Vanderbilt University Department of Economics Working Paper Series
Nashville, TN 37235-1819

Vanderbilt University Department of Economics Working Papers 19-00012

Blockchain as a Decentralized Mechanism for Financial Inclusion and Economic Mobility

John P. Conley
Vanderbilt University

Abstract

The World Bank's mission is to end extreme poverty and increase shared prosperity. A key driver for this is increasing financial and social inclusion, especially for poor and marginalized populations. Essential first steps to achieving these goals are providing providing official identities to the estimated one billion or more displaced and impoverished people who do not at present possess them, and bringing the even larger number of unbanked and under-banked out of the shadow economy and into the formal sector. This paper explores how blockchain fits in as a key enabling technology to achieve these goals while at the same time protecting the privacy and security of vulnerable populations. We also discuss the role blockchain could play in empowering people to obtain fair value for their skills and efforts, even in environments with weak or corrupt institutions.

This paper was commissioned by the Chief Economist office of the Equitable Growth, Finance and Institutions Practice as part of the World Bank Productivity Project. Our thanks to Bill Maloney, Stephanie So, and the attendees of World Bank Mini Boot Camp on Crypto, Information and ICT Economics for helpful discussions and comments. The author takes full responsibility for the opinions expressed as well as for any errors or omissions.
Citation: John P. Conley, (2019) "Blockchain as a Decentralized Mechanism for Financial Inclusion and Economic Mobility", *Vanderbilt University Department of Economics Working Papers*, VUECON-19-00012.
Contact: John P. Conley - j.p.conley@vanderbilt.edu.
Submitted: August 17, 2019. **Published:** August 17, 2019.
URL:http://www.accessecon.com/Pubs/VUECON/VUECON-19-00012.pdf

Blockchain as a Decentralized Mechanism for Financial Inclusion and Economic Mobility[1]

John P. Conley[2]
Vanderbilt University
August 2019

Version 1.0

Abstract

The World Bank's mission is to end extreme poverty and increase shared prosperity. A key driver for this is increasing financial and social inclusion, especially for poor and marginalized populations. Essential first steps to achieving these goals are providing providing official identities to the estimated one billion or more displaced and impoverished people who do not at present possess them, and bringing the even larger number of unbanked and under-banked out of the shadow economy and into the formal sector. This paper explores how blockchain fits in as a key enabling technology to achieve these goals while at the same time protecting the privacy and security of vulnerable populations. We also discuss the role blockchain could play in empowering people to obtain fair value for their skills and efforts, even in environments with weak or corrupt institutions.

1 This paper was commissioned by the Chief Economist office of the Equitable Growth, Finance and Institutions Practice as part of the World Bank Productivity Project. Our thanks to Bill Maloney, Stephanie So, and the attendees of World Bank Mini Boot Camp on Crypto, Information and ICT Economics for helpful discussions and comments. The author takes full responsibility for the opinions expressed as well as for any errors or omissions.

2 Professor of Economics, Vanderbilt University, j.p.conley@vanderbilt.edu, and Chief Economist for the Geeq Project, www.Geeq.io.

Table of Contents

1. Introduction

Blockchains are designed to create distributed, immutable, non-refutable, uncensorable, records of transactions and other data without the need for trust between parties. They come in many forms and are useful in a variety of contexts. There are also many situations in which blockchains provide no value at all.

This paper has two primary purposes. First, to explore and explain what blockchain is, how it works, and the advantages and disadvantages of the many different approaches. Second, to focus more specifically on a set of use cases that fit the mission of the World Bank and outline how blockchain can be an integral part of the solution.

We begin in Section Two by explaining the two key cryptographic technologies that are the foundation of blockchain: Hash functions and Public Private Key Encryption. Blockchain is one of several approaches to distributed data systems. In Section Three, we describe the major types of blockchains and other distributed data solutions, and in Section Four we compare them and describe their strengths and weaknesses.

The stated mission of the World Bank is to end extreme poverty by reducing the share of the global population that lives in extreme poverty to 3 percent by 2030 and to promote shared prosperity by increasing the incomes of the poorest 40 percent of people in every country.[3] A key driver for this is increasing financial and social inclusion, especially of poor and marginalized populations. Section Five discusses how blockchain can be used to provide identities to impoverished people while at the same time protecting their privacy and security. Section Six builds on this to show how blockchain can address the problems of the unbanked and the under-banked and bring more people out of the shadow economy and into the formal sector. Section Seven outlines several categories of use cases where blockchain can be used to empower people to get fair value for their skills and efforts even in environments with weak or corrupt institutions. Section Eight concludes.

2. Technical Background

Blockchains are based on two fundamental cryptographic techniques: hash functions and public private key (PPK) pairs. Since they are critical to understanding what blockchains do and why they are useful, let's begin with a brief explanation.

A "hash" of a digital file of any length is a 256 bit binary number that can be thought of as its "fingerprint". The important properties of hash functions are: (1) they are noninvertible – you cannot learn anything about the original file from its hash, (2) a given file always hashes in the same way – this is why it is sometimes referred to as fingerprint, and (3) similar files have completely different hashes – in fact, two files that differ by even a single bit will have hashes that appear to have been independently drawn from a uniform distribution of 256 bit binary numbers.

3 https://www.worldbank.org/en/who-we-are

Blockchains are designed to be "append only" through a cryptographic process of recursive hashing. The basic idea is that the hash of the previous block in included in the next block. This creates a hash tree that makes blockchains tamper evident. Suppose, for example, there is a single blockchain with a "height" of 5000 blocks and I wanted to change a transaction in block 4000 for some reason. This would mean that the hash of block 4000 would change and so the hash included in block 4001 would not match its original. I would therefore have to put the new block 4000 hash into block 4001. This would change the hash of block 4001, and so I would have hash it again, put this into block 4002, and continue this process all the way up to the current block, 5000. Thus, I could not insert new blocks or alter existing blocks without recreating the hash tree all the way up to the end of that chain.

Public private key encryption is a form of asymmetric key cryptography. Public private key pairs are mathematically entangled numbers with the following important properties: (1) anything that is encrypted with a public key can only be decrypted with the corresponding private key, (2) anything that is encrypted with a private key can only be decrypted with the corresponding public key, (3) public private key pairs are easy to generate, but the public key cannot be derived from the private key and the private key cannot be derived from the public key, and (4) at least until quantum computing arrives, it is computationally impractical to break PPK encryption.

PPK is the basis of digital signatures and the security of blockchain transactions. Signing and verifying signatures works as follows:

1. The signer produces a hash of the transaction request or other digital document.

2. The signer encrypts this hash with his *private key*.

3. The signer attaches this encrypted hash to the unencrypted (cleartext) document

4. To verify the signature, the reader decrypts the hash using the signer's *public* key. The decrypted hash could only have been encrypted in this exact way by the holder of the complementary private key (that is, the signer). Thus, the reader knows that this is the correct hash of the document as it was signed by the private key holder.

5. Finally, the reader produces his own hash of the cleartext document. If the hashes match, then he knows the cleartext document is exactly what was signed by the holder of the private key and has not been changed in any way.

For this to work, the reader must have access to the public key that can decrypt the encrypted hash and believe that this public key belongs to a specific person or entity. The reader also has to believe that the owner of the public key had control of the corresponding private key when the document was signed. If a hacker managed to get his hands on the private key, he could use it to sign documents just as easily as the true owner. Thus, if we think the private key has not been stolen or compromised and we are confident that we know the identity of real world person or entity that owns and controls the key, then we can be equally confident that that same person or entity signed the document verified by the matching hashes.

In the case of blockchain, individual accounts are identified by public keys. In principle, this means that the users who own the accounts are anonymous since there is nothing that directly ties any real world individual to the public key. To create a transaction request, the user writes something like "transfer 50 bitcoins from public key account XXX to public key account YYY", hashes the request and then encrypts it with the private key corresponding to XXX (that is, he signs the transaction request). A miner or validating node on the blockchain verifies this transaction by (1) seeing if public key account XXX exists and has at least enough tokens/coins to its credit to fund the transaction (2) using public key XXX to decrypt the hash of the transaction request (3) hashing the transaction request itself to make sure it matches the one just decrypted. If the hashes match, then the miner can be sure that someone who knows the private key corresponding to public key XXX created the transaction request. The strength of this approach is that signatures cannot be faked or forged. The weakness is that control of the account is completely tied to control of the private key and not to any real life individual.

3. Blockchain Protocols

There are five major approaches to Distributed Ledger Technology (DLT) and so let's begin with a brief overview.

Proof of Work (PoW) blockchains, such as Bitcoin and Ethereum, require that the "miners" who help maintain the ledger compete with one another to solve a difficult cryptographic puzzle for the right to propose the next block in the chain and receive mining rewards and transactions fees as a result. The only way solve the puzzle is through brute force guessing and checking. Thus, finding the solution is positive proof that the winner expended a great deal of computational work in the process.

The winning block proposer communicates his block to other miners using a gossip network. A gossip network only requires that each of the thousands of miners/nodes knows the IP address of a few other nodes, who in turn know the address of a few others, and so on. No central registry of nodes or addresses exists, and nodes can anonymously join the network by announcing their presence and connecting to a small number of nodes anywhere in the network. Newly mined blocks are transmitted from node to node until everyone in the gossip network is aware of them. Similarly, users can send transactions requests to any node they happen to know and count on them being gossiped to the rest of the network. Once a miner receives a newly mined block, it is supposed to verify that the transactions it contains are valid under the blockchain's protocol and then "commit" it to the version of the chain that it keeps. Each miner then stops working on the block it was trying to mine since it can no longer be appended to previous block once it commits the block it just received. All miners then choose a new set of transactions, put them into a new candidate block, and start to work on mining it instead. Note that this means that all the work unsuccessful miners put into the previous candidate block are wasted and the miners receive no reward for their efforts.

Proof of Authority (PoA) blockchains all have their roots in Castro and Liskov's 1999 work on Practical Byzantine Fault Tolerance (pBFT). Nodes are run by a small set of non-anonymous, registered, real world agents. Nodes take turns proposing new blocks of transactions which are commit-

ted to the chain if they receive the approval of the required majority. To the extent that there are incentives not to improperly alter the ledger, they come from a common desire of the voters to have an honest record and a fear that they will suffer reputational damage if they were to behave dishonestly. This is most often seen in permissioned blockchains such as Hyperledger Fabric and Ripple.

Proof of Stake (PoS) blockchains choose a random node to propose the next block on the basis of the proportion of the total coinbase held in each node's account on the chain. This proposal is circulated via a gossip network, in most cases, and if other nodes find that the block is correct under protocol, each node is supposed to commit it to its version of the blockchain. There are endless variations on this basic protocol including those employed by Tendermint, Honey Badger, Cosmos, Algorand, and NEO, for example. These variations are generally aimed at addressing different attack surfaces or improving efficiency of transactions throughput. Typically, if two thirds of the stake-weighted vote agrees that a proposed block is correct, it is committed to the chain and the ledger updated to reflect the new transactions. PoS protocols follow the same sort of recursive hashing strategy as PoW and PoA so that if any block is changed, all the blocks that follow must also be rewritten.

Distributed Acyclic Graphs (DAG) are a non-blockchain approach to DLT and come in permissionless and permissioned varieties. Iota and Hashgraph are examples of each, respectively. The basic idea is to create a topological ordering of transactions where new transactions (called vertices in the language of graph theory) are linked to existing transactions by hashing them together. The starting vertex (the existing transaction) is said to be linked to the ending vertex (the new transaction) by an "edge" which places the starting transaction before the ending transaction in the topological order. Users are only supposed to hash the new transaction with an existing transactions if they believe that it, and every transaction that it is backwards linked to it, are valid. Eventually, assuming that users choose which valid transactions to hash to in a sufficiently random way, a directed acyclic graph is created so that one can start at any end point of the graph and be able to find a path that links to any other transaction that is sufficiently old. Under certain assumptions, this creates an unambiguous ordering of these historical transactions. The key is that if we know this correct ordering, we can execute the transactions sequentially to find the current state of all accounts in the ledger. Double spends will not be included since one of the transactions will be deemed to have come earlier in the order which makes the second transaction that attempts to spend the tokens in the account a second time *per se* invalid.

Finally, conventional distributed databases such as those used by large companies and government agencies are the most common form of DLT in use. The major difference is that such databases are under the control of a single real world agent often referred to as a Trusted Data Intermediary (TDI). Unlike blockchain, there are no conflicts of interest between the nodes that keep and update the data. The major similarity to blockchain is that it is important to have a single view of the data (or ledger state) and to have this view available for use at each of the nodes for the users that it serves. If latency or network partitioning prevents data centers from coming to a common view, then conflicts such as double spending could arise. For example, suppose I withdraw money from my account at an ATM in Paris and my wife does the same thing at about the same time in Los Angeles. The US and European servers might show that the account has enough to cover each withdrawal, but not both. However, the bank would not realize we had overdrawn our account until

both servers recorded both transactions. If the bank tried to guard against this by not letting us complete the transaction until it knew all servers were synchronized, it might be forced to impose long waiting times before it dispensed money, much to the annoyance of its customers.

4. Pros and Cons of Different Approaches to DLT

Blockchain and other forms of DLT have various advantages and disadvantages that make them suitable for different sorts of applications. In this section, we outline and evaluate these differences.

4.1. Immutability

One of the chief claims of blockchain is that it creates an immutable record of transactions and other data. Different types of blockchains and distributed data systems approach this is various ways. None of them, however, create records that are truly immutable. It is more accurate to say that the records they contain are difficult to mutate once written, or that the records they create are tamper evident.

A good way to understand the immutability claim for PoW blockchains is to think of each block of transactions as a page in a paper ledger book. This ledger book has three special characteristics. First, each page is made up of thousand dollar bills (or gold foil, or must be handmade from rare materials at high cost). Second, all transactions are recorded in indelible ink. Pages cannot be altered or reused once transactions are written on them. Finally, a tiny copy of the previous page is written at the top of the next page in the ledger (actually, this is the "hash" discussed above).

Suppose that I wanted to change a transaction recorded on a page 50 back from the most recent one. First, I would have to create a new blank page of thousand dollar bills to write my new transition on. But since this would change the hash of page, I would also have create 49 additional new blank pages so that the recursive hash tree was consistent. This implies that the more deeply a transaction gets buried under new pages in the ledger, the more expensive it is to alter it without detection. Thus, the ledger is not immutable, it is simply very expensive to mutate. Eventually these costs become prohibitive. Unfortunately, this security guarantee comes at a high cost. Each page costs tens of thousands of dollars to create, mostly in the form of wasted electricity.

PoA blockchains rely on vetting nodes for honesty before they are admitted as validators and the hope is that nodes will stay honest to preserve their valuable reputations. For example, twenty banks might agree to write a shared ledger of the transfers they make between one another. It might seem unlikely that any bank would ever behave dishonestly, but dishonesty is sometimes in the eye of the beholder. For example, several of the banks might decide that they want to reverse transactions to one of their partners because they view it as having participated in a fraud. Courts or legislation might require that banks reverse certain transactions that involved illicit goods, that might be construed as money laundering or tax evasion, or that went to undesirable – in some

sense - groups or nations. In PoA blockchains, changing the ledger only requires getting the agreement of the majority of the nodes. There is no other cost or impediment. Thus, PoA ledger is not immutable and transactions can never really be considered to be finalized. The integrity of such ledgers requires trust in the honesty of the majority of nodes. This means that PoA can never be a real foundation for the kinds of trustless interaction between agents that blockchain is supposed to provide.

PoS Blockchain ledgers can also be mutated, rewritten, or forked if enough of the stakeholders agree. Like PoA, the ledger says whatever a qualified stake-weighted majority says it does. Often, a minority of stakeholders can halt block writing as well, although they may not be able to rewrite transactions history. The many variations of PoS follow different strategies to make such collusion difficult or expensive. Ultimately, if more than one third of the stake weighted voters manage to collude, such ledgers offer no security guarantee to users. How likely this is to happen is a matter of debate, but there are many attack surfaces in PoS protocols and no real proof that the incentives for good behavior are sufficient to prevent coalitions of self-interested nodes from manipulating the ledger.

The immutability guarantee of DAGs is founded on transactions being independently verified by many agents who create the graph of interlinked hashes. The idea is that altering the graph would require the complicity of an impractically large number of agents. Unfortunately, there are serious problems with this dependency. First, if more than a third of the hashes/edges are contributed by dishonest users, they can prevent or alter consensus conclusions about the validity and order of transactions. This makes DAGs vulnerable to Sybil attacks in which one agent pretends to be many Some platforms attempt to deter this by adding a limited a PoW element to the protocol, but this adds significant costs, wastes electricity, and in any event, mitigates rather than solves the problem. Second, permissioned DAGs with a fixed set of presumably honest nodes run into the same problems as PoA. That is, the DAG they produce can be rolled back or rewritten if the majority of nodes choose to, or are forced to by legislative, legal, or criminal actors. Third, permissionless DAG implementations such as Iota end up having a privileged set of trusted or highly reputable nodes who ultimately decide on the validity of graph edges, and therefore, the state of the ledger. This places a small set of actors in a position to alter or choose the correct state of the ledger and so does not provide a strong immutability guarantee.

Distributed private databases, of course, are never immutable by construction. Whatever organization controls the servers can rewrite or erase any data it pleases. To the extent that it is difficult to do so, it is because users would lose trust in a bank or brokerage house if it became known that it altered its data in an arbitrary way. This is one of the reasons that paper statements and records are traditionally provided to clients. To the extent these are difficult to forge, they provide record of what the database said at a specific point in time (sometimes referred to as a “checkpoint” in blockchain) and so can be used to prove that alterations took place that were inconsistent or unjustified.

4.2. Distributed

A second claim of blockchain is that it is distributed and decentralized. There are two primary reasons that this is desirable. First, if a blockchain, ledger, or any type of data, is stored redundantly on a widely distributed set of servers, it becomes more difficult to censor or destroy. This is especially true if it is kept by anonymous nodes in different jurisdictions. DDoS (Distributed Denial of Service) attacks against thousands of servers at once are expensive and may be impractical. Forcing all of these copies offline through legal or illegal means is similarly difficult. Second, the more independent nodes keeping and validating the blockchain there are, the more difficult it is to coordinate them to dishonestly validate or alter the ledger. It should be added that while this is intuitive, there are no formal proofs linking the number of nodes to any metric of ledger security.

Bitcoin and Ethereum both had on the order of 10,000 full nodes on their networks as of May 2019. Other PoW blockchains have much smaller networks. It would surely be difficult to censor or destroy the information in these blockchains, but coordinating nodes for malicious purposes may not be so difficult. In the case of Bitcoin, nodes form mining pools that coordinate activities to maximize profits. At the present time, three such pools working together would be capable of mounting a 51% attack on Bitcoin, so it is not clear that having large numbers of nodes automatically leads either to decentralization or wide distribution of validation power.

PoA is by construction relatively centralized. Typically, networks consist of 10 to 25 nodes and if the blockchain they keep is permissioned, only those nodes have copies. PoS approaches give voting power to agents in proportion to how many tokens they have staked, rented, or had delegated to them. This means that even if tokens are widely distributed, it may be that only a relatively small number of agents are keeping copies of the blockchain and actively participating in block proposing and transaction validation.

As we say above, existing DAGs either have a small set of permissioned validators maintaining the graph, or have privileged agents with disproportionate power over transaction finality. Having a truly open DAG with a broad set of anonymous agents contributing transactions and verifications is problematic for two reasons. First, all such agents would have to maintain copies of all the data in the graph in order to verify transaction hash trees. This is resource intensive and not even feasible for IoT devices with limited bandwidth, processing power, and storage capacity.[4] Second, open DAGs are extremely vulnerable to Sybil attacks since power can be concentrated in this way by a malicious agent.

Finally, private decentralized databases provide redundancy, but all the servers are coordinated by design. Thus, decentralization does not contribute to the trustworthiness of the data beyond the trustworthiness of the TDI.

4 See Attis Elsts' 2018 Medium piece "Lessons learned from evaluating IOTA on Internet of Things devices"

4.3. Trustlessness

PoA, permissioned and permissionless DAGs, and private databases all require the users to trust the honestly of the validators. PoW and PoS, on the other hand, attempt to set up protocols and incentives so that users have a degree of confidence that self-interest or the difficulty of getting away with dishonesty will protect the integrity of the ledger. If at least 51% to 67% of nodes are moved by these incentives, then users can count on the ledgers' correctness.[5]

4.4. Scalability

Bitcoin can process about seven transactions per second (TPS), and Ethereum approximately fifteen. Lightning networks are supposed to handle larger numbers of transactions through side channels, but costs, security, *de facto* centralization, and the lack of expensive-to-establish escrow connections between counterparties make it unlikely that lightning networks will allow PoW blockchains to scale significantly.[6] Some of the newer PoS and PoA chains can manage several hundred to a few thousand TPS, and in principle DAGs can scale infinitely.

Ultimately, the binding constraints on scale are the bandwidth and the storage needed to process large numbers of transactions. Public blockchains (including DAGs) that use anonymous nodes are bound by the resources available to the nodes in their network. This could be overcome through a truly federated structure of independent, interoperable blockchains, but as long as there is a single chain or a master chain to which all others must ultimately report, it will not be possible to overcome these limitations.

Permissioned approaches, including private databases, have a much better ability to scale. This is because nodes and servers can be set up on high capacity cloud platforms that can provide as much bandwidth, computation, and storage as needed. The Visa network has a capacity of tens of thousands of TPS, for example. Of course, this comes at the cost of centralization and the need for users to trust in the honesty of the nodes.

4.5. Cost

PoW protocols are fundamentally expensive. They use significant computational resources by design as the basis of their security models. Transactions costs to users on these networks vary, but

5 There are many attacks that do not require this degree of dishonesty(see Eyal and Sirer 2014 and Houy 2014, for example). In any event majority attacks are, in fact, a significant problem. Bonneau (2018) estimates that it would cost $1M per hour to rent enough capacity on EC2 to mount a 51% attack on Ethereum, and $1,5B to purchase enough capacity to mount such an attack on Bitcoin. Given that Bitcoin's token cap is approximately $140B at this writing, $1.5B seems like a relative bargain to gain full control. Other authors have placed the cost of a rental attack on smaller PoW blockchains such as EthereumClassic, Monero, and Dash at less than $10k per hour (see https://www.crypto51.app/). A number of such attacks have actually occurred on such chains.

6 See, for example, Jamie Redman's 2018 Bitcoin.com piece "Looking Beyond the Lightning Network Hype: Every Day Users Experience Issues", or Jonald Fyookball 2017 Medium piece "Mathematical Proof That the Lightning Network Cannot Be a Decentralized Bitcoin Scaling Solution".

they are typically on the the scale of $.10 to $5.00 depending on transactions demand. The fundamental costs of PoA and private databases can be very low. This is because these networks are typically small and costs per transactions amount to resource cost of processing and storage on ten or twenty servers. What users get charged, however, is another matter. Visa charges 2%-3% plus $.25 per transaction. Part of this is because of the monopoly power that they have, but another reason is that they are providing valuable and costly services in addition to simply maintaining the ledger. This is in the form of insuring users and merchants against fraud. On blockchain, if someone has your private key and uses it to take coins from your account, you are out of luck. Visa, on the other hand, makes an effort to minimize fraud, but then eats the cost of any that manages to get through.

PoS solutions charge whatever fees they wish and sometimes have block writing rewards similar to PoW. Costs are reduced when the approach limits block writing, validation, and chain storage to a small set of wealthy stakeholders. If only 100 nodes communicate and store the chain, the costs are lower than if 10,000 do so (as with Ethereum and Bitcoin). On the other hand, some approaches such as Algorand require that all users be ready to participate in the validation process and this might mean that hundreds of thousands of nodes must communicate and keep copies of the chain.

DAGs are similar in this respect. Permissioned DAGS with small pre-determined validators sets can process transactions cheaply. Open approaches require huge amounts of communication and storage by many nodes/users and sometimes include additional PoW costs to reduce Sybiling.

4.6. Evaluation

There is no perfect solution. On one extreme, there are TDIs and private databases. These are relatively inexpensive, can scale, but require a high degree of trust that the TDI will make the data continuously available in unadulterated form. In the middle, there are permissioned PoA blockchains and DAGs. These are also relatively inexpensive and can scale to varying degrees. Users are not left at the mercy of single TDI but must trust that a sufficiently large majority of a small, nonanonymous group will behave honestly. On the other extreme are permissionless, public PoS and PoW solutions. PoS is more costly and less scalable than PoA or private databases, and PoW even worse in those dimensions. On the other hand, such protocols do not require trust in the honesty of the validators, instead depending on the incentives the protocols provide for honest behavior. When validators are anonymous, numerous, and widely distributed, state actors, courts, and criminals should find it difficult to force nodes to behave in ways outside of protocol or to censor the blockchains and ledgers that they keep.

5. Identity, Privacy, and Blockchain

Identity is at the core of what it means to be human. Self identity, legal identity, social identity, and even anonymous personae we take on for various purposes, are all elements that define who and what we are as individuals. Certain aspects of identity confer rights and responsibilities, or generate social expectations and obligations. There are some elements of our identity that we would

like to broadcast, others that we would like to keep private or share in a limited way, and still others that we would like to deny.

Individuals without identities are at a substantial social and economic disadvantage. In particular identification is required to do such things as:

- Vote in elections
- Get access to health care
- Get access to public education
- Get access to social benefits including food vouchers, pensions, or cash transfers
- Participate in the financial system or the formal economy
- Be allowed to travel internally or cross national boarders
- Be able to exercise legal rights, such as filing petitions in courts, owning property, or receiving an inheritance

The United Nations High Commissioner for Refugees (UNHCR) estimates that there may be more than 1.1 billion people, without any form of officially recognized identification[7] There are a number of consortia that have come together to address this issue, most notably, the Digital Identity Foundation, and ID2020. In addition, there are many blockchain startups at work on different aspects of the identity problem. See Dunphy, Fabien, and Petitcolas (2108) for a useful analysis.

The right to have an official identity is also intertwined with issues of individual rights to privacy and freedom.[8] India's Aadhaar biometric ID system includes more than 1.3 billion people. While Aadhaar is useful in keeping track of the distribution of social benefits and fighting financial fraud, it has enormous potential for other less desirable forms of social control. For example, the government could decide that women should not have bank accounts or hold certain kinds of jobs, or that minorities should be forced to submit to onerous social monitoring or have their rights to travel internally or internationally revoked. China's increasing use of biometric surveillance and its proposed "social credit system" will allow it to identify and punish protesters, people with dissident views, religious minorities, and whistle-blowers, as well as control social behavior, public debate, access to resources such as credit, and scientific inquiry.

In this section, we review the basic technologies involved in establishing identity, their major costs and benefits, and how blockchain may fit in as part of a solution.

5.1. Identification Technologies

There are three fundamental ways that people establish their identities:

7 Filippo Grandi, United Nations High Commissioner for Refugees, (2017) "Opening statement at the 68th session of the Executive Committee of the High Commissioner's Programme".

8 Data security is a high priority for the UNHCR and related agencies. For example, the Joint Inspection of the Biometrics Identification System for Food Distribution in Kenya (UNHCR and WFP) notes: Network intrusion or remote hacking of UNHCR's system could compromise sensitive information stored in the database. This sensitive information could be accessed remotely by unauthorized persons, endangering UNHCR's mandate to protect the confidentiality of refugee data.

Something you own: for example, passports, driver's licenses, smart cards, and so on. This is a fairly weak approach from a security standpoint. Documents can be faked, stolen or lost.

Something you know: for example, passwords, social security numbers, private encryption keys, collections of personal information (address + birthday + where you went to elementary school), and so on. This is also a weak approach to establishing identity. People can forget, accidentally reveal or share, or be forced or tricked into divulging such information.

Something you are: for example, fingerprints, iris scans, facial or hand geometry, or even DNA. Biometrics such as these cannot be forgotten and are difficult to lose. On the other hand, they can sometimes be stolen, directly or indirectly, and have relatively high rates of false positives and false negatives.

Below, we will refer to passports, passwords, fingerprints, etc. as being different types of "identity tokens". These identity tokens, in turn, connect an "identity owner" to "data items" and/or "permissions". For example, a fingerprint or social security number are identity tokens that connect individual identity owners to specific data items such as a criminal or employment record. Similarly, passports or passwords are identity tokens that give an identity owner permission to cross a border or access funds in a bank account.

Things you own or know can be changed if they are lost or compromised, although sometimes it is costly or difficult. At least in principle, a password can be changed and driver's license can be replaced. This is often limited by a bootstrapping issue. For example, if a refugee arrives in a resettlement camp with no documents and a limited knowledge of the language or understanding of technology, there is very little one can do to verify any claim he might make to being a specific individual. In such cases, governments may be reluctant to issue new passports and banks may not be easily persuaded to issue new passwords to such people. People who wish to hide their identity, perhaps because of a fear of persecution or a desire to escape responsibility for crimes, can also destroy their documents or claim no knowledge of the identity they are trying to escape.

On the other hand, it is possible to force a person to give a fingerprint or submit to an iris scan. Facial geometry and even a person's gait can be observed from a significant distance and cross checked against databases. If a person's fingerprint scan is connected to the record of a person wanted for a crime, perhaps through a clerical error, hacking, or by a hostile government, then he is at risk with little way to clear his name.

5.2. Identity and Trusted Data Intermediaries

Things you own are usually physical representations from trusted parties that attest to something about the owner. Clearly, a birth certificate, driver's license, or a passport is an attestation that a government body has done some kind of due diligence and is willing to state that you are a specific individual who has certain attributes. Historically, a picture or signature on an identity document is used to verify that the human who offers it is the same one that the document certifies can drive, has a certain nationality, lives at a certain address, has certain educational or professional certifications, and so on. The physical documents allow us to make these claims without being online, but it is almost always the case that such documents refer to a record in some official database.

Things you know and things you are are usually even more directly connected to digital records, and in turn, these records are usually under the control of a trusted body that attests to an identity or provides access to goods or services on the basis of the identity. An online bank account, a social media account, a phone or computer accessed via a finger print, and so on, are examples of agreements that the human in question has rights linked to the identity token.

The point here is that people have identity elements scattered over a wide range of government, commercial, and other actors, and these actors are key in that they attest to something on the basis of an identity token of some kind. Thus, trust in the attestors is the foundation for many of the most important types of identity. This is problematic because it means identity can never be truly free of centralized elements of control, nor fully under the control or authority of the individual in question. More specifically:

1. No individual can prevent identity data (financial, medical, criminal, educational, or any other kind of record) from being disclosed without his permission. Privacy can only come from legal restrictions placed on the attestor or the attestor's good behavior.

2. No individual can ever prevent an attestor from changing, deleting, or denying access to identity data.

3. Like all data, once identity information is seen, it can never be unseen. For example, if a doctor is allowed access to your medical record, there is no way to prevent him from keeping a copy and then distributing it to anyone he pleases. Again, we must rely on enforcement of privacy laws or the doctor's good behavior.

5.3. Identity, Privacy, and Blockchain

Given all of these concerns, is it possible to protect individuals' privacy and the integrity of their identity records? Is it possible to prevent abuses? To what extent can we give individuals sovereignty over their identities? To what extent should we? Finally, can blockchain play any significant role?

Let's start with the foundational unit of identity data: an attestation to a fact, or a granting or access or rights connected to an identity token. Think of a passport as an example.

An individual need not show his passport on demand. In general, however, if he wishes to open a bank account, become employed, cross a border, etc. it may be a necessary condition. The passport contains much more information than is required in many cases. For example, a bank does not need to know where you have traveled, and may not even need to know your citizenship or age. It does need to complete Know Your Customer (KYC) and Anti-Money Laundering (AML) checks by law, however. Thus, if the bank was confident that the human in front of it had a specific name, legal residence, and was not a criminal or terrorist, they might be happy to open an account. Similarly, an employer might need to know that an applicant has a high school or college degree and be able to file a tax withholding form with the government; however, it may not need to know the date or even the place of graduation or the applicant's SSN.

In effect, we are trying to create a firewall that allows people to provide enough information to interact and do business without giving up too much privacy and freedom. How can we do this?

The first line of defense is the TDI's themselves. A passport authority, for example could allow a person to register an identity token of some kind. This might be a password, an RFID chip on a card, or an iris scan. The individual could then use it to authenticate himself to the TDI in the presence of the banker and authorize the passport authority to certify that he met the bank's regulatory KYC/AML requirments as well as provide whatever actual data (such as a name) the bank needed. An individual might use his identity token to give a doctor limited access to his medical record. For example, a general practitioner may not need to know about a psychiatric intervention ten years ago or the medicines a patient was taking then. A radiologist may not need to know about a patient's time in rehab or his dental records. One might even create a system where a doctor would add his intention to prescribe a certain medication to a patient's medical record and then be informed of any current prescriptions only in the event of a potential drug interaction. One might also allow emergency workarounds. If a patient was in a car crash, for example, an EMT or emergency room doctor might use his own identity token to authenticate himself to the TDI, attest to the nature of the emergency, and be given whatever broader access was required. Such a system could be abused, but the holder of the identity token making any information request could be held accountable.

Doing this would require a new sovereign identity infrastructure and regulatory environment. For example, what a bank, a doctor, an admissions committee, or an employer needed to know would have to be codified in law and then implemented in a data management system. As we discussed above, identity tokens based on what you have or know can be stolen, compromised or lost, but as soon as this becomes known, they can also be replaced and the old token invalidated. Tokens based on what you are, on the other hand, can't be replaced and may allow individuals to be forced to identify themselves or authorize access to information or privileges against their will, but are more difficult to falsify in controlled environments such a doctor's office or a bank.

Finally, what role does blockchain play here? The major weak point in this schema are the TDI's. If they are not trustworthy, what can be done?

1. Blockchain can do little to prevent a TDI from releasing information without a person's consent. TDIs may be hacked, have dishonest employees or agents, or be compelled to release information by governments. Blockchain might be used to make this more difficult in the following ways:

    a. A TDI might agree to keep only encrypted copies of certain data and get rid of any cleartext copies. For example if a patent, copyright, notary public office placed an encrypted record in a blockchain with the only key in the possession of the record owner, it would allow the owner to establish priority without directly having to post it in public. By producing a cleartext copy of a preliminary patent application and showing that a signed hash exists in the patent office blockchain in a block before the one containing a signed hash of a competing patent claim, then the sequence of filing could be established as it is needed. This depends on trusting the TDI to destroy any cleartext copies, however.

b. A TDI might set up an automatic system that placed a record of any request for release of data into a blockchain. That is, suppose someone requested a credit check on a data owner and had the right credentials to get the request granted. If the only way to get this data resulted in the fact of the request or release of data being recorded in a public blockchain, then the data owner would know. If the requester used stolen credentials, the owners could cancel them so no more unauthorized access would be allowed. He would also know the identity of the agent (the bank, perhaps) that requested the data since their identity token would be part of the record as well. Finally, if the credentials were incorrect or the request did not fit the release requirements, the data owner could hold the TDI responsible and could prove it. While this would not help if the TDI was compromised or colluded in the unauthorized release, it would make it much for difficult for others to exploit and use the data when held by an honest and secure TDI.

2. Attestors often have a genuine need to change the data regarding an identity holder. For example, a driver's license could be suspended or revoked, a car or house could be sold to another person, medical records are updated every time an individual goes to a doctor, and a person's credit history, bank balance, and unused credit limit change all the time. On the other hand, dishonest TDI's may change or delete records improperly. For example, passports or driver's licensees might be revoked to prevent people from voting and deeds might be transferred to a political crony of the regime without a proper sale being executed. However, if the state of a record and any transactions that could legally change the record's state are recorded in a public blockchain, such behavior could be proved. It would also not be possible to deny that records or transaction existed by simply denying access. The TDI might still be powerful enough not to care that it can be shown to have acted illegally, however, it could not support the claim that it was acting properly. The TDI could also stop recording any data in the blockchain, but then it is signaling that it has no interest in transparency or external validation. Blockchain cannot force any agent to do anything in the real world, however, it can force an agent to reconcile his actions with an honest record of what took place or admit that it was or is acting dishonestly.

3. The so called "analog hole" cannot be fixed by blockchain or any data technology. Once a thing is seen, it can never be provably unseen. A screen can be captured, a phone can record a live video or audio stream, or a person can simply remember what he saw. What blockchain can do is facilitate the transfer of just enough information to allow people to interact without opening the analog hole too widely.

   a. We will say more about the importance of financial privacy below, but this is the most obvious and important way that blockchain can contribute to sovereign identity. What we purchase, what we consume, where we travel, what we own, how much money we have, how much we are paid, and so on, are some of the most important elements of our identities. They are tied to our tastes, our abilities, our responsibilities, and even our weaknesses. If we use checks, debit cards, ACH transfers, or credit cards, a transaction record is created that ties it to our identity. In the US, there are two credit card and two ACH providers that handle more than 95% of these types of transactions. Thus, a complete financial picture of any individual is very easy to to construct. But what business is it of Visa or the Federal Reserve Bank if I donate to Green Peace, buy halal food, seem to buy more liquor than is good for me, travel

to China to see relatives, like to read books on cryptography, or drive a Ford F-150? If instead people were allowed to transact securely and anonymously with cryptocurrencies, they could retain their privacy and sovereignty over this most important element of their identities. In the past, cash served this function, but cash is analog. Cryptocurrencies are the bulwark against the surveillance state in the digital future.

b. The same argument extends to many other aspects of our identities. Should I be allowed to post my art, my music, my investigative journalism, or my opinions, without revealing my true identity? Should I be able to offer my help, sell my services, or collaborate on projects anonymously? As it stands, there are several barriers. First, there is the financial side, discussed above. Second, communication and social media platforms are very centralized (and largely American). This allows censorship and requires that users deanonymize themselves. Blockchain, on the other hand, allows the creation of sustainable, decentralized platforms for all kinds of purposes that can set their own standards and are difficult for central authorities to censor. Third, the only real alternative to identifying yourself right now is to be completely anonymous. It is difficult to transport anonymous digital identities across platforms or create an integrated pseudo-identity. Blockchain allows people to create their own identity tokens anonymously and without a central authority. For example, I could register a name or avatar such as “cryptosquid” by attaching it to a pubic key in an sovereign identity blockchain. I could then sign all of my posting and activities on all the platforms I used, and this would allow others to confirm that the same real human using the pseudonym “cryptosquid” was responsible.

5.4. Evaluation

People need to have identities if they are to do business, work together, and create value. Governments, corporations, and other TDI’s must be part of this identity structure since their attestations are the foundation of some of the most important elements of a person's identity. Unfortunately, centralization and concentration in the financial, communications, and technology sectors give a small number of actors disproportionate power. Big data, machine learning, inexpensive cameras and other sensors, and more recent emerging technologies give governments an unprecedented ability to tie a person’s actions to his identity, and to store, process, and interpret them.

Blockchain is a tool that can be used to protect people from this future in several ways. The most important is allowing people to continue to make financial transactions with one another without requiring them to reveal everything to the government or corporations. In addition, blockchain can be used to control the flow and use of private information to protect peoples’ privacy while still allowing the information to be useful. Finally, blockchain can be used to create decentralized platforms where people can speak and interact though avatars without fear of reprisal or oppression.

6. Financial Inclusion and Fintech

One of the primary application spaces for blockchain is Fintech. Bitcoin was launched in 2009 as an experimental payment mechanism that was self-supporting and completely independent of any government or institution. Ethereum was launched in 2013 and built on the idea by adding smart contracts that allowed agents to make binding commitments without a TDI. The third largest cryptocurrency powers the Ripple network which is an interbank settlement system meant to compete with SWIFT. Most of the other top twenty blockchain platforms support "alt-coins" which compete with Bitcoin and Ethereum. Many other startups exist to provide brokerage, payments, international transfers, custody solutions for securities, derivatives of various kinds, loans, and a wide array of other financial services. There are even a number of blockchain startups whose purpose is to help other blockchain startups get funding.

In this section we focus on two applications that connect directly to the mission of the World Bank: financial inclusion, and resilient financial systems.

6.1. The Problem of the Unbanked

It is estimated that about 35% of the world's population did not have bank accounts of any kind as of 2017. Citizens of low income countries, the poor in general, and women in particular are disproportionately affected.[9] Refugees and the displaced can lose contact with their banks or have accounts locked or confiscated. In most countries, banks are not allowed to open accounts without doing KYC and AML checks and this automatically excludes the billion or more people who have no official IDs.

Being unbanked leads to financial exclusion and makes it difficult for people to save money, get credit, seek jobs, start their own business, invest in education or health, manage risk, receive remittances or money transfers, keep their wealth safe, and in general, forces them into the shadow economy. Not surprisingly, the World Bank takes the position that:[10] "Financial inclusion is a key enabler to reducing poverty and boosting prosperity."

This unfortunate situation is not the fault of banks. Setting up a bank is costly. There are any number of regulatory and compliance measures that must be satisfied and this requires lawyers, accountants, payment of fees, taxes, and sometimes bribes. Physical infrastructure is also required including buildings, employees, and IT systems. On-boarding a new account holder at the least requires KYC and AML and this alone costs in the range of $40 per customer. Of course these costs must be passed on to the customer. Even in the US, accounts with low balances may pay monthly fees of $10 or more plus fees for each transaction. Holding $1000 for a year in an account could easily cost $100 or more. The fixed cost of setting up accounts may simply not justify the benefits to either the bank or the customer when balances are too small.

9 Gender gaps for bank accounts in developing countries average 9% and can range up to 30%. In low income economies more generally, less than half of the population are typically banked (see Demirguc-Kunt, *et al*. 2017).

10 The the world banks also sees financial inclusions as an enabler of seven of its seventeen sustainable development goals (see http://www.worldbank.org/en/topic/financialinclusion/overview).

This leaves the poorest and most vulnerable with a limited set of expensive and unattractive options. For example, the use of mobile phones to make money transfers is a growing business (especially in East Africa). However, costs are 1-2% on a $100 transaction and can range up to 10% on smaller transactions. Such services are not designed to make transfers over borders or in different currencies, and require the user to place his faith in the phone company as a TDI. Receiving remittances from overseas can be quite expensive for the unbanked. Transaction fees ranged from 4% to 8% on average in 2018, and significant additional charges are added for foreign exchange services, using credit cards and debit cards to fund transfers, and dispensing cash to the receiver. As a result, the unbanked often simply choose to transact only in cash. This puts them at risk of being robbed, which can be especially punitive if they attempt to build savings or accumulate enough cash to establish an identity.

6.2. Public Blockchain as a Solution

People who can afford it choose to have bank accounts because banks can generally be trusted to keep money safe. Banks make it easy to make payments between individuals, merchants, and businesses, at a distance, even overseas. Cash carries security risks, and in an increasingly globalized and digital world, the uses of cash are becoming more limited.

The unbanked need an alternative to the formal banking sector and cash. Public, permissionless blockchain is a technology that has the potential to provide it. The most obvious advantage of blockchain and cryptocurrencies over banks and fiat accounts is cost. Although many existing implementations of blockchain have significant transactions fees, new approaches are fundamentally cheaper. This is for a number of reasons:

- Blockchains have no brick and mortar infrastructure.
- Blockchains are decentralized. They have no employees and do not have to pay auditors or lawyers to assure regulatory compliance.
- It is easy to use blockchain without KYC/AML. Anyone can set up an account on the Bitcoin or Ethereum ledger, for example, and then any other user can transfer tokens into the account. By design, such transactions are anonymous.
- The fundamental cost of blockchain transactions is the value of the resources required by nodes to run the network.

Blockchains are ideally suited for small transactions and small accounts. Indeed, micropayments of less than a penny are one of the most important blockchain use cases since it would enable all kinds of Machine to Machine and Peer to Peer markets that do not currently exist.

Blockchains are also very secure, when correctly implemented, and do not depend on the TDIs. Such applications would be very well-suited for environments where local authorities may be corrupt or where institutions are weak. On the blockchain, no one knows you're a dog.[11] This means

11 Repurposing this famous cartoon: https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog.

that women, religious or ethnic minorities, and other marginalized people can transact freely and anonymously without needing the permission or assistance of any authority. Blockchain by its nature is transnational. Cryptocurrencies move freely across borders and can be accessed by the displaced anywhere the internet is available.

6.3. Concerns and Limitations

Public blockchain has the potential to greatly expand financial inclusion safely, cheaply and securely, for the unbanked, the under-banked, and for those who may be endangered or extorted if they tried to access existing financial services. There are, however, a number of concerns that need to be addressed and limitations that must be acknowledged. In some cases, advances in blockchain and other technologies will make these less important in the future, and in others, fundamental policy choices will need to be made.

To begin with, public blockchains are designed to allow anonymous transaction of cryptocurrencies. In particular, there is no way to force account holders to undergo KYC/AML in most cases. This gives blockchain three absolutely key advantages over banks. We discussed these above, but to recap: low costs make low balance account and small transactions feasible, an ability to provide financial services to those without formal identification, and an ability to provide protection through anonymity to people and populations that might otherwise be at risk of exploitation or violence. The obvious concern is that forgoing KYC/AML and allowing people to transact anonymously will provide new avenues for money laundering and tax evasion. This might seem to be a deal breaker that makes cryptocurrencies completely unacceptable to any government or banking institution. We would argue that these concerns are over-stated.

First, while it is structurally impossible to impose KYC/AML requirement on users within the blockchain environment itself, converting tokens into fiat currency and then moving them on or off chain usually requires making contact with the conventional banking system. Typically, a user would wire or make an ACH transfer into an account to set up an account on a cryptocurrency exchange and then use the fiat balance to purchase tokens. To reverse the process, a user would sell tokens to someone else on the exchange for fiat and then have the proceeds wired back into his bank account. Thus, KYC/AML, tax reporting, and other regulatory requirements must be met when token value is moved off chain and into the real world.

Second, the gray economy is already enormous. Tax evasion, official corruption, weak institutions, embezzlement, financial crimes, cash transactions, barter, and a wide variety of money laundering techniques support a huge gray or underground economy worldwide. European countries as a group had gray economies that averaged 16.6% of official GDP in 2017. In 2015, 70 out 159 countries worldwide had underground economies that were over 30% of official GDP with Zimbabwe topping the list at 67% (see Medina and Schneider 2018). Clearly, KYC/AML and the other expensive efforts of the international banking system have had limited success at best in moving the underground economy into the open, and have been least successful where people are the poorest.

This failure cannot be blamed on cryptocurrencies. Bitcoin and Ethereum already provide a perfectly adequate avenue for any sort of money laundering or tax evasion that might be contemplated.

To the extent that cryptocurrencies provide a cheaper or more secure way to launder money or make illegal transactions, they are already being exploited. It is worth noting that the total market cap of all publicly traded cryptocurrencies was about $250B as of this writing, while in 2018 Total World Product (GWP) was about $85T and total money supply including demand deposits worldwide was about $40T. In other words, cryptocurrency amounted to .6% all money and .3% of GWP. Given this, it is hard to believe that outlawing cryptocurrencies would have a significant impact on the underground economy. Similarly, it is hard to believe that creating new cryptocurrencies would create many new opportunities for underground activities above those already provided by existing cryptocurrencies. The fact remains that people who are paid by legally registered companies or who transact with legally registered merchants will still have their transactions reported and taxed. This is true regardless of whether credit cards, checks, cash, or cryptocurrency facilitate transactions. More importantly, to the extent that wider user of cryptocurrencies leads to greater financial inclusion and economic prosperity, the result is likely to be a reduction is the size of the shadow economy.

A different set of concerns relate to how well-suited cryptocurrencies are to taking on this role.

First, cryptocurrencies are notoriously volatile. On the positive side, Bitcoin increased in value by a factor of 10 between January 2017 and May 2019 and by a factor of 2 between January 2019 and May 2019. On the negative side, the path that Bitcoin followed over this time was to increase from a price of about $1000 to $20,000, fall to $6,000, rise to $12,000, fall again to $3,500, and then rise again to $8,000. This is quite a wild ride, and most of the larger cryptocurrencies mirrored it. This might look fairly bad compared to the US Dollar or the Euro, but on the other hand, more than 20 countries had inflation rates of over 10% in 2017. Many others have restrictive exchange rate and money transfer rules. Moreover, the volatility Bitcoin and other tokens is largely driven by thin trading margins and an over-representation of speculative traders. If a cryptocurrency was set up with a sensible algorithmic monetary policy and had significant transactional, as opposed to speculative, usage, its value is likely to be at least as stable as any national fiat currency.[12]

Second, why would any company or merchant agree to payments in tokens, and if they don't how can the tokens be of any use in helping the unbanked? In fact, approximately 6500 merchants accepted crypto-payments in 2018 including Microsoft, Newegg, Overstock.com, Namecheap.com, and Shopify.com,[13] The reason is that it turns out that cryptocurrencies provide a largely risk-free way to accept payments. The nature of blockchain prevents fraud in the sense of bad checks or reversed charges. Finality is also relatively quick, an hour or so at worst. Perhaps more critically, a company can simply convert any tokens it accepts into fiat on a daily, or even more frequent, basis. Thus, the company is only subject to volatility risk over a short window. Finally, especially when dealing with larger volumes, transactions and other fees to sell crypto and move the proceeds as fiat into the real banking sector can be minimized, and certainly would be smaller than the 2% or more charged by credit cards.

12 See Conley (2018a) and Conley (2018b) for a discussion of cryptocurrency monetary policies and approaches to stable and stabilized tokens.

13 https://www.virtualcoinsquad.com/

Third, is it realistic to think that the unbanked would ever be able to use cryptocurrencies in day to day transactions? Recall, that converting cryptotokens into fiat often requires the involvement of a bank. Fortunately, there are many other ways that the unbanked can access and use cryptocurrencies. For example, an employer who has a bank account could transfer tokens to his employees' blockchain accounts. If local merchants were willing to accept tokens for goods, there is no reason for the employee ever to make contact with the formal banking sector (and as we argued above, merchants would have no particular reason to avoid doing so if their customers demanded it). Employees could simply keep their tokens on the ledger and never convert them into fiat. If a token account holder really needed fiat for some reason, tokens could be bought and sold, person-to-person, for cash. For example, if a user had 100 tokens worth $250 at current prices, he could transfer them to the account of a broker in exchange for a cash-in-hand payment (or buy tokens in the same way). Such brokers might charge fees, of course, but token transfers on a well-designed blockchains are extremely secure, easy to verify, and cost very little in transactions fees. Competition between such brokers should keep their fees relatively low.

Finally, many of the unbanked may not be very technologically sophisticated and so using cryptocurrencies would have to be extremely easy. Here, some barriers remain. Fundamentally, access to blockchain accounts is controlled by private keys that no human could possibly remember. Thus, many users keep digital files that list their keys in some secure or encrypted place. This works, but is less than optimal, even for people with ready access to technology. A more practical solution is to have keys stored in online digital wallets and connect them to owner via some other identity token (a password, fingerprint, cellphone, or some combination of these). Ultimately, accessing an account on a blockchain should not be more difficult than using a mobile phone for payments, but more work is needed before this is a reality.

6.4. Distributed Data for Disasters and Emergencies

Disasters of all kinds can lead to a temporary inability to access, or even the complete destruction of financial and other data. Island countries such as Haiti and Jamaica experience devastating hurricanes that can simply obliterate server farms. Even if they survive, getting servers back up and connected requires rebuilding power and communications networks. Many nations also have data sovereignty laws that prevent certain kinds of sensitive information from being stored outside of the country. This may lead to a dangerous centralization of data in the capital city or some other place. Public records kept by local governments and all sorts of data kept by small and medium sized businesses may also be kept only locally.

The obvious solution is to keep distributed copies of such data. This is already quite easy to do using any number of cloud service providers at fairly modest cost. In fact, it is almost always much cheaper to do so than to maintain one's own servers. Data sovereignty and privacy need not be an issue. Duplicate records could simply be encrypted before they are sent out for replicated cloud storage while the working unencrypted copy is maintained locally.

Clearly, the low hanging fruit here is replicated distributed storage. In many cases, blockchain adds nothing and may not be the best approach. Private or proprietary records such as those kept by small businesses do not need the trustless security of blockchain. Records that the government

or other institutions maintain, attest to, and can change at will, also may as well be privately stored. A dishonest government could just as easily alter a land title record in a database before an earthquake hit as it could while it restored its systems afterwards from a backup copy. Thus, while there may be a case for placing such records on blockchain to prevent any such tampering, protecting them from destruction by keeping distributed copies does not require using blockchain.

That said, consider banking on a blockchain compared to using a local bank with replicated records that can be recovered after a disaster. The key difference is this: the blockchain bank keeps operating without interruption. Nodes that were not destroyed by the disaster continue to accept transactions and update the ledger as if nothing had happened. The brick and mortar bank has to rebuild itself, gather its employees, recover its data, and wait for power and communications to be restored. In other words, a brick and mortar bank is a whole collection of things which work together, not just data. A blockchain, on the other hand, contains the entire bank in the form of data, protocols, and code. Thus, relatives and friends outside the disaster zone could still send money, and any user inside the disaster zone could get full access to his accounts anytime he is able to connect to the internet.

This example can be extended to many other things. For example, if land titles are kept on a blockchain, they can be accessed, used as collateral for loans, or sold. If educational or professional credentials are kept on a blockchain, they can be accessed from a refugee or resettlement camp to help rebuild lives. Similarly, medical records, properly encrypted and protected, can be accessed by people who may be in immediate need of help. In other words, blockchains not only keep distributed, trustworthy, tamper resistant and secure data of all types, but can also run almost any kind of business or application logic needed to use the data. No recovery is needed. It just keeps on ticking.

6.5. Evaluation

Blockchain is a young technology, fees are higher than they soon will be, and security is still something that needs work. However, very soon the technology will make it feasible to facilitate large numbers of low value transactions securely and with very low transactions costs.

The SEC and other regulatory bodies concerned with money laundering and criminal activity, and national governments concerned with tax evasion or wishing to actively surveil and control the financial lives of their populations may resist cryptocurrencies. Some of these concerns are legitimate, but they must be balanced against potential benefits. Allowing blockchain technology to develop can extend financial inclusion to populations that are cost prohibitive for the formal banking sector to serve. The people who will benefit the most are the poor, displaced, and marginalized. Fighting, limiting, or prohibiting blockchain and cryptocurrencies, on the other hand, is unlikely to prevent much illegal activity and in fact, makes it more difficult to bring much of the underground economy into the open.

7. Other Applications of Blockchain

There are five key criteria that make it likely that Blockchain as opposed to more conventional distributed data systems or cloud based Software as a Service (SaaS) is the right approach to addressing a problem:

1. The problem involves many different actors from different organizations whose interests do not align.

2. The problem requires secure transfer of value, possibly in very small increments.

3. The problem involves agents who do not know or do not trust each other.

4. The problem requires objective provability of facts or data.

5. The problem involves agents who might wish to censor, alter, or hide data.

Note that the problem of the unbanked satisfies all five of these criteria. In this section, we give a high level outline of several other broad categories of blockchain applications that might be of particular interest to the World Bank.

7.1. Distributed Business Processes

The first criterion defines what are sometime called distributed business processes. Examples include logistics, real estate transactions, proving provenance, and maintaining medical records. When many companies, agencies, or individuals from different organization must cooperate to accomplish some goal, the first question is where to keep the data connected to the process. There is no single central agent who would naturally serve as data-master, no reason for any of the agents involved to trust one another to share a complete and correct view of the data, and no assurance that they will necessarily agree on what the correct view is at any given moment.

Blockchain is the obvious solution for this type of situation. Since the ledger is maintained, updated and synchronized by many independent nodes, there is no need to appoint a TDI. All agents involved have their own copies of the data, and to the extent that the blockchain is well-designed, they all know that they have a complete, correct, and commonly shared view of the ledger and its supporting data.

More recent blockchain implementations support smart contacts and the creation of Distributed Applications (DApps). In effect, these bring SaaS onto blockchain and allow data to be processed correctly in a trustless way. For example, a DApp could be written to record the transfer of a deed to a house with the county clerk only after inspection reports, loan approvals, title searches, and funds transfers were complete, attested to, and accepted by all the required parties. The loan officer could access the blockchain and see that other parties had completed their part of the process, and then use his bank's private key to bind his bank to funding the loan. An escrow agent could fol-

low a similar process to certify that the funds had arrived in his account and authorize the simultaneous release of authority to transfer the title and move the funds into the account of the seller.

Blockchains are also well-suited to problems that require establishing a chain of custody. For example, a farmer could pack a box of fruit or a sack of coffee and hand it off to truck driver for delivery to cooperative or warehouse. The truck driver would cryptographically sign a receipt saying that he accepted so many pounds of produce from a specific farmer, at a specific time, and record this in a blockchain. Each time the produce was handed off from one agent to another as it made its way to the dock, got through customs, was unloaded and eventually shipped to a grocery store for sale, a similar receipt would be produced and recorded. The same thing could be done for controlled substances, pharmaceuticals, industrial chemicals, or manufactured goods.

Chain of custody problems generally satisfy all five of our criteria. Blockchain contributes two major elements to the process. First, blockchains allow us to know and prove the origin of things, for example, whether our strawberries raised on an organic farm, our coffee is fair trade, the drugs we are prescribed are from a genuine source and are not part of a batch that has been recalled, or our shirt was manufactured in a factory that does not use child labor or exploit its workers. Second, blockchains allow us to assign blame if something goes missing or is mishandled. For example, a box of farm-raised shrimp going from Vietnam to Chicago must have a certain weight, contain a certain kind of shrimp, and must have been kept frozen for the entire journey. Each agent has an incentive to verify these things before he accepts custody because the next agent in the chain may refuse acceptance if the shipment is not as specified. This leaves the last agent to accept custody responsible for the loss since the blockchain shows that he claimed the shipment was in good condition when he took custody.

Examples of potential uses include:

1. Creating incentives that reward farmers or manufacturers for following good practices that consumers are willing to pay for. The blockchain makes it possible to prove that the product in question was produced in a certain way or at a certain place and thereby solves both the moral hazard and incomplete information problem. Both producers and consumers capture more value as a result.

2. Making sure that aid gets to its intended recipients. Blockchains create accountability for both funds and physical goods. For example, it might be required that refugees use biometrically connected identity tokens to attest to the fact that they received a certain allotment of food. If more food was shipped than distributed, it would be clear where it disappeared. In a similar way, funds could be tracked with signed hand-offs all along the way ending with the final recipient attesting to what he received and what he gave in exchange.

The major limiting factor in all chain of custody applications is the quality of the data inputs. A dishonest agent might empty a bag of high quality coffee and substitute lower quality beans. A box of shrimp might have thawed at some point on its journey, been refrozen, and then passed on to the next agent down the line. Receipts could be produced for goods or services that were never provided. Blockchain can only control what is on its ledger, and the problems above are off-chain in

the real world. Thus, while blockchain is a tool that allows a clear, non-refutable, immutable record of attestations to be created, this only has value if it is used within a real world system which includes incentives, monitoring, and other mechanisms that ensure that the correct data gets into the ledger in the first place.

7.2. New Kinds of Markets

Blockchain can create new types of markets that were not possible before. Blockchain allows parties to make very small transactions when neither party has an expensive bank account, credit card, or merchant service. Neither party needs to know or trust the other, and in fact, the parties need not even be human. Machine to machine markets are also possible.

Examples include:

1. Decentralized content platforms: As it stands, users must subscribe to streaming content and news services at relatively high monthly rates. This is because the transactions costs of accepting credit card and other payments make it economically infeasible to sell content *à la carte*.[14] This means that a user who wishes to listen to single song, watch a particular video, or read a a single interesting story from the Wall Street Journal is out of luck. Individual content producers such as musicians, writers, photographers, visual artists, and video creators typically don't produce enough content to be able to employ such a subscription model. As a result, they are forced to use platforms such as YouTube, SoundCloud, Shutterstock, and Etsy. These platforms impose their own rates of payment, promote content as they choose, and can also remove or censor content they don't like. Blockchain, on the other hand, will allow micropayments to be made with very low transactions fees which will make it economically feasible for creators and consumers to connect directly without a platform imposing rules or taking a cut. This could make it possible for talented creators worldwide to make a living and for consumers to have access to a much wider array of offerings.

2. Direct person to person markets for goods and services: New types of on-demand services also become practical. Users might be willing pay $.10 or $.25 a minute to get help with a computer problem, or to get advice from a plumber, a nurse, or a tutor. Blockchain based micropayments could allow people in developing countries to sell their knowledge and talent directly to consumers without a middle man taking a share or the need to find ways to accept payments from someone overseas without having transaction fees eat the majority of the transfer. Arts, crafts, and other manufactured items could similarly be transacted using escrow agents as intermediaries. Again, lowering financial transactions costs makes these kind of direct sales possible and more importantly, allows the producer to capture more of the value they create.

3. Machine to machine markets: DApps can be created that allow machines to operate as agents for their owners and to improve resource allocation. For example, a smart electric meter could

14 Services that offer content for "free" such a YouTube in fact extract a form of micropayment by requiring the users watch advertisements as a condition of seeing content. There are large fixed costs involved in signing up and billing advertisers, showing these ads to users that data analytics suggest would be responsive, and in sharing some portion of these revenues with popular content producers. Thus, even here there are significant economies and scale and network externalities that prevent the model from supporting direct person to person content markets.

accept a small payment in exchange for reducing power consumption when demand is high or buy surplus power from solar panels installed on a neighbor's roof (which would save all the power that is typically lost when electricity is transited over long distances). Routers or cell phones could negotiate with each other to buy and sell surplus bandwidth, and computers could rent their surplus compute cycles to other users on blockchain based market places. These devices would follow rules that are programmed in by their owners and only make or accept offers that meet the parameters they include. The key is that the device owners would not need to be directly involved or pay attention, but would still be assured that any services provided by their devices would be compensated through secure payments on a blockchain.

7.3. Civil Government, Civic Good, and Smart Cities

At its root, blockchain is a decentralized source of truth and a secure record of data and actions. This suggest many potential uses that increase government transparency, reduce official corruption, and protect the rights and welfare of citizens. For example:

1. Video: Police dashboard cameras are widely deployed and body cameras are becoming more common. Recording hashes of 10 minute intervals of video as they are uploaded to a blockchain would give citizens assurance that the video record has not been modified to protect misbehaving officers or to make citizens appear guilty of crimes. If metadata was included indicating the time the video was recorded and the context (by what officer, at what location, etc.) then citizens would also be able to know that relevant video existed and was not simply forgotten or erased. Note that this does not require that the video itself be automatically released. This decision could be made by policy or through courts. Knowing the video exists and has not been altered, however, is a necessary first step. The same model could be extended to traffic, security, and any other camera deployed by a government agency.

2. Official proceedings: Audio, video, and transcripts of court proceedings and legislative debates could receive the same treatment as outlined above.

3. Allocation of public services: Police vehicles, road repair equipment, snow removal equipment, etc. could be instrumented to record their location and perhaps some part of their activities. Placing these records in a public blockchain would allow citizens to know that government resources were being allocated fairly. Are certain neighborhoods receiving too much or too little police attention? Has the pothole on your street been fixed or ignored? If it was ignored, was this selective and unfair? If it was fixed, how long did the fix last and what was the cost? Governments and government employees could be required to make real-time attestations regarding their actions. If these later proved to be false, the correct actors could be held accountable.

4. Public records: Land and car titles, certain tax and legal records, and licenses and permits are examples of records that the public has a right to know. Blockchain has two things to offer here. First, putting full copies of public records in an immutable and replicated blockchain gives the public easy and equal access to information they have a right to see. As it stands, getting such access often requires going to a specific office and requesting a specific record. This makes the information effectively invisible to the majority of the public. Second, it allows public records to

be updated and amended in an externally verifiable way. As it stands, information brokers buy and aggregate such records and then sell access to facilitate background and credit checks. The problem is that brokers have little incentive to spend the effort to keep their data up-to-date and there is nothing a citizen can do to force the broker to remove inaccuracies. A citizen is unlikely even to know what this aggregated record contains. As a result, a person might be denied jobs, loans, or benefits because of an incorrect record of a DUI conviction, a lien, an unpaid student loan or other debt, or a court ruling. This might be due to new information the broker does not have, an identity theft, or even an error made by the agency that generated the data. When such records are keep current, visible, and accessible, citizens are able to find inaccurate data, get it corrected, and have the correct data propagated.

7.4. Evaluation

At the highest level, blockchain facilitates direct, anonymous, secure, exchange of data and value between agents and even machines. Because even small amounts of value can be exchanged and no trust is needed between parties, blockchain does this without the need for TDIs, large technology and communications companies, or the permission of possibly corrupt governments. Blockchain's potential impact is especially large for people who do not have access to well functioning institutions or who cannot afford to access the formal economy. Finally, blockchain makes it possible for governments, corporations, and other organizations to prove that they are honest actors who follow the rule of law.

8. Conclusion

The World Bank has a mission to end extreme poverty and increase shared prosperity. Centralization of almost any kind is more often a point of resistance rather than help in this regard. Institutions and organizations with the power to control how people trade, work, or produce have an unfortunate history of becoming more focused on their own welfare than the well-being of their charges. Governments and their agencies have a tendency to be captured by powerful interests and economic incumbents. Monopolies resist competition and focus on serving only the most profitable markets. Political and social organizations work to support the status quo or advance the agenda of its members over the interests of the rest of society. The poor are not well equipped to use tools of centralized control or to readily gain access to centers of power.

Most recent technological innovations include elements that work in favor of centralization. Google, Facebook, Twitter, Amazon, and other cloud-based platforms depend on network externalities and economies of scale which makes for a winner take all environment. The Internet of Things (IoT) includes an array of inexpensive sensors and communications devices that all funnel data to corporations or governments, and new techniques for data analytics make it possible to use this information at an extremely granular level. The international banking system is almost completely interconnected and has the ability to control the most important aspects of our lives.

Blockchain is the singular emerging technology that works against this tide. Permissionless blockchain is by its nature decentralized and impossible for any authority, centralized or otherwise, to control. It allows people and devices to connect directly and anonymously which makes it very difficult to prevent unfavored genders, minorities, or other groups for interacting and creating value on a level playing field. Blockchain applications can be built to serve almost any purpose. Not only can existing cloud based SaaS be provided cheaply and without the censorship or permission of any nation or corporation, but entirely new services directed specifically at the poor and disenfranchised become feasible and sustainable.

Much of this will happen on its own, but the World Bank can play a key role. First, while blockchains can operate cheaply, setting up DApps and building understanding, usage, and acceptance takes vision and initiative. The free market will concentrate on the most profitable sectors, but the World Bank could take a leadership role in creating and deploying blockchains directed at the less profitable mission of improving the welfare of the poor. Second, although most of the applications discussed in this paper focus on the poor, some have the potential to be more broadly disruptive. Corporations, governments, and other powerful incumbents may see these innovations as contrary to their interests and oppose them. Again, the World Bank could take a leadership role in persuading governments and decisions makers that increasing the power and agency of citizens, giving the poor direct access to markets without exploitative middlemen, and creating transparency and accountability, are ultimately things that benefit the entire country, powerful incumbents included. Not doing so creates a risk of being surpassed by more forward thinking nations and economies. Third, for blockchain to realize its full potential, enabling legislation to legalize its use and to give the power of the law to things like title transfers or contract agreements executed or recorded on blockchains are needed. In addition, while the great majority of blockchain applications are not winner take all, some level of network network externality is typically present. The encouragement and endorsement of the World Bank and like-minded institutions would do much to speed the adoption blockchain applications that would benefit the poor, and ultimately, the world as a whole.

9. References

Allen, Christopher, (2016) “The Path to Self-Sovereign Identity” http://www.coindesk.com/path-self- sovereign- identity/.

Bonneau, Joseph (2018) “Hostile Blockchain Takeovers (Short Paper)”, Financial Cryptography Workshops 2018, DOI:10.1007/978-3-662-58820-8_7.

Castro, M and B. Liskov (2002) “Practical byzantine fault tolerance and proactive recovery”, *ACM Trans. Comput. Syst.*, Vol 20, pp. 398–461.

Conley, J. (2018a) “The Geeq Project Tokenomics” https://geeq.io/2018/10/30/the-geeq-project-tokenomics-2/

Conley, J. (2018b) "ETFs Rule, Stablecoins Drool: How to Make Cryptocurrencies go Mainstream" *https://medium.com/@JPConley/etfs-rule-stablecoins-drool-how-to-make-cryptocurrencies-go-mainstream-b713a054b311*.

Crypto51 (2019) "PoW 51% Attack Cost" https://www.crypto51.app/.

Demirguc-Kunt, Asli, Leora Klapper, Dorothe Singer, Saniya Ansar, and Jake Hess (2018) "Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution" World Bank https://openknowledge.worldbank.org/handle/10986/29510.

Elsts, Attis (2018) "Lessons learned from evaluating IOTA on Internet of Things devices" https://hackernoon.com/lessons-learned-from-evaluating-iota-on-internet-of-things-devices-a44575e606de.

Elsts, Atis, Efstathios Mitskas, and George Oikonomou. (2018), "Distributed Ledger Technology and the Internet of Things: A Feasibility Study" In *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems* (BlockSys'18), Gowri Sankar Ramachandran and Bhaskar Krishnamachari (Eds.). ACM, New York, NY, USA, 7-12. DOI: https://doi.org/10.1145/3282278.3282280.

Fyookball, Jonald (2017) "Mathematical Proof That the Lightning Network Cannot Be a Decentralized Bitcoin Scaling Solution", https://medium.com/@jonaldfyookball/mathematical-proof-that-the-lightning-network-cannot-be-a-decentralized-bitcoin-scaling-solution-1b8147650800.

Fabien, Paul, and A.P. Petitcolas (2018) "A first look at identity management schemes on the blockchain", *IEEE Security & Privacy* Vol. 16 DOI 10.1109/MSP.2018.3111247.

Grandi, Filippo (2017) "Opening statement at the 68th session of the Executive Committee of the High Commissioner's Programme" United Nations High Commissioner for Refugees, *http://www.unhcr.org/en-us/admin/hcspeeches/59d1f3b77/opening-statement-68th-session-executive-committee-high-commissioners-programme.html*.

Medina, Leandro and Friedrich Schneider (2018) "Shadow Economies Around the World: What Did We IMF Working Paper Learn Over the Last 20 Years?" World Bank Reports WP/18/17.

Redman, Jamie (2018) "Looking Beyond the Lightning Network Hype: Every Day Users Experience Issues", https://news.bitcoin.com/looking-beyond-the-lightning-network-hype-every-day-users-experience-issues/.

UNHCR Inspector General's Office (2015) "Joint Inspection of the Biometrics Identification System for Food Distribution in Kenya" Inspection Report INS/15/02 http://documents.wfp.org/stellent/groups/public/documents/reports/wfp277842.pdf.

World Bank (2019) "Who we are" https://www.worldbank.org/en/who-we-are.

World Bank (2019) "Financial Inclusion Home" http://www.worldbank.org/en/topic/financialinclusion/overview.

VirtualCoinSquad (2018) "Businesses that Accept Bitcoin, Litecoin, Dogecoins and other Altcoins in 2018" https://www.virtualcoinsquad.com/.