Cryptocurrencies, Blockchain, and a new view of Money

Fromm Institute
Winter 2019
Bebo White - bebo.white@gmail.com
Makeup on March 4
slides are always subject to change from those posted and those used


I will take periodic lecture breaks for Q&A
What we're about

We are a decentralized global community that shares a passion for crypto, blockchain and how it's going to change the world in dramatic ways. Crypto Mondays San Francisco will offer fantastic content from panelists to presentations, and offer a place to network with people sharing their views, learning and having a blast. All funds raised via Crypto Mondays will be given to charities chosen by its decentralized governance (i.e. every Crypto Monday gets a vote). If you or someone you are know are interested in hosting a Crypto Mondays in your town, please email cryptomondays@cryptooracle.io. For San Francisco specific questions please email sfcryptomondays@gmail.com.
MON, JAN 28, 6:00 PM
ICO's are dead! Fundraising in a post ICO world

ICO's skyrocketed in 17 and grew even further in '18 but in the latter half of the year we saw a steep decline in the # of ICO's. With few ICO's being profitable and a misalignment between investors buying tokens and communities wanting to use the token do ICO's have a future and if...

18 attendees

MON, FEB 18, 6:00 PM
Blockchain for Enterprise

We are a decentralized global community that shares a passion for Crypto and how it's going to change the world in dramatic ways. There is no content at Crypto Mondays other than like-minded people sharing their views, networking, learning and having a blast

1 attendee

MON, MAR 25, 6:00 PM
Exchanges

We are a decentralized global community that shares a passion for Crypto and how it's going to change the world in dramatic ways. There is no content at Crypto Mondays other than like-minded people sharing their views, networking, learning and having a blast
IF YOU CAN’T TRUST THE AARP, WHO CAN YOU TRUST?

Bitcoin
A bunch of computer code that a bunch of criminals, idealists and speculators agree is worth “real” money. Sadly, its real-money value swings widely, making it impractical except for criminals, idealists and speculators.

Blockchain
1. A different bunch of computer code containing an unalterable record of a series of transactions. The most famous is a digital ledger recording all bitcoin transfers.
2. A word often uttered by companies hoping to snare investors’ attention — and dollars.
Questions (1/7/2019)

• If a pointer breaks or is deliberately broken, how do you keep the damage from propagating?

• Is a particular chain limited regarding amounts/additions of data… or is it infinite?

• How much CPU resources are required to support this blockchain database?

• Doesn’t blockchain run on the Internet? So, if each is a platform then blockchain is a platform on a platform. Stable?

• You said blockchain is a P2P network - wouldn’t a distributed structure be a better defense to corruption or failure?
Blockchain Size

SanDisk Cruzer 256GB USB 2.0 Flash Drive (SDCZ36-256G-B35)
by SanDisk

$42.99  $69.99  ♻️prime | FREE One-Day
FREE Delivery by Tomorrow, Jan 9

More Buying Choices
$39.98  (8 used & new offers)
BACK TO TYPES OF MONEY - FIAT CURRENCY

- **fiat**: 1630s, “authoritative sanction,” from Latin “let it be done” (used in the opening of Medieval Latin proclamations and commands)

- currency without intrinsic value (except maybe the paper)

- has value only because a government or bank decrees and maintains its value or because parties engaging in exchange agree on its value

- trust in government or issuer

- rai has value simply because the community agrees?
SUMMARY - WHAT IS MONEY?
(3 OF 3)

- characteristics (according to multiple economists):
  - a market-born institution
  - tool of exchange and saving
  - material commodity
  - divisible into units
  - imperishable
  - rare/scarcely
  - homogeneous
  - easily stored
  - not subject to wide fluctuations in value
  - always in demand among those you trade with
In 1944, the United States government chose the Mount Washington Hotel as the site for a gathering of representatives from 44 countries. This was to be the famed Bretton Woods Monetary Conference. The Conference established the World Bank, set the gold standard at $35.00 an ounce and chose the American dollar as the backbone of international exchange. The meeting provided the world with a badly needed post war currency stability.
Bretton Woods (1 of 2)

• goal was to rebuild the international economic system post-World War II by establishing a system of rules, institutions, and procedures

• established the International Monetary Fund (IMF) and the International Bank for Reconstruction and Development (IBRD) which today is part of the World Bank Group

• Soviet representatives declared them “branches of Wall Street”
BRETTON WOODS (2 OF 2)

• the United States (at that time) controlled 2/3 of the world’s gold

• the Bretton Woods monetary system rested on gold and the $US

• most of the member countries moved large amounts of their gold reserves to the US and received $35/ounce

• the physical movement of gold was unnecessary

• the US Federal Reserve acts as the world’s central bank and all the world’s central banks act as regional banks
TRIFFIN’S DILEMMA (IMF)

• “providing reserves and exchanges for the whole world is too much for one country and one currency to bear”

• in order to meet global demand for the $US, the US must run persistent current-account deficits with the rest of the world

• the $US could become a weapon in geopolitical disputes (e.g., trade wars)
In their impossibly good book *Money, Markets, and Sovereignty* (2009), Benn Steil and Manuel Hinds make the point that over the last four thousand years, the only period in which humanity has not consistently based its currency in metal, specifically gold, is the last forty. That’s right. Ever since President Richard M. Nixon announced forty years ago today, on August 15, 1971, that the U.S. would no longer officially trade dollars for gold, we have been enjoying a new era of human history.
AUGUST 15, 1971

• my wife and I were in Europe and could not exchange money

• Nixon effectively “killed” the Bretton Woods system

• the global economy effectively converges on fiat currency
I am a piece of paper and I control your entire life.
SO, IS CRYPTOCURRENCY/BITCOIN MONEY? (1 OF 2)

- if so, what kind?
- what characteristics of money apply?
- who is its community?
- what is its connection with fiat? is it fiat since its community “decrees” it?
- could it truly be a new form of money for a new era and a new age?
So, is cryptocurrency/bitcoin money? (2 of 2)

- Commodity Futures Trading Commission (CFTC) - cryptocurrency is a commodity
- Security and Exchange Commission (SEC) - cryptocurrency is a security
- Treasury Department/Financial Crimes Enforcement Network (FinCEN) - cryptocurrency is subject to currency rules
- Internal Revenue Service (IRS) - cryptocurrency is property
REP. SOTO, MEMBERS INTRODUCE BIPARTISAN BILLS PREVENTING VIRTUAL CURRENCY PRICE MANIPULATION

December 6, 2018 | Press Release

Legislation commissions research on potential cryptocurrency risks and preventative methods

Washington, D.C. – Today, Congressman Darren Soto (D–FL–09) along with Ted Budd (R–NC–13), introduced two pieces of legislation to help prevent virtual currency price manipulation and position the United States to be a leader in the cryptocurrency industry. The Virtual Currency Consumer Protection Act of 2018 and the U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2018, will analyze what can be done to protect consumers from price manipulation and to ensure America remains a global leader in fostering innovation in this evolving global marketplace. Reps. Soto and Budd released the following joint statement:

“Virtual currencies and the underlying blockchain technology has a profound potential to be a driver of economic growth. That’s why we must ensure that the United States is at the forefront of protecting consumers and the financial well-being of virtual currency investors, while also promoting an environment of innovation to maximize the potential of these technological advances. This bill will provide data on how Congress can best mitigate these risks while propelling development that benefits our economy.”
PAYMENT SYSTEMS

- any system used to settle financial transactions through the transfer of monetary value, and includes the institutions, instruments, people, rules, procedures, standards, and technologies that make such an exchange possible

- systems which use fiat currencies but do not require in-person cash transactions

- let’s only address (for now) personal transactions
SOME FAMILIAR PAYMENT SYSTEMS

- stored value smart cards - e.g., Clipper - operates like cash (?)
- debit cards - requires path of validation
- credit cards - requires path of validation
- checks - requires path of validation - “notational money”
- money orders/wire transfers - transaction fees
- online money transfers - e.g., PayPal - requires path of validation
How Credit Card Processing Works

1. Card presented by customer
2. Card is inserted into terminal
3. Processor communicates with card networks
4. Card network sends authorization to customer's bank
5. Card network relays approval to processor
6. Processor sends approval to terminal
7. Bank sends approval to card network
8. Sale is complete
PAYMENTS IN A DIGITAL WORLD

• one of the “killer apps” (IMHO) of WWW was e-commerce - consider what has happened to the “mom and pop” and “brick and mortar” stores

• the community that wants to exchange value is the whole world

• exchange of value between people who don’t know and/or don’t trust one another - who gets to set the conditions - the buyer or the seller?

• how does this align with fiat currencies and existing payment systems?

• the first “solution” was/is to “fit” existing currencies and payment systems to the digital/cyber community

• credit cards seemed to be a good fit

• later came systems like PayPal, but underneath they were just variations of the old payment systems…
TYPICAL CONCERNS ABOUT DIGITAL PAYMENTS

• security and privacy - e.g., credit card info protection, personal info protection, lack of anonymity, personal shopping history tracking, etc.

• what’s all this stuff about “https,” digital certificates, and SSL? (e.g., lock icon on your browser)

• consumer protection - “where’s my stuff?” - non-repudiation

• fiat currency conversion, transaction fees

• I’m sure that many of you have stories…
MICROPAYMENTS

• what happens when a payment amount is less than the minimum unit of a fiat currency?

• why is this even a relevant question?

• value of intellectual property online

• “almost free” concept - marketing ploy?

1 mill = “lowest money of account, of which 1000 shall be equal to the federal dollar”
- Continental Congress, 1786
DEVELOPMENT OF A NATIVE DIGITAL PAYMENT SYSTEM BECAME A TECHNOLOGICAL “HOLY GRAIL”

“The one thing that’s missing, but will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A”

- Milton Friedman
THE BIG ISSUES WERE

• trust
• anonymity
• de-centralization
• the “double spending” problem
• non-repudiation
• convertability to/from fiat currency
• adoption - not just a crazy computer science exercise
EARLY ATTEMPTS AT E-CASH

(1 OF 4)

• eCash, DigiCash
  • 1982/1990 - David Chaum
  • allowed two parties to transact without having to know one another
  • supported micropayments
  • uses a bank (mint) as the trusted holder of accounts
  • but, a third party vouches for signatures and can censor any individual party
• limited success, terminated operations around 1997
EARLY ATTEMPTS AT E-CASH (2 OF 4)

- Hashcash

  - 1997 - Adam Back
  
  - originally to combat e-mail spam and hacker attacks
  
  - used cryptography, but not really anonymous
  
  - attempted to be decentralized
  
  - the act of computing creates stored value that could be moved around
  
  - it was difficult set up an account so few did
EARLY ATTEMPTS AT E-CASH
(3 OF 4)

• Bit Gold
  • 1998 - Nick Szabo
  • core focus on minimization of trust, particularly from third parties
  • used a network of computers working towards creation of a trust model
  • described a mechanism very similar to blockchain
  • never implemented
EARLY ATTEMPTS AT E-CASH
(4 OF 4)

• B-money
  • 1998 - Wei Dai
  • defined an anonymous, unjammable broadcast method
  • participants interacted via cryptography
  • ledger was shared by all (or servers)
  • value was created through solving hard computational problems of known difficulty
  • believed impossible due to network constraints
“I don’t believe we shall ever have good money again before we take the thing out of the hands of government, that is, we can’t take it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can’t stop.”

-Friedrich Hayek (1984)
What are you talking about?
A digital currency should be adopted as the world's leading reserve currency

A geopolitically neutral currency will offer important protections against the increasing threat of trade wars.

Image: REUTERS/Jim Young
THE CYPHERPUNK MOVEMENT

• consists of activists who advocate the use of strong cryptography and privacy-enhancing technologies as a route to social and political change

• “privacy is necessary for an open society in the electronic age…we cannot expect governments, corporations, or other large, faceless organizations to grant us privacy…we must defend our own privacy if we expect to have any…cypherpunks write code. We know that someone has to write software to defend privacy, and…we’re going to write it.” - A Cypherpunk’s Manifesto, Eric Hughes, 1993

• original communication mechanism was through the cypherpunk electronic mailing list (1992)
THE CYPHERPUNK MOVEMENT INCLUDES

• researchers, faculty, entrepreneurs from around the world including
  • Adam Back, Wei Dai, Nick Szabo, et. al.
  • David Chaum - *Security without Identification: Transaction Systems to Make Big Brother Obsolete*
31 October 2008

• in the middle of one of the worst financial crises in history

• a paper was posted to the cypherpunk mailing list entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*

• the paper claimed to offer an alternative to the traditional banking system

• it was not posted through typical academic channels

• it laid out the fundamentals of Bitcoin, bitcoin, and blockchain

• the author was listed as *Satoshi Nakamoto*

• Satoshi had communicated with some of the cypherpunks previously but no one knew who he/she/they were
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will; accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.
3 January 2009

• the first ever cryptocurrency was officially launched

• known as “the Genesis block” - the first transaction/block on the Bitcoin blockchain

• Satoshi makes a statement:

RAW HEX VERSION

BITCOIN GENESIS BLOCK

Chancellor Alistair Darling on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up “toxic assets”, The Times has learnt.
“Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending...You can get coins by getting someone to send you some, or turn on Options->Generate Coins to run a node and generate blocks. I made the proof-of-work difficulty ridiculously easy to start with, so for a little while in the beginning a typical PC will be able to generate coins in just a few hours. It’ll get a lot harder when competition makes the automatic adjustment drive up the difficulty...The software is still alpha and experimental. There’s no guarantee the system’s state won’t have to be restarted at some point if it becomes necessary, although I’ve done everything I can to build in extensibility and versioning.”

-Satoshi Nakamoto in an e-mail to the Metzdowd cryptography mailing list
12 January 2009

• first BTC payment

• 100BTC, Satoshi to Hal Finney (a noted cryptography expert)
Bitcoin.org

Bitcoin v0.1 Alpha Release

Announcing the first release of Bitcoin, a new open source peer-to-peer electronic cash system that's completely decentralized, with no central server or trusted parties. Users hold the crypto keys to their own money and transact directly with each other, with the help of the network to check for double-spending.

Windows NT/2000/XP/Vista. Open source C++ code is included.

Download link: bitcoin-0.1.5.rar
WHY WERE THE CYPHERPUNKS ATTRACTED TO BITCOIN?

• loss of trust in banks and financial institutions as third parties?

• bad investment decisions by banks and financial institutions?

• techies had become a financial force and sought better solutions in technology?

• politics?

• anarchy and greed?
“Bitcoin for me is not an instrument for financial investment. Bitcoin for me is a declaration of our monetary independence.”

-Nick Spanos, founder, NYC Bitcoin Center
“The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.”

-Satoshi, in a forum post, February 11, 2009
SATOSHI SAW A WAY

• “The network is robust in its unstructured simplicity. Nodes work all at once with little coordination.”

• a distributed, peer-to-peer network of payments ledgers (non-centralized)
  • impossible (?) to forge/modify - based on rigorous technologies and techniques
  • doesn’t allow double-spending and provides proof-of-payment (non-repudiation)
  • supported by “the power of the crowd”

• not based on dollars, euros, pounds, etc., but a currency “for the digital age” - bank-free, government-free, empowering
Satoshi’s Response to Micropayments?

- 1 bitcoin (BTC) is divided into satoshi (SAT)
- 1 SAT = 0.000000001 BTC (one hundred millionth)
- To put into perspective, for 1 SAT = 1¢, 1 BTC = $1,000,000
- As the value of BTC increases, it is likely that most transactions will be in SAT
- 1 bit = one millionth or $10^{-6}$ BTC (not universally accepted)
SATOSHI’S RESPONSE TO MONEY SUPPLY AND INFLATION?

• the protocol dictates that the maximum number of BTC (ever) = 21*10^6 = 21 million

• maximum number of SAT = 2.1*10^{15} = 2,100,000,000,000,000

• to put into perspective, the amount of $US in the world = 10^{12} = 1,000,000,000,000

• new BTC are introduced via “mining” (more about that process later)

• some economists attribute BTC volatility to the fixed limit
Total bitcoins in circulation over time (millions)
WHO IS SATOSHI?

• still no one knows

• many claims and suspicions, but no proof

• is in possession of 980,000 bitcoins - none have been used
SPECULATIONS

• Vili Lehdonvirta
• Shinichi Mochizuki
• Dorian Nakamoto *
• Nick Szabo *
• Hal Finney *
• Craig Wright *
• Neal King, Vladimir Oksman, and Charles Bry
• Elon Musk *
• a secret government agency *
Satoshi Nakamoto: Mysterious Bitcoin Creator World’s 44th Most Powerful Person in Finance
HOW CAN A PAPER BY AN OBSCURE AND UNKNOWN AUTHOR MAKE A DIFFERENCE AND START A REVOLUTION?

Because the world was ready for it
**Virgin No-Coiner**

Believes debt is the only way to grow an economy

Feels that central banking is necessary

Only understands what 'fiat' means in reference to the automobile

Thinks money should be printed whenever it is needed

Thinks cryptos are a ponzi scheme while ignoring the fact that there will always be more debt owed to the Federal Reserve than there is USD in existence, and to pay off debt would require more loans from the Federal Reserve.

**Chad Bitcoiner**

Thinks hashing has something to do with making weed

Trusts that the government will not make financial laws favoring the wealthy

Thinks Satoshi Nakamoto is an anime

Thinks an inflationary currency is a good thing

Believes in a monetary system where wealth is generated via work instead of debt

Understands that there is no need for centralized banking anymore

Trusts in currency which is mathematically designed to increase in value over time, rather than one regulated by greedy financiers.

Knows that no man should have control the supply of money; this will only lead to it's devaluation due to greed.

Knows that every time someone says Bitcoin is crashing it is a Virgin No-Coiner speaking.

Enjoys market instability; sells off on every high and buys in on every low for massive gains

Knows Satoshi Nakamoto personally and regularly has drinks with the fellow at bars which accept cryptos.

Has not owned a single USD since the gold standard was removed and the USD declared fiat. Purchased all of his Bitcoins and mining equipment with saved up gold bullion.

Able to mentally calculate implicit trade values accross several markets simultaneously.
Today, bitcoiners the world over will celebrate the anniversary of the most expensive pizzas in history.

Bought on 22nd May 2010 by Laszlo Hanyecz, the programmer paid a fellow Bitcoin Talk forum user 10,000 BTC for two Papa John’s pizzas. Back then, when the technology was just over a year old – that equated to roughly $25, but is $5.12m by today’s exchange rate.