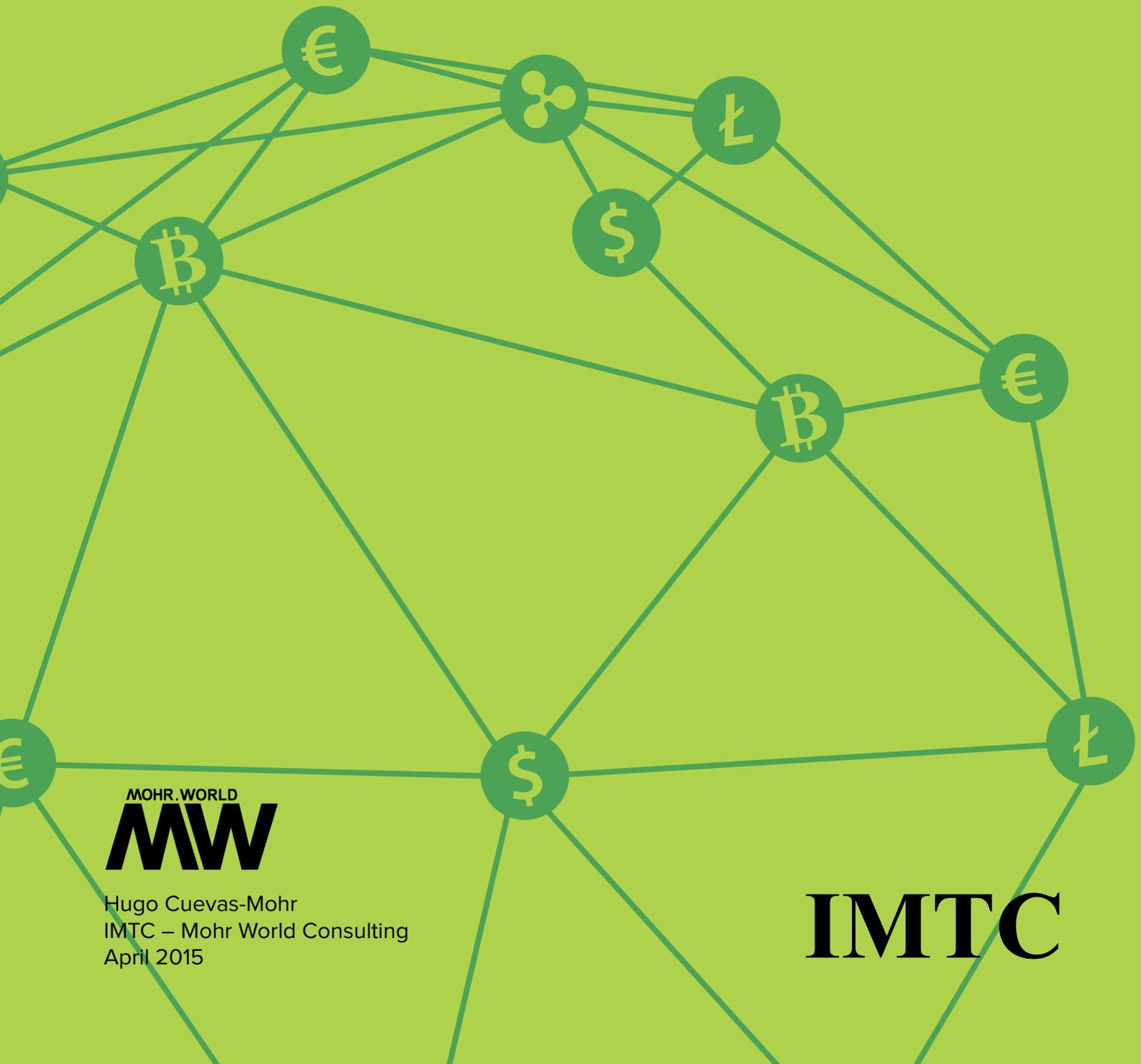# MTBIT
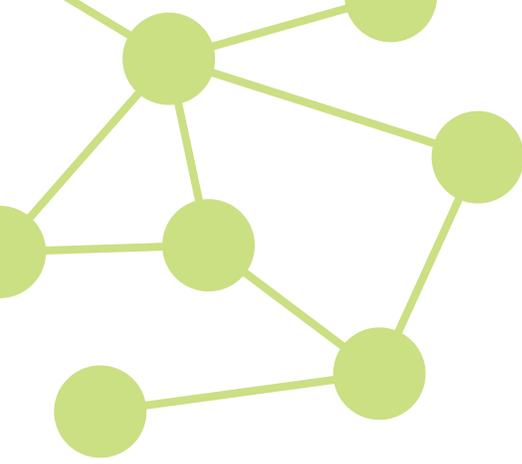## REMITTANCES AND BLOCKCHAINS

Hugo Cuevas-Mohr
IMTC – Mohr World Consulting
April 2015

MTBIT
Remittances and Blockchains

(English version)

The information herein is based on the author's experience and knowledge
of the industry. The internet references were all accessed in March & April 2015

IMTC – Mohr World Consulting

16135 SW 109 Street

Miami, Florida, USA

www.mohrworld.info

FIRST EDITION

First Printing (April 2015)

Online

English Version can be downloaded from here

http://www.imtconferences.com/mtbit/remittances-and-blockchains/

Contents

If you have been working with cryptocurrencies, distributed networks, shared and public databases or ledgers, like Bitcoin, Ripple, or Stellar, or if you have been reading about the Blockchain or you are a virtual or digital currencies enthusiast, this document is not for you. You will probably find it to be too basic. This document is meant to be read by my colleagues in the financial services sector, especially Money Transfer, Remittance and Forex colleagues and the regulators involved with such matters, who know little about the subject and want to better understand the blockchain revolution.
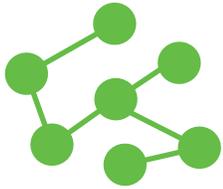
BLOCKCHAINS

Blockchains must be understood as a software concept, first and foremost. This software concept *"represents a paradigm shift in how software engineers will write software applications in the future, and it is one of the key concepts behind the Bitcoin revolution that needs to be well understood"*[1] wrote William Mougayar this past December (2014). This is not science fiction or utopic, it is real, it is happening, and it will change the way many industries operate. Since we are in the financial world, I have no doubts that blockchains will create significant changes in the industry in the years to come. The "rails" will change, the business models will change accordingly, and service providers, tools, and companies will come forward with their innovations based in these blockchain protocols.

Let's get technical for a second. Blockchains[2] are sequential transaction databases that are the basic structure that cryptocurrencies rely upon. These databases are decentralized, so no central database rules the validity of the information going in or out. For now, let's call this information transactions, or better yet, blocks or sets of transactions. These new decentralized schemes, called protocols, transfer authority and trust to decentralized virtual and public networks that enable dozens, hundreds, and thousands of nodes (independent servers all around the globe) to keep the shared databases synchronized, validating blocks or sets of transactions and linking every block or set of transactions with the previous one, continuously and sequentially recording them. These transaction blocks or sets create a unique, distinctive, chain, like a DNA molecule; these chains are called blockchains. They are also called trees, global ledgers, etc.

Blockchain-based protocols are mathematical models and software programs designed to authenticate, validate, and store valuable information in unbroken sequences that are synchronized all over the world. These protocols have unique sets of validations that make the whole system safer by reducing fraud, duplicity, and forgery as much as possible. At the same time, these systems are open source (which promotes innovation), public or semipublic (so anyone can verify the information handled), and promote the possibility of agreed standards that makes the transfer of digitally stored information reliable the world over.

> Blockchainbased protocols are mathematical models and software programs designed to authenticate, validate, and store valuable information in unbroken sequences that are synchronized all over the world. These protocols have unique sets of validations that make the whole system safer by reducing fraud, duplicity, and forgery as much as possible.

These protocols and cryptocurrencies have differences that most of the time, I have decided not to understand, because it is hard to know whether the differences are based on the terminology more than on the procedures, or if they are based on the effort of individuals trying to put very technical information into nontechnical words, thus blurring an already complex landscape.

Let's explain the Bitcoin Blockchain (BBlock). The BBlock is a public ledger of all the blocks of transactions that have ever been executed. The BBlock is constantly growing

as 'confirmed' blocks are added to it with new sets of recordings. The blocks are added to the BBlock in a linear, chronological order. Each node gets a synchronized, replicated copy of the BBlock.

William Mougayar, already quoted, describes the BBlock like this: *"Each successive block contains a "hash" (a unique fingerprint) of the previous code, therefore cryptography (via hash codes) is used to secure the authentication of the transaction source and removes the need for a central intermediary. The combination of cryptography and blockchain technology together ensures there is never a duplicate recording of the same transaction."*

In the BBlock every transaction has the originator's signature on it, but only you (an individual, a company, or a program) can unlock the BBlock because only you have the digital key; thus, you are responsible for keeping your key safe. It is like a constantly moving train where wagons (the addresses) are placed at the front and locked forever with the previous ones. Try to take one wagon out and you derail the whole train. The order of these wagons is crucial because the blockchain constantly authenticates the sequence of the blocks of transactions.

The BBlock has complete information about the addresses and their balances from the original starting block, through the most recently completed blocks. The blockchain grows infinitely and this unbroken chain of transactions is the backbone of the system which ensures its transparent and secure nature.

A good explanation of the BBlock is found in many websites, like Investopedia[3] and other websites.

I found perhaps the best explanation of the BBlock in Scott Driscoll's Curious Inventor

videos, and I encourage you to watch "How Bitcoin Works Under the Hood" (http://bit.ly/1zIOR8h).

I also like how Kariappa Bheemaiah[4] explains the way internet communication was launched and how we all can communicate digitally now through email, texts, etc. using the SMTP protocol. With blockchainbased protocols we can exchange value: I can give you a "piece of that digital block" (my wagon, a part of my wagon) that you accept because you recognize its value; you can store that piece of block, group it with other pieces, acquire stuff – digital or material, save it, and send it to others. Now, we can exchange trusted, validated, digital information.

> "The Internet we use today is the Internet of Communication, the Blockchain is the Internet of Value".

Brock Pierce[5], venture capitalist and serial entrepreneur, Board Member of the Bitcoin Foundation, in the video entitled "Bitcoin might fail but the blockchain is here to stay"[6] says: *"The Internet we use today is the Internet of Communication, the Blockchain is the Internet of Value. The one is a communication protocol while the other is a value exchange protocol. What made the internet so successful was its open protocol where anyone could innovate and build upon; the blockchain is the same thing. If you wanted to innovate in finance and payments, there were no real open system […] by having a baseline protocol that allows you to innovate and build around finance and payments, there were no real open system […] by having a baseline protocol that allows you to innovate and build around finance a lot of interesting things are happening."*

Block 1   Block 2   Block N
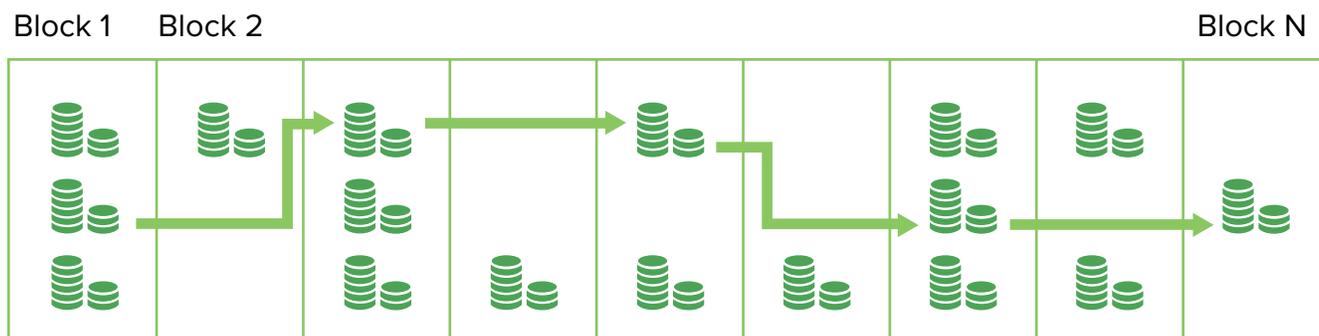
There are many blockchain solutions and as you read this, blockchain developers everywhere are working on the next great products, services, and ideas. Millions of dollars are being poured over this technology close to 500 million dollars in 2014 alone. One company, Blockchain. info, one of the world's most popular online bitcoin wallets, was used by 2.3 million individuals and raised 30.5 million dollars of venture capital in 2014[7].

Many different solutions are being implemented. Some of them – the most talked about ones – are the cryptocurrency solutions (Bitcoin, Litecoin, etc). Developers are creating other solutions of a similar nature in that they all are distributed, shared, and public, and that they utilize open source protocols and consensus ledgers. However, the similarities of these solutions to the Bitcoin Blockchain, for example, depends on your distance from the solutions and how much stress you put on the various aspects.

The TCP/IP[8] protocol is to the internet what a blockchain protocol – Bitcoin or the "next best" one – will be for the financial industry. Other nextgeneration protocols will probably be built on top of the BBlock, like SMTP for email, HTTP for webpages, and XMPP for chat have been built on top of TCP as a common underlying data layer[9].
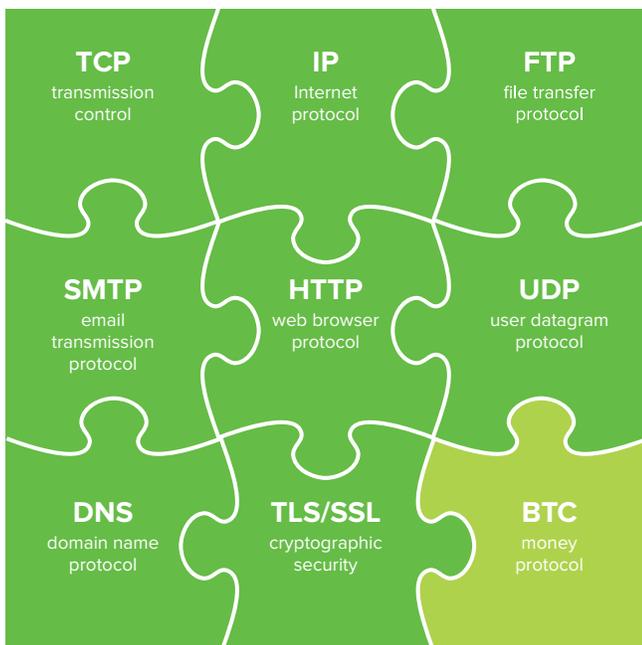
Dan Morehead from Pantera Capital sees Bitcoin as the final piece of the protocol puzzle made by all the internet protocols that exist of today: the money protocol[10].

As an example that we will analyze further, the Ripple Network is one of these open standard, distributed networks based around a shared, public database or ledger, where the participants in the network agree to changes in the ledger via a process called consensus. Ripple is being developed for financial institutions as the system that will revolutionize banking, foreign exchange and the MT&RI. Ripple's internal currency is named XRP and is listed as a cryptocurrency but it acts as a "trusted medium of exchange" within the network. The Ripple Network accepts payments denominated in other currencies (or assets) where the Ripple ledger only records the amounts owed by one user to another. You can jump to the section on Ripple or proceed in the order that I have laid out this document.

Another more recently developed protocol is the Stellar Network that we will also look and briefly comment.

There is also great excitement behind Ethereum[11], labeled as the next-generation cryptocurrency and decentralized application platform that will be launched in 2015 and that we will also describe briefly at the end of the document.

We will also mention Epiphyte[12], a bitcoin-based international transfer technology designed for banks and other financial institutions, *"a solution that avoids traditional money movement avenues and instead converts currency to bitcoins, moves the coins, then cashes them out on the other end in the local tender"*[13].

TCP transmission control	IP Internet protocol	FTP file transfer protocol
SMTP email transmission protocol	HTTP web browser protocol	UDP user datagram protocol
DNS domain name protocol	TLS/SSL cryptographic security	BTC money protocol

CRYPTOCURRENCIES

Cryptocurrencies are also known as virtual, digital, and mathbased currencies. The first fully implemented decentralized cryptocurrency is Bitcoin, which is now accepted and traded every day, despite the fact that many skeptics believe it's just a fad that will fade away. The Market Cap of Bitcoin is US $ 3,573 million (3.5 Billion USD). Ripple, which follows Bitcoin, is more than ten times smaller. Now there are many developed cryptocurrencies. Some of them compete with Bitcoin and Ripple, some present different qualities, and others project themselves as better substitutes. The alternative cryptocurrencies launched after the success of bitcoin are frequently called altcoins.

Examples of altcoins include Litecoin, Dash, BitShares, Dogecoin, Peercoin, Feathercoin, Zetacoin, Novacoin, etc. Litecoin is seen as the closest competitor to Bitcoin due to its speed of transaction approval and security[14]. Every "coin" starts and uses a different blockchain; this means that every "coin" has a different public ledger. As of 3/10/2015 Gola Yashu of NEWSBTC named the best altcoins to trade in the year 2015, based on their price stability. He mentions Dogecoin Dark, Unobtanium, Digitalcoin and Darkcoin.

There were more than 500 cryptocurrencies available for trade in online markets at the start of 2015. Only 13 of them have market capitalizations over $5 million as of April 7th, 2015[15]:

MARKET CAP	USD
Bitcoin	$3,573,301,018
Ripple	$289,453,001
Litecoin	$63,488,132
Dash	$20,095,734
BitShares	$14,247,372
Dogecoin	$12,111,472
Stellar	$11,541,629
Nxt	$11,211,167
MaidSafeCoin	$9,884,650
Peercoin	$6,914,656
PayCoin	$6,601,573
BanxShares	$5,943,002
Monero	$ 5,533,037

There are now companies that trade between one type of coin and the others and many people are investing in Bitcoin and altcoins to realize revenue out of the fluctuations. As a regular fiat currencies do, each altcoin has its own value that fluctuates with the market. As of 4/7/2015, 1 Bitcoin was worth $254.71 Dollars or €234.29 Euros, 1 Litecoin was worth US$1.79 or €1.54 and 0.00658 Bitcoins.

COIN	PRICE IN USD	PRICE IN €	PRICE IN BTC
Bitcoin	$254.710	234.290 €	0.00004
Ripple	$0.009	0.008 €	0.00658
Litecoin	$1.670	1.540 €	0.01501
Dash	$3.820	3.510 €	0.00002
BitShares	$0.006	0.005 €	0.00000
Dogecoin	$0.000	0.000 €	0.00001
Stellar	$0.003	0.002 €	0.00004
Nxt	$0.011	0.010 €	0.00009
MaidSafeCoin	$0.022	0.020 €	0.00122
Peercoin	$0.311	0.286 €	0.00170
PayCoin	$0.433	0.398 €	0.00540
BanxShares	$1.370	1.260 €	0.00307
Monero	$0.781	0.718 €	0.00004

The 2015 Innotribe Startup challenge, the second annual contest run by the international payment network SWIFT, provides fintech startups the opportunity to present their ideas to bankers, financial technology experts, and investors to win the ultimate prize. Last year one of the winners was Epiphyte, which we will describe at the end of the document as one promising bitcoinbased financial system. Out of the 60 startups chosen as semifinalists in 2015's challenge, about one sixth of them were digital currency companies. We see here how cryptocurrencies are moving into the heart of the financial system and that SWIFT is paying attention. The digital currency companies that were included are Asian bitcoin exchange BitSpark[16], cryptocurrency debit card Shift Pay[17], bitcoin remittance company Xendit[18], and decentralized digital asset ledger Hyper.

> Out of the 60 startups chosen to be semi-finalists in 2015's challenge, about one sixth of them are digital currency companies.
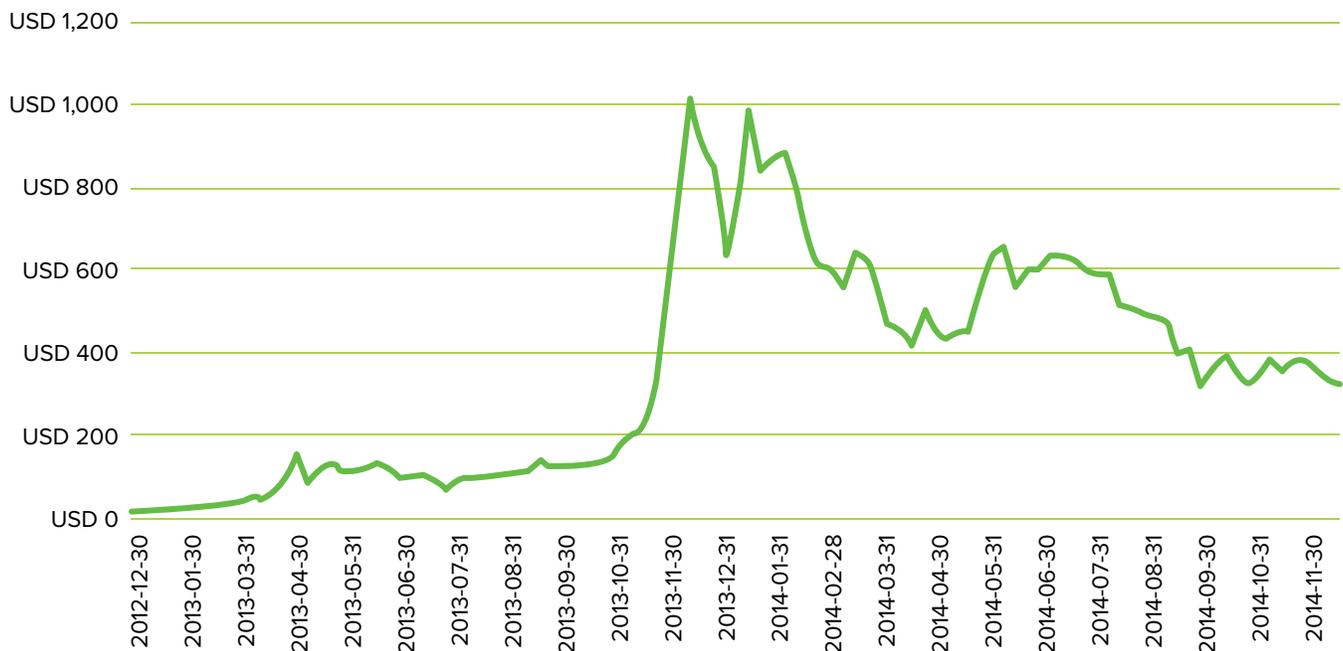
BITCOIN

An interesting article from Inside Bitcoins on November 2014 compares the internet developments from 1995 to bitcoin in 2014. It shows a very funny YouTube video of a 1995 episode of "Computer Chronicles"[19] where "electronic mail" and the concept of downloading are explained. I am here, in 2015 trying to explain blockchains, cryptocurrencies, bitcoins and you are probably as puzzled as those viewers were in 1995 when they were first hearing about the internet. I got my first AOL email account in 1999 and my first bitcoin wallet in 2014!

Ron Glantz and Dan Morehead of Pantera Capital[20] explained: *"Bitcoin venture capital investments are outpacing the investment rate of Internet companies in 1995. Just for fun... some of the companies funded in 1995 included Yahoo!, Amazon, and eBay."* In their 2015 presentation at the North American Bitcoin Conference in Miami, they wrote:*"Bitcoin: The Final Piece of the Protocol Puzzle"*[21]: *"The best way to see the future of Bitcoin is to see where the venture money is going. In 2014, there was a tripling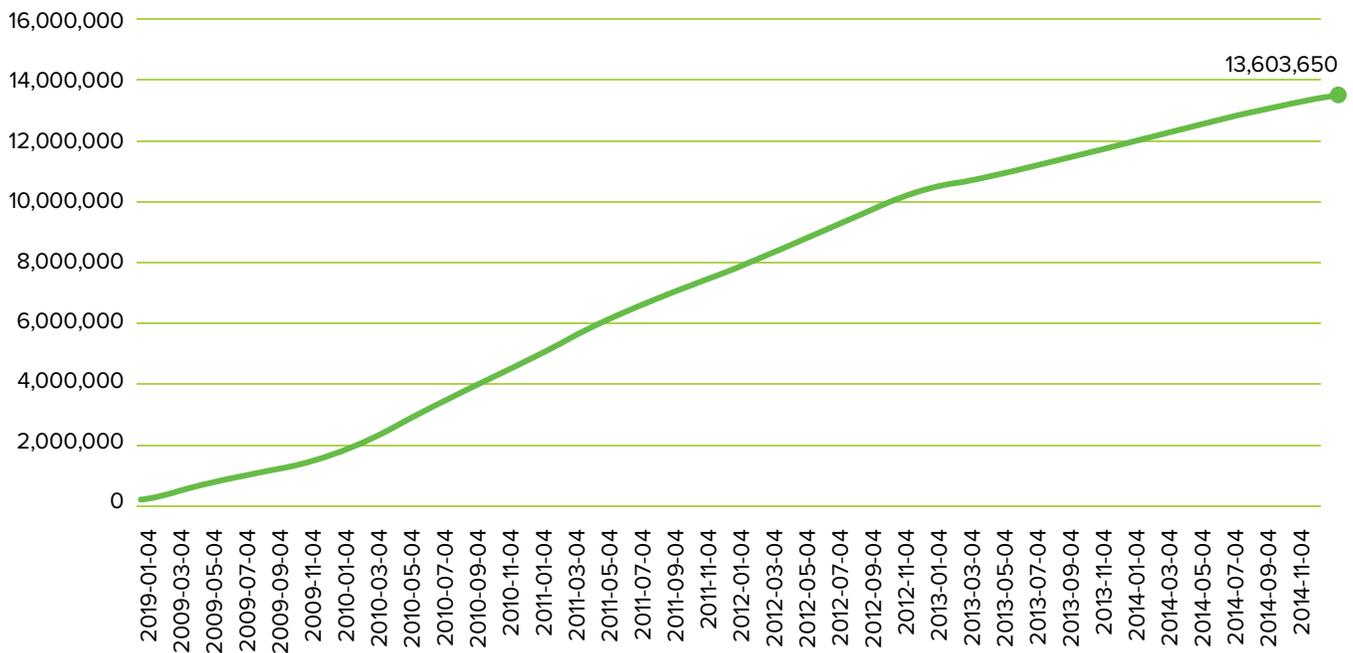 of venture capital going into bitcoin companies. It's up to around a $300 million dollar run rate for 2014 and that's the same as the Internet in 1995. It's also interesting to note that 2015 has already exceeded 2013's and we're just a month into the year".* Pantera has a great Bitcoin Primer[22] that you can read; I recommend it.

Because it's the most widely used cryptocurrency, Bitcoins are produced by many servers around the globe. They are expensive to produce because the software that both produces bitcoins and adds blocks to the blockchain needs large servers and computer hardware that uses great amounts of energy. The people that produce bitcoins are called miners, and they are similar to miners digging for gold, because they are attracted by the profits they gain from creating bitcoins, despite the high mining costs. When they mine bitcoins, they earn some bitcoins in return for their effort. The higher the price of bitcoins, the larger the profit. There is guidance and there are parameters to follow. Most legislations that are being developed do not require bitcoin miners to be licensed. Bitcoin mining companies also make money by authenticating transactions and maintaining the blockchain synchronization and replication.

BTC-USD

TOTAL BTCs

Chart showing total Bitcoins in circulation from 2009-01-04 to 2014-11-04, rising from near 0 to **13,603,650**. Y-axis marked in increments of 2,000,000 up to 16,000,000.

> "Bitcoin venture capital investments are outpacing the investment rate of Internet companies in 1995".

A. Who invented and controls the Bitcoin Blockchain?

A paper published in the Cryptography Mailing List in November 2008 is the first public appearance of the bitcoin protocol idea. In 2009 Satoshi Nakamoto released the first version of blockchain software client and he participated with other developers on the project via mailing lists until he faded from the community toward the end of 2010. Nobody knows for sure who Satoshi is or was, and the search for his identity is very intriguing[23]. Hundreds of developers around the world continue to collaborate and work on developing the open source protocol. The Bitcoin Blockchain or "protocol" runs in its network of independent nodes distributed all over the world, with the US having 40% of them and Europe having about 25%.

Perhaps one of the best known developers of the Bitcoin Blockchain is Gavin Andresen, the "core maintainer" or "chief developer" of the open source code defining the rules of Bitcoin and providing the software needed to

make use of it[24]. Andresen, with other bitcoin investors and enthusiasts the US, founded the Bitcoin Foundation— a nonprofit established in 2012— which is the most prominent overseer institution in the world of Bitcoin. As of December 25th, 2014, there were 13,642,875 Bitcoins in circulation and 155,795 Bitcoin users (unique addresses). Since Bitcoin's inception in 2009, there have been almost 55 million Bitcoin transactions.

In summary, nobody knows exactly who created the Blockchain and nobody fully controls the Bitcoin Blockchain. Rather, you might say it's "collectively" controlled and maintained, which is something that may be difficult to understand in the traditional payments world.

Who determines the value of one bitcoin?

Nobody… and everybody. Like gold, the price of bitcoin is determined by the buying and selling of bitcoins on the market; Fiat's currency[25] exchange rates allow you to determine how much of one fiat currency you can exchange for another. As anyone in the remittance industry knows, exchange rates change every day as currencies are traded on the foreign exchange market (forex). A fiat currency's forex value depends on a large number of factors, some real and some perceived, and it is influenced by the

issuing country's central bank interest rate, the country's debt levels, and the strength of its economy compared to other countries. Governments buy or sell fiat currency reserves to manipulate its price in the market, to control inflation, and to stimulate imports or exports.

Bitcoin, as another currency, also sees its price fluctuate. In December of 2013 its price shot up to over USD 1,000 and went down to around USD 400 in April. Since September, it has been fluctuating below USD 400 (see graph).

Although there have been numerous articles about the volatility of Bitcoin, many experts believe that as people mine and use more and more bitcoins, the price will be more stable and the price will fluctuate less and less. Today, there are investors that speculating about the prices of bitcoin, and some suggest that there are correlations between bitcoin and gold[26].

Is Bitcoin creation infinite?

The best answer will be nono in the sense that the Bitcoin protocol – the rules that guide the creation and transfer of bitcoins – has capped a limit of 21 million bitcoins on the production of this currency. However, bitcoins can be divided into very small parts: the smallest divisible amount is one hundred millionth. A one hundred millionth of a bitcoin is called a "Satoshi." About 13.7 million bitcoins have been created up to the end of 2014 from 12.1 million at the start of the year[27]. The first bitcoins were created in 2009.

> "Ecoins offer criminals no secrecy and only a trivial amount of anonymity. Every Ecoin transaction requires a computer or device to have a unique (anonymous) identity on the Ecoin peer to peer network".

As you see in the graph, the production of new bitcoins is decreasing at a predictable rate. The number of new bitcoins created every year will decrease until bitcoin

production halts completely once 21 million have been mined. As more miners join the bitcoin network, it becomes increasingly difficult to make a profit, and miners are seeking efficient methods to be to cut their operating costs. However, as production goes down, its price will probably increase.

Each bitcoin has a unique address that consists of an alphanumerical string with a length up to 34 characters [it excludes: the capital "O", the capital "I", the lowercase "l" and the number "0"]. This allows for millions of possible combinations, which makes a bitcoin address unique and makes duplication almost impossible. Some of the positions within a bitcoin address are used for a checksum and error correction. This is an example bitcoin address: 1JBrS7jzE3AJ9Sz5aFij1BmTcpFGgN88hc.

Another interesting fact is that every bitcoin address has a matching private key, similar to a protective password, which is saved in the wallet of the person who owns it. The private key is mathematically correlated to the bitcoin address, and it's designed so that the bitcoin address can be constructed from the private key. As a matter of fact. bitcoins are never really "in your wallet", they are merely tagged in the blockchain with your private key.

One problem with the Bitcoin Blockchain is that with every transaction, it continues to grow up to the point that *"Bitcoin may be a victim of its own success. The blockchain is now around 28 gigabytes, and as more people jump on the Bitcoin bandwagon, it will only grow faster"*[28]. But there are solutions being developed and the size problem might be solved soon.

If you want to become an expert on bitcoin, I encourage you to watch *"How Bitcoin Works in 5 Minutes"* (http://bit.ly/1D8fqpS), a video by Scott Driscoll the Curious Inventor, whom I mentioned earlier in this document. This video offers a great technical explanation that is easy to follow.
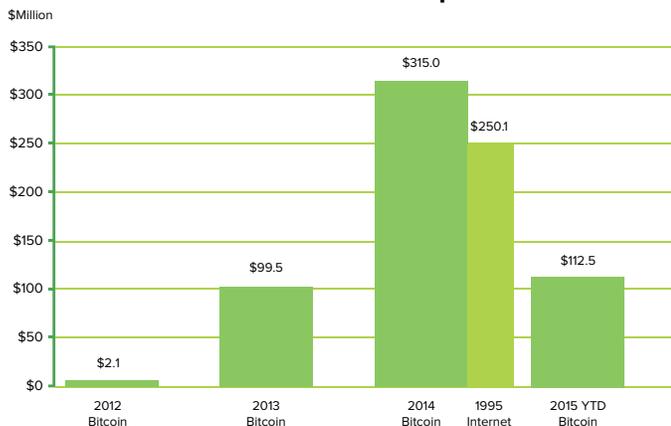
B. Because it's virtual, can it be used easily for money laundering?

Actually, it is the other way around, and even the media and some regulators and

law enforcement agencies were misinformed early on when the initial money laundering cases surrounding bitcoin caught the public's attention. With the Silk Road case[29] in October 2013 (Ross Ulbricht) and a second Silk Road case in November 2014 (Blake Benthall), the US Marshals Service (USMS) seized 30,000 BTC and 50,000, respectively, then auctioned them off.

"If anonymity and secrecy are good for crime, Ecoins are bad for crime"[30]. Because every bitcoin has a unique address and because all transactions create part of the blockchain, the system is transparent, and therefore it's traceable. Regulations all over the world require bitcoin "sellers" to keep the ID information of every bitcoin wallet holder, so even if all of the transactions in the blockchain are anonymous, law enforcement can, with warrants and with respect of the privacy laws in each country, trace any transaction that has ever been completed and find identities of the individuals from company records. *"Ecoins offer criminals no secrecy and only a trivial amount of anonymity. Every Ecoin transaction requires a computer or device to have a unique (anonymous) identity on the Ecoin peer to peer network. While each individual's identify on the network is anonymous, it is unique. Almost all web devices are identifiable by location or owner. The real anonymity of Ecoins is the anonymity the consumer gets, not the type of anonymity that protects or hides illegal activities. For the most part, law enforcement seems to be embracing the Ecoin movement, perhaps in part because it may make their jobs easier"*[31].

Bitcoin Venture Capital

$Million

$2.1	$99.5	$315.0	$250.1	$112.5
2012 Bitcoin	2013 Bitcoin	2014 Bitcoin	1995 Internet	2015 YTD Bitcoin

C. Is bitcoin secure?

I will take the answer from www.bitcoin.org, which I encourage you to visit to know more about bitcoin: *"The Bitcoin technology - the protocol and the cryptography - has a strong security track record, and the Bitcoin network is probably the biggest distributed computing project in the world. Bitcoin's most common vulnerability is user error. Bitcoin wallet files that store the necessary private keys can be accidentally deleted, lost or stolen. Fortunately, users can employ sound security practices to protect their money or use service providers that offer good levels of security and insurance against theft or loss. Security flaws have been found and fixed over time in various software implementations. Like any other form of software, the security of Bitcoin software depends on the speed with which problems are found and fixed. The more such issues are discovered, the more Bitcoin is gaining maturity.*

There are often misconceptions about thefts and security breaches that happened on diverse exchanges and businesses. Although these events are unfortunate, none of them involve Bitcoin itself being hacked, nor imply inherent flaws in Bitcoin"[32].

It is important to note that there are risks associated with bitcoin. Prableen Bajpai[33], founder of FinFix Advisors & Planners, a financial planning and investment advisory firm in India, reminds us in his article that as with any other investment or payment mechanism, there are risks in the following areas: technology, volatility, regulation, consumer protection, taxes, fraud, and theft. We experience these the technologyrelated risks as the system matures and concerned parties discuss the rules, which is not an easy task with the open structure of the Bitcoin Ecosystem.

Izabella Kaminska, a blogger for the London Financial Times, has a long series of articles about Bitcoin called the "Bitcoinmania Series"[34]. She is a bitcoin skeptic, and is criticized by the bitcoin community as a "naysayer." However, if you have concerns and you would like to read a contrarian view, check out her series. In her latest (2/8/15) blog post,

she comments on some of those technological risks mentioned above[35]. If you are interested in Bitcoin's scalability problems and i would like to study this topic further, read the paper "The Bitcoin Lightning Network"[36] by Joseph Poon and Thaddeus Dryja, which discusses some of Bitcoin's scale problems and explores possible solutions.

> **Bitcoin is legal, no doubt about it. "Has it been regulated?" should be the question that needs to be asked.**

D. Is bitcoin legal?

Bitcoin is legal, and there's no doubt about it. "Has it been regulated?" should be the question you're asking. The response to that is yes, bitcoin is been slowly regulated, and we will see more and more regulations coming up in 2015 and beyond. Many regulators in different countries have issued statements regarding bitcoin and will continue to do so. The November 13, 2014 Virtual Currency Advisory[37] by Katten Muchin Rosenman LLP is a good article that might be of interest to you if you are worried about US bitcoin regulation. Many countries are waiting to see what Benjamin Lawsky, the New York State Superintendent of Financial Services, will publish in 2015, after his office received 3,700 public comments when the proposed licensing for bitcoin-related firms was posted publicly. It seems that the so-called BitLicense won't be required for bitcoin software developers, virtual currency miners, bitcoin denominated gift cards, investors holding virtual currencies for personal investment, and for retailers accepting bitcoins. Plus, start-ups operating in the virtual currency space within the US will be given two years to become fully compliant with the licensing law[38]. Other bitcoin uses will probably require a state Money Transmitter's License, as it is required by any MTO and RSP in the US. If you ask our money transfer colleague Juan Llanos, now a bitcoin expert, he will tell you, as he did in a recent panel in a conference in Rio de Janeiro: "Bitcoin was born regulated"[39].

In my general opinion, Companies using

Bitcoin as a Money Transfer Service will require the same license as other MTOs or Foreign Exchange firms. The problem is in the countries where the license for MTOs or Forex firms is too costly and difficult to obtain, or where the capital requirements are too high, and because of the very nature of Bitcoin people or firms dealing with cryptocurrencies are going to have major problems adjusting to the regulations. Bitcoin firms will probably become more "unregulated" in those markets, and they might engage in undesirable practices by working in the margins of the financial system.

It is important to add that a few countries have declared Bitcoin illegal and here are a few examples:

- Bolivia: On May 2014 the Banco Central de Bolivia officially banned[40] any currency or coins not issued or regulated by the government including Bitcoin. It also states that citizens are prohibited from denominating prices in Bitcoin.

- Ecuador: On July 2014[41], the National Assembly of Ecuador banned Bitcoin and at the same time created its own, state-run, electronic currency (nothing to do with blockchains). Signup for accounts began in Dec 2014 with only 11,000 accounts by April, far from the 500,000 users expected by the end of 2015[42].

A number of other countries have restricted the use of bitcoin. For example, China prohibited financial institutions to trade bitcoins but allows individuals; Russia has a de-facto ban on Bitcoins that might be clarified soon; Thailand declared Bitcoin illegal at the end of 2013 but in a later date the Bank of Thailand stated that Bitcoin can be traded in the country so long as it's only converted to/ from Thai baht.

Other regulations have been published in several countries concerning the taxing of Bitcoin gains or the use of VAT in commercial transactions involving Bitcoin.

More information about legality of bitcoin can be found in Wikipedia[43], Forbes[44], Coindesk[45] and this paper published in March 2015 by Nishith Desai Associates in India: "Bitcoins: A Global Perspective"[46]

E. Should I really pay attention to Bitcoin?

Anyone in the payments industry should analyze and understand bitcoin. John Mauldin[47], the Chairman of Mauldin Economics, a financial expert, author, advisor, and the host of the Strategic Investment Conference, wrote an article published in November 2014, entitled "Is Bitcoin the Future?" This article really made me react and helped me decide to pay closer attention to bitcoin by getting a wallet and actually buying bitcoin in order to study the growth of Money Transfers & The Blockchain. John says: *"If you ask me whether I truly believe that in 2050 the main medium of exchange will be paper money, the very quick answer is that I don't. I also think there is a better than reasonable chance that it won't be a fiat currency. But will it be Bitcoin? My best guess is that it will not be Bitcoin as currently constructed but rather an evolved version".*

> **"If you ask me whether I truly believe that in 2050 the main medium of exchange will be paper money, the very quick answer is that I don't.".**

I encourage you to read it because it offers the perspectives of two skeptics, John and his colleague Worth William Wray[48], and with the information on bitcoin that you are reading here, you will better understand their ideas and realize why I am urging the money transfer industry to pay attention. The chronological analysis of the key financially-important bitcoin-related events [Silk Road, Mt. Gox, China, Cyprus] gave me a clear light on the bitcoin evolution.

If you want to "play" with Bitcoin, and by that I mean opening a wallet and buying Bitcoin, I encourage you to do so. First, download a Bitcoin Wallet with your phone. You can use the mobile wallet of the Bitcoin Exchange in your country that will probably have local "channels" for you to buy bitcoins and load them into your wallet and pay with a card or debit from a checking account. There are also chains of stores that accept cash to buy bitcoins. Airbitz Wllet, available in The App Store or Google Play keeps the information

of the Bitcoins you hold so you can use them, transferring them to other wallets (or receiving from other wallets). It doesn't actually keep the Bitcoins for you, you keep them in your wallet. It has also a nice directory of places where you can use the Bitcoins.

Coinbase, Circle, and others are licensed in the US so you can buy and sell Bitcoins from them by linking your card or bank account. They will require a large amount of information as part of their KYC requirements. Once you have Bitcoins, and a wallet you can test it with us sending us by emailing your wallet address (a long string of letters and numbers) and we will send you USD $1.00 dollar. You will be dipping your toes in the Bitcoin world. You can also scan the QR Code:
to read our Wallet Address.

At the last IMTC USA 2015 in Las Vegas, we got about one third of our attendees to download and use a wallet, and gave them USD $5.00 to purchase open bar tickets. We will do it again in other IMTCs.

I leave you with this quote from the same article: *"The Bitcoin blockchain technology allows for the most secure electronic transactions ever devised. Its adoption and acceptance seem inevitable to me. It will be used to validate everything we purchase: stocks, homes, investments, airplane tickets, etc. It will be a far cheaper and much more secure way to validate your ownership of anything, from your home to your stocks".*

> **"The Bitcoin blockchain technology allows for the most secure electronic transactions ever devised. Its adoption and acceptance seem inevitable to me".**

F. The Bitcoin Ecosystem

The year 2014 may be looked back on as a year when bitcoin began to move toward a mainstream market with a growing and maturing ecosystem. Some 6.6 million bitcoin wallets have been set up so far this year, according to Coindesk, a fivefold increase over 2013. And 75,000 merchants now accept the digital currency, including giants like Dell, Expedia and Overstock[49] [and now Microsoft too]. From the miners, to the developers, and the wallets to the trading desks, the ecosystem has truly diversified.Any form of categorization is merely a way to catalogue sectors of the ecosystem and the companies that are making the digital financial revolution a reality:

Any form of categorization is merely a way to catalogue sectors of the ecosystem and the companies that are making the digital financial revolution a reality:

- **Infrastructure & Miners:** Hardware is extremely important for both the Bitcoin ecosystem and for the Bitcoin software because the protocol runs on these servers. The computational speed of server farms and the intercommunicating nodes are vital for the system to function. Every Bitcoin transaction carries a very small fraction of bitcoins to pay for the maintenance of these server and nodes.

Both smart phones that run efficient and user-friendly wallets and ATMs that offer services in public places are also part of the bitcoin infrastructure.

- **Exchangers:** Bitcoin Bitcoin Exchanges (BExs) or digital currency exchangers (DCEs) are the companies where you buy and sell bitcoins, like an online Forex business. Here, you can trade bitcoins for fiat currencies [or different digital currencies] and they make money from the bid/ask spreads or they charge fees as transaction commissions for their services. They can be brick & mortar locations where cash is accepted or they can use ATMs, but most of them are online businesses that accept wire transfers and debit or credit cards as forms of payment.

At the end of 2014, the largest full trading exchanges by volume were Bitfinex[50] (Hong Kong), Bitstamp[51] (US), BTC-e[52], (Bulgaria?), Kraken[53] (US), Huobi[54] (China), OKCoin[55] (China), Cryptsy[56]. and BTC China[57]. These and other exchanges offer different services and loading or exchange mechanisms.[58] US bitcoin exchange Coinbase[59] has been eagerly seeking Money Transmitter Licenses in the US.

- **Products & Services:** We can place the software developers and firms providing software products that, independent of the blockchain, connect it to the rest of the world in this very broad category. Here we can place, for example, AlphaPoint[60], a white-label financial technology platform that powers global digital currency exchanges. Identity and KYC software providers, and all of the merchants that are accepting bitcoin as a form of payment fall into this category, as well as all types of other products and services, from food to clothing, hardware, software, tipping, donations, gaming, etc.

Also, the Bitcoin Blockchain is being used to build on top of or to build

around, with open source or closed source solutions for individual needs. Joel Monegro explains in his article "The Blockchain Application Stack"[61]: *"Developers are starting to build networks that work in parallel to the Bitcoin blockchain to perform tasks that the Bitcoin network can't, but that make use of the Bitcoin blockchain to, for instance, timestamp or validate their work."*

IMTC has started accepting bitcoins to pay for the conferences and we are waiting for the first bitcoin-paying attendee.

Bitcoin Remittance Companies (BRCs), also called "Rebittance" Companies are just appearing in the bitcoin ecosystem. These are companies that are actively providing tools and services for senders or beneficiaries of remittances.

- **Payments:** Bitcoin's more notorious applications are Digital Wallets, both the original online ones and the newer, mobile ones. Every bitcoin-owner needs a bitcoin wallet to hold its coins. Bitcoins can be bought into the wallet and spent or transferred from it. There are hundreds of wallets, some of the most popular ones are Blockchain[62], Coinbase[63], Circle[64] and Airbitz[65]. Tens of thousands of merchants now accept bitcoin payments. According to US based Bitcoin Payment Service Provider (BPSP) Coinbase, more than 25,000 merchants are using their platform to attract new customers. BitPay, another US BPSP, has over 20,000 merchants currently accepting bitcoins with their payment interface[66]. Two years ago this number stood at few hundred; when the numbers for 2014 are released, they will be large. A list of more than 30 BPSPs is found here: http://bit.ly/1Ezl870

Bitcoin Bill Payment Providers (BBPPs) is another payment service that was launched in 2014. Bylls[67], one of the world's first, is a Canada-based service that allows users to pay bills in bitcoin at more than 6,000 organizations, including the government. In Australia, the Living Room of Satoshi[68] (LRoS) pays anyone on that country's BPAY network [a universal bill-payment system in Australia that allows people to pay by phone or online by entering two numeric codes]. Singapore-based Quantified[69], Mexico's Pademobile[70], Argentina's enBitcoins[71], Indonesia's TuKarCash[72], Thailand's Bahtcoin[73] are other BBPPs making offerings in this space[74].

- **Financial Services:** This emerging sector of the bitcoin ecosystem is attracting entrepreneurs who are seeking to emulate the financial services provided by the traditional services, such as banking, lending, and insuring. The BitLendingClub is a peer-to-peer Bitcoin lending firm that has more than 600 active loans and had more than 2,600 loans repaid at the end of 2014. Germany's Bitbond[75] and San Francisco's BTCjam[76] are also matching borrowers and lenders for crowdfunded Bitcoin loans.

Insured Bitcoin Custody Services are also new services for 2014. UK based Elliptic Vault[77] offers an insured storage scheme (encryption coupled with multiple offline vaults and locations) to insure bitcoins against theft or loss.

Bitcoin Banking might not be a service that will be available anytime soon, although, in a way, bitcoin wallet providers are holding bitcoins and letting you use you bitcoins to buy, sell, and transfer... and providers might even start offering interest on the bitcoins you are holding. Isn't this banking? Luxembourg's Blockchain My Wallet slogan states:*"Be Your Own bank"* and then explains: *"My Wallet is a free online bitcoin wallet, which you can use to make worldwide payments for free. We make paying with bitcoins easy and secure available*

anywhere on your phone or desktop. We are not a bank; you retain complete ownership of your Money. We cannot view your balance, see your transactions or make payments on your behalf"[78].

Traditional Banking Services for Bitcoin firms are another matter. If Money Transmitters have problems getting Bank Accounts, Bitcoin firms are not much better positioned, although I do feel this is about to change, and this change might help the Money Transfer Industry as a whole.

> Consultants offering all types of regulatory, legal and compliance consultancy, help companies assess the risks and opportunities that the bitcoin ecosystem presents.

Bitcoin Remittance Companies (BRCs) also called "Rebittance" Companies are just appearing in the bitcoin ecosystem. These are companies that are actively providing tools and services for senders or beneficiaries of remittances to use Bitcoin, either as a medium of exchange or better yet, using Bitcoin "in the middle".

The service can be Person-to-Person (P2P), Business-to-Business (B2B) or even Person-2-Business (P2B)

- **Investment, Information, Training & Support:** The VCs & Investors have been crucial to the state of the bitcoin ecosystem. Investment in bitcoin has outpaced the rate of investment in the internet in 1995. Yes, bitcoin might be a bubble [that has already busted?] but similarly, few people could foresee the fortunes that were to be made with the internet expansion. **The US Bitcoin Foundation**[79], with its mission to fund development for the Bitcoin Core Project and to support common-good bitcoin infrastructure, has been key to the advancement of the industry. With its ups and downs, the recent news (April 2015) of its lack of funding, the

Foundation is coming of age now that its international expansion has been built with local chapters in a number of countries (Australia, Bangladesh, Canada, Denmark, France, Germany, Mexico, The Netherlands, Romania, Slovenia).

There are more than 600 Bitcoin Meetups in the World with more than 90,000 members in more than 70 countries[80]. Three of the largest ones are in New York (from 2,000 to 3,000 members each), followed by London (2,300), San Francisco (2,100), and Tel Aviv-Safo (1,780).

Major Bitcoin Events are taking place everywhere in the world. Inside Bitcoins[81] is being hosted in more than 6 cities in the world; Smile Expo[82] is hosting Bitcoin events in Russia, St. Petersburg, Kiev and Prague; the North American Bitcoin Conference (Miami), the Virtual Currency Summit[83] (Boston); The Texas Bitcoin Conference[84]; The Bitcoinference in Amsterdam; the Bitcoin Africa Conference[85], (just Launched in S. Africa); the LaBITconf[86] (B. Aires, Rio, next in Mexico) and others we are probably missing here. Specialized events like IMTC's MTBIT[87] on Remittances & Bitcoin are now hosted as part of the International Money Transfer Conferences.

There are **Associations** in several countries in the world: US, France, The Netherlands, Switzerland, Belgium, Hong Kong, Australia, Israel, Ireland and others, mostly recently formed.

Consultants offering all types of regulatory, legal and compliance consultancy, help companies assess the risks and opportunities that the bitcoin ecosystem presents. Money Transmitter consultants, especially the ones already involved with digital payments, are becoming bitcoin experts too, and their years providing services to money transmitters and payment companies is valuable. They are teaming up with Coinsultants, a term used by many bitcoin consultants nowadays.

G. What are bitcoin's more interesting characteristics from a money transfer point of view?

In my opinion there are promising characteristics, whether Bitcoin is used by the consumer or a Rebittance Company uses Bitcoin "on the back", as a medium of exchange.

Used by the consumer (P2P):

A. Like an email, a bitcoin (or a fraction of a bitcoin) can be sent digitally from one person to another, across the world, almost instantly.

B. You can hold your Bitcoins in a digital or virtual wallet and send Bitcoins from one wallet to another wallet.

C. The recipient, who can be can be anywhere in the world, can buy goods and services in the internet or in a domestic market where bitcoins are accepted or exchange them for local currency with other people or using specialized businesses (even ATMs). The larger the local ecosystem, the easier is to use.

D. Transaction fees are minimal. Bitcoin exchangers can charge fees for distribution through domestic payment systems or to exchange bitcoins into fiat currency.

Used by a Business (B2B):

To use it as a medium of exchange:

- MTO A in sending country takes the order from sender and receives local currency in cash or debited from Bank Account, Card or Mobile Wallet.
- MTO A buys Bitcoin
- MTO A sends order and transfers Bitcoin to MTO B in receiving country
- MTO B pays beneficiary in local currency either in cash or using existing remittance distribution channels.

The promising characteristics in such a business model are:

- Provided the Bitcoin market is active in both ends, the transaction costs can be minimal, almost zero, as both MTO A & MTO B are each one benefiting from the exchange rate spread.
- There is no credit risk between MTO A & MTO B and liquidity is kept at a minimum with no advances as it is customary nowadays.

- No use of a Bank: this keeps the costs low and reduces the risk of losing bank accounts (if the Banks closes account).

If MTO A and MTO B are already money transfer companies there are other added advantages:

A. Fund receipts from sending clients by MTO A don't need to be modified.

B. Fund dispersal by MTO B to remittance beneficiaries don't need to be modified.

C. No change in KYC, AML, CTF procedures already in place.

D. A competitive advantage over competitors since the drop in price, even slight, can reap large benefits.

Consumer to a Business (P2B):

MTO B can decide to cater to any Bitcoin holder in the world that wants to send funds to a beneficiary in the country that they serve. They could have an online or Mobile application where the sender transfers Bitcoins to the corporate wallet of MTO B and provides the information of the intended beneficiary who can be paid instantly with local currency at an agreed exchange rate.

If you are an MTO you are probably right in thinking on the legality of such a service. This type of service might be labelled illegal in the country where the sender is located if MTO B is not licensed in that jurisdiction. I agree that the regulatory challenges ahead are going to be major. But let's remember that there are many similar systems being used today where funds (USD, EUROS) are placed in virtual wallets or virtual cards and moved, cashed in or cashed out, in other countries.

It is also important to understand that there are many challenges, most of all the need for strong and active Bitcoin markets at both ends of a remittance corridor and that is why not every corridor will likely see the appearance of MTOs using Bitcoins or Rebittance companies challenging established players. I strongly suggest that any MTO or Foreign Exchange firm finds potential Bitcoin partners that it could work with. As MTOs partner with Foreign Exchange Brokers, why not look for Bitcoin Exchanges and see if there is a possibility of working together.

H. Are there companies doing remittances with Bitcoin?

Yes, there are. We know a few that are in the early stages as of Q1 2015. We are going to name a few by region (Americas, Europe, Africa, Middle East, Asia & Pacific) that have made the news or have contacted us as part of our MTBIT events.

We are going to use REBIT as an example to explain a rebittance system. Rebit is a company operating in the Hong Kong-Philippines Corridor. Rebit is a service of Satoshi Citadel Industries[88], a Philippine-based holdings company for Bitcoin-related ventures. Rebit is using Bitcoin to connect its partner in Hong Kong with its office in Manila.

The sender hands down Hong Kong Dollars (HKD) to a teller in the World-Wide House arcade in Central, a shopping center popular with Filipinos in HK. In Manila, Rebit delivers the corresponding Philippine Pesos (PHP) to the recipient in the Philippines, sometimes in cash at their office, but usually by the remittance distribution networks already well-established in the country, such as banks, ATMs, Mobile Wallets, and courier services.

The operation is quick and very inexpensive, plus the HKD-PHP exchange rate is very competitive.

The operation is managed internally without the client on both ends ever receiving Bitcoins or even knowing what Bitcoins are. The HK agency internally exchanges the HKDs into Bitcoins and transfers those Bitcoins from their wallet to Rebit's Wallet in Manila, who in turns exchanges the Bitcoins into PHPs. Buying and selling Bitcoins at both ends is not a problem, and in fact, it is the revenue from these exchanges that allows the sender of the remittance to pay an extremely low fee.

For more information on Rebit's Rebittance Service see Rebit's co-founder Luis Buenaventura's presentation at IMTC USA 2015 in Las Vegas at MTBIT on March 23rd, 2015[89]. We are inviting Rebittance companies to IMTC's MTBIT days to showcase their service and to partner with Money Transfer distribution networks in the countries where they are pioneering these services.

1   2   3   4   5   6
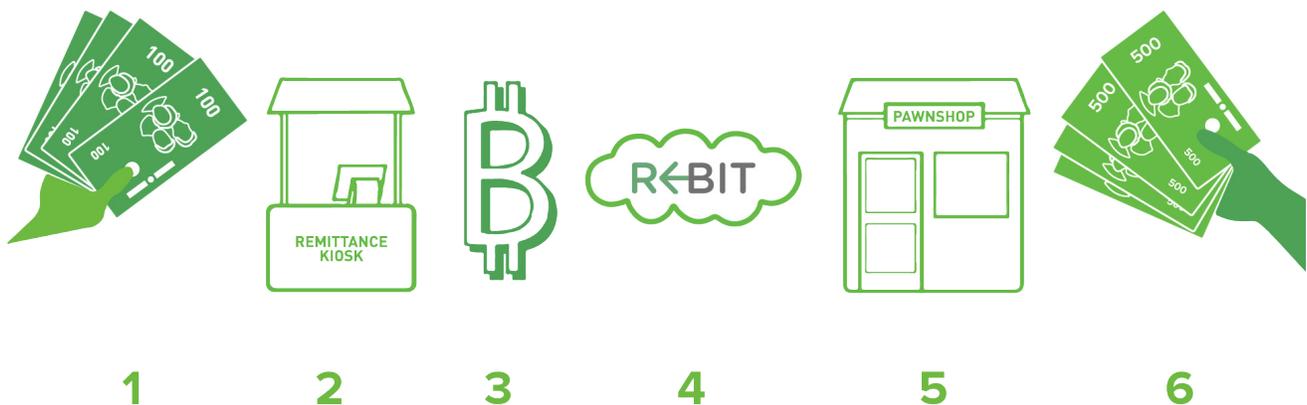
Cash-in, cash-out remittances — powered by Bitcoin

RIPPLE

While we can draw differences and similarities between Ripple and Bitcoin, we will not take this approach because it may complicate our explanation of Ripple as a distinctive use of a "bitcoin-like technology." The two protocols do share basic ideas and behave in similar fashion: they are both based on "distributed, shared, public, open source protocols, consensus ledgers". Understanding the BBlock has undoubtedly helped me to understand the Ripple Network, as it will help you. Many people arrive at the Ripple Network by analyzing Bitcoin, which is more widely known because of the media's coverage and because Bitcoin is more of a consumer product while Ripple is a business product.

A. How was Ripple invented?

Let's start with some history. Ryan Fugger, a web developer in Vancouver, Canada created Villages.cc, a self-contained community in 2005. He then created Rippleplay.com as a financial service to provide secure payment options to members of the online community via a global network. He was inspired by the alternative currency system developed by Michael Linton, also a Vancouver resicent, in the 80s. Ryan's work lead to the development of a new Ripple system in 2011 by Jed McCaleb; he arrived at this idea when bitcoin, especially bitcoin mining, was being questioned: *"It will be a bit obscene how much will be spent mining if the network ever gets large. It would be cool to come up with a bitcoin that doesn't need miners."* McCaleb founded OpenCoin Inc. and continued developing the Ripple system. In 2013, he changed the name to Ripple Labs and brought in CEO Chris Larsen who had previously founded the lending service companies E-Loan and Prosper. Here, you can find a great company presentation that gives you an understanding of the compant and its management team: http://bit.ly/1CInBdJ[90]. In 2014 the company was reorganized (with

McCaleb's exit to form Stellar[91]) and it set the company onto a new corporate path that the business community endorses. At this time, Ripple signed its first banks, such as Fidor in Europe and Cross River Bank in the US.

B. In a nutshell, what is Ripple?

As Ripple Labs explains it in its Ripple Primer Brief: *"Ripple is a universal protocol for money transfer that allows independent payment systems to communicate as easily as email systems do. Just as SMTP created a shared standard for email, Ripple provides a shared standard for payments."* Ripple is competing to become the backbone for financial transactions across the globe. However, instead of focusing on peer-to-peer (P2P) transaction, it is focusing on institution-to-institution (I2I). These institutions are financial services companies, from Central Banks to MSBs, who can use Ripple as a common ledger to clear and settle transactions in real-time. They offer bilateral settlement - eliminating intermediaries, midpoint failure, delays, lifting fees -- and real-time funding by minimizing exchange spreads, credit risk and collateral costs.

While Ripple was developed by Ripple Labs, who does continues to develop it, the protocol is open-source, so anyone can download it and build the applications that you want on top of it for your institution to use. It functions as a consultant and advisor, which helps institutions adapt the system to their internal processes and to become part of the Ripple Network (RNxrp).

> "Ripple is a universal protocol for money transfer that allows independent payment systems to communicate as easily as email systems do".

C. How can Ripple be important for the MT&RI?

I think the best way to understand Ripple for the MT&RI is to remember the origins of the industry when Forex Companies dominated the industry and served MTOs or became MTOs themselves. Forex firms maintained a trust relationship with each other and honored

their trades with their reputation. A Forex firm in Buenos Aires could call a Forex firm in New York and trade, promising to pay immediately after a rate was negotiated. That firm in Buenos Aires also had trust relationships with other smaller firms within the country's borders; this network of trust was the basis of the business. In many parts of the world it was, and it still is, the same case. From Hawala to all other informal systems, currency exchangers built cross border businesses by helping merchants pay each other and trade their currencies from one country to the other. My grandfather, a "cambista" knew that his reputation was at stake if he didn't fulfill his promises. He also knew his liquidity and his credit limits, and he knew when to take risks or not.

The RNxrp is the millennial version of a Forex network. Instead of having an informal and very personal network of trust and reputation, the trust is now placed in a protocol where all of the Forex firms can take part and where limits, rules, terms, and conditions are set, so trades can flow safely, in real time, and perhaps most importantly, the protocol will always find the best exchange rate possible.

But let's explore Ripple in the context of the MT&RI today. We all know that our operational systems, as an industry, relay on an interconnected domestic and cross-border collection of very heterogeneous networks, mostly using the internet protocol to communicate, but with varying degrees of complexity, automation, security, and speed. These networks vary from email and chat to webservers, VPNs, etc.

Communication of transaction information, which needs to be wuick, goes one way while the funds travel a very different route, mostly using a manual (or semi-automated) pathway, jumping through hoops and obstacles, until it reaches its destination several days later. If there is a foreign exchange transaction in the middle, which there is most of the time in the case of cross-border transfers, another process is required, to make sure that no money is lost in the spread (or that the maximum possible amount is made). Because the transaction information travels fast while the funds take days to move, the system needs liquidity, which is provided by our own capital in addition to the lines of credit that we issue and receive. If we add to that the problem with the financial access for MTOs, we have to use several banks – or not, or intermediaries, to help in the process.

Bear with me. I don't want to explain to you how an MTO runs - you know how it works, but I am using this simplification to explain how Ripple can function in this environment. Let's start with a simple model, when an MTO A in one country works with an MTO B in another country (an MTO in Belgium making payments through an MTO in Congo, or an MTO in Texas with an MTO in Mexico).

MTO A collects funds from agents in Belgium and it keeps a ledger with each one so it can control its credit limits for all of them.

Liquidity provider A
FX cost: $

Liquidity provider B
FX cost: $$$
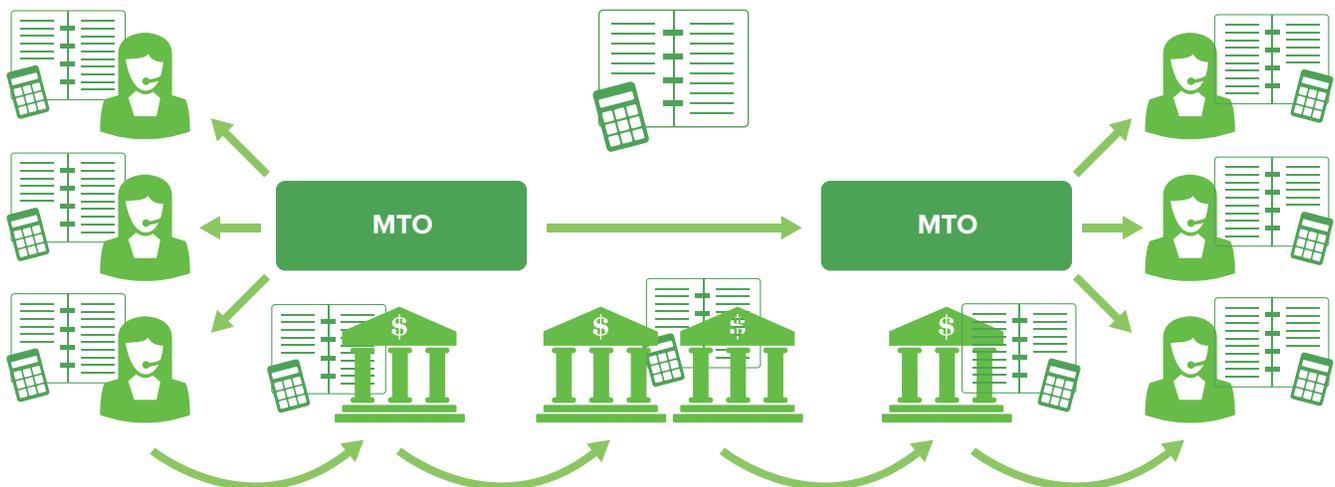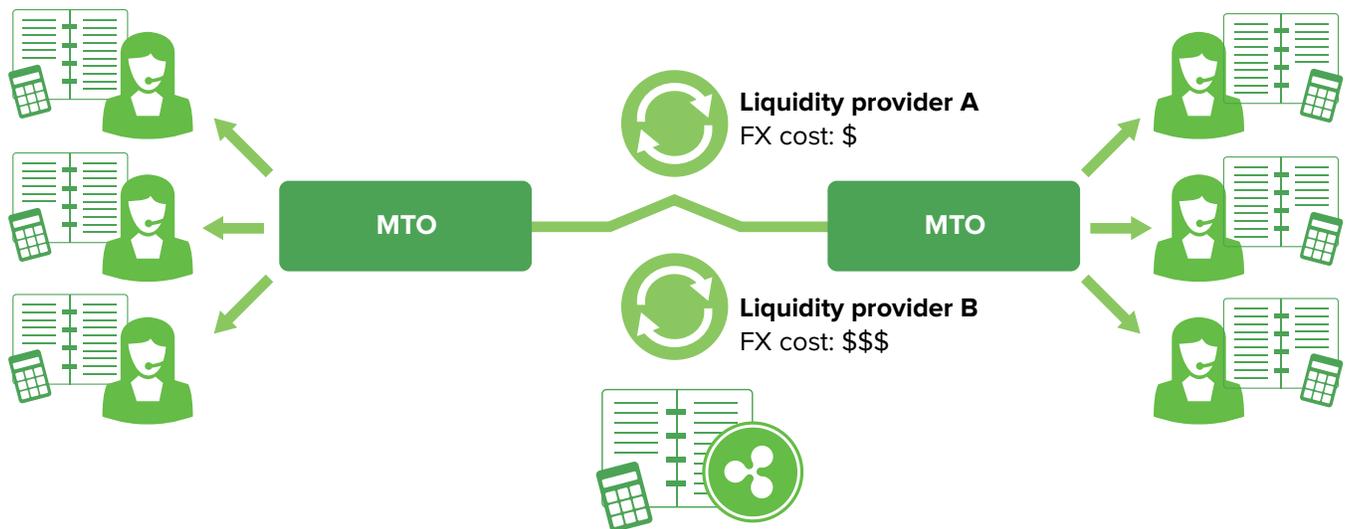
The collected transaction information is sent to MTO B in Congo that, in turn, sends the transaction information to its paying agents to distribute the funds. While the transaction information flows, it alerts the treasury departments that money is needed here and there, and that funds are becoming short or that credit limits are reached. Funds then travel from financial institution to institution, from cash to bank deposits, to a wire transfer, to a forex transaction, or to a bank deposit.

Most MTOs basically have to accept the Bank's FX rates in the process, unless the MTO can shop for the best FX rate in the market and channel its funds through the institution that offers the best rate. However, this is only available in certain corridors (and mostly available for the larger Tier 1 and Tier 2 companies).

> MTOs can settle transactions point-to-point as a straight-through process.

What if, instead of having the funds to go through this complex, slow, and expensive process, there existed a company that could receive the funds and deliver them immediately at the other end? What if MTO A using the Ripple Network could settle in real time with MTO B at almost no cost and at an exchange rate that is difficult to match in the market? It is possible, then, that the transaction information from MTO A (both communication and settlement information) can arrive at MTO B at the same time? All

three answers are, of course, yes. The RNxrp, with a liquidity provider in the center, makes all of this possible.

MTO A, now part of the RNxrp and using the distributed ledger, will then post a bit for USD or local currency for MTO B and in a matter of seconds, the system finds a liquidity provider with the best deal. MTO B is then credited in the ledger with the corresponding amount.

Who is this Liquidity Provider? Any financial institution can be a liquidity provider in the RNxrp, from a Bank to Forex firms--any institution that has capital and is willing to buy and sell currencies while making revenue in the process. With Ripple, a liquidity provider has the funds available in different currencies and trusts the members in the network; it also sets limits, in order to process transactions, bid, trade, etc. There is no risk at either end of a Ripple Transaction; only the institution in the center carries that risk, and these institutions in the RNxrp are called Market Makers

Let's review some facts about the RNxrp before we proceed:

- Financial institutions use the Ripple protocol to clear transactions via a common distriubuted ledger and use ripple to settle obligations via a distributed funds-exchange – all in realtime (every 5 seconds), 24/7/365 and at the most competitive exchange rate.

- This distributed ledger clears transactions (providing real-time record of obligations).

- Transaction clearing is the result of consensus, a process native to the Ripple protocol, that authorizes a collection of counterparties to validate Ripple transactions all day long, providing the trust, authenticity and fluidity the system needs.

- MTOs can settle transactions point-to-point, as a straight-through process. For currency conversion, the MTOs access through Ripple a funds-exchange, a marketplace of authorized liquidity providers, which always results in a competitive FX rate.

- The larger the Ripple Network, the larger the Ripple Marketplace, and the more pathways will exist to channel payment orders. Anyone can post bids or offers in the system and the Ripple Network finds the most efficient path to match trades There is no network fee, and there is no minimum transaction size.

D. How can institutions be part of the Ripple Network?

Institutions can be part of the RNxrp in three different ways:

1. As customers or clients of a Ripple Gateway
2. Becoming a Ripple Gateway
3. Becoming a Market Maker
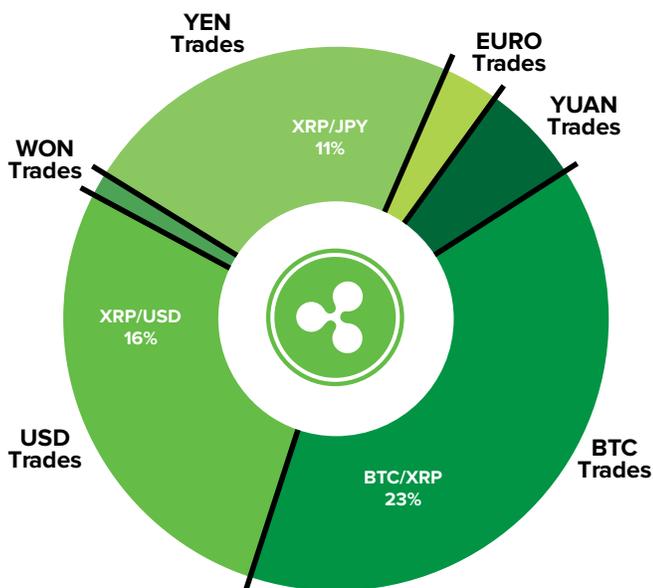
The "Ripple Gateways Brief" defines a Ripple Gateway as *"a business that provides onboard and offboard ramps to the Ripple network"*. A Ripple Gateway then provides access to trade in the RNxrp, accepting funds (fiat, cryptocurrencies) from clients and moving those funds into the RNxrp or providing funds from the RNxrp to clients. Gateway A receives funds from Client A sending those funds through the RNxrp to Gateway B that releases funds to Client B. A gateway is, in this simplified example, an MTO in one country, Gateway A in the country of origination, Gateway B in the country of destination.

Ripple gateways can choose to have their customers' accounts be independent or hosted. Independent accounts will have a unique address on the RNxrp connected to the gateway. Hosted accounts have indirect access to the RNxrp through their gateway's Ripple account. For example, a client that is an individual can have indirect access to RNxrp (meaning that the client's account is only with Gateway A) while a client that is institutional can receive its own a unique address on the RNxrp.

For those two Gateways to trade, we need a Market Maker in the center. Any Gateway can post bids and offers to trade currencies on Ripple's distributed exchange. Market Makers post both buy and sell orders, providing liquidity to the market in order to earn bid/ask spread. Market Makers play the critical role of facilitating payments between Gateways. Market Maker A "advertises" a price to exchange, for example USD/EUR, that maybe higher or lower than Market Maker B's price. The system uses the best bet, but Gateway A can trust Market Maker A more and sets its system to use it (within limits).

Market Makers can be Banks, but they can also be Forex Firms, or institutions founded on the RNxrp to make money in the spread.

E. Is Ripple also a cryptocurrency?

The answer will be no, rather, it is a protocol. However, the Ripple Network does have a cryptocurrency or math-based currency called XRP (sometimes pronounced "ripples") that is native to the Ripple Network, which
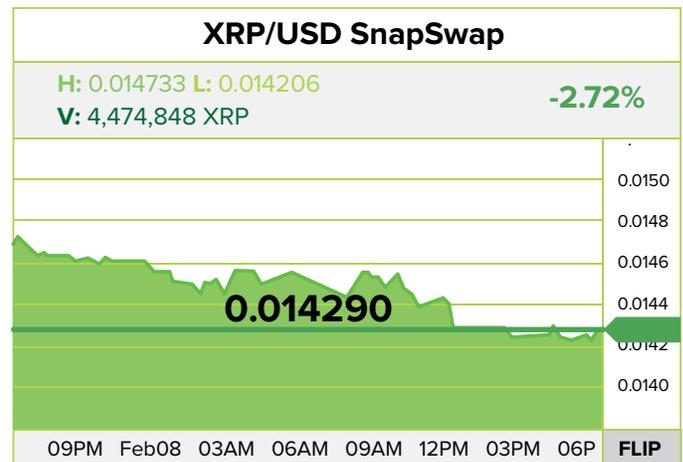
we labeled in the beginning RNxrp. In the same way bitcoin exists on the Blockchain, XRP exists natively within the RNxrp as a counterparty free currency. Because XRP is an asset as opposed to a redeemable balance, it does not require that users trust any specific financial institution to trade or exchange it. You can buy and sell XRPs and you can also exchange it globally, and the RNxrp will choose the best exchange rates in the network to settle. Users of the Ripple network are not required to use XRP as a medium of exchange or as a store of value.

It is important to understand that the RNxrp is currency agnostic. Users can use their preferred currency, whether that's USD, EUR, and even Bitcoin. XRP is intended to fulfill two primary network functions – network security and to act as a currency bridge. XRP can fill in as a neutral currency with no counterparty risk. An institution can find advantageous to convert their currency to and from XRP to be able to transact with each other. Bitcoin Remittance Companies do it with Bitcoin all the time; with Ripple you have the ability to use XRP, BTC or any other currency.

Three factors make XRP an ideal bridge currency on the Ripple network:

- It can be sent directly to any account with no transfer fees

- XRP has no counterparty risk. It is the only currency native to the Ripple network and thus requires no trust relationship with any gateway or third party.

- XRP cannot be debased – a finite amount exists. 100 billion XRP was "minted" with the creation of the protocol, and by definition, no more will ever be created.

> In 2014 the number of Ripple Accounts duplicated, from around 62,000 accounts to more than 135,000 accounts and growing by about 7 to 8,000 a month.

XRP/USD SnapSwap

H: 0.014733 L: 0.014206
V: 4,474,848 XRP

-2.72%

0.0150
0.0148
0.0146
0.0144
0.0142
0.0140

0.014290

09PM Feb08 03AM 06AM 09AM 12PM 03PM 06P | **FLIP**

F. How large is the Ripple Network?

In Ripple's Executive Summary for Financial Institutions[93], a must read, the company says: *"Ripple Labs is engaged with dozens of regulators, central banks, banks, payment networks, and liquidity providers globally (Americas, Europe, Asia-Pacific). Public engagements include: CBW Bank (US), Cross River Bank (US) Fidor Bank (Germany), and Earthport (global interbank payment network operating in 65 countries). Private engagements include: top-20 EU and US banks, EU and US bank consortiums, multibillion-dollar hedge funds and quantitative trading firms, top-10 global remittance operators, and top-15 global Telcos"*.

You can view at any given moment, 24/7, the trade volume in the RNxrp by clicking here: https://www.ripplecharts.com/.

You can see how USD, Bitcoin, and Japanese Yen transactions were at this moment more than 2/3 of the trades that were being posted at this particular time.

In Ripple Charts you can also see a graph with the Total Network Value and the 24 hr. Transaction Volume, as well as charts for the time variation of the conversion rates.

You can also see that in 2014 the number of Ripple Accounts doubled, from around 62,000 accounts to more than 135,000 accounts and growing by about 7 to 8,000 a month.

PROTOCOLS AND INNOVATIONS TO WATCH

STELLAR

Stellar is a newer blockchain-based protocol entering the market. It can be easily said that it is an offshoot of Ripple, and, as we mentioned earlier, it grew out of Jed McCaleb's exit. In addition to Jed's knowledge of blockchains, Stripe's early founders also had input in Stellar by investing US 3 Million in July 2014[94].

Another group of technology and investment personalities has moved to help Stellar grow. Its board has Stripe[95] co-founder Patrick Collison, Khosla VC and former Square COO Keith Rabois, and its advisors are well-known in the silicon-valley scene: security expert Dan Kaminsky, Joi Ito, Ronaldo Lemos, Linda Stone, and Combinator's Sam Altman, Naval Ravikant, Jackson Palmer, Greg Stein, and WordPress' Matt Mullenweg[96]. Lately, Professor David Mazieres from Stanford University joined Stellar and news were published[97] that he had invented (perfected?) SCP, the Stellar Consensus Protocol.

Stellar's technology might be similar to Ripple's, but it differs on the intentions and goals that it has set for its protocol, and with its non-profit aspect. While Ripple is building its system to serve bank and large financial institutions (from ebanks to larger traditional banks, as well as central banks), Stellar wants to fill the gap and be a protocol that can be used not only with virtual currencies but also with fiat currencies--Stellar wants to be a bridge and an enabler to convert all of the currencies between one and the other.

In August of 2014, writers Cade Metz and Marcus Wohlsen wrote a WIRED article entitled "New Digital Currency Aims to Unite Every Money System on Earth"[98], outlining the ideas behind Stellar and raising questions everyone about its true potential. Let's take two quotes from the article: *"...this new project aims to bring digital currencies to a much wider audience and provide a much smoother way of moving all sorts of money over the internet"*. It is *"an effort to create a worldwide network that lets anyone send any currency*

and have it arrive as any other currency. You can send bitcoin and have them arrive as dollars. You can pay someone in euros, and he can receive them as litecoin. You can transmit yen and turn them into dogecoin or Brazilian real". For anyone in the Money Transfer industry these sort of statements are worth listening to.

A. How can Stellar be a solution for MTOs?

Stellar[99] is based on the same mainframe ideas of Bitcoin & Ripple. If you have read the document, you then have a good grasp of the basic ideas that Stellar shares with other blockchain-based systems:

> "Gateways are simply entities that people trust to hold their deposits and issue credits into the Stellar network for those deposits".

- Decentralized Network: *"the Stellar network does not depend on any single entity. The idea is to have as many independent servers participate in the Stellar network as possible, so that the network will still run successfully even if some servers fail."*

- A Ledger-based approach: *"the Stellar ledger records a list of all the balances and transactions belonging to every single account on the network. A complete copy of the global Stellar ledger is hosted on each server that runs the Stellar software. Any entity can run a Stellar server."*

- A network consensus: *"The Stellar servers communicate and sync with each other to ensure that transactions are valid and get applied successfully to the global ledger."* Every 2-5 seconds all servers synch themselves and authenticate the transaction and it becomes true and final.

- The need for Gateways and a distributed exchange: *"Gateways are simply entities that people trust to hold their deposits and issue credits into the Stellar network for those deposits. They act as a bridge*

between different currencies and the Stellar network." The success of the Stellar network will depend on the number and strength of these gateways to trade, issue credit, handle deposits and withdrawals, and interact with the consumers.

- Multicurrency Transactions: *"Stellar allows you to send any currency you hold to anyone else in a different currency through the built-in distributed exchange. People can receive any currency through a gateway they added."* The interconnected gateways all over the world will share exchange prices and the system will pick and choose the best conversion (and a number of other considerations) to perform the fast and final settlement.

- Gateways are working on ways to make the user's experience completely independent of the technology behind the system. The tools being built on top of Stellar will be key to the adoption of the protocol. With Stripe, Stellar will have access to all the merchants already using Stripe, which might be a plus for the system. As we learn more about the Stellar network, we will be updating this document as we analyze the system further to see if it can become the protocol of choice for MTOs in the years to come.

EPIPHYTE

Epiphyte says in its Homepage[100] exactly what it intends to be: *"Bridge the gap between established finance and cryptofinance - Enterprise software solutions for financial service providers to securely integrate with cryptofinancial networks"*. In a way Epiphyte is going head to head with Ripple but not developing its own blockchain but building on top of Bitcoin. It is a *"bitcoin-based international transfer technology designed for banks. Epiphyte's solution avoids traditional money movement avenues and instead converts currency to bitcoins, moves the coins, then cashes them out on the other end in the local tender"*[101].

ETHEREUM

Ethereum is another blockchain protocol that is being develop and its used will broaden the use of these distributed public ledgers to a large number of uses that need agreements of parties to be excuted, like payment of dividends, use of joint savings accounts, corporate investments, agreements that are called *"self-enforcing smart contracts"*, smart in the sense that the rules for enforcement are part of the programming and are executed. The use of Ethereum's blockchain protocol in financial services or money transfers is hard to predict but we can envision a system where pensions are distributed digitally to hundreds of recipients in a matter of seconds without complex human interactions. Let's just leave it at that.

> "Bridge the gap between established finance and cryptofinance".

But to explain what Ethereum is in a more technical manner to those of you that want a better introduction to this protocol I have to quote Primavera De Filippi in an article[102] written in April 2014: *"Ethereum is a contract validating and enforcing system based on a distributed public ledger (or blockchain) such as the one implemented by the Bitcoin cryptocurrency. Yet, Ethereum also features an internal Turing-complete scripting language that can be used to encode advanced transaction types directly into the blockchain. This allows for the deployment of self-enforcing smart contracts (such as joint savings accounts, financial exchange markets, or even trust funds) as well as distributed autonomous organizations (DAOs) that subsist independently of any moral or legal entity. These algorithmical entities are both autonomous and self-sufficient: they charge users from the services they provide so as to pay others for the resources they need"*.

To pay, to transact value, to debit charges, etc. Ethereum uses its own cryptocurrency, the Ether, which still has no value since it hasn't started trading. Ether, like all cryptocurrencies can be exchange into Bitcoin and other altcoins.

[1] http://bit.ly/mtbitblock1

[2] I created the term Blockchains, in plural, as a way to group and describe sequential, transaction-database protocols.

[3] http://bit.ly/1xXw5eV

[4] http://bit.ly/mtbitblock2

[5] https://www.crunchbase.com/person/brock-pierce

[6] http://bit.ly/1uoeLim

[7] https://blockchain.info/

[8] TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet providing end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed and received at the destination.

[9] From a paper by Vitalik Buterin on January 23, 2014 that we will mention again later.

[10] http://bit.ly/1NLxjif

[11] http://ethereum.org

[12] http://www.epiphyte.us/

[13] http://bit.ly/1Glw9aO

[14] http://www.investopedia.com/terms/a/altcoin.asp

[15] https://coinmarketcap.com/

[16] https://bitspark.io/

[17] https://shiftpayments.com/

[18] http://www.xendit.co/

[19] http://bit.ly/1y53buE

[20] http://bit.ly/1NLwLsz

[21] http://bit.ly/1NLxjif

[22] http://bit.ly/1NLwLsz

[23] http://bit.ly/1AOx9RO

[24] http://bit.ly/1rlHF10

[25] Wikipedia:"Fiat money is currency which derives its value from government regulation or law [US Dollars, Euros, etc.]. It differs from commodity money, which is based on a good, often a precious metal such as gold or silver, which has uses other than as a medium of exchange. The term derives from the Latin fiat ("let it be done", "it shall be")"

[26] http://bit.ly/1A0jtlu

[27] http://bit.ly/1ClIMMr

[28] http://bit.ly/1vssqWp

[29] http://bit.ly/1zoG4Wc

[30] http://bit.ly/16VOnSp

[31] http://bit.ly/16VOnSp

[32] http://bit.ly/1AbO40F

[33] http://bit.ly/1COZ6v6

[34] http://ftalphaville.ft.com/tag/bitcoinmania/

[35] http://on.ft.com/1KG3Cvx

[36] http://bit.ly/1OOCn75

[37] http://bit.ly/1zMyEkC

[38] http://onforb.es/1D1WYgM

[39] http://bit.ly/1zMyFoR

[40] http://bit.ly/1JR6Hu1

[41] http://bit.ly/1yCX2Gl

[42] http://bit.ly/1G2c5ce

[43] http://bit.ly/1yD3Fsb

[44] http://onforb.es/1lnzpS9

[45] http://bit.ly/1Ebbtn9

[46] http://bit.ly/1CXtb6u

[47] http://bit.ly/1H7M5fZ

[48] http://bit.ly/1wUMcIQ

[49] http://bit.ly/1AXkjB2

[50] https://www.bitfinex.com/

[51] https://www.bitstamp.net/

[52] https://btc-e.com/

[53] https://www.kraken.com/

[54] https://www.huobi.com/

[55] https://www.okcoin.com/

[56] https://www.cryptsy.com/

[57] https://vip.btcchina.com/

[58] http://bit.ly/1wv5tv5

[59] https://www.coinbase.com/

[60] https://alphapoint.com/

[61] http://bit.ly/1A2r058

[62] http://blockchain.info/

[63] https://coinbase.com/

[64] https://www.circle.com/en

[65] https://airbitz.co/

[66] http://bit.ly/1Ezl870

[67] https://bylls.com/

[68] https://www.livingroomofsatoshi.com/

[69] https://quantified.com.sg/

[70] https://www.pademobile.com/

[71] http://enbitcoins.com/

[72] https://tukarcash.com/

[73] http://bahtcoin.com/

[74] http://bit.ly/1rtMUMl

[75] https://www.bitbond.com/

[76] https://btcjam.com/

[77] https://www.elliptic.co/vault

[78] https://blockchain.info/wallet

[79] http://bitcoinfoundation.org/

[80] http://bit.ly/1JcHAkh

[81] http://insidebitcoins.com/

[82] http://www.smileexpo.ru/en/

[83] http://summit.virtualcurrencytoday.com/

[84] http://texasbitcoinconference.com/

[85] http://bitcoinconference.co.za/

[86] http://labitconf.com/

[87] http://imtconferences.com/mtbit

[88] http://sci.ph/

[89] http://bit.ly/1NBmxuN

[90] http://bit.ly/1ClnBdJ

[91] If you like drama then read the sad coming of age stories of Ripple's founders: http://bit.ly/1zGsNMM

[92] This is Ripple's Basic Protocol Primer Brief: https://ripple.com/files/ripple_primer.pdf

[93] http://bit.ly/1FnmXAJ

[94] http://bit.ly/1zQpFL3

[95] Stripe (https://stripe.com/) is a payment processor that is competing against PayPal with technology and customer service and is the processor of choice for newer ecommerce sites.
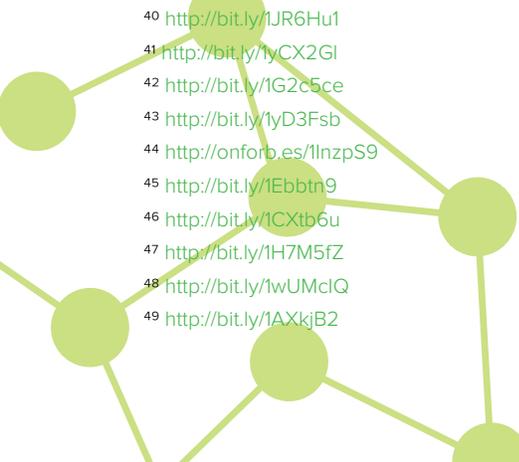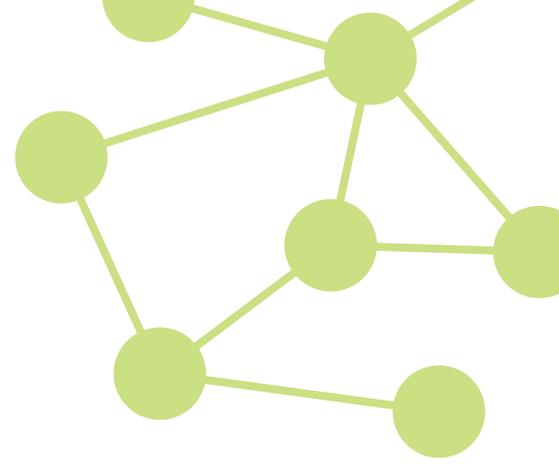
[96] http://tcrn.ch/1E7gsnT

[97] http://bit.ly/1DqpnLF

[98] http://wrd.cm/1CeqpiJ

[99] http://bit.ly/1CerYNU

[100] http://www.epiphyte.us/

[101] http://bit.ly/1Glw9aO

[102] http://bit.ly/1CY9jF9

Mohr World Consulting

MWC was created in 2001 to provide a basis for the consultancy work being given by Hugo Cuevas-Mohr to money transfer companies in North, Central and South America, the Caribbean and Europe. Mohr World Consulting advises money transfer entrepreneurs, companies, corporations, financial institutions, multilateral and government agencies on remittances & money transfers.

MWC has consulted for a number of companies and institutions and has recently expanded its consultancy work to include strategic, business, marketing, legal, compliance, technology, product development and other areas with partners, associates and colleagues in different fields and regions of the world.

You can check the company's website for information: www.mohr.world

Mohr World Consulting
16135 SW 109 St,
Miami, FL 33196
+1 786 2387857
hugo@mohr.world

About the Author

Hugo Cuevas-Mohr is President and CEO of Mohr World Consulting, a consultancy based in Miami, Florida. Hugo is a Money Transfer Expert and has been a consultant for a number of companies and financial institutions in the Money Transfer Industry in Latin America, United States and Europe. Since 2001 he began offering his consulting services. He is invited regularly as a Speaker in International Payment Conferences on Remittances, Financial Inclusion, Mobile Money, Regulation, etc. His work as a consultant lead to the development of IMTC, the International Money Transfer Conferences which he directs since 2010.