create a false data entry, they would have to change every single block already structured for every transaction in the past to match their new false entry, and this is impractical to do because it is impossible to change past entries on the blockchain. There are also other mechanisms in certain blockchains designed to help prevent hacks or even attempts of hacks, one is gas fees application to the problem of "infinite loop of code". Gas fees are basically best thought of as a service fee on an account, many times when there is a transaction or input of data in a blockchain there is a gas fee that comes along with it, typically they are small in regard to the size of the transaction or code ran. However, when there is a lot of use in a network, the gas fees begin to elevate. If someone was to try to hack into a network to have access to this data they would be running an absurd amount of code and the gas fees in turn would begin to raise high enough to the point where it would not be financial viable for the person or group to still

hack the network even if they were able to get control of 51% because of the amount of money they would be paying in gas fees.

## **Blockchain Applications**

Now that we have laid a basic framework as to what a blockchain is, we can briefly touch on how it often applies business applications outside of just cryptocurrency and NFT's. Despite uses in the business world such as banking or fintech, blockchain can also apply to other areas as well. Many institutions are implementing this technology to access healthcare processing and storage of customer information more efficiently on a blockchain, others are using it to tokenize (separate value of assets into smaller portions) real estate to make larger properties more affordable for investors with less capital to work with. Despite all these uses, I want to explore the idea of running a digital identity on a blockchain to help people all around the world achieve self-sovereign identity. More specifically, I like to focus on this application being deployed to underdeveloped areas where suppressed people do not have ownership over simple things such as their own identity and this solution could not only help them professionally but could stop many crimes that have eroded those nations. This movement or idea of self-sovereign identity is simply defined as the concept of people being able to not only own their own identities in entirety without a governmental body intervening, but also that they own all accomplishments in that digital capture, such as foreign degrees or certifications that can be overlooked if moving to another country in the world.

## **Personal Background**

My interest in this area started the Spring of 2021. I participated in an independent study through the University last spring with just three other students. Our direction was to explore the

idea of Blockchain applications, and then at the end of the semester we completed research projects for a company that supports the University heavily called IOHK or Input Output. IOHK is a blockchain software development company, over the past couple years they have developed a blockchain that not only do they run a cryptocurrency on, but they also are attempting to run many other applications like digital wallets or identities on. After this, I was offered an internship with the company. During my time from roughly June to September with this company I worked primarily in their Atala Prism department. Atala Prism is IOHK's digital identity solution. Their approach to a digital identity is from the monetary standpoint, however. Something I will touch on later is that if a country invests in a digital identity, they will unlock anywhere from a three to thirteen percent increase in their GDP, this number ranges based on the status of the country but is always higher for a developing country. IOHK plans to pitch this idea of digital identity to many underdeveloped countries in Africa and Latin America to make their institutional systems such as schools, health care, and government more effective when many aspects of IDs will then be running on a blockchain. IOHK will then obviously charge a fee but will implement everything themselves and run the ID on their blockchain. As I did many weeks' worth of market research and product development in this space, I could not help but sympathize with the humanitarian side of this argument. Every meeting I sat in, the company was asking how they needed to construct price models and how to deploy to countries in the most efficient way to see the smallest costs, but my mind was on something else. I realized that yes, this technology has the potential to absolutely create an entire new industry, which means more jobs, and better quality of life for many people not only involved in the technology side but also the countries that implement the IDs. But I was more so focused on the fact that this could revolutionize people's lives who are trying to make ends meet in those impoverished countries.

Whether that simply means they now have access to a bank account and can safely store their money, or the chance this could heavily cut down on crimes that prey on human identity such as human trafficking. Because of this, I got involved in some other companies that promote and fight for digital identifying around the world because of the positive impacts it could have on people in impoverished nations. I began researching this process heavily and decided to model my honors capstone around a thorough analysis of this concept, including the pros and cons and evaluation of a real case study in the area, all while communicating in a way anyone can understand because that is so crucial in an industry that can be confused due to heavy technological jargon. My interest also involves expanding the idea of digital identity to a point where governments and corporations alike can develop Self Sovereign identity for all citizens. This idea of self-sovereign identity would be a secured, portable, and digital identity that is owned entirely by the citizen, not a government or individual corporation.

## **Introduction**

Currently, over one billion people spread across the globe do not have access to any form of legal identity. This is often because their country failed to keep track of their citizens documents, or they live under a corrupt government that has no tracking systems or destroyed the documents intentionally. Regardless of the reason, this denies these people access to any sort of financial or educational services, does not allow them to establish any sort of life outside of their country, and makes them more vulnerable to crime. Shanti, an Indian citizen referenced in an article from the World Bank, relies entirely on wages from MNREGA (India's rural employment guarantee program) and a pension for her and her disabled husband. Shanti does not have a secure way to save and protect her money though because she does not have access to a bank account. To open a bank account, Shanti would need a government-issued ID, which not only

her, but many other women in her region do not get. This same article references Mariam, a Ugandan woman in a similar situation to Shanti. Her income is dependent upon cross border trading, however, since she does not have the necessary IDs provided by her government, she is forced to take a longer distance to deliver goods exposing her to crimes of theft and human trafficking. Not only this, but the access to legal identification allows these citizens to take part in basic civic duties such as voting and taking part in their legislative systems. I will refer to digital identity as the use of digital technology all throughout the aspects of an identity, from data capture, to storage, to verification and management. But the aspect of storage is where a blockchain will come into the equation to ensure safety of the information and instant verification.

### **Access to Financial Systems**

There are many business applications having a self-sovereign ID would allow, but the first one I will touch on is allowing larger access to financial systems such as banks for people that do not have bank accounts currently. In 2017, the World Bank Global Findex survey stated that lack of ID was a key barrier to financial services and even heightened as a barrier to marginalized populations, saying “The survey found that the poorest 40 percent of women in low-income countries are, on average, about 30 percent less likely to have an ID than men in the same wealth quintiles.” Without access to financial systems or institutions, they cannot protect their assets. They must store any money they have at their house or another physical location that makes it more susceptible to robbery or seizure. To open an account at a bank, customers need a legal and verifiable ID to prove their citizenship, this is something that could all be done through a blockchain because the customers information would be automatically stored on the blockchain, and they would simply grant the bank access to their data like someone does when



they show the bank an ID. This access to financial services through a digital ID would provide a better quality of life to this population and the nation in many ways. They could then start storing and investing money through the bank, they could also have paychecks direct deposited to the bank. This is an aspect that is very important as many studies point to high robberies in impoverished nations on pay days. Thieves will wait outside of workplaces where people are paid every Friday for manual labor, and they are often accosted and lose their money simply trying to get home from work. If the money was sent directly into the account, or wired along a blockchain, this would also provide greater protection for financial assets. This technology would not only be beneficial to the customers at the bank, but also provides benefits across the board to the institutions and public authorities as well. A large part of banking in our modern day is figuring out ways to apply with KYC/AML laws (know your customer and anti-money laundering). This technology would allow the banks easier tracking and verification of customer data to protect these laws. This also protects against identity theft and fraud in these areas of the world. It would also provide not only access to credit for the customers, but better credit scoring by the institutions which benefits comes back not just on the institution but the customer as well.

### **Reduction in Crime**

The issue of human trafficking is also one that is heavily associated with this idea of self-sovereign identity and its potential solutions. The international labor association estimates that twenty-one million people around the world are affected by human trafficking, many in the form of sex slavery. Even more disturbingly, roughly twenty six percent of those people are qualified as children. A large source of these kidnappings comes down to the fact that so many people do not have the correct IDs to ensure a safe crossing of the border to a new land. Because of this, people in impoverished countries try to cross borders illegally and take deals with organizations

they do not know are part of the slave trade that promise to discretely transport them across the border for a small fee. Of course, though, they do not transport them across borders to their actual destinations, instead, they traffic them into a slave trade where they are sold. These individuals having access to a Self-Sovereign identity would allow them to both effectively cross the borders whenever desired and escape captivity in these impoverished nations without concern of having a physical representation of legal identity to get away. It would also help governments or border officials notice and track when people are being taken away by these organizations. Many of people, especially in rural areas, never were registered as citizens or their documents were destroyed due to internal conflict, such as the Peruvians. However, with a digital ID, stored directly onto a blockchain the governments they live within could have historical records of them as citizens and it would be much more difficult to make anyone disappear like they currently can. This solution, like all others, does not come without its downsides, however. To successfully install this technology to prevent these crimes there would have to be mass adoption across the country. Referencing a case study done by the Transparency Lab in Moldova, there are conclusions of how this technology could be detrimental instead of beneficial if implemented wrongly. This is an area well known for its high amount of kidnapping and forced labor. The reason these crimes persist so highly in this region is because of the lack of government issued IDs and corrupt border officials. Because they have no actual IDs given to them, it makes it incredibly easy for the traffickers to move them across borders with either fake ids or simply by bribing the officials at the border. The transparency lab comments:

“While a self-sovereign, immutable digital identity for Moldovans might seem like a workable fix, well-established criminal networks that cooperate with corrupt officials will likely find a way around enforcement steps, like checkpoint verification. In an already unstable

political environment, workarounds, bribes, and further abuses of power could easily undermine a more secure identity system and place vulnerable Moldovan citizens in greater danger.”

This illustrates just how this technology could potentially go wrong and why many people argue against it in developed areas with unstable political climates. Not only this, but if a digital ID was running without a blockchain, all the information would be stored centrally to the government or a third-party corporation and could easily be accessed and bought away from the individuals themselves. Therefore, the implementation is just as important as the technology. If these IDs were to be used in underdeveloped areas, the people who push them forward and implement them would have to thoroughly educate the populous on the benefits and how to use the IDs. They would have to be backed by concrete legislation, buy in from the government, and could not be manipulated by crime organizations and internal factors. A blockchain could also help solve many of these problems by ensuring that the information is solidly encrypted in a network that only the individual has access to and cuts out any possible opportunities for tampering or third-party risk.

### **Potential Risks**

Digital IDs come with risks as well though. They are not simply a solve all for the developing world. Some of these risks that people who are against this idea bring to the table are handling of customer data, specifically the possibility of data misuse or data leaks. This concern is very real and something that has slowed down implementation of digital ids all over the world. However, it is something a blockchain can stop when used to implement IDs instead of a traditional database. If all the data is stored in a centralized database ran by the government, there is a high probability of a hack or data leak. There is also no way for the citizens to ensure that their data is not being sold to third parties or misused. The way a blockchain could stop this

is that each person will own their identity and data wholly and be able to determine who can access it. All personal information would be securely and privately stored on each user's smartphone or other means to the blockchain (such as a smartcard). Leveraging this blockchain technology, the governments and institutions can ensure that all transactions are secure and peer to peer-to-peer. Each user would be the only person with the access to their data and credentials stored on the blockchain, removing all questions of data breaches or misuse of information. Another argument is how will these be implemented to include all persons in a country. This is again a valid argument that needs to be thoroughly addressed by all people in the decision-making circle to ensure the effectiveness of this technology. If not, all people are included in this revolutionary ID process, we are right back to square one with a high percentage of people that are without necessary ID requirements in underdeveloped countries. Because of this, this technology would have to be pursued to the degree of mass adoption. Not just the high class or government officials, we would need government and institutions to work hand in hand educating and deploying this technology to their entire populous.

### **Implementation**

When discussing the process of implementation, it all revolves around technology. Currently there are about 10 billion internet connected devices in the world and that is projected to grow to 20 billion by 2025. These IDs will require these connected devices for storage. Decentralized storage is the most important concept of secure identity data management. In a decentralized framework, information is usually stored directly on the user's device (smartphone or laptop) or securely held by private identity stores, such as a smart card. A smart card would be both a physically and digitally accessible card that governments or institutions can issue that will store all the people's data individually. Although it can be

deployed in physical form, if lost or not in possession at time of need the people can access their smart card or credentials through an internet service as well. Data under the user's control makes the information more interoperable, allowing the user to employ data on multiple platforms, such as financial services, use the information for different purposes, and protect the user from being locked into one specific platform. There are a couple key steps to take to make sure the implementation is all inclusive and successful before this storage process, according to McKinsey, "Many governments around the world have introduced ID systems that incorporate digital technology... Governments have had mixed success getting citizens on board. While some countries, including Estonia, Denmark, and Sweden, have achieved almost universal adoption, others have signed up relatively few users". Yes, there are some western European countries that have achieved the satisfied level of adoption; however, you cannot just simply copy their model. Those countries are developed and have little to no rural areas without communication. My discussion centers around the less developed areas of the world. The biggest goal to achieve here to me would be establishing trust in the population. This way they agreed to get on board with the new technology. This trust would have to be established through a couple different steps, firstly, making sure the population you deploy too is educated thoroughly on the topic and understand how this would help them and improve their quality of life. They would also need to establish a strong technical system they could guarantee would not fail and, strong regulatory structures to uphold the integrity of the. Interoperability is also exceptionally important in these cases. The governments would need to work with institutions to allow and make sure this technology works well with other systems around the globe like financial processes. According to McKinsey, there are two steps to achieve this, the first is "committing to standards in accordance with international best practice". This helps

develop interoperability in both their technology and data that will be used throughout the government and institutional systems. The second is “implementing technologies enabling data transfer to and from other systems, including technical interoperability layers, web services, and application programming interfaces”. This step is just as important as the first because it allows the business applications of these IDs to surface. If the IDs are not operational with other systems, then the quality of life for these people is not truly enhanced past the basic functions of an ID. Another step of implementation in these countries that would be crucial to build trust would be ensuring that the technology includes either Multi-Factor or Cryptographic authentication to access the data. When each citizen owns their own facet of this technology, their data will be encrypted heavily to not allow leaks or access from outsiders. Multi-Factor authentication is something that requires users to prove themselves to be the person owning the information by a combination of either something they know (password or seed phrase), own (token or phone) or are (biometrics). This is basic level security and not as highly encrypted as cryptographic authentication, that is something required when breach of information could lead to personal harm, significant financial loss, harm the public interest or involve civil or criminal violations. Cryptographic authentication is based on proof of ownership of a key through a cryptographic protocol. This type of authentication is used to achieve the strongest level of authentication assurance and is typically done through hardware cryptographic modules. Finally, when discussing implementation, comes about the question of addressing how these identities would function completely independent from a government. This is difficult to address because of the varying levels of stability across the world and how important this concept is. The way I see this working is yes, governments should oversee setting up the deployment of these identities if it is a stable nation, or if they are running the technology through an independent company

(IOHK mentioned in my paper) then that company can be responsible for distribution in function with the government. It is important to have the government involved to make sure all people, especially women and children, are accounted for. However, once this solution is rolled out, it will function completely independently from the government's power. No government officials or organizations will have access to the data encrypted on the blockchain unless the individual gives consent. Only the user will have access to the cryptographic authentication, and they will control this information in its entirety. This concept becomes convoluted when addressing developing nations with corrupt governments, however. In this sense, the best arrangement I see happening would be a humanity-based organization helping to deploy these identities to all suppressed individuals, especially women and children. They could set up the technology on a trusted platform and then roll out implementation to the people of these impoverished nations so then regardless of any global or country wide events, they always have verifiable proof of their identifies and accomplishments. Again, although this organization would implement the identities to the people, once the data was encrypted on the blockchain, only the user would have control or access to it in entirety. It would be impossible for this information to be accessed by a person or organization that does not have access to the authentication key.

### **Case Study**

A case study done in this field that I want to analyze and discuss highlights of is *Identified but Unheard, Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalized Communities*, done by NDI in communication with Dem Tech. This is a thorough case study that highlights an in-depth analysis of digital ID in global adoption specifically for democracy and civil rights, along with three more specific case studies highlighted in the appendix. This case study touches heavily on two concepts that I highlight as

very important in the implementation space of this technology, community involvement and education. NDI believes heavily that educating the public on not only how to use, but the thorough ins and outs of the benefits is crucial to this technology working and increasing quality of life for people in impoverished nations saying “Information on the purpose and registration process of digital ID systems should be made accessible and understandable for all members of the public, especially marginalized populations”. They also believe that governments and institutions need to collaborate effectively not just with each other but also the community, “Sufficient community consultation with marginalized groups during the design and rollout process of a digital ID system is needed to ensure that potential barriers to uptake for marginalized populations have been addressed.” This supports the thought process of mass adoption for an all-inclusive system. Certain populations cannot be left out during this development period, or it will ruin the entire point of the technology. This case studying does a great job of also highlighting very specific details that need to be included when considering how the implementation occurs to include everyone. Many people in low-income societies can have a hard time getting off work or finding the time in general to go wait in line and register for a digital identity. NDI references the Philippines and how they did this, implementing nation ID registration centers in shopping malls and other commonly accessed community cites to make it easier for citizens to get in and out without using much time. Another aspect of this case study that is empathized that would clearly expand the quality of life in these areas is this technology’s impact on the voting process. As NDI explains, “Beyond its potential as a tool for reducing election fraud through elimination of duplicate or deceased voters, biometric voting technology is often touted as a mechanism for enfranchising all eligible citizens by modernizing the register and instituting new processes to reach those who may have been excluded from previous

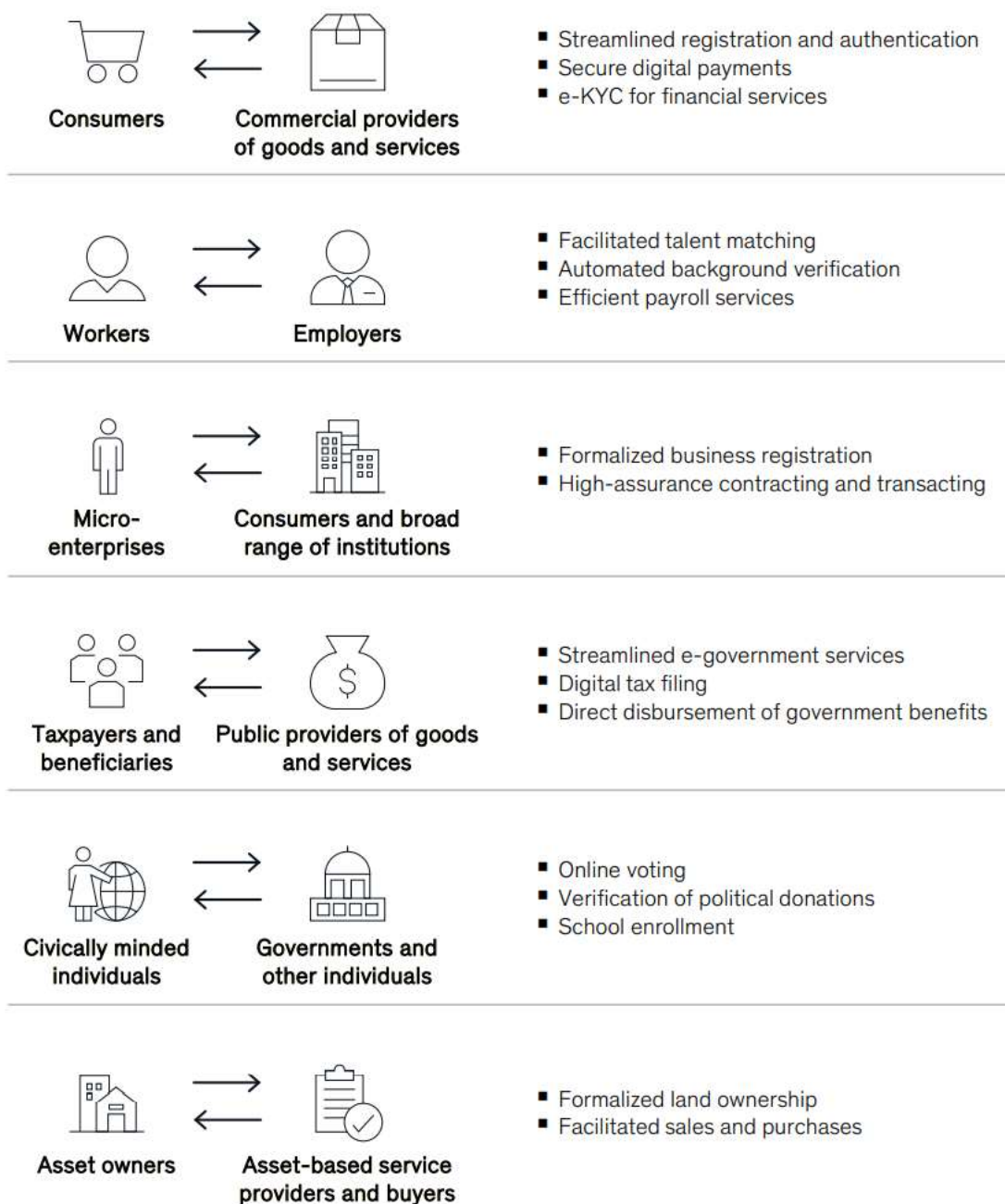


registration exercises due to factors such as gender identity, disability, geographic location, and ethnic or religious divides”. What they are explaining here is this technology provides both exclusion and inclusion in the best of ways for the voting process in all countries. It provides exclusion because it is impossible for duplicate votes or illegal votes (such as deceased or nonexistent people) to count. This is clearly not just an issue in the developing world as every election in the United States sees vast controversy over this topic as well. This technology makes that impossible because of its instant verification and immutable data structure. On the other hand, it allows a new way of including all people’s votes, it is no secret that in developing worlds some people are barred from voting based on gender identity, sexual orientation, and many other factors. However, if a voting mechanism was set up through a digital identity, all people could vote and vote easily from their phones or an internet connection device. There would be no more controversy of destroyed ballots or tampered elections because the data from the blockchain would be immutable. The final part of this case study I wanted to touch on was one of their independent case studies they reference in the appendix. They touch on privacy concerns in Nigeria, more specifically, as Nigeria began the data collection process for a digital ID there were worries raised all over the country pertaining to why this collection was happening and so required of all citizens, one saying “The idea of a multiple data collection in a period where the government is clamping down on those who speak out against irregularities in governance is worrisome for me. Why now? and What is the Data for? These questions have yet to be answered.” These are very valid questions and concerns as data sharing with third parties and infringements upon citizens personal privacy is becoming more of a common thing. However, I wanted to address this as something that could be totally erased when implementing this technology using a blockchain instead of a centralized database like Nigeria or many of these

other countries. If the government communicates that each person will have complete ownership of their own identity without anyone else being able to access it, that should erase this concern and furthermore, the pushback this technology receives when individuals do not trust it.

### **Financial Potential**

Another advantage I wanted to briefly discuss when evaluating idea of self-sovereign identity on a blockchain is the mass financial potential it can unlock for the Countries that implement a digital ID. According to a study done by McKinsey institute, implementing a digital ID could unlock economic value equivalent to anywhere from three percent to thirteen percent of a nation's GDP by 2030. In places like the United States that number is four percent, however, in developing countries like Nigeria it is up to seven, and in areas such as Brazil where the populous is so large and hard to track, the value jumps to thirteen. This extreme economic value is enabled through many different facets of using a digital ID and are highlighted in this figure from the McKinsey study.



The most important aspect of this value creation is how it can incentivize countries to people to adopt this technology. That value creation is not coming back to the people who built the technology, it is coming back into the countries, which means more wealth being passed around, more jobs, and better development across the landscape for all people. This will undoubtedly

lead to an increase in the quality of life for all peoples in this country as more wealth becomes available.

## **Conclusion**

In final analysis, there is no question that digital identity, ran on a blockchain or not, has extremely high potential to change people's lives for the better and positively impact entire nation's economies. However, there are many important aspects to consider during the development and implementation stage of this technology. This idea was inherently designed and delivered for people in impoverished nations who are already susceptible to crime and discrimination. This technology has the ability to make their lives easier and increase their quality of life. If the correct steps are not taken when delivering this new form of identification, it can make impoverished citizens even more vulnerable to the crime and oppression that already affects them. The need to ensure the identities are all inclusive and encrypted on a blockchain are some of the most important steps. These guarantee that everyone is included and out right owns their own data, making this a true form of self-sovereign identity. After this we would see a decrease in crime and an increase in empowerment to people all over the world. Along with an increase in efficiency of all business processes form financial details to verification of government forms that creates value brought into each nation. This is all possible through a simple change in how we currently deploy and track identities, and this change has the potential to dramatically increase the quality of life for impoverished people all over the globe. The only step now to take is making sure the deployment is done in a responsible matter that protects citizen's data and allows for the growth in economic potential and better standard of living for all people regardless of their location or background.

## Works Cited

*Atala Prism*. atalaprism.io/. Accessed 3 Mar. 2022.

Bhrott, Priyal. "Identified but Unheard Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalized Communities." *ndi.org*, June 2021, [www.ndi.org/sites/default/files/Identified%20but%20Unheard%20FINAL.pdf](http://www.ndi.org/sites/default/files/Identified%20but%20Unheard%20FINAL.pdf). Accessed 4 Mar. 2022.

"Digital ID on the Blockchain & Human Trafficking." *Medium.com*, 17 Dec. 2017, [medium.com/@emergetechlab/digital-id-how-to-reduce-human-trafficking-7445da7f337a](https://medium.com/@emergetechlab/digital-id-how-to-reduce-human-trafficking-7445da7f337a). Accessed 4 Mar. 2022.

Domeyer, Axel. "How governments can deliver on the promise of digital ID." *McKinsey Institute*, 31 Aug. 2020, [www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id](http://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id). Accessed 5 Mar. 2022.

"Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable." *Worldbank.org*, 14 Aug. 2019, [www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable](http://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable). Accessed 4 Mar. 2022.

Lubin, Joseph, et al. "BLOCKCHAIN FOR GLOBAL DEVELOPMENT." *transparencylab.org*, 2017, [transparencylab.org/Documentation/Additional%20resources/Literature/Lubin%20et%20al\\_Blockchain%20for%20Global%20Development\\_2018.pdf](http://transparencylab.org/Documentation/Additional%20resources/Literature/Lubin%20et%20al_Blockchain%20for%20Global%20Development_2018.pdf). Accessed 4 Mar. 2022.

"OWASP Top Ten Proactive Controls 2018." *owasp.org*, 1 Jan. 2018, [owasp.org/www-project-proactive-controls/v3/en/c6-digital-identity](http://owasp.org/www-project-proactive-controls/v3/en/c6-digital-identity). Accessed 12 Mar. 2022.

Parekh, Nidhi. "Digital IDs: The good, the bad, and the unknown." *povertyactionlab.org*, 6 Oct. 2020, [www.povertyactionlab.org/blog/10-6-20/digital-ids-good-bad-and-unknown](http://www.povertyactionlab.org/blog/10-6-20/digital-ids-good-bad-and-unknown). Accessed 4 Mar. 2022.

Pillay, Suren, and Sean Moutan. "Why self-sovereign digital identity is a game changer for financial inclusion in Africa." *CNBCAfrica*, 9 Sept. 2021, [www.cnbc africa.com/2021/why-self-sovereign-digital-identity-is-a-game-changer-for-financial-inclusion-in-africa/](http://www.cnbc africa.com/2021/why-self-sovereign-digital-identity-is-a-game-changer-for-financial-inclusion-in-africa/). Accessed 24 Apr. 2022.

"The Potential Drawbacks to Digital Identification." *Working Capital Review*, [workingcapitalreview.com/2021/04/the-potential-drawbacks-to-digital-identification/#:~:text=Fourth%2C%20all%20the%20systems%20of,put%20entire%20systems%20at%20risk](http://workingcapitalreview.com/2021/04/the-potential-drawbacks-to-digital-identification/#:~:text=Fourth%2C%20all%20the%20systems%20of,put%20entire%20systems%20at%20risk). Accessed 13 Mar. 2022.

Schmidt, Kai, and Philipp Sandner. "Solving Challenges in Developing Countries with Blockchain Technology." *Frankfurt School Blockchain Center*, 1 Oct. 2017, [explore-ip.com/2017\\_Solving-Challenges-in-Developing-Countries-with-Blockchain-Technology.pdf](http://explore-ip.com/2017_Solving-Challenges-in-Developing-Countries-with-Blockchain-Technology.pdf). Accessed 22 Mar. 2022.

SRINIVASAN, JANAKI, and ELISA OREGLIA. "The Myths and Moral Economies of Digital ID and Mobile Money in India and Myanmar." *estsjournal.org*, 2020, [estsjournal.org/index.php/ests/article/view/276/255](http://estsjournal.org/index.php/ests/article/view/276/255). Accessed 4 Mar. 2022.

Taylor, Liam. "Millions of Ugandans denied vital services over digital ID cards." *reuters.com*, 8 June 2021, [www.reuters.com/article/us-uganda-tech-rights/millions-of-ugandans-denied-vital-services-over-digital-id-cards-idUSKCN2DK28W](http://www.reuters.com/article/us-uganda-tech-rights/millions-of-ugandans-denied-vital-services-over-digital-id-cards-idUSKCN2DK28W). Accessed 22 Apr. 2022.

Wang, Fennie, and Primavera Filippi. "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion."

*www.frontiersin.org*, 23 Jan. 2020,

*www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full*. Accessed 24 Apr. 2022.

White, Olivia, et al. "Digital identification: A key to inclusive growth." *Mckinsey.com*, 17 Aug.

2019, *www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-*

*identification-a-key-to-inclusive-growth*. Accessed 4 Mar. 2022.