Impact of Blockchain technology on US financial inclusion

By

Alin S. Dragos

M.B.A, University of Arkansas, 2006
B.B.A, Academia de Studii Economice din Bucuresti, 2003

SUBMITTED TO THE MIT SLOAN SCHOOL OF MANAGEMENT IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN MANAGEMENT OF TECHNOLOGY
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2017

Signature redacted

Signature of Author: ____________________

MIT Sloan School of Management
May 12, 2017

Signature redacted

Certified by: ____________________

Simon Johnson
Ronald A. Kurtz (1954) Professor of Entrepreneurship, MIT Sloan School of Management
Thesis Supervisor

Signature redacted

Accepted by: ____________________

Johanna Hising DiFabio
Director, MIT Sloan Fellows Program
MIT Sloan School of Management

Impact of Blockchain technology on US financial inclusion

By

Alin S. Dragos

Submitted to MIT Sloan School of Management
on May 12, 2017 in Partial Fulfillment of the
requirements for the Degree of Master of Science in Management of Technology.

Abstract

This paper describes how blockchain technology alters the dynamic within financial services and focuses on the impact on US financial inclusion. First, I provide an overview of the financial services industry and the issues associated with financial inclusion. Second, I provide a framework for reviewing blockchains. Lastly, I take an in-depth look at the economics of offering checking accounts, and identify approaches for how blockchains will redefine the value chain in financial services.

Blockchain technology brings new avenues for companies within the payments value chain to work more closely together to reduce costs for all parties involved. Banks are leading the way in exploring how blockchains will make them more efficient. By partnering with merchants, banks stand to make the most out of the lower costs to network securely promised by blockchains. In this process, banks set themselves up to offer no-fee checking accounts to all consumers, without taking a loss on each account, as they do today. Banks' ability to profitably offer no-fee checking to unbanked and underbanked customers is the key to increasing financial inclusion in the US, and ultimately across the globe.

Thesis Supervisor: Simon Johnson
Title: Ronald A. Kurtz (1954) Professor of Entrepreneurship

Contents

Summary

In this paper, I describe how blockchain technology alters the dynamic within financial services and I focus on the impact on US financial inclusion. First, I provide an overview of the financial services industry and the issues associated with financial inclusion. Second, I provide a framework for reviewing blockchains. Third, I take an in-depth look at the economics of offering checking accounts, and identify approaches for how blockchains will redefine the value chain in financial services.

In 2016 a basic checking account cost banks an estimated $349[1]/year to maintain. These high costs make their way to the consumers, becoming the primary reason why 67M Americans are either unbanked, or underbanked. I analyze banks' costs for offering checking accounts, and then zoom in on their main functionality – to make payments from consumers to merchants. The payments value chain has five main players: consumers, merchants, merchant acquirers, payment networks and banks. When consumers pay merchants (e.g., a consumer buys toys from Amazon), the merchant pays a fee (i.e., cost of payments) to the merchant acquirer, who manages all payment related complexity for the merchant. This fee represents revenue for which acquirers, payment networks and banks are competing. I'm analyzing how blockchains will affect this vertical competition dynamics (e.g., between acquirers, networks and banks) and which functions performed by each of the three players will be impacted by blockchains.

I start by comparing the top three[2] cryptocurrencies today: Bitcoin, Ethereum and Ripple on a three-pillar framework to understand which of them is better suited for the financial services industry.

- Transactions and scripts – I take an in-depth look into the mechanics of how each of these blockchains works, how are they similar and how are they different.
- Consensus and mining – I start from what I consider Bitcoin's principal innovation, the Nakamoto consensus. The consensus means the method used to prioritize who gets to extend

[1] American Bankers Association, "2016 ABA Issue Summary: Fees and Pricing of Banking Products", (2016): 97-99

[2] Coinmarketcap.com, "Crypto Currency Market Capitalizations", accessed Mar 31, 2017, http://coinmarketcap.com/

the blockchain, by solving a computational puzzle. The nodes solving the puzzles, called miners, are incented to continue working by receiving cryptocurrency as reward.

- Peer to peer communication network – used for communication and discovery, designed with decentralization and low latency in mind, this pillar is important for public blockchains.

Second, I explain the three main categories of blockchains today (public, consortium, also called permissioned, and private):

- Public blockchains – anyone can read the blockchain; anyone can propose transactions to be written and expect them to be included if certain criteria are met; anyone can participate in the consensus process.
- Consortium (or permissioned) blockchain – consensus process is decided by a pre-selected set of nodes, and read permissions may be public or restricted to a certain set of participants
- Private blockchain – central authority controls consensus process and the read/write permissions

I wrap up this part of the thesis by evaluating each type of blockchain for industrial scale implementations, and point to consortium blockchains as holding the most promise for financial services.

The best proxy of what it means to offer bank accounts to the underbanked is given by prepaid account providers, who serve this audience almost exclusively. I've analyzed the leading provider of prepaid bank accounts, and have found that they were able to cut their costs to $149/year, split between $112/year cost to service the account and $37/year costs to reach the consumers. Banks can learn from this lean business model, and improve on it by deploying blockchains to reduce their costs even further. My calculations point to reducing costs of servicing an account from $112 to $66 by deploying blockchain technology. In order to achieve such savings though, banks need to partner with merchants. Merchants' value proposition for blockchains is clear, as they stand to benefit from much faster payments, and even small reductions in cost of payments. If the banks are able to reduce costs to the level I anticipate, they will be able to offer checking accounts at no cost to the consumer, while remaining profitable. A no-fee checking account is the most important step towards increasing financial inclusion.

I conclude by pointing that blockchain technology brings new avenues for companies within the payments value chain to work more closely together to reduce costs for all parties involved. Banks are well positioned to lead the way, yet merchants who sell goods and services to consumers stand to play an even more meaningful role than they do today. By supporting blockchain technology, merchants will be able to reduce their cost of payments, and receive the funds for their goods sold much faster, thus improving their working capital structure. Banks are leading the way in exploring how blockchains will make them more efficient. By partnering with merchants, banks stand to make the most out of the lower costs to network securely promised by blockchains, and in the process set themselves up to offer no-fee checking accounts to all consumers. These accounts are the key to increasing financial inclusion in the US, and ultimately across the globe.

Financial inclusion

What is this and why does it matter?

Financial inclusion[3] means that individuals have access to useful and affordable financial products and services that meet their needs – transactions, payments, savings, credit and insurance – delivered in a responsible and sustainable way. The benefits coming from access to financial products can be classified in the following categories: lower transaction costs, safety (carrying cash it is riskier than carrying a plastic card), earnings smoothing, asset protection (via insurance) and access to opportunities (long term planning, education, etc.). Out of the 17 sustainable development goals published by the United Nations (UN), 7 point to financial inclusion as an enabler. The World Bank has declared Financial Inclusion a priority, and has a Universal Financial Access 2020 initiative dedicated to offering access to a transaction account to everyone. More than 50 national level policy makers have committed to improving financial inclusion for their countries. However, after all these concerted efforts, there are still 2billion people globally without access to a basic account. The United States alone identifies 15.6[4] million adults unbanked and another 51.1million adults underbanked. This is truly a global issue, yet it is also an issue where the US is not a leader, it ranks a modest 23 out of the 35 countries in the OECD.

[3] The World Bank, "Financial Inclusion Overview", accessed May 02, 2017. http://www.worldbank.org/en/topic/financialinclusion/overview#1

[4] "2015 FDIC National Survey of Unbanked and Underbanked Households", *Federal Deposit Insurance Corporation,* (2016), 1.

Why is financial inclusion such a hard problem to solve?

The number of unbanked and underbanked individuals in the US has been roughly constant in the past twenty years. The FDIC has published in October 2016 its 2015 version of the study of National Survey of Unbanked and Underbanked. This shows no statistically significant change in the numbers (need details here). While there are many reasons of why this number proves so hard to change, below are the three main categories:

1) **Convenience.** The best case made for cash is that it is convenient, and it is deeply embedded in all of our behaviors. Much has been said about the decline in cash usage, yet the reality continues to be that it is still very prevalent. A recent study shows that between 46 percent and 82 percent of all payment transactions in seven developed economies are conducted in cash. Cash is an alternative that is not without merit. Below are a few of the benefits that cash brings[5]:
    a. Anonymity – once one presents cash, for most purchases no other form of id is needed, which is often a benefit for the unbanked population.
    b. Censorship resistant – no one party can keep anyone from spending cash. This is different from what banking offers, in that a bank hold may impact someone from accessing their funds.
    c. Convenience – cash is accepted everywhere, including in places where no infrastructure exists.
    d. Resistance to negative interest rates – this is not the case in the US, but elsewhere in the developed world, negative interest rates may be applied to deposits, but not to cash.
    e. Cash does not have credit risk – having money in the bank introduces risk, however small. Not really an issue in the US, but countries that have experienced recent upheavals, such as Greece, can attest to how significant this risk can become.
2) **Costs.** From a consumer perspective, using a bank account is not cheap, especially if the balance maintained on the card is low. From a bank perspective, the math is easy,

[5] JP Koning, "Fedcoin: A Central Bank-issued Cryptocurrency", 11. https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/58c7f80c2e69cf24220d335e/1489500174018/R3+Report-+Fedcoin.pdf

the more money flows through an account, the more profitable that account is. Banks have established their practices to court high earners, and are basically ignoring low earning customers. All bank accounts have non-sufficient funds (NSF) fees, and these average around $33 (in 2016 – study here). Even without NSF fees, there are ATM fees, statement fees, etc.

3) **Trust.** Banking practices have disenfranchised a good amount of consumers who view banks as institutions to be avoided, rather than service providers. Between questionable credit card and mortgage practices, NSF fees, and a pricing method that disfavors the low earners, a lot of consumers are deciding to opt out.

Why are people excluded?

The term unbanked is used to address a combination of diverse individuals that do not have a bank account. This can happen either by choice, or by necessity. Currently in the US there are ~9[6] million unbanked households, comprised of 15.6 million adults and 7.6 million children. This compares favorably to 9.6[7] million household two years ago, so while declining, the number is relatively stable. The most common groups of unbanked persons include low-income individuals and families, those who are less-educated, households headed by women, young adults and immigrants[8]. The causes too seem to be quite well established, and the reasons most frequently invoked are below:

1. **Fees are too high.** In the FDIC studies from 2015 and 2013, this has been the biggest reason for staying outside of the banking system. This is related to the perception that banks have high fees, and the efforts for establishing a bank accounts are outweighing the benefits.
2. **Privacy.** The underbanked associate banks with a loss in privacy, and from this perspective, cash does provide a good alternative.
3. **Bad experience with a bank.** We can include poor credit history and/or bankruptcy, high costs, difficulty in producing the paperwork necessary to establish a bank account.

[6] "2015 FDIC National Survey of Unbanked and Underbanked Households", *Federal Deposit Insurance Corporation,* (2016), 1.

[7] "2013 FDIC National Survey of Unbanked and Underbanked Households", *Federal Deposit Insurance Corporation*, (2014), 1.

[8] Martha Perine Beard, "In-Depth: Reaching the Unbanked and Underbanked", *Federal Reserve Bank of St. Louis*. Accessed May 2, 2017.
https://www.stlouisfed.org/publications/central-banker/winter-2010/reaching-the-unbanked-and-underbanked

as we've established before, the banks do not typically cater to lower income people, and the vast majority of unbanked qualify as lower-income. [need quote here} this is widely believed to be the main group.

4. **Bank accounts too complex.** As of 2015, less than a third of American adults had been offered financial education at a school, college, or workplace, and only one in five say they participated in financial education[9]. This means that a lot of the education needed comes either through self-education, or from the family. The US has recognized this need, and as part of the Fair and Accurate Credit Transaction Act of 2003, the Financial Literacy and Education Commission has been established to develop a national financial education website: MyMoney.gov.

Alternative Financial Services providers

In an environment where banks are clearly not meeting everyone's needs, a number of specialized Alternative Financial Services (AFS) providers appeared, and thrived. These AFS provide services that can be categorized as providing credit or solving for a very specific transaction.

1. **Provide credit:** Pawn shops / Pay day lenders/ Refund anticipation loans/ car title loans / rent to own agreements that extend credit using different types of assets as collateral:

Name of AFS provider	Obtain cash in exchange for...
Pawn shops	Assets owned (e.g. electronics/jewelry, etc,)
Payday lenders	Future paycheck
Refund anticipation loan	Future tax refund
Car title loans	Car title
Rent to own	New furniture/TVs, etc.

Table 1.1 – Types of collateral needed to obtain credit from AFS

2. **Use case driven:** These are specific transactions such as
   a. Check cashing, where the holder of a check, either given to them by the employer or by a different individual (e.g. for mowing lawns, house-cleaning jobs, etc.) goes to a check cashing location, hands in the check, and receives cash in return. Fees for check cashing vary from a fixed rate of $3/check (at locations such as

[9] "Promoting Financial Success in the United States: National Strategy for Financial Literacy, 2016 Update", *Financial Literacy and Education Commission*, (2016), 7-8 https://www.treasury.gov/resource-center/financial-education/Documents/National%20Strategy%20for%20Financial%20Literacy%202016%20Update.pdf

Walmart) to a percentage based model, with percentages varying between 1% (PLS Check Cashing) and 5% (All American Check cashing).

b. Money orders, in which an individual needing to make a payment to an entity where cash is not appropriate (e.g. rent), goes to an institution selling money orders, pays with cash for the face value of the order plus any applicable fees, receives the money order, and then hands it in to the initial recipient

c. Remittances, defined as transfers from a sender in a country to a recipient that is typically in another country. In this case, the initiator of the remittance goes to a location that offers the service, hands in the money and the applicable fee, receives a proof of payment, and notifies the recipient who in turn needs to act to receive the funds from the remittance service in their country.

3. **Prepaid cards:** These instruments are not true AFS, they are a mix between a bank account and an alternative financial service.

While the distinction between traditional banks and Alternative Financial Services providers is very clear, a third, intermediary category gained ground - Prepaid cards. Similarly, to bank accounts, Prepaid cards allow for withdrawing cash from ATMs, paying for goods and services either at the point of sale or online and other types of transactions that are typically done via a bank. The differences come mostly in branding and channel of distribution. In terms of branding, these are called prepaid cards, although they are for all intents and purposes debit cards linked to a bank account. In terms of channels of distribution, it is where prepaid providers have contributed the most, going to employers, retailers, universities, etc. basically reach the underbanked wherever they live/work instead of going to a bank.

Pillars of financial inclusion

Financial inclusion is a very broad term, which is very helpful to define the issue (absence of significant segments of the population from the mainstream financial system) at a macro-economic level. However, at a micro-economic level, there are a number of pillars based on which universal access to financial services can grow. Described below:

Identity

A key step towards being accepted in the mainstream financial systems is to have an established identity, and to be able to prove it via some sort of government issued photo id. All banks are required to ask, collect and maintain the identity of their customers. However, a customer with documents that prove identity has access to the most basic level of access, a bank account with a debit card. Obtaining credit requires a credit history, and this is where things get difficult for a lot of unbanked and underbanked individuals. A credit history and the score that comes with it that assesses credit worthiness requires steady income, unblemished management of one's finances, quality of managing previous credit, etc. Getting a good credit score is not easy, and takes time. Without a good credit score, it is very difficult to get credit from a bank – and this is where alternative financial services have thrived.

Security

Security is a big deal for banks, and with good reason. The core idea of banking as we know it is that the bank will safeguard our money and information. When consumers lose faith in a bank, they take their funds elsewhere, and if enough customers do that, the bank disappears. Banks treat that as seriously as any institution, yet even banks will recognize that it is becoming harder and harder to maintain trust in existing system. Banks have built large data silos with a lot of valuable data, which has placed a large target on their backs. Data breaches are becoming more and more prevalent, and a lot has been written with regards to identity theft – one of the fastest growing crimes in the United States, with more than 15 million[10] fraud victims in 2016, up 18% from 2015 . Increasing financial inclusion is a relevant goal only if being in the system clearly bests the alternatives. Especially post 2008 crisis, with all of the news and finger pointing at banks, the unbanked individuals have lower (and declining) incentives to join.

Payments

Financial systems work better when more people are participating, which is a trait characteristic to multi-sided networks. Another characteristic is that every new member that joins makes the network more valuable for all of the other members. These two principles are key for the banking industry, which has very high fixed costs, and low marginal costs. Facilitating payments is a core activity for banks, and they are more effective at doing that when everyone has a bank account. Paying with cards is safer and more convenient, and that is why in the US they have been so successful. Different participants in the industry have acted in two main

[10] Javelin Strategy & Research," Identity Fraud Hits Record High with 15.4 Million U.S.", accessed May 3, 2017. https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

directions here: a) increase the number of locations accepting electronic payments, and b) reduce the number of locations accepting cash. Acceptance of payments thus becomes a major force in increasing financial inclusion. It basically increases the rewards for being in the financial system, while simultaneously increasing the penalties for being outside of it.

Quality of financial products offered

There are few easy ways to measure quality of financial products offered. In terms of breadth of the offering, the US is probably amongst the best world, but it is also far from perfect. a few dimensions make sense here: speed, uptime, customer service, cost/quality ratio, diversity, ease of use, etc. Internet and mobile phones have dramatically improved the quality of the offering of financial services provided. For the US, this is not considered to be a major factor.

Acceptance (Outreach)

For individuals with a bank account, the two most important uses are paying for goods (either at a point of sale, or online) and taking cash out from an ATM. While the vast majority of merchants in the US accept electronic payments, ATM access is somewhat more complicated. First of all, ATMs are affiliated with institutions, and those institutions will offer free access to their members, and will charge members of other institutions (so called out of network ATM fees, which are perceived as high, and are increasing). Also, while ATMs are ubiquitous in urban areas, in rural areas this is a different story, ATM locations are far less accessible. There are ways to obtain cash from a POS device, but not all merchants offer those, and not all consumers know about this feature. In a large country, like the US, geographic reach is a limiting factor.

Costs

An overburdened cost structure is the main reason why banks are failing to address the lower income individuals. In 2016, banks where spending $349 per account per year to maintain a checking account[11]. Prepaid account providers, which have virtually identical features to those of checking accounts, have stepped in the space, and, benefitting from a much leaner cost structure, have offered products designed specifically for the needs of the unbanked individuals. However, prepaid cards also have limited appeal, and have gotten a reputation for high, predatory fees, which have attracted the ire of regulatory bodies such as the CFPB. There is no

[11] American Bankers Association, "2016 ABA Issue Summary: Fees and Pricing of Banking Products", (2016): 97-99 http://www.texasbankers.com/docs/FeesandPricingofBankingProducts.pdf accessed Mar 29 2017.

escaping the fact that if financial inclusion is to increase, the costs to service customers need to decrease. Assuming the existing infrastructure, heavy regulatory burden and increased fraud, any improvements are likely to be evolutionary. There are very few revolutionary technologies for financial institutions, and blockchain is one that promise, as this thesis will investigate in the following chapters.

Infrastructure required

Financial services are additive to the quality of life of an accountholder only if they can be used whenever and wherever necessary. The investment in infrastructure required to provide good coverage to a large country, like the US, should not be underestimated. The current system in place in the US is a creation that can mostly be attributed to banks. It is not a perfect system, and it is not directly adaptable to the twenty-first century, but it works for most people, and it has served the US well over the past century. On the plus side, it works, and it does so at scale, serving the largest economy in the world. On the minus side, it lacks in security, it is expensive, certain types of transactions are slower than they should be, and it is designed for older types of identification documents. There are two main types of infrastructure relevant for the purpose of this paper, payments infrastructure and access points (or geographical footprint).

Payments infrastructure[12]

The payments infrastructure is a complicated network that involves a lot of specialized players, each of them with unique infrastructure and business model.

Banks. The institutions at the core of this network, as they are allowed to hold money on behalf of the consumers. Importantly, banks are insured by the Federal Deposit Insurance Corporation (which ensures deposits up to $250,000/account), which increases trust in overall system.

Payment networks. Networks that allow for movement of funds between banks. VISA, MasterCard, Discover, American Express and First Data own the vast majority of the payment networks in the US.

Interbank system for retail electronic funds transfers (Automated Clearing House – ACH). The ACH Network is at the center of commerce in the US, moving money and information from

[12] Committee on Payments and Market Infrastructures - World Bank Group, "Payment aspects of financial inclusion", (2016), 31-33.

one bank account to another through Direct Deposit and Direct Payment via ACH transactions, including ACH credit and debit transactions; recurring and one-time payments; government, consumer and business-to-business transactions; international payments; and payments plus payment-related information. Each year it moves more than $40 trillion and nearly 23 billion electronic financial transactions, and currently supports more than 90 percent of the total value of all electronic payments in the U.S.[13] this is maintained by a not-for profit called NACHA (National Automated Clearing House Association), which is funded by the members served – more than 10,000 financial institutions.

Payment card processing platforms (Payments switch) – entities such as First Data, that allow for transactions to be processed timely, and routed to the appropriate networks. These entities perform several key functions, but the most important one is acting as an intermediary between merchants accepting payments and the entire payments ecosystem. Typically, merchants do not accept one means of payment, they accept a number of them. For a merchant to maintain a relationship with each network is expensive and requires specialization outside the merchant's scope, so this is why payments processors exist.

Large-value interbank settlement system. CHIPS (Clearing House Interbank Payments System – a private institution, member owned, similar to ACH, focusing on large payments) and Fedwire (operated by the US Federal Reserve Banks). These two networks function in tandem, and both of them ensure that the communication between banks is fast, secure, and it is done on networks that are different than the ones processing consumer payments. They are very important to the US economy, and while they are interoperable, they do have distinct differences. CHIPS is privately owned by the member participants, versus Fedwire which is part of a regulatory body (Federal Reserve Banks). CHIPS is smaller (and cheaper), only having 47 members compared to 9000+ banking institutions eligible to make payments via Fedwire. Lastly, CHIPS is a netting engine (which means it is not real time), while Fedwire is real time.

Data-sharing platform (e.g. credit reporting system). Sharing data amongst multiple providers provides value to all involved. To banks, sharing data is valuable because it allows banks to do their due diligence on their customers, as well as finding ways to minimize information

[13] National Automated Clearing House Association, "What is ACH?" Quick Facts About the Automated Clearing House (ACH) Network". Accessed Jan 15, 2017. https://www.nacha.org/news/what-ach-quick-facts-about-automated-clearing-house-ach-network

asymmetry (the more information a bank can gather, the better they can assess the risk a customer poses, and the better they can price the services provided to that customer). One key example of such data sharing platforms are the credit reporting systems (in the US, the key players are Equifax, Transunion and Experian). These platforms act as independent third parties that collect as much information as possible from the consumers from both banks and non-bank sources, aggregate the data and create a credit history and a credit score. These attributes are then shared for a fee with the interested parties, including consumers who are interested in knowing what these credit reporting systems know about them.

Identification infrastructure. For banks, and for a lot of other players too, identifying consumers is central to their business model. Currently, there are a number of ways used to identify consumers, but they are all variations of:

- Find out and maintain personal identifiable information, which gets stored in a large database controlled by a business entity
- Use some combination of phone/email/address, etc. of the individual to authenticate them

All US banks require a combination of personal information and government issued photo id when opening an account, together with a few other questions. This is an example that shows one of the issues with the current systems in place, which is that is built on top of identity instruments that worked perfectly for face to face transactions, but are flawed for most e-commerce transactions.

Access points

Accessing the funds stored in a bank account is a key factor in the decision process for any individual currently not owning a bank account. The move from cash to electronic payments is one that is heavily influenced by lifestyle. The challenge for entities offering financial services is to make the move to electronic services as easy as possible – yet that is a significant challenge.

Points of sale (Points of purchase)

This represents the time and/or place where a transaction is completed, when it comes to in-person transactions. For online purchases, this becomes an internet enabled smart device (pc, phone, tablet, etc.). Establishing a point of sale presence requires a POS device, preferably connected to the Internet, that can accept electronic transactions in addition to cash (EFTPOS).

This is where a smart device, connected to the internet, can transfer electronic funds via an interbank network. These interbank networks are owned by a very small number of players (VISA, MasterCard, American Express, Discover, Star, NYCE, etc.).

Automated Teller Machines (ATM)

The number of ATMs in the US is currently estimated to be around 425,000[14], and the market for ATM owners is highly fragmented. The top five players are Cardtronics, Payments Alliance, Bank of America, JPM and Wells Fargo, together accounting for 24.4%. These machines are installed in a physical location, and they need to connect to interbank networks that allow the cards in consumers' possession to connect to the bank issuing the card, and allow for a number of transactions, typically cash disbursement. These interbank networks too are owned by a very limited number of players, such as Visa, MasterCard, Discover, STAR, NYCE.

Bank branches

The number of bank branches has long been declining in the US, and recent data confirms this trend. The total number of branches has declined from 98,115 as of Sep 2012 to 92,385 as of Sep 2016. Another significant trend in banking is consolidation, and that is also reflected in the number of branches. Even after considering this though, the US market is fairly well served by the network of physical branches, and they continue to serve a purpose. These are highly visible locations, generally perceived as safe, and they do allow access to cash 24/7, as well as to more complicated services. While shifts in technology, demographics and user preferences are all contributing factors to the decline in number of physical branches, it is also clear that these will not outright disappear, at least not in the short to medium future.

Financial service providers' locations

In addition to the decline in the number of branches, another trend has been for financial services to be offered increasingly closer to where the customers are, namely in retail locations. Retail giants such as Walmart have clearly recognized this need, and while Walmart does not own a bank, it does offer financial services in many of its 5,332 US stores. The popularity of the prepaid cards can largely be explained by the increasing number of channels where these cards are distributed, from employers and retailers to schools and transit providers. What all of these

[14] Statistic Brain, "ATM Machine statistics", accessed Feb 15, 2017. http://www.statisticbrain.com/atm-machine-statistics/

locations have in common is convenience – the primary reason they exist is to serve a consumer need.

A technical analysis of blockchain technology

Blockchain Technology - precursors

Cryptographically secured chains of blocks have been discussed in academia starting with the 90's. One of the first major contributions came from David Chaum, who introduced the concept of secure digital cash in the '80s. Additional significant steps came, amongst others, from Adam Back (inventor of haschash, a proof of work system, in 1997) and Nick Szabo (proponent of bit gold in 1998, and creator of the "smart contract" concept). In 2008, an individual, or a group of individuals, operating under the Satoshi Nakamoto pseudonym conceptualized the first blockchain with the introduction of the paper "Bitcoin: A Peer-to-Peer Electronic Cash System". Roughly a year later, in 2009, Satoshi Nakamoto released the source code for Bitcoin Core, and that led to the creation of the first blockchain database - Bitcoin. What sets this particular solution apart from all previous attempts to create digital cash is the fact that it was the first to present a solution for the double spending problem for digital currencies. Bitcoin has been continually running since 2009, which makes it not only the first, but also the longest running blockchain. While Bitcoin is the most important blockchain, there are hundreds of other blockchains, both public, consortium (also called permissioned) and private. The combined value of all cryptocurrencies is estimated to be around $37billion[15], with Bitcoin ($23.2B), Ethereum ($7.1B) and Ripple ($2.0B) being the top 3, accounting for 87% of all of the market cap. There are twelve blockchains with a market cap exceeding $100million, so clearly blockchains have captured the imaginations of technologists, entrepreneurs and corporations alike.

Bitcoin

The digital currency made popular by Satoshi Nakamoto is ground breaking in more ways than one, and this paper will point to those new concepts introduced by Bitcoin. In 2017,

[15] Coinmarketcap.com, "Crypto Currency Market Capitalizations", accessed May 2, 2017, http://coinmarketcap.com/

after a lot of research and resources going into developing competing currencies, it is not obvious that a significantly better design exists.

How does Bitcoin work? Bitcoin, like any other blockchains, is a chain of blocks. The first block, called a Genesis block is the only one that does not have a precursor (it has been created with no inputs, only an output of 50BTC; it also has a message that provides insight into the creator's rationale for starting Bitcoin). All of the subsequent blocks are interconnected, and new blocks are added continuously, at the pace of roughly one block every 10 minutes. Blocks are interconnected in such a way that they mirror an important cryptographic structure called a Merkle tree. This type of structure acts as a tree in which every non-leaf node is labelled with the hash of its child nodes. It is this characteristic that makes a Merkle trees an efficient and secure method for verifying the contents of large data structures. Demonstrating that a leaf node belongs to a hash tree requires processing an amount of data proportional to the logarithm of the number of nodes of the tree. It is possible to trace every single block back to the genesis block, which is a key characteristics of Bitcoin. Since inception, all blocks have a hard coded limit of 1Mb. This has helped tremendously with popularizing Bitcoin, yet it is also a key limitation of its existing design, as well as a source of conflict amongst the developer community. The Bitcoin blockchain, which is about $118Gb[16] in size, is stored by each miner, and that is what makes it a distributed ledger. Each miner competes with the other miners for the right to extend the ledger, by solving a cryptographic puzzle, and by advertising the solution to the network, in order to collect the reward. When a node advertises a solution, the unsuccessful miners validate it, and if the solution is correct, they drop the work in progress, and start mining a new block. The framework below, found in an academic paper published by Joseph Bonneau at al.[17]. is a good starting point to understand the key components of Bitcoin, and other public blockchains, as well as point to the key design decisions made by Satoshi Nakamoto.

1) Transactions and Scripts
   a. **Transaction format.** The state of the system in Bitcoin is a series of transactions, stored in blocks, which are all sequentially interconnected. As transaction

[16] Coin.Dance, "Bitcoin Statistics", accessed May 1, 2017.
https://coin.dance/stats#blockchain

[17] Joseph Bonneau et al., "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", IEEE Symposium on Security and Privacy, 2015.
http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf

involving transfer of bitcoins happen, they are all advertised to the entire network. From there on, they are coupled with other transactions into a block that is added to the blockchain. transactions have a rather simple format including one or many inputs and a single output. The hash of the output is included in subsequent transactions, as well as a set of rules that instructs the protocol on how a transaction can be redeemed.

b. **Transaction scripts.** Each transaction output has a short snippet of code, in a special scripting language called *scriptPubKey*, representing the conditions under which bitcoins can be redeemed. This scripting language includes the hashing of a public key, together with a signature validation routine. It is a language with fewer than 200 instructions (called opcodes). It is a deliberately restrictive language, with most of the opcodes being marked as unusable.

c. **Conservation of value.** Another key, hard-coded requirement for all Bitcoin transactions is that the sum of all outputs is smaller or equal to all inputs. If inputs are larger than outputs, the difference is retained by the miner successfully mining the transaction. This applies to all types of transactions, with the exception of coinbase transactions (those are the transactions where new coins are created and allocated to the miner who successfully adds a block to the blockchain)

d. **From transactions to ownership.** The choice to design Bitcoin as a series of transactions leads to there being no inherent notion of identity or account ownership within the ecosystem. Simple knowledge of a public key leads to creating a signature which allows redemption (or transfer) of BTC to another address. In essence, everyone owns as many bitcoins as they can redeem. Hashes of public keys function as addresses, and act as pseudonymous identity throughout the system. no real-world names or other identifying information are required. This is a source of much appeal amongst users, as well as much angst amongst national regulatory bodies.

2) <u>Consensus and Mining.</u> A transactions based digital currency system solely based on users exchanging transaction information between them would not be secure. It would be impossible to prevent users from spending their value twice. This issue, called a double spending attack, has been the key factor stopping other digital currencies from emerging

pre-Bitcoin. The way Bitcoin addresses this is to publish all transactions in a permanent and global transaction log, with any individual transaction output being used as an input only once. This log is implemented as a series of blocks – this global, permanent log is called a blockchain. this design still requires that all nodes in the system agree on the content of the blockchain. This could be done in one of two ways: either via a central trusted authority, or via a decentralized, pseudonymous protocol called Nakamoto consensus.

a. **Nakamoto consensus**. This is Bitcoin's core innovation, and most likely the ingredient most responsible for its success. Any party can try to add to the blockchain by collecting a set of valid pending transactions, and merging them into a block. This is where Bitcoin introduces a method to prioritize who gets to add to the blockchain, by publishing a challenging computational puzzle (called proof of work), to decide which party gets to add the block to the blockchain. whichever party solves shows proof of work gets to add the block and collect the reward. When a miner solves the puzzle, it publishes the solution, the other miners verify it, and if they find it is correct, they stop processing the transactions which have been posted to the blockchain, and start on a new block. At any given time, the consensus blockchain is considered to be the chain that is the hardest to produce (most of the time, however not always, this is the chain with the most blocks).

b. **Block confirmation**. Given this gradual consensus mechanism, actors in a transaction cannot be immediately sure a transaction has been published. However, the more blocks have been published after a transaction, the likelihood of success increases exponentially. In practice, most Bitcoin clients require 6 confirmation blocks in order to accept that a transaction is published. For an average user, this means that it takes 1 hour (6 blocks x 10 min/block) for a Bitcoin based transaction to be considered complete.

c. **Incentivizing correct behavior**. The underlying requirement for the protocol to work is that the miners who solve these computational problems have a reason to do so. This incentive is provided in Bitcoin by giving a certain reward to each miner who adds a bloc. Because bitcoins can be exchanged for real currencies, miners have a way to make money, which is the reason why Bitcoin continues to exist. A consensus protocol always requires some sort of mechanism to incent the miners.

d. **Mining details**. The puzzle solved by miners is to find a block (consisting of a list of transactions, the hash of the previous block, a timestamp and version number, plus an arbitrary nonce value) whose SHA-256 hash is less than a target value. This target value is used to calibrate the difficulty of the puzzles, in such a way that it takes on average 10 minutes to solve these puzzles. These puzzles are randomized in such a way that each miner has a probability to collect the reward that is equal to their share of the computational power of all the miners. The difficulty is adjusted every 2016 blocks (or every two weeks) so as to maintain the 10 minutes' lag time between blocks.

e. **Mining rewards and fees.** Miners are compensated for their work in two ways: block rewards and transaction fees. Initially, each block created was compensated with 50BTC. The reward is halved every 210,000 blocks. At the time this paper is written, the reward is 12BTC per block. This structure means that in 2140 no new Bitcoins will be created, meaning the maximum number of bitcoins in circulation can be 21millions. Transaction fees are currently a very small portion of a miners' revenue stream (a few percentage points), but that's likely to increase as the rewards for new block creation drops.

f. **Mining pools.** The all-or-nothing nature of the block rewards means miners that function independently of other miners will have large sporadic payouts. In practice though, it is more convenient for miners to join mining pools so as to get smaller, frequent payouts, that more accurately match their expense schedule. Ultimately, pool members receive lower variation in revenue in exchange for a small fee paid to the pool manager. While pools present the perfect vehicle for cartel formation, and pools could easily reach the threshold needed to control the blockchain (51% of processing power), there are no incentives to do so. Mining pools get paid in bitcoin. If mining pools do something to jeopardize the well-being of the system, bitcoin prices in real currencies drop, so mining pool revenue drops.

3) Peer to Peer communication network. This is the third and least innovative component of Bitcoin. It is a de-centralized, ad-hoc peer to peer broadcast network, used to announce new transactions and proposed blocks.

   a. **Impact on consensus.** there are two reasons why the communication network impacts the design. First, the higher the latency between the discovery of a block and its receipt by all other nodes, the higher the probability of a temporary fork. Temporary fork reduce reliability in the system, so this was a direct factor in deciding on 10 minutes as the block creation time. Second, a malicious miner with significant resources might attempt to prioritize their own blocks, or might attempt to block certain transactions. A decentralized, low latency broadcast network helps the overall design of Bitcoin.

   b. **Network topology and discovery.** Any node who joins the network attempts to contact randomly other nodes (by default, each node sends 8 outgoing connections and is prepared to receive up to 125 incoming connections). Once a connection is established, peer nodes also communicate details about themselves, and receive details about other nodes' list of known addresses. This establishes a well-connected random network, which works great for distribution of information.

   c. **Communication protocol.** Bitcoin's communication is optimized in such a way to maximize transparency, and make the bitcoin network as resistant to censorship as possible. What this means is that nodes send messages to all of their peers, containing the hashes of new blocks AND pending transactions, whenever they first hear of them. There are a number of rules set up to optimize performance, as well as eliminate propagation of incorrect data, but otherwise the system is set up to be as transparent as possible. This is yet another example of a design choice that choses transparency over performance.

   d. **Relay policy.** Bitcoin nodes only relay transactions and blocks which satisfy validation rules that are stricter than typical transactions. The implications of this setting is that users of the system wishing to include non-standard transactions in the blockchain can do so only by contacting a miner that agrees to cooperate. This design choice was made with an eye towards defending the Bitcoin system from various types of denial of service attacks.

Without standard literature and with limited agreed upon documentation, this is only one of the ways in which one can look at Bitcoin. There are other ways, but the main benefit of this approach is that it allows for looking at various design choices individually, and evaluating each design choice on its own merit. An in-depth analysis on how to implement bitcoin shows what mattered to the author, and that is best described as "Social scalability"[18]. Social scalability is the ability of an institution to overcome shortcomings in human minds and in the motivating or constraining aspects of said institution that limit who or how many players can successfully participate. This refers to the human limitations, not to the technological limitations. The technical setup has some elements of novelty (key among those is the Satoshi consensus), but ultimately it is the consistent design choices maximizing transparency that allowed for Bitcoin's spread. The same design choices limit the scalability of the Bitcoin network as currently implemented. The network can indeed scale up, and there are various proposals to achieve that scalability, but that improved performance will be achieved at the expense of transparency, and to some extent security.

Ethereum

Ethereum has been introduced in 2013 by Vitalik Buterin, a Bitcoin developer advocating for introducing a more robust scripting language (remember, the Bitcoin scripting language has less than 200 commands, most of which are not used). After the white paper was introduced, development of the code was funded by a crowd-sale in July-August 2014, with the first live block on the Ethereum blockchain going live July 30 2014. Ethereum maintains many of the elements that made Bitcoin successful, yet it also adds a significant number of features and design choices that resemble a true evolution of the Bitcoin ecosystem. This paper will focus more on the differences, rather than the similarities, understanding though that Ethereum is a creation derived from Bitcoin.

1) Transactions and Scripts.

[18] Nick Szabo's comment on "Money, blockchains, and social scalability." Unenumerated blog, comment posted February 09, 2017, accessed February 14, 2017 http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html

a. **Transaction format.** One of the main design choices that differ from Bitcoin is the introduction of objects called accounts. The transfer of value and information is done via direct transfer between accounts. There are two type of accounts, either "externally owned accounts", controlled by users of Ethereum with private keys or "contract accounts", controlled by their contract code. The term contract in the Ethereum ecosystem is basically an execution of a piece of code triggered by specific messages or transactions. An additional important distinction is that between messages and transactions. At the core, they are the same thing, signed data packages containing a particular message. A message is similar to a transaction but differs in that it's produced by a contract as opposed to an external actor

b. **Transaction scripts.** One of the main differentiators of Ethereum is the addition of a Turing complete scripting language, as opposed to the Turing incomplete one present in Bitcoin. One example of functionality present in Ethereum is that of loops – allowing for much more flexibility in designing applications on top of Ethereum. Turing completeness means a computer language allows for replication of any real-world general purpose computer language. This one of the key components needed to create smart contracts, the feature mostly responsible for the spread of Ethereum.

c. **Conservation of value.** Transactions are considered valid if they have enough gas to pay for the transaction fees.

d. **From transactions to ownership.** Ownership is treated significantly different in Ethereum when compared to Bitcoin. Bitcoin stores user balances as the sum of all Unspent Transactions Output (UTXO), thus the available balances for a user is the combined set of coins for which a user can produce a valid signature. Ethereum is deploying an approach more similar to the design applicable to banking, where the state of the system stores a list of accounts, with each account having a balance (as well as some additional Ethereum data). Transactions are considered valid as long as an account has sufficient value in it to cover the transaction amount. This structure makes Ethereum more friendly to identity management services, such as Domain Name Systems (DNS).

2) Consensus and Mining. In this area too, Ethereum is introducing a number of new ideas compared to Bitcoin. The addition of universal Turing-complete scripting language is one of the major addition, and it has widespread ramifications throughout all Ethereum design choices. In Bitcoin, all transactions are equal in terms of computing power, and are not computation intensive. In Ethereum, transactions have different computing power needs. That lead to the introduction to the mandatory transaction fees in Ethereum (voluntary transaction fees as in Bitcoin would end up opening the door to various types of attacks). The fundamental unit of computation in Ethereum is called "gas", and it can only be purchased with ETH. That means every transaction in Ethereum will have a price, and more computation demanding transactions will be more expensive.

   a. **Consensus.** Ethereum uses a slightly different type of consensus than Bitcoin, namely a simplified version of the GHOST protocol (Greedy Heaviest Observed Subtree)[19]. The GHOST protocol was introduced as a solution to reducing block time in Bitcoin. It is still proof of work consensus. Blockchains are designed to have many miners competing to append blocks, so it's bound to happen that in some cases two different miners create valid blocks, and only one is added. The other one is called "stale" and in Bitcoin is not rewarded, and are quite rare, given the 10 minutes' block time. Reducing block time though increases dramatically the probability for stale blocks (Stale blocks are valid blocks propagated to the network, and verified by some nodes, that ultimately are set aside as a different longer chain emerges). Ethereum addresses the issue of stale blocks by including them the blockchain (calling them "uncles" in Ethereum jargon). These uncles do have lower coinbase rewards than other blocks, and do not receive any transaction fees. This protocol also reduces some (not all) of the incentives for mining as part of a pool.

   b. **Block confirmation.** The length of time between blocks in Bitcoin is currently 10 minutes, and that has not changed since inception. Ethereum has started with 12 seconds (currently 12.8 seconds).

[19] Yonatan Sompolinsky and Avir Zohar, "Accelerating Bitcoin's Transaction Processing, Fast Money Grows on Trees, Not Chains", Cryptology ePrint Archive, (2013), 18-22, accessed March 31, 2017. https://eprint.iacr.org/2013/881.pdf

c. **Incentivizing correct behavior.** A consensus protocol always needs some sort of mechanism to incent the miners, and Ethereum is no different. It is currently done similarly to Bitcoin, according to a Proof of Work method, but the Ethereum Foundation has announced its intention to move to a Proof of Stake method, which, if functional, addresses some of the criticism towards Bitcoin, its energy consumption. Ethereum miners are paid in one of three ways: 1) the coinbase transaction, where ETH is awarded for mining a block, 2) the reward for uncle blocks and 3) the transaction fees, calculated in gas.

d. **Mining details.** The same principles of mining apply to both Bitcoin and Ethereum. The differences come from the fact that miners now include uncle blocks. A stale block receives 87.5% of the coinbase reward, with the nephew that includes this uncle block in the blockchain receiving 12.5% of the coinbase reward. Transaction fees are not awarded to the uncle block. Miners also decide which transactions to prioritize in their blocks based on the gas amount that each transaction delivers.

e. **Mining rewards and fees.** As of now, Ethereum is issued in perpetuity, with the reward for each block being set at 5ETH. There is also a reward for introducing uncle blocks (1/8 of the standard reward – the other 7/8 goes to the miner who created the uncle block). Miners also receive the transaction fees, calculated in gas. The Ethereum foundation is also considering limiting the number of ether to be issued in the future, but at this time that has not yet happened.

f. **Mining pools.** The reasons to create mining pools are still there, although they are not as pronounced in Ethereum as in Bitcoin. The fact that blocks are created more often increases the likelihood of obtaining revenue on a daily basis. Even if not daily, it's a certainty that the frequency is lower than in Bitcoin.

3) <u>Peer to Peer communication network.</u> The communication network is very similar to Bitcoin. It is a de-centralized, ad-hoc peer to peer broadcast network, used to announce new transactions and proposed blocks.

Ripple

Ripple's solution is built around an open protocol called Interledger. It is made up of independent and diverse ledgers linked by connectors. Each account "on the Interledger" is part of a particular ledger, but they may transact with others by sending Interledger payments through different ledgers and connectors. Interledger is not a single network, but a collection of interconnected networks. Interledger uses conditional transfers[20] to allow senders to receive cryptographic proof that the receiver got the payment, or a guarantee that senders receive their money back. Conditional transfers are the equivalent of a payment process called Authorization Hold, or the database technique called two-phase commit. Ripple (previously named OpenCoin, then Ripple Labs) is the main developer of the Ripple protocol. While Ripple the protocol is considered an open source protocol, Ripple the company is a for profit entity, offering solutions such as remittances and payments to banks, merchants and private exchanges. For simplicity, Ripple the company is for Ripple the protocol what Red Hat is for Linux – a company that sells for profit a particular implementation of an open source software.

How does Ripple work? Ripple per se is not really a blockchain (notably, the white paper that introduces the Ripple Protocol Consensus Algorithm (RPCA) does not mention blockchain), but it is a distributed ledger that makes use of very similar terms as Bitcoin. The role of the miners is now played by servers, who host and run the Ripple server software, and participate in the consensus mechanism. Ripple the company maintains and publishes a list of trusted servers which run the consensus. New transactions are added to the Ripple ledger every few seconds, creating a state of the system called Last Closed Ledger. There are no blocks, but there are cryptographic signatures that link transactions with the node that initiated those transactions.

1) Transactions and Scripts
   a. **Transaction format.** The Ripple network stores information in accounts, and moving value is done via transactions. The RPCA is closing the ledger every few seconds, and keeps adding transactions that the servers agree upon. Newly created ledgers include the state of the system (similar to Ethereum), although the full history is not stored on all servers. There are multiple types of transactions within Ripple, allowing for transfers in either fiat money (USD, EUR, RMB, etc.) or cryptocurrency (XRP)
   b. **Transaction scripts.** There are no transaction scripts in Ripple.

[20] Interledger.org, "Interledger Architecture", accessed Apr 21, 2017. https://interledger.org/rfcs/0001-interledger-architecture/

c. **Conservation of value.** Candidate transactions in Ripple can fail for a number of reasons, such as transactions not providing enough fees to cover the base fee. The concept of transaction fees is native to RPCA, and each transaction comes with a fee, computed in XRP. The XRP allocated to a transaction is not considered revenue for the servers though, it is instead destroyed. To some extent, the amount of XRP in circulation keeps decreasing, but that's likely to become an issue in the next century, and given amazing success.

d. **From transactions to ownership.** Ripple introduces the concept of Gateways, which are existing businesses that are subject to KYC/AML regulations, so establishing provenience of transactions is possible. These gateways can act in one of three ways: issuers, merchants and private exchanges.

2) Consensus and Mining.

a. **Ripple Protocol Consensus Algorithm (RPCA)**. The white paper introducing the RPCA in its current iteration has been published in 2014. The consensus algorithm is applied every few seconds by all nodes to maintain correctness on the network. Once consensus is reached, the current ledger is considered "closed" and becomes the last-closed ledger. The RPCA is applied in rounds with ever increasing approval rates. The final round of consensus requires 80% of a server's Unique Nodes List (UNL) to agree on a transaction. Basically, as long as 80% of the UNL is honest, no fraudulent transaction can be included in the ledger.

b. **Block confirmation**. in the Ripple network, there are no blocks. Transactions are grouped in candidate sets, which are then subject to consensus, which is run every few seconds (based on conversations with the Ripple team, at the time of this paper, this period is between 3 and 5 seconds).

c. **Incentivizing correct behavior**. The servers on the Unique Nodes List (UNL) are all maintained by Ripple currently. When looking for a set of validators, a server downloading the Ripple server by default looks to the UNL. However, servers do have the choice to deviate from the default. With UNL being maintained by Ripple, incentivizing correct behavior is not a problem.

d. **Mining details**. Mining as proposed by Bitcoin and Ethereum does not exist in Ripple. This role is played by servers, who are of two types: the validators, who do the computational work, and only maintain a portion of the ledger, typically one month, and generic stock servers that maintain the full history.

e. **Mining rewards and fees.** The Ripple network implemented transaction fees as a defense from spam, or other types of attacks such as Distributed Denial of Service (DDOS) or Sybill attacks. Transactions fees are not source of revenues for servers – and all of the ripples used during a transaction are destroyed. Each transaction has a reserve minimum (20XRP currently), and a cost that changes depending on network congestion.

f. **Mining pools.** This is not an issue in Ripple, as there are no miners.

3) <u>Peer to Peer communication network.</u> There is a communication network in Ripple, although it is not as important to the wellbeing of the ecosystem as in other public ledgers.

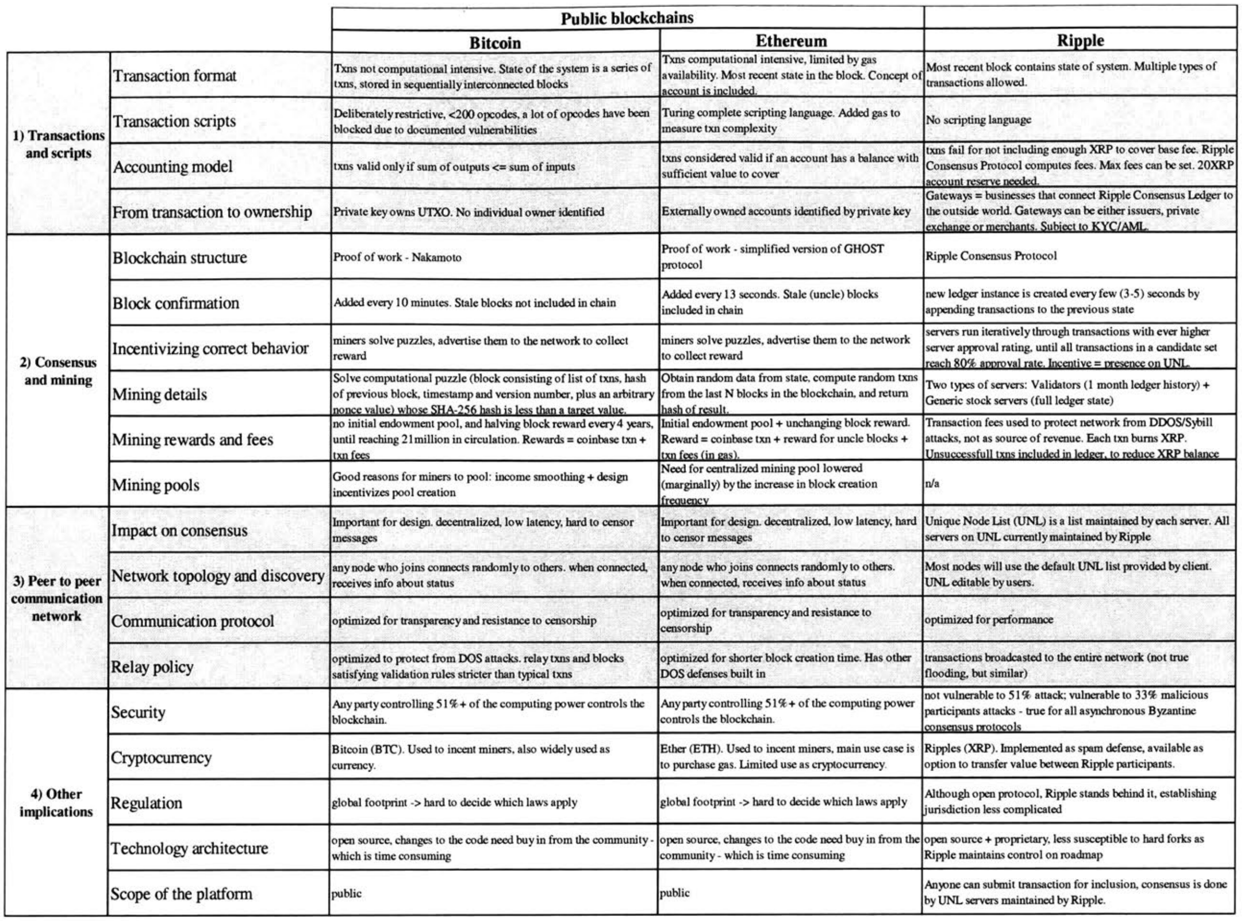
   a. **Impact on consensus.** The Unique Node List (UNL) is a list maintained by each server. All servers on the UNL are currently maintained by Ripple, although that can change at any time.

   b. **Network topology and discovery.** Most nodes will use the default UNL list provided by client software, although the list of validators can be edited by users.

   c. **Communication protocol.** New blocks and pending transactions are broadcasted to the entire network by a technique similar to flooding.

   d. **Relay policy.** Most decisions in Ripple with regards to the relay policy are made with an eye towards defending the network from spam or other types of attacks.

A framework to compare blockchains



		Public blockchains		
		Bitcoin	Ethereum	Ripple
1) Transactions and scripts	Transaction format	Txns not computational intensive. State of the system is a series of txns, stored in sequentially interconnected blocks	Txns computational intensive, limited by gas availability. Most recent state in the block. Concept of account is included.	Most recent block contains state of system. Multiple types of transactions allowed.
	Transaction scripts	Deliberately restrictive, <200 opcodes, a lot of opcodes have been blocked due to documented vulnerabilities	Turing complete scripting language. Added gas to measure txn complexity	No scripting language
	Accounting model	txns valid only if sum of outputs <= sum of inputs	txns considered valid if an account has a balance with sufficient value to cover	txns fail for not including enough XRP to cover base fee. Ripple Consensus Protocol computes fees. Max fees can be set. 20XRP account reserve needed.
	From transaction to ownership	Private key owns UTXO. No individual owner identified	Externally owned accounts identified by private key	Gateways = businesses that connect Ripple Consensus Ledger to the outside world. Gateways can be either issuers, private exchange or merchants. Subject to KYC/AML.
2) Consensus and mining	Blockchain structure	Proof of work - Nakamoto	Proof of work - simplified version of GHOST protocol	Ripple Consensus Protocol
	Block confirmation	Added every 10 minutes. Stale blocks not included in chain	Added every 13 seconds. Stale (uncle) blocks included in chain	new ledger instance is created every few (3-5) seconds by appending transactions to the previous state
	Incentivizing correct behavior	miners solve puzzles, advertise them to the network to collect reward	miners solve puzzles, advertise them to the network to collect reward	servers run iteratively through transactions with ever higher server approval rating, until all transactions in a candidate set reach 80% approval rate. Incentive = presence on UNL.
	Mining details	Solve computational puzzle (block consisting of list of txns, hash of previous block, timestamp and version number, plus an arbitrary nonce value) whose SHA-256 hash is less than a target value.	Obtain random data from state, compute random txns from the last N blocks in the blockchain, and return hash of result.	Two types of servers: Validators (1 month ledger history) + Generic stock servers (full ledger state)
	Mining rewards and fees	no initial endowment pool, and halving block reward every 4 years, until reaching 21million in circulation. Rewards = coinbase txn + txn fees	Initial endowment pool + unchanging block reward. Reward = coinbase txn + reward for uncle blocks + txn fees (in gas).	Transaction fees used to protect network from DDOS/Sybill attacks, not as source of revenue. Each txn burns XRP. Unsuccessfull txns included in ledger, to reduce XRP balance
	Mining pools	Good reasons for miners to pool: income smoothing + design incentivizes pool creation	Need for centralized mining pool lowered (marginally) by the increase in block creation frequency	n/a
3) Peer to peer communication network	Impact on consensus	Important for design. decentralized, low latency, hard to censor messages	Important for design. decentralized, low latency, hard to censor messages	Unique Node List (UNL) is a list maintained by each server. All servers on UNL currently maintained by Ripple
	Network topology and discovery	any node who joins connects randomly to others. when connected, receives info about status	any node who joins connects randomly to others. when connected, receives info about status	Most nodes will use the default UNL list provided by client. UNL editable by users.
	Communication protocol	optimized for transparency and resistance to censorship	optimized for transparency and resistance to censorship	optimized for performance
	Relay policy	optimized to protect from DOS attacks. relay txns and blocks satisfying validation rules stricter than typical txns	optimized for shorter block creation time. Has other DOS defenses built in	transactions broadcasted to the entire network (not true flooding, but similar)
4) Other implications	Security	Any party controlling 51%+ of the computing power controls the blockchain.	Any party controlling 51%+ of the computing power controls the blockchain.	not vulnerable to 51% attack; vulnerable to 33% malicious participants attacks - true for all asynchronous Byzantine consensus protocols
	Cryptocurrency	Bitcoin (BTC). Used to incent miners, also widely used as currency.	Ether (ETH). Used to incent miners, main use case is to purchase gas. Limited use as cryptocurrency.	Ripples (XRP). Implemented as spam defense, available as option to transfer value between Ripple participants.
	Regulation	global footprint -> hard to decide which laws apply	global footprint -> hard to decide which laws apply	Although open protocol, Ripple stands behind it, establishing jurisdiction less complicated
	Technology architecture	open source, changes to the code need buy in from the community - which is time consuming	open source, changes to the code need buy in from the community - which is time consuming	open source + proprietary, less susceptible to hard forks as Ripple maintains control on roadmap
	Scope of the platform	public	public	Anyone can submit transaction for inclusion, consensus is done by UNL servers maintained by Ripple.

Table 2.1 – Comparison of the top 3 cryptocurrencies

Blockchain as foundation for financial services

Description

A blockchain, as the name implies, is a chain of blocks, with each block containing a set of transaction records, together with their attributes. From a technological point of view, blockchain is a technology for shared databases, and a good amount of features built into blockchains are also available for other types of databases. While Satoshi Nakamoto designed and implemented the Bitcoin blockchain to maximize for social scalability, the trade-offs made led to low computational efficiency and even lower scalability in consumption of resources. This opened the door for others to start making changes to each of the design parameters described above for Bitcoin, Ethereum and Ripple. Industry interest came from a lot of varied verticals (a study by

Goldman Sacks identified strong use cases for sharing economy, distributed smart grids, real estate title insurance and AML/KYC compliance in addition to capital markets[21]). The interest was particularly strong coming from the Financial Services industry, as a number of factors converged:

- Bitcoin's potential as a digital currency is particularly interesting for banks. The emergence of such a currency would fundamentally alter the existing business model for banks, so there are certainly strategic implications to this interest.
- New regulations post 2008 crisis meant significant changes to the banks' technical infrastructure, meaning technology is changing in banks at a high pace. Banks have also slowly started to have very sizeable IT departments, which means very large IT budgets that can be reduced by cost-savings technologies, such as blockchain.
- At a more fundamental level, ledgers for financial assets (which is what banks do) are the most natural fit for shared databases with interdependent transactions created by non-trusting entities (which is what blockchains do).

In other words, banks do not need to look very far to recognize value from implementing blockchains – those cost savings are sufficient to raise interest internally.

What is special about this technology?

The reason why so many participants across many industries have become so interested in blockchain technology is that the technology made popular by Bitcoin exhibits characteristics found in general purpose technologies. Richard Lipsey[22] and other authors of the late 90s identified the following four criteria to single out transformative general purpose technologies:

1. It is a single, recognizable generic technology.
2. Initially has much scope for improvement but comes to be widely used across the economy
3. Has many different uses
4. Creates many spillover effects

[21] James Schneider et al., "Profiles in Innovation, Putting theory to Practice: Blockchain", *The Goldman Sacks Group Inc.,* (2016). http://www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf

[22] Richard G. Lipsey, Kenneth I. Carlaw, and Clifford T. Bekar, "Economic Transformations: General Purpose Technologies and Long Term Economic Growth", (Oxford University Press, 2006).

Blockchain technology appears to match the criteria, and join other key technological advancements that have left an imprint on human development, such as Computers, Internet and Artificial Intelligence. It is not yet clear that blockchains will become as transformational as the Internet, but even the promise is enough to warrant the attention it is receiving. With regards to what exactly makes blockchains special, the following is a list of the most important traits:

1. **Shared ledgers that store transactions between parties** – this means a shared repository of information, used by multiple parties, meaning blockchains are a database
2. **Allow multiple writers to record transactions** – transactions can be recorded by anyone, using pseudonyms – which appeals to individuals who value privacy.
3. **Remove the need for participants to trust each other** – the default state in the largest blockchain is that no trust is needed from users – the system is designed by deploying cryptographic principles in such a way to not need trusted participants
4. **Decentralized** – each participant can freely store a copy of the entire database, and it does not need a gate-keeper to confirm any information stored in the blockchain.
5. **They allow for transaction dependencies** – transactions in blockchains can interact with each other. This means transactions created by different writers often depend on one another. An example illustrating this is: imagine Alice needs to send funds to Bob, then Bob needs to send funds to Charlie. Bob's transaction is dependent on Alice's transaction, and one cannot verify Bob's transaction without checking Alice's first.
6. **Transactions are recorded securely and identifiably according to logic transparent to all participants** – each transaction is timestamped and written in a blockchain after being verified for accuracy. This basically makes blockchains large audit trails that cannot be changed – they are immutable, or better said, they are extremely expensive to change. In theory, it is possible to change even public blockchains, but in practice it has not been proven yet – the cost is considered prohibitive.
7. **Validation of transactions can be made by parties that do not need to be individually trusted.** Establishing trust on the internet is expensive, so blockchains are designed in a way to not need transaction verifiers to be trusted. This is one of the main appeals of Bitcoin, that it is a Common Trusted Party, and that it can be accessed by anyone. The importance of this Bitcoin characteristic is hard to overstate.

8. **Considered tamper proof** – with copies of the blockchain scattered all over the world, and with all transactions time stamped, and unchangeable, records stored in blockchains are considered sources of truth. As mentioned before, they are not impossible to change, but doing so would be extremely difficult.

In addition to these traits, blockchain technology has one more characteristic that is common to the Internet – it enables permisionless innovation. This means any party can start writing applications to solve for particular use cases, without needing anyone's permission – which is a great enabler for innovators.

What aspects of financial inclusion can this technology improve?

At the highest level, technologies create value for consumers in one of two ways, they either improve the end-user experience, or they save money in the value chain. Blockchain technologies stand to bring considerable value to consumers by eliminating costs from the value chain offering financial services to consumers. There are other types of improvements available, most notably reducing time between transactions – a customer demand that has been long ignored, but ultimately the bulk of the value is going to be extracted by eliminating costs from the value chain of delivering bank-like services at a fraction of the cost – or better yet, as this paper will show in a subsequent chapter, blockchain technology makes it possible for financial institutions to offer bank accounts at no cost to the consumer. There are experiments where this has been tried by various players in small scale implementations, but typically that's been done by subsidizing certain products with profits from other products (e.g. offer no-cost checking for bundling accounts to reach a certain amount of assets under management for a typical bank). Chase was one of the first large banks to exit the prepaid market in 2014, followed by other players such as Citi in 2016. The underlying reason is high costs to offering services to customers who do not move enough money to allow banks to make profits. In their paper "Some simple economics of the blockchain", Christian Catalini[23] and Joshua Gans address two large categories of costs:

1. **Cost of networking**. This pertains to the costs of linking the entity that holds the funds to the entity that receives the funds, in exchange for products or services

[23] Christian Catalini and Joshua Gans, "Some simple economics of the blockchain", *The National Bureau of Economic Research*, working paper number 22952, 2016

2. **Cost of verification**. The established ecosystem today has a verification system in place that is expensive, and takes time (payment networks verify availability of funds almost instantaneously, but the movement of funds is done typically 1-3 days later).

Digital currencies such as Bitcoin have shown the way in which money can move much faster – in hours, not days. Building on these findings, advancements in blockchain technology, as well as other adjacent technologies (such as digital identities) will offer banks the tools to offer better products to their customers, at lower costs. As detailed in the Financial Inclusion chapter blockchain technology will not address all of the issues that that cause certain aspects of the population to be excluded from the financial system. It will however address the most important factor, costs, by reducing the number of participants in the value chain and by making the operations of the existing players more efficient.

Public vs. permissioned vs. private blockchains

Public blockchains: This was the first use case of blockchain, Bitcoin. The second blockchain, by market cap, Ethereum, is also a public blockchain. Public blockchains assume very low trust amongst categories of users and they have the following characteristics:

- Anyone in the world can read this blockchain
- Anyone in the world can propose transactions to the blockchain, and expect to have them added to the blockchain if they meet certain criteria for inclusion
- Anyone in the world can participate in the consensus process

Permissioned (also called Consortium) blockchains: These types of blockchains mean that the consensus process is decided by a pre-selected set of nodes – which also leads to the inherently higher degree of trust required amongst the participants. Read permissions may be public, or restricted to certain participants. It is also possible to have a mixed set of permissions, where the root hashes of the blocks are made public together with an API that allows members of the public to make a limited number of inquiries, and get back cryptographic proof of parts of the blockchain state – and these are called "partially decentralized" blockchains.

Private blockchains: These are the blockchains that have a central point of control that controls the consensus process and write permissions. Read permissions may be granted as deemed necessary by the central point of control – which leads to the high degree of trust needed for this application. However, the main value of using a blockchain-type database versus a regular database is having cryptographic authentication. How the cryptographic authentication is done, whether it's via a series of hash-linked data packets containing Merkle tree roots or some other method (e.g. Zero knowledge proofs) is a choice entirely under the central authority's control.

The arguments for public blockchains to be the superior choice are made around:

1. **Network effects**, either of the direct variety (users are better off the more users accept the token issued by a certain blockchain) and of the indirect variety (merchants are better off the more users pay with a certain currency)
2. **Permisionless innovation,** in that this approach is better suited to harness the widely recognized value brought by the open source community.
3. **Social scalability,** the fact that public blockchains are not bound to a particular jurisdiction makes them easier to scale, and thus access the network effects that come with scale.

The arguments for permissioned blockchains fall into the following categories:

1. **Governance**, meaning that rules can be adjusted when legislation changes, or in some case where the original design ignored a certain rarely encountered event
2. **Known validators,** which reduces risks for 51% attacks – considered to be the main risk for public blockchains, especially in a scenario where mining is heavily concentrated
3. **Cheaper transactions,** because transactions and computations do not need to be done by all nodes, but only by a subset of nodes. In their current form, public blockchains have material scalability concerns – although that might change as technology improves.
4. **Privacy,** because unlike public blockchains, permissioned ones allow for multiple level of access to the information.

The answer to which type of blockchain is better is that it depends on the use case. We do not need to have only one global blockchain, instead it is more likely that specialized blockchains will co-exist. The good news is that there already are technical solutions to allow for collaboration across chains. Use cases will drive the type of blockchains needed, and that is one of the great strengths of this technology, and why it stands a chance to be one of the very few general purpose technologies human kind ever developed[24] (less than thirty such technologies).

Should firms build on a Bitcoin foundation, or not?

As mentioned above, when companies consider what technology solution fits their needs best, they should consider all types of blockchains, not just the Bitcoin one. Given all of the momentum that blockchain technology is experiencing, and to some extent the miss-understanding of what use cases are best addressed by blockchains, it is also important to assess whether blockchain technology really is the best solution for a particular need (and for this purpose, the following framework may prove valuable[25]).

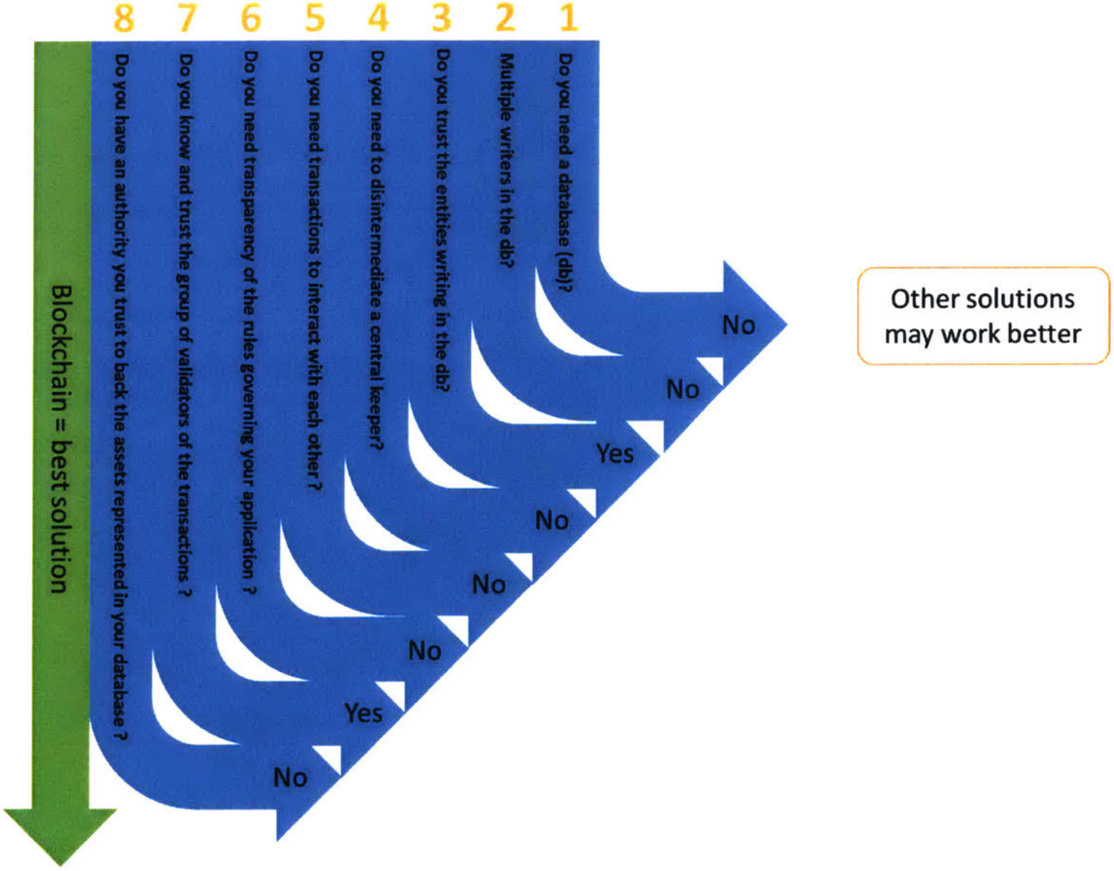

8
7
6
5
4
3
2
1
Do you need a database (db)?
Multiple writers in the db?
Do you trust the entities writing in the db?
Do you need to disintermediate a central keeper?
Do you need transactions to interact with each other?
Do you need transparency of the rules governing your application ?
Do you know and trust the group of validators of the transactions ?
Do you have an authority you trust to back the assets represented in your database ?
No
No
Yes
No
No
No
Yes
No
Other solutions may work better
Blockchain = best solution

Table 3.1 – What are the use cases for which blockchain is the best solution?

[24] Lipsey, Richard; Kenneth I. Carlaw; Clifford T. Bekhar (2005). Economic Transformations: General Purpose Technologies and Long Term Economic Growth. Oxford University Press. pp. 131–218

[25] Gideon Greenspan's comment on "Avoiding the pointless blockchain project" Multichain.com, comment posted November 22, 2015, accessed March 23, 2017
http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

From a technological point of view, Bitcoin is very solid – it's been running continuously since 2009, and while it has had issues, the community of developers that maintains it is by far the strongest available in the blockchain ecosystem, and it always addresses issues as they arise. However, there are significant topics to consider when building a long term business on a Bitcoin foundation.

1. **Regulatory aspects.** It is important to remember that Bitcoin does not belong to any jurisdiction. Its nodes are spread across the globe, its miners, although concentrated in China, have presences all over the globe. The Bitcoin Core team members certainly fall under countries' jurisdiction, yet they do not have power over the ultimate direction of the code. Bitcoin is designed to be censorship resistant, so even if a country were to try to ban it, there is no easy way to do it. deciding to incorporate Bitcoin into a solution then becomes a trade-off: benefit from all of the capabilities and innovation it fosters, versus foregoing control over the direction in which the platform is going, and potentially becoming a target for government looking to stop Bitcoin's use.
2. **Technical aspects.** At the time this paper is written, a Bitcoin fork is a very real possibility, but it has not yet happened. Ethereum has experienced a hard fork in 2016, as a result of the DAO attack, and it certainly has not stopped it from reaching all-time highs as recent as March 2017. This type of events causes major expenses for large financial institutions. Additionally, the scalability issues that are well documented for Bitcoin (and other public blockchains) are not yet solved. There are proposed solutions, of which the Lightning network appears to be most promising, yet they are not yet implemented.
3. **Strategic aspect.** Bitcoin, and all of the other public blockchains have a particular vulnerability to a 51% attack (also called a Goldfinger attack), in which either one entity, or a number of entities acting together take over the blockchain, and make it essentially unusable. A simple calculation illustrates that as of March 28 2017, the Bitcoin Hash rate (the combined processing power of the Bitcoin network) is 3,601,565,858 GH/s. One of the most popular mining equipment, the Antminer S9, retails on Amazon for $2,319[26], and has a hash rate of 13.5TH/s or 13,500 GH/s. That means the retail value of the equipment processing all of Bitcoin is about $619million. Reaching 51% of the hash rate

[26] Amazon.com, Antminer S9 ~13.5TH/s @ .098W/GH 16nm ASIC Bitcoin Miner, price as of March 28, 2016.

is not easy, but the amount involves is also not something to scare away state actors. This suggests that the Bitcoin network is just not designed to become a single digital currency network to replace nation states currencies.

These are significant challenges, which combined indicate to why the leading financial institutions in the world are opting for a permissioned blockchain model. One has to consider that a permissioned blockchain that is modeled off of Ethereum, and which maintains compatibility with Ethereum would solve for a lot of the problems encountered by public blockchains, while benefiting from the innovation and to some extent network effects deriving from using Ether as digital currency. Incidentally, this is the direction taken by Microsoft, with its offering of Blockchain as a Service on the Azure cloud platform.

However, all the permissioned blockchains achieve consensus by deploying protocols that do not include mining. Critics of Proof of Work protocols deploy other types of consensus protocols, such as Byzantine Fault Tolerance (BFT). This is not necessarily new technology (BFT protocols became available in late 90's), and unlike the tested Proof of Work, it is unclear how well these protocols could withstand attacks.

How does a Blockchain-based business model look?

How does the banking model look today?

Today's banks have evolved into large multi-national entities that provide a multitude of services to both individuals and businesses. In the US, after the Great Depression, the Glass-Steagall act of 1933 established two types of banks: Commercial banks and Investment banks. Banks generate revenues from services offered to consumers (this is where most retail banks are focusing on) and businesses (where merchant/investment banks are focusing on). The category of banking that is most relevant for increasing financial inclusion is retail banking (also known as consumer banking), and credit unions. These two types of banks focus extensively on offering bank accounts, and one of the major aspects of their activity is moving money (making payments) as instructed by their cardholders. From a banking perspective, most type of payments are of the open loop variety. Open loop payment instruments refer to funds can be spent anywhere a particular cardholder decides – and that applies across multiple merchants. Open loop payment instruments are typically branded Visa/MasterCard/Discover/American Express in the US[27]. There are other smaller networks, but these account for the vast majority of transactions. Visa is the distant predominant entity. Open loop instruments are divided into three main categories: Debit cards, Credit cards, and charge cards. Debit cards act as vehicles for spending money owned by an individual. Credit cards serve the same purpose, with the added benefit that the issuing bank provides credit up to a certain limit that is dependent on a customer's credit worthiness. The customer typically enjoys a 20-day window to pay the balance due, and in case the consumer pays less than the full balance, interest is charged on the outstanding balance. Charge cards work very similarly to credit cards, with the added twist that balances have to be repaid in full – there is no option to pay less than the full amount.

The vast majority of open loop electronic payments in the US are set up to involve four major players (in addition to the cardholder):

1. **Merchants**. These are sellers of goods/services. Their main interest is to sell to as broad an audience as possible. The merchants contract with an acquirer/processor, and pay discount fees for accepting electronic payments. This discount fee includes interchange, network fees and the acquirer's profit margin. Merchants see discount fees as costs, and are actively looking for ways to reduce them, either by accepting lower cost means of payments, or by forcing the hands of other players in the value chain to reduce their margins. The relationship between merchants and payments brands is notoriously contentious.
2. **Acquirer/Processor** (Merchant's bank) These are either third party technology companies (First Data, Vantiv) or large banks (JP Morgan Chase, Bank of America) who act on behalf of the merchant in order to process electronic transactions. This is a highly competitive business, where banks have an advantage given the depth of the business relationship with the merchants. A portion of the discount fee (typically between 10% and 15%) is paid to the acquirer processor. First Data (20%), Vantiv (19%), Chase Commerce Solutions (16%), Bank of America (16%) and Heartland (4%) ranked as the top 5 acquirers in the US in 2015[28], accounting for 75% of the purchases in the US.

[27] There is another significant type of payments, called closed loop payments, meaning funds can only be used within the locations of one particular merchant (also called issuer). For the purpose of this paper, these types of payments are considered out of scope.

[28] "Top Acquirers in the US 2015", *The Nilson Report*, issue 1082 (2016): 10-11

3. **Payments brand:** With regards to payments brand, the instrument that addresses directly the need to make electronic payments is the debit card, that is the instrument that has the least amount of risk from a bank's perspective. The modern debit card has a history that is intertwined with Visa, the network that made the existing model popular. Visa was started by Bank of America, who ultimately allowed all other banks to join the network as issuers, and as co-owners. Visa became a publicly owned entity in 2008, with what was the largest IPO in the world at that point in time, raising just over $19billion. Although Visa is the predominant[29] player in the payments space, MasterCard, Discover and American Express perform largely similar functions – the difference is in how widely accepted each network is used, and by how many users.
    1. Visa currently works as a network, although it originally started as part of Bank of America. It does not issue its own cards, and it monetizes by charging a small fee per each transaction to both issuing banks and merchants for using its network. Visa publishes interchange rates that apply to all merchants. Direct deals with merchants to offer better than published interchange rates (i.e. cheaper transactions) are very rare, and reserved to only the largest merchants. In the US, Visa is the market leader in terms of card issuance (*47% as of 2015*).
    2. MasterCard works very similarly to Visa, partly because of their common bank-driven heritage – MasterCard was Wells Fargo's answer to Bank of America's Visa. It had an IPO in 2006, and in the US it is the second largest player in terms of issuance (*21% as of 2015*).
    3. American Express is different from both Visa and MasterCard in that it also issues its own cards. Until 2004, Visa and MasterCard had rules in place that prohibited their issuing partners to also issue American Express cards, although that is no longer applicable. American Express is also known for their strategy to charge higher fees to merchants and return more rewards to its cardholders. The downside to that approach is that a lot of merchants, particularly the smaller ones, do not accept American Express. American Express does not publish its interchange rates, and it is the third player with regards to issuance (*12% as of 2015*)

[29] "U.S. Payment Cards Purchase Volume 2010 – 2020", *The Nilson Report*, issue 1097, (2016): 8

4. Discover is the also issuing its own cards, and also does not publish its interchange rates. It is a network that. It has positioned itself as a more merchant-friendly network, which in turn reduces the incentives for issuers to work with it, which is a main factor in its low issuing volume (*2% as of 2015*).

These four entities control 80%+ of the purchases in the USA, with Visa being larger than all the three others combined. Payments brands collect small fees from both merchants and issuers, and are the most profitable entities in this value chain.

4. **Issuer (cardholder's bank).** Issuing banks collect the large majority of the discount fee charged to the merchants, in the form of interchange. Interchange is established by the payment networks, but it is actually paid to the issuing banks, to cover for their expenses of issuing cards. A detailed explanation of the issuing ecosystem to follow here. Here too, the top issuers are the top banks, with American Express, JP Morgan Chase, Bank of America and Citi are the top issuers. One key item here is that in order to issue accounts, an entity has to be classified as a bank. Prepaid card providers, the alternative services most closely addressing the needs of the underbanked are either explicitly a bank (Green Dot) or partner very closely with one (Money Network, Netspend). This is a highly regulated activity, and a lot of scrutiny is placed upon these banks. An issuer maintains an issuing platform, that interacts with all of the other external providers that result in products and features available to cardholders.

Example of an issuing ecosystem:

Below is an attempt to model what an issuing bank ecosystem looks like. Banks act like platforms, onto which other third party providers offer services. This adds features, yet it also adds costs, and complexity. It also shows one of the significant barriers to adoption for blockchains. It takes for a lot of determination, and resources, from a bank to convince all of the partners enabling their ecosystem to be blockchain compatible, and to do so with very limited interruptions in service.

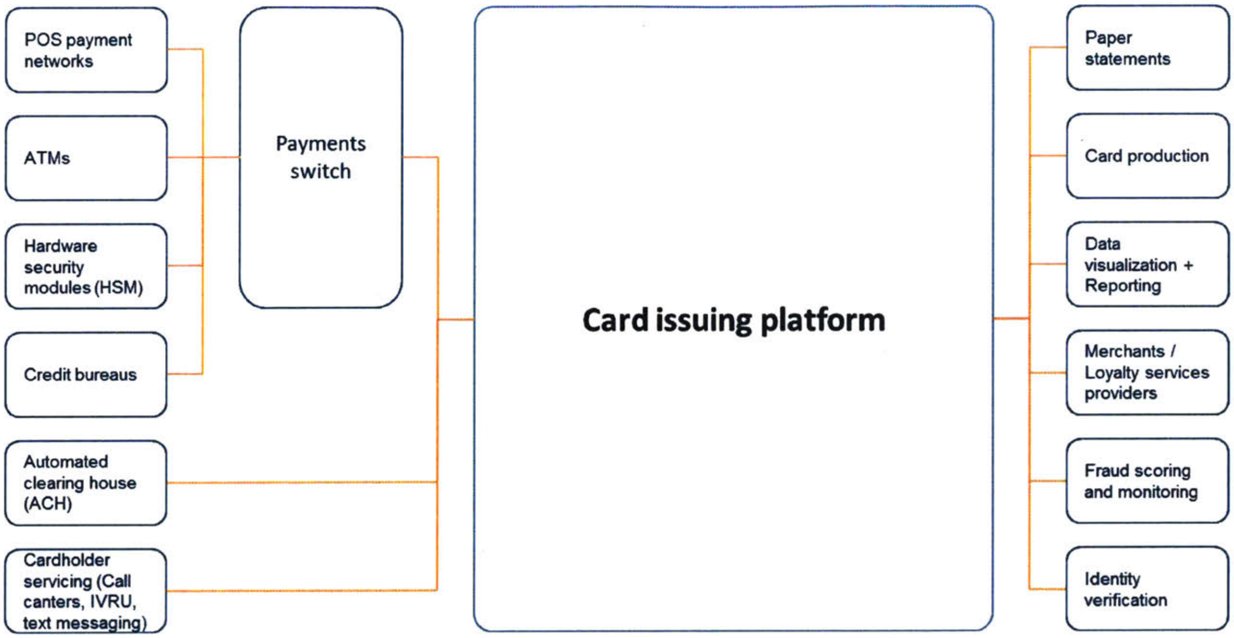

POS payment networks
ATMs
Hardware security modules (HSM)
Credit bureaus
Automated clearing house (ACH)
Cardholder servicing (Call canters, IVRU, text messaging)
Payments switch
Card issuing platform
Paper statements
Card production
Data visualization + Reporting
Merchants / Loyalty services providers
Fraud scoring and monitoring
Identity verification

Table 4.1 – Issuing bank ecosystem

Limitations of existing model

The current model has had a lot of success, truly making a dent into the use of cash in the US economy since its introductions. However, it is not a perfect system, and some of its flaws are shown below:

1) **Fraud**. The system as it is established today is very susceptible to fraud. Each key constituent is a potential point of failure, and over time, breaches have happened at all levels, although the payment networks are probably the safest component. The industry saying goes that large stores of data are divided in those that know they've been breached, and those that do not yet know. While it is impossible to know whether that is factually correct, the reality is there is some truth to that. Top breaches happened at all levels: merchants (eBay, Target, Home Depot), acquirers/processors (Heartland Payment Systems, Global Payment Systems), payment networks (Discover), banks (JPMorgan Chase, Citibank). Of course, identity theft is the largest growing crime in the 21st century, and most paths lead to the system design that allows for major data repositories to exist in the first place. The industry has recognized this problem, and it has instituted certain defense mechanisms (tokenization, PCI-DSS), but the payment system as designed today has a certain amount of fraud expense built in. Most recently, the Dodd-

Frank's Durbin amendment had shed some light on the topic, and for every transaction in the US, 5BPS (0.05%) of the ticket size is considered as expense dedicated to covering fraud expenses.

2) **Costs**. This is a complex system to run, and in addition to multiple points of failure, this translates to expenses. Merchant discount fees, paid originally by merchants, are included in the markup applied to the products sold to the consumers. Banks on the other hand, need to cover their costs, and that is why they charge a host of fees that consumers have to pay. In one way or the other, the costs accumulate to the consumer.
3) **Concentration risk**. The business model for payments is as such that it has high fixed costs, and low variable costs, which means that scale constitutes a large advantage. Excluding merchants, concentration exists at all levels in the system, and that makes this system inflexible and vulnerable. Rolling out EMV (a technical standard for cards and POS devices that accept them, which enhances transaction security) has been an example of how difficult it is to drive change even when all parties agree that it is the right thing to do over the long run. Issues with any one of the large players into the system would translate to severe impacts to the US economy overall.
4) **Privileged position of the payment networks**. Through a combination of business model (multisided platform, benefiting extensively from network effects), strong execution and the power to set the rules governing the entire system, payment networks are in a key position within this ecosystem. While imperfect, they have proven to be good stewards throughout their existence, but the risk still remains. One dynamic in the industry now is that VISA, as the largest player, also has the deepest pockets, and that translates to better market share.
5) **Lack of anonymity.** Participating in the financial system means losing some level of privacy. Invariably, being part of the system means a set of tradeoffs between functionality and privacy. This debate has been going on for the past two decades, since the rise of the Internet, and consumers are willing to sacrifice more and more privacy for better services, but there are still segments of the economy where participants prefer the anonymity of cash. To great extent, the design of Bitcoin has been influenced by this problem.

6) **Difficulty handling international transactions.** Some products, although not all, do allow for international transactions, yet the experience is very limited, and it is expensive. First, the issuing bank needs to enable these transactions, and be comfortable that these transactions won't be reversed in the future (thus reducing issuer's profitability). Second it requires cross-border traffic, which means different settlement times, different currencies, and sometimes different types of transactions processing rules.

Envisioning a blockchain based model

Banking is a highly regulated space, and risk aversion is deeply embedded in all banks' culture, regardless of geography or size. After the 2008 Great Recession, where most banks' weaknesses have been exposed, regulations have increased dramatically, and that resulted in costs increasing further. Additionally, the banking industry has been consolidating consistently over the past three decades, and the trend accelerated following 2008. Between these two macro trends, and the increasing number of engineers employed by banks, the claims of cost reductions and operational efficiencies claimed by blockchain technology have been very well received, resulting in almost any bank having some sort of project to understand blockchain technology. If banks are uncertain if they want to investigate the technology by themselves, they join one of the blockchain consortia announced in the past two years. Most notably, R3, Hyperledger and Enterprise Ethereum Alliance have participation from global banks, technology companies and other interested parties. However, most banks currently working on blockchains are doing so in Innovation Labs, via investments in startups, or in pilots deployed by particular groups. A recent study done by Deloitte, a consultancy, mentions 12%[30] of the surveyed financial services companies have a blockchain deployed in production. That is likely to increase, of course, but it will be a lengthy process. To add to the complexity, the banks that stand to benefit the most from blockchains are large entities, with a global footprint, and a very rich product portfolio. It is likely that blockchain will start by proving particular use-cases, and only after proof of concept will broader rollouts proceed.

[30] Deloitte, "Deloitte survey: Blockchain reaches beyond financial services with some industries moving faster", (2016), accessed April 4, 2017.
https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-survey-blockchain-reaches-beyond-financial-services-with-some-industries-moving-faster.html

As stated previously, a design that looks promising for checking accounts is one that would rely on a consortium blockchain. This would make use of a cryptocurrency that can be used for transaction purposes (in order to avoid using the payment network approach deployed today). Such a concept has been undertaken by UBS, BNY Mellon, Deutsche Bank, and Santander who have joined tech companies Clearmatics and ICAP to work on what they call a Utility Settlement Coin (USC). These USC are envisioned to be the blueprint for central bank issued digital currency, and have as main benefit the quick movement of money. Such USC are valuable for moving money fast between banks, but an equally attractive scenario would be to have banks and merchants on the same blockchain. It is more ambitious than having a bank-only blockchain, but it is certainly possible.

Should central banks lead the charge on digital currencies?

When the Federal Reserve Bank system identifies a function that has systemic implications, such as large value transactions, it does not have a problem with taking lead on establishing infrastructure that benefits all participants. Fedwire is the precedent that paves the way for future similar actions. So the true conversation becomes does the Fed identify digital currency as similarly important, or not, or perhaps not yet. Currently, Fedwire, the Real Time Gross Settlement system that 9200+ member institutions use to transact large values, offers instant settlement, irrevocable transactions, it is designed to be highly resilient, and most of all it works well (averages $3Trillion in transfers each day). And it does so by being owned by the Federal Reserve Bank system. This means the bar for the value brought by any digital currency would be fairly high, as it would have to build significantly on existing functionality available. Those two directions would be either to 1) extend the participants to more than the 9,200+ member participants today, or 2) make the system more efficient for small transactions. They are both important value propositions, that would add significant value to the economy. It would however be an uphill battle to convince the Fed that it would need to assume a leading role in this space. Another alternative model would be the one deployed by Fedwire' s competitor, CHIPS, which is privately owned by a small number of banks (although because it is designated as a systemically important financial market utility or SIFMU, it does receive heightened regulatory scrutiny by the Federal Reserve Board). Given how strong the interest displayed by financial institutions is, and the way they've formed consortia to investigate blockchains, it is possible that one or more of these consortia that works on digital currencies becomes prominent. In that case they'll be designated as a SIFMU, and the Fed gets scrutiny rights. To some extent, it's a model that has more promise for the Fed, as it would stand to benefit from the innovation from the private sector, and only support the systems that have proven indispensable.

Yet another version of this model would be to establish a new bank, that establishes an account with the Federal Reserve, and sets up a digital currency at parity with the USD. All other banks, wallet providers, etc., would then have accounts at this new type of bank, and that would provide the vehicle for money to move faster, via blockchains. This is the model pursued by MIT's Digital Currency Group, and it has the main advantage that can be tested out quickly, without having the central bank needing to take major decisions. It shows promise in that it does not need major commitments from the Fed, as well as the fact that it can be opened up to stakeholders of all types (e.g., merchants), not necessarily financial institutions.

Why does the consumer care about blockchains?

Blockchain technology is not a consumer friendly technology. It is complicated to explain, it requires a high degree of computer literacy, and to most consumers it appears like a black box. It has major implications for companies that want to become more efficient, but ultimately it does not need customer buy-in to gain adoption. It will change the way we all interact with our devices, and it opens up new avenues for technological advances. A similar parallel was TCP/IP – the technology that made possible the Internet, which ultimately re-shaped the way people leave their lives, but TCP/IP remains an unknown for most consumers. A big part of the banks, or other entities interested in offering bank-like services, will be to hide that complexity from consumers. If the fast scalability of Whatsapp, Facebook and others like it provided any lessons, they show the importance of simplicity when facing consumers.

Use case – does blockchain really cut costs?

The overarching theme of this paper is that costs can be reduced by using blockchains. That is a big claim, and I wanted to investigate more on how exactly blockchains can do that. I will detail my research in the next pages. Banks' cost structure is not widely advertised, or understood for that matter. This happens for a variety of reasons, out of which two stand out:

1. **Banks do not advertise their costs.** Like all businesses, banks guard their cost structure. They are intensively competing for business with one another, and a public cost structure would make that competition harder, not easier. Additionally, especially after the 2008 crisis, scrutiny on banks has increased. Regulatory bodies such as the Consumer Financial Protection Bureau (CFPB) have tried to dig deeper, but that is no easy task. One reliable source of information has been the ABA – Americans Bank Association, which is the main industry body representing banks. The numbers that the ABA have been quoting throughout the years for maintaining a checking account have varied across the years, from $250 to $300 per year (in June 2010[31]) to $349/year in 2016. This reflects only annual maintenance costs, and the ABA is also stating a cost to open an account of $150-$200.
2. **Complicated cost structure, in complicated firms.** In order for banks to offer what the checking accounts that the customers are now expecting, many technology providers come together. Banks manage complex networks of partners, each of them with their own pricing method. Pricing for merchant acquirers is complicated, pricing for networks even more so. To make things even worse, banks themselves are entities that have multiple lines of businesses, multiple internal P&Ls, and overall a slew of internal stakeholders that come together to bring a unified experience for the customer.

Why look at open loop prepaid bank accounts?

As described previously, one of the alternative financial services instruments that have emerged to serve the unbanked and underbanked population is the prepaid bank account. The term prepaid identifies the fact that the value in the account is owned by the account holder (as opposed to credit cards, where a bank is extending credit and expecting to get paid at a later point). From a consumer perspective, there is no difference between prepaid account and a regular checking account. Additionally, for the purpose of this paper, prepaid accounts cater specifically to the demographic that banks have given up on – the folks who are highly mobile (making them difficult to verify and reach), risky to extend credit to, with irregular incomes, and most of all, with low earnings (for example, payroll cards, which are the most profitable form of open loop prepaid cards, have a monthly load of about $1,284[32]). From a bank's perspective,

[31] American Bankers Association, "The Cost of a Checking Account", (2010): 1 https://www.aba.com/aba/documents/press/CostofCheckingAccountsJune2010.pdf

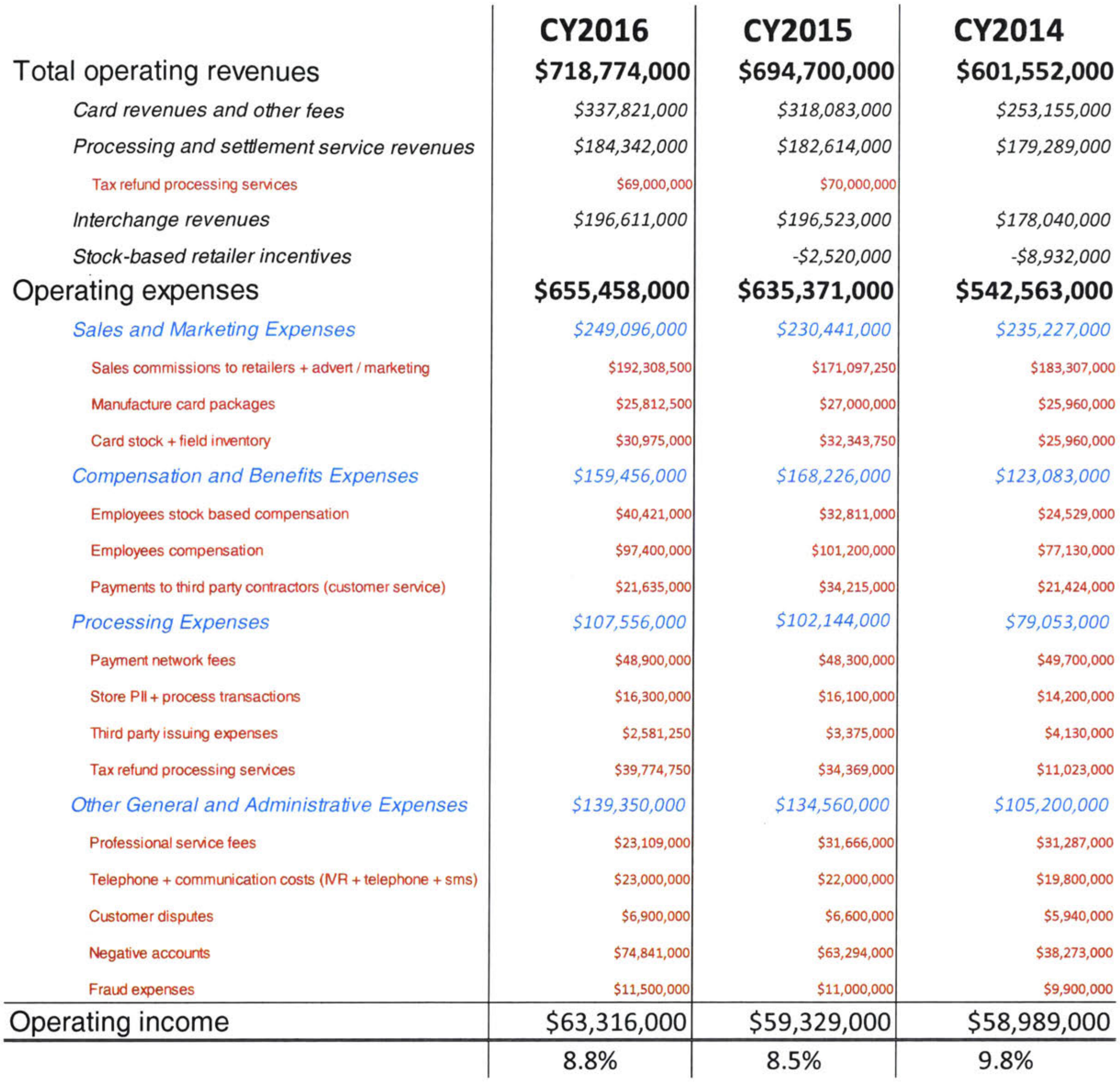
[32] Payment Cards Center- Federal Reserve Bank of Philadelphia, "Consumers' Use of Prepaid Cards: A Transaction-Based Analysis", (2012),68

these are the customers that are clearly not profitable. Yet from a financial inclusion perspective, these are the customers that need to be included.

Why is Green Dot Corp the right proxy for an industry?

Green Dot Corporation (GDOT) is a publicly owned company, founded in 1999. As of Apr 2017 it has a market cap of $1.7B. It is the leading provider of open loop prepaid cards, and it has become a bank holding company in December 2011, by acquiring Utah based Bonneville Bank. To sum it up, Green Dot is a bank that caters to the unbanked and underbanked segments. As a publicly owned company, Green Dot has to disclose a lot of information about their costs, and with enough information about the space, an informed user can estimate a lot of information with regards to Green Dot's cost for offering prepaid checking accounts. Additionally, as of December 2016, Green Dot had 4.13 million active accounts, compared to Bank of America's 34 million active account[33]s. While not on the same level as Bank of America, Green Dot is also not small. Below is a custom view of the data in Green Dot's Consolidated Statements of Operations Data.

[33] Bank of America Corporation's annual report, (2016), 20



	CY2016	CY2015	CY2014
Total operating revenues	**$718,774,000**	**$694,700,000**	**$601,552,000**
Card revenues and other fees	*$337,821,000*	*$318,083,000*	*$253,155,000*
Processing and settlement service revenues	*$184,342,000*	*$182,614,000*	*$179,289,000*
Tax refund processing services	$69,000,000	$70,000,000	
Interchange revenues	*$196,611,000*	*$196,523,000*	*$178,040,000*
Stock-based retailer incentives		*-$2,520,000*	*-$8,932,000*
Operating expenses	**$655,458,000**	**$635,371,000**	**$542,563,000**
Sales and Marketing Expenses	*$249,096,000*	*$230,441,000*	*$235,227,000*
Sales commissions to retailers + advert / marketing	$192,308,500	$171,097,250	$183,307,000
Manufacture card packages	$25,812,500	$27,000,000	$25,960,000
Card stock + field inventory	$30,975,000	$32,343,750	$25,960,000
Compensation and Benefits Expenses	*$159,456,000*	*$168,226,000*	*$123,083,000*
Employees stock based compensation	$40,421,000	$32,811,000	$24,529,000
Employees compensation	$97,400,000	$101,200,000	$77,130,000
Payments to third party contractors (customer service)	$21,635,000	$34,215,000	$21,424,000
Processing Expenses	*$107,556,000*	*$102,144,000*	*$79,053,000*
Payment network fees	$48,900,000	$48,300,000	$49,700,000
Store PII + process transactions	$16,300,000	$16,100,000	$14,200,000
Third party issuing expenses	$2,581,250	$3,375,000	$4,130,000
Tax refund processing services	$39,774,750	$34,369,000	$11,023,000
Other General and Administrative Expenses	*$139,350,000*	*$134,560,000*	*$105,200,000*
Professional service fees	$23,109,000	$31,666,000	$31,287,000
Telephone + communication costs (IVR + telephone + sms)	$23,000,000	$22,000,000	$19,800,000
Customer disputes	$6,900,000	$6,600,000	$5,940,000
Negative accounts	$74,841,000	$63,294,000	$38,273,000
Fraud expenses	$11,500,000	$11,000,000	$9,900,000
Operating income	$63,316,000	$59,329,000	$58,989,000
	8.8%	8.5%	9.8%

Table 4.1 – 3 Year P&L for Green Dot Corporation (GDOT) based on 10-K reports

Additionally, below are some key metrics that I have used in the analysis, and are very relevant for an entity in the business of offering checking accounts.

	CY2016	CY2015	CY2014
Number of Active Cards	4,130,000	4,500,000	4,720,000
Avg. cost / account	**$159**	**$141**	**$115**
Avg. Revenue / account	**$174**	**$154**	**$127**
Gross Dollar Value	$23,000,000,000	$22,000,000,000	$19,800,000,000
load/account/year	$5,569	$4,889	$4,195
load/account/month	$464	$407	$350
Point of Sale Spend	$16,300,000,000	$16,100,000,000	$14,200,000,000
POS spend per year	$3,947	$3,578	$3,008
POS spend per month	$329	$298	$251

Table 4.2 – Relevant metrics for an issuing business

Number of active cards – this the number of individuals that have had any type of transaction in the past 90 days. The customers addressed by Green Dot are very mobile, and in fact their average cardholder life is 5 months. This means that in order to maintain a portfolio of 4M+ accounts, Green Dot needs to distribute 10M accounts each year. This is not only very difficult to achieve; it is also very expensive. For regular bank accounts, the turnover is dramatically lower – and cheaper to maintain.

Gross Dollar Value – this is the total amount of loads on the Green Dot portfolio. As mentioned before, the more money moves through a bank, the more money the bank makes – that is shared across all banks. The higher this number, the better. Additionally, this tells us how much money each active user loads each month – in this case in 2016 this was $464, which is just above industry averages. That also speaks to income of the typical customer served by Green Dot. This is a key metric in identifying how profitable a customer is going to be for a bank.

Point of sale spend – This is the total amount of the funds loaded that is spent on purchases. For issuing banks, this is a significant source of income, in the form of interchange. This is a good indicator for how good (or bad) the usage pattern is for a customer. The higher the customer spends on purchases, the better.

A simple calculation shows us how much does Green Dot spends on average to provide bank accounts to their customers – and that number is $159/account/year. I adjusted for expenses for a new line of business GreenDot entered into (Tax processing services), and that takes us to $149/account/year.

What does a bank do for a consumer?

1. **Verify identify of the consumer** – this means establishing that this consumer says who they say they are, have a valid id, store that information securely, and of course, stay in compliance with the data storage policies. Additionally, after the September 11 attacks, additional questions have been added to the screening questions to try and identify potential terrorists.
2. **Ensure the consumer gets possession of the card** – This means manufacturing the card, potentially embossing the cardholder's name on it, sending it to the cardholder's address, pay for shipping expenses, etc. it also means setting up a distribution network to make cards accessible to consumers, and make sure enough of those cards are in the field. This also means maintaining inventory of raw materials for the stock of cards, envelops, and other marketing materials involved in creating a package that gets sent to the consumer.
3. **Activate the card** – this means the cardholder and the card are paired in the bank's system. This means either a call with an agent, or with an Interactive Voice Recognition Unit (IVRU) that tells the customer what needs to happen to make sure they confirm the right card reached the right individual.
4. **Load funds onto cards** – once the accountholder takes possession of their account, adding value is either done by direct deposit (typically from an employer) or by taking cash to a retail location, handling cash to the retail clerk, who then updates the balance of the card. This also means setting up that retail location, incenting them to do the transaction (e.g. paying them some sort of fee), making sure they follow a set of rules, and investigate them annually. This means the retail location that accepts money on behalf of the consumer is a certified Money Service Business, meaning it meets a set of requirements published by each individual state. Recently new ways of loading funds onto cards have emerged, such as remote check deposit, which means customers can take a picture of a personal check and load that value onto an account.
5. **Manage money** – banks need to offer a variety of ways for consumers to access their funds, from online banking, to mobile apps, to live agents, IVRU calls, text message

notifications, paper statements, etc. all of the feature that are offered by banks that facilitate money management.

6. **Spend money** – customers need to access their funds whenever they need them. this can be done either by purchasing something directly (via VISA and the other payments networks) or by withdrawing money from ATMs (via networks owned by VISA and the other payment networks), or by writing a check, or by remitting money to friends/family/others.
7. **Something goes wrong** – this is the single most expensive category of services involved in offering a checking account, making sure that the customer has a smooth experience. This means having large teams of agents ready to take calls, but it also means covering the losses perceived by customers in the case of unauthorized use of their card, sending out new cards in the case of a breach, etc. Also, a lot of investment goes into making sure issuers can prevent fraud before it happens. Specific to debit cards is that due to specific transaction timing issues, even debit accounts can go into negative balance (when the customer owes something to the bank – if the customers decide it's cheaper to get a new card rather than pay the bank, they do just that, and the bank covers the loss). A trend in the past few years, data breaches have ballooned the costs of banks, because the identity of most consumers is available for sale on the internet. Under payment network rules, the consumers are not at fault for identity theft expenses – bank issuers are, and fraudsters know that.
8. **Comply with the laws** – this is not customer facing, but banks have a lot of regulators. The bigger the bank, the more regulators apply, and the more frequent audits. As an example, below are all regulators which banks need to accommodate. Also, regulations have been increasing as well (Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, Dodd-Frank Act, Patriot Act, Bank Secrecy Act, etc.) This has translated to ballooning costs in this environment. It is one area where prepaid account providers have been benefitting, in that the scrutiny has been less intense.

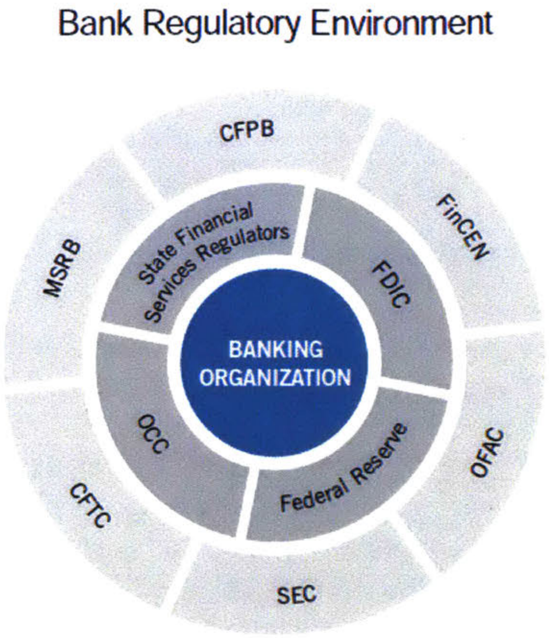


Table 4.3 – Illustration of banking regulators[34]

9. **Life cycle management** – banks also need to make sure they store the information of their account holders for seven years after a banking relationship ends, as well as send any unspent money to the state (called escheatment), under a state-by-state law model. This also means mailing notices to the last known address on file, and any attempt to get funds to the rightful owner.

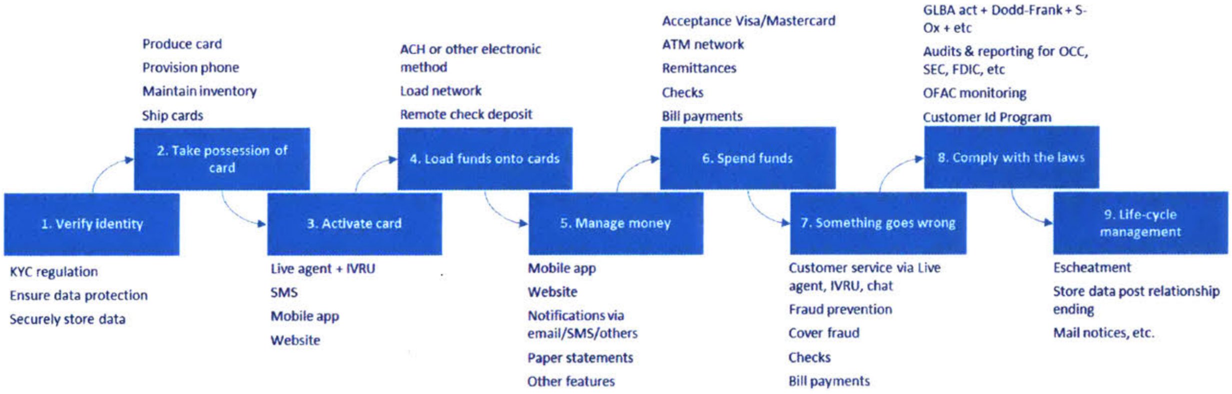
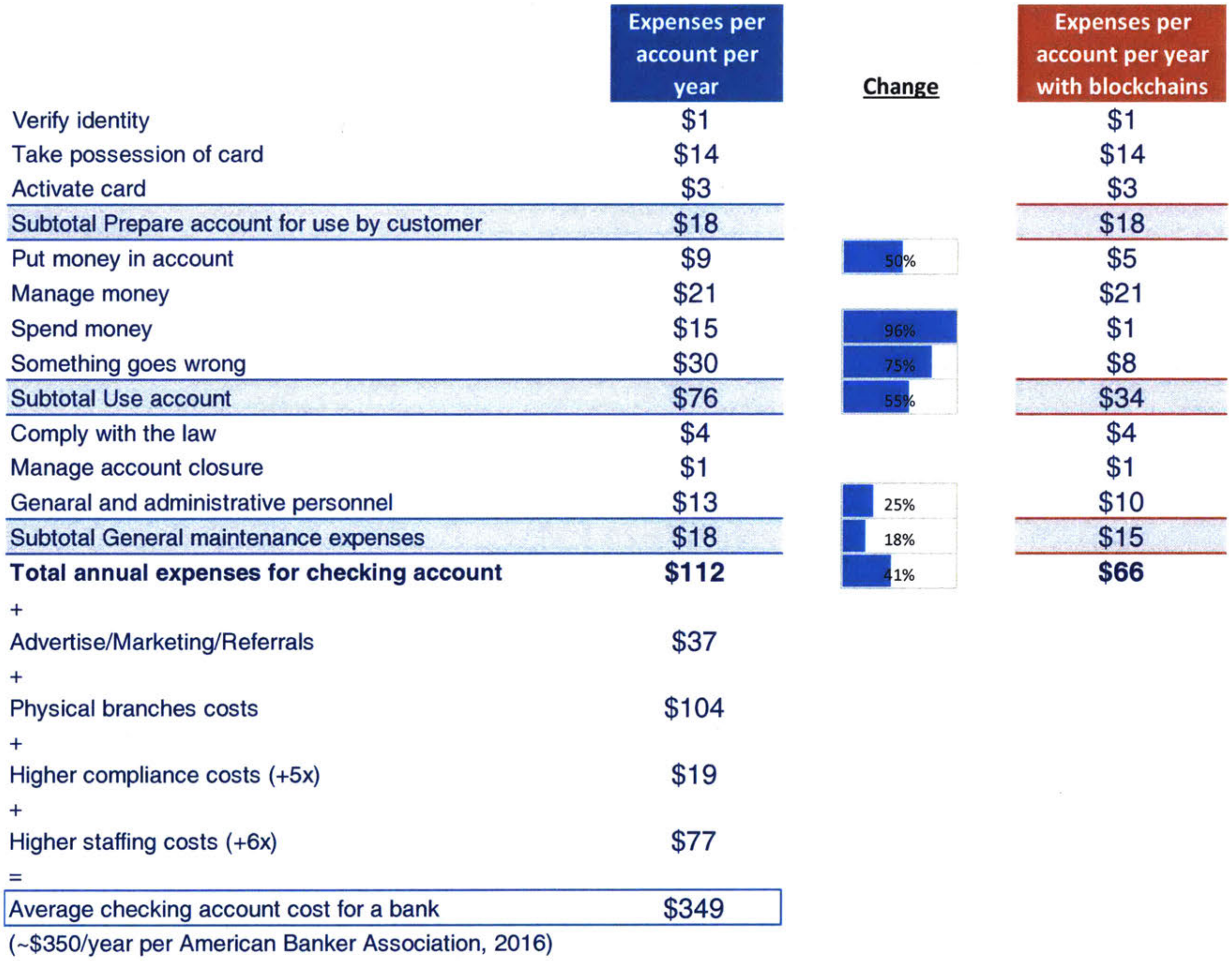


Table 4.5 – Categories of work done by banks to service accounts

[34] American Bankers Association, "The Business of Banking: What Every Policy Maker Needs to Know", (2013), 46 http://www.aba.com/Tools/Economic/Documents/Businessofbanking.pdf

These are the major categories of expenses that banks have to cover, and they do that with revenues from cardholder fees, interchange, and interest on the balances held (called float). One major category of costs not included above is how much banks themselves spend on convincing customers to use their products, instead of the competitors' products – via referral fees, advertising, marketing, etc. This is a business decision of course, but the costs are very real, and very high. I am estimating these expenses below, together with what I estimate them to be in a blockchain-centric context.



	Expenses per account per year	Change	Expenses per account per year with blockchains
Verify identity	$1		$1
Take possession of card	$14		$14
Activate card	$3		$3
Subtotal Prepare account for use by customer	$18		$18
Put money in account	$9	50%	$5
Manage money	$21		$21
Spend money	$15	96%	$1
Something goes wrong	$30	75%	$8
Subtotal Use account	$76	55%	$34
Comply with the law	$4		$4
Manage account closure	$1		$1
Genaral and administrative personnel	$13	25%	$10
Subtotal General maintenance expenses	$18	18%	$15
Total annual expenses for checking account	**$112**	41%	**$66**
+			
Advertise/Marketing/Referrals	$37		
+			
Physical branches costs	$104		
+			
Higher compliance costs (+5x)	$19		
+			
Higher staffing costs (+6x)	$77		
=			
Average checking account cost for a bank	$349		
(~$350/year per American Banker Association, 2016)			

Table 4.5 – Costs per active account per year

Physical branches are particularly expensive for banks, yet they are still around because the consumers do see value in having them around. The costs used in this analysis where the ones identified by Bancography[35], assuming 10 years useful life, and 2% property taxes, and it

[35] Bancography.com, Bancology quarterly journal, volume 60, 2016, 1-4

approximates the costs for a bank such as Bank of America, with 4,600 branches and 34million active cardholders.

Conclusion

Much has been said about the promise of blockchain technology for financial services. Whether it's World Economic Forum, World Bank, Deloitte, Accenture or other companies, everyone has an optimistic view with most caveats centering not around the merits of blockchain technology, but around the organizational ability to implement it properly. My conclusions for what blockchains mean for financial inclusion are a bit more nuanced.

1. Blockchains will impact financial inclusion indirectly, by reducing the costs of banks for servicing checking accounts. the banking space is competitive, and ultimately these cost savings will be passed on to the consumers, although that will not be an immediate process.
2. The financial services industry is leading the way with regards to adoption of blockchains in an enterprise setting. This is encouraging, and offers a good blueprint for other industries to join. Merchants of all types will also need to recognize the value of blockchains and start working with banks for the full potential savings shown in this paper to materialize.
3. Public blockchains (e.g. Bitcoin, Ethereum, etc.) are here to stay – they offer tangible benefits, and the amount of talent behind them is enough to bypass the technical challenges that come ahead. Whether the question refers to resource consumption, concentration of miners, specialization of miners or scalability – there are plenty of answers around, as a result of increasing interest from academia. However, public blockchains are best suited for niche use cases, where reaching scale would prove difficult. Additionally, public blockchains offer a great testing ground for innovation, which is extremely valuable. However, for highly regulated industries such as financial services, consortium blockchains are a better solution – however imperfect.
4. Consortium blockchains are a powerful tool for large implementations across organizations, and I believe it is by deploying these solutions banks are going to cut

http://www.bancography.com/downloads/Bancology1016.pdf costs. A model in which public blockchain pave the way, test and prove ideas, and then consortium blockchains implement the winners in their offering some time later is likely. To some extent, this is already happening, as proven by the announcement in February 2017 of Enterprise Ethereum Alliance, anchored by names such as Microsoft, Accenture, JP Morgan and Santander.

5. The big question stemming out of this paper is how exactly will these savings materialize? I believe there are at least two potential alternatives, and both of them deserve further consideration.
    a. A newly established blockchain centric bank, that is offering a bare bone, no cost solution to accountholders, which would cut the costs even beyond what I've described in this paper (by not offering a physical card, by offering a self-service customer service model, etc.). This is a major departure from the current banking practice, and I believe a new venture is needed to take such a drastic approach.
    b. A more moderate approach, in which large banks deploy blockchains and do not reduce functionality, yet that would need additional support to address high costs of distribution. One way in which states or federal governments can help here is by offering to reduce such high costs of distribution, either by supporting these no-cost solutions (e.g. by loading unemployment payments on these cards) or by outright advertising these instruments on their websites. Bottom line here is that costs of distribution (also called cost of acquisition) are very high in banking, and state/federal bodies can help reduce them – although that is likely to be a politically controversial move.

Bibliography

1. American Bankers Association, "2016 ABA Issue Summary: Fees and Pricing of Banking Products", (2016): 97-99
2. American Bankers Association, "The Business of Banking: What Every Policy Maker Needs to Know", (2013), 46
3. American Bankers Association, "The Cost of a Checking Account", (2010): 1
4. Bancography.com, Bancology quarterly journal, volume 60, 2016, 1-4
5. Bank of America Corporation's annual report, (2016), 20
6. Martha Perine Beard, Federal Reserve Bank of St. Louis, "In-Depth: Reaching the Unbanked and Underbanked", (2010)
7. Joseph Bonneau et al., "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", *IEEE Symposium on Security and Privacy*, 2015
8. Christian Catalini and Joshua Gans, "Some simple economics of the blockchain", *The National Bureau of Economic Research*, working paper number 22952, 2016
9. Coinmarketcap.com, "Crypto Currency Market Capitalizations"
10. Coin.Dance, "Bitcoin Statistics"
11. Committee on Payments and Market Infrastructures - World Bank Group, "Payment aspects of financial inclusion", (2016), 31-33
12. Deloitte, "Deloitte survey: Blockchain reaches beyond financial services with some industries moving faster", (2016)
13. Federal Deposit Insurance Corporation, "2013 FDIC National Survey of Unbanked and Underbanked Households", (2014), 1
14. Federal Deposit Insurance Corporation, "2015 FDIC National Survey of Unbanked and Underbanked Households", (2016), 1
15. Financial Literacy and Education Commission, "Promoting Financial Success in the United States: National Strategy for Financial Literacy, 2016 Update", (2016), 7-8
16. Gideon Greenspan's comment on "Avoiding the pointless blockchain project" Multichain.com, posted 2015
17. Interledger.org, "Interledger Architecture"
18. Javelin Strategy & Research," Identity Fraud Hits Record High with 15.4 Million U.S."
19. JP Koning, "Fedcoin: A Central Bank-issued Cryptocurrency", 11

20. Lipsey, Richard; Kenneth I. Carlaw; Clifford T. Bekhar (2005). "Economic Transformations: General Purpose Technologies and Long Term Economic Growth.", Oxford University Press. pp. 131–218
21. National Automated Clearing House Association, "What is ACH?" Quick Facts About the Automated Clearing House (ACH) Network"
22. The Nilson Report, "Top Acquirers in the US 2015", issue 1082 (2016): 10-11
23. The Nilson Report, "U.S. Payment Cards Purchase Volume 2010 – 2020", issue 1097, (2016): 8
24. Payment Cards Center- Federal Reserve Bank of Philadelphia, "Consumers' Use of Prepaid Cards: A Transaction-Based Analysis", (2012),68
25. James Schneider et al., The Goldman Sacks Group Inc., "Profiles in Innovation, Putting theory to Practice: Blockchain", (2016)
26. StatisticBrain.com, "ATM Machine statistics"
27. Nick Szabo's comment on "Money, blockchains, and social scalability." Unenumerated blog, posted 2017
28. Yonatan Sompolinsky and Avir Zohar, "Accelerating Bitcoin's Transaction Processing, Fast Money Grows on Trees, Not Chains", Cryptology ePrint Archive, (2013), 18-22
29. The World Bank, "Financial Inclusion Overview"