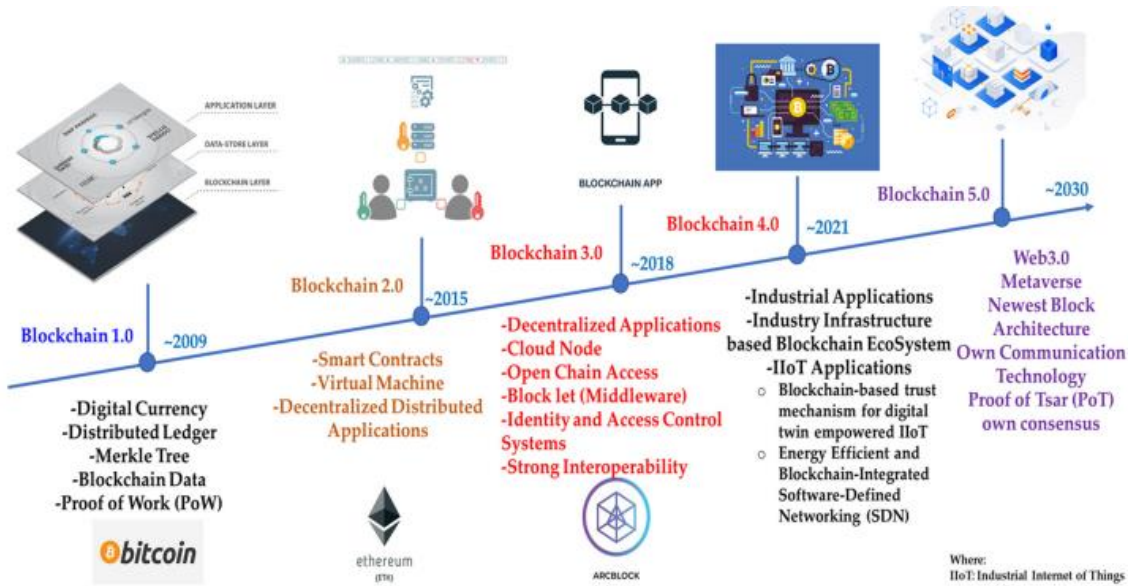


# BlockChain Technologies

What is blockchain





# THE HISTORY OF MONEY



**BARTER**



**GOLD**



**METALL  
COINS**



**PAPER  
MONEY**



**PLASTIC  
CARDS**

# THE HISTORY OF MONEY

- Gold-Based Money
- Fiat Money

What is **Money** by the way?

- Fungibility
- Scarcity
- Divisibility
- Durability
- Transferability
- Liquidity
- Legitimacy



# ONLINE SHOPPING

- Credit card transactions are the dominant payment method that is used on the web today.
- If you have ever bought something from an online seller, you know how the arrangement goes.
  - There is a company that sits between you and the seller, so you send your credit card details to this intermediary, which approves the transaction and notifies the seller.
- Cash offers two additional **advantages**:
  - **Better anonymity**
    - Since your credit card is issued in your name, the bank can track all your spending.
  - **Offline transactions**

# EARLY ATTEMPTS

- The earliest ideas of applying cryptography to cash came from **David Chaum** in 1983.

The bearer of this note may redeem it for one dollar by presenting it to me

*MySignature*

123456789

If people trust you and consider your signature unforgeable, they can pass around these pieces of paper just like banknotes.

We can do the same thing electronically with digital signatures, but that runs into the “double spending” problem

→ Unique serial number

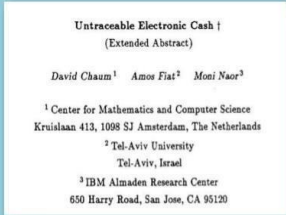
- Only need a server to do signing and record-keeping of serial numbers

# PROBLEMS WITH THE SCHEME

- It's not **anonymous**: when I issue a note to you, I can record the serial number along with your identity, and I can do the same when someone else later redeems it.
- Chaum's innovation to both keep the system anonymous and prevent double-spending:
  - When I issue a new note to you, **you** pick the serial number.
  - You write it down on the piece of paper, but cover it so that I can't see it.
  - Then I'll sign it, still unable to see the serial number.
  - This is called a **blind signature** in cryptography.
- This was the first serious **digital cash** proposal.
- It works, but it is not **offline**.
  - It requires a server run by a central authority, such as a bank, and for everyone to trust that entity.

# DIGICASH

- In 1988, Chaum, Fiat and Naor proposed **offline** electronic cash.
- The clever idea is to stop worrying about preventing double-spending and focus on detecting it, after the fact, when the merchant re-connects to the bank server.
- If you ever double-spend a coin, eventually both recipients will go to the bank to redeem their notes, and when they do this, the bank can put the two pieces of information together to decode your identity completely



Untraceable Electronic Cash †  
(Extended Abstract)


David Chaum<sup>1</sup> Amos Fiat<sup>2</sup> Moni Naor<sup>3</sup>

<sup>1</sup> Center for Mathematics and Computer Science  
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

<sup>2</sup> Tel-Aviv University  
Tel-Aviv, Israel


<sup>3</sup> IBM Almaden Research Center  
650 Harry Road, San Jose, CA 95120

CRYPTO 1988



David Chaum

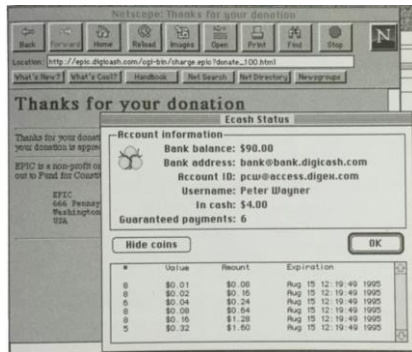
Photo: Declan McCullagh [2002]





# DIGICASH

- Chaum formed a company in 1989 called **DigiCash**, probably the earliest company that tried to solve the problem of online payments.
- The actual cash in DigiCash's system was called **Ecash**.
- There were banks that actually implemented it: a few in the US and one in Finland.
- Chaum had several patents on DigiCash technology, in particular, the blind-signature scheme that it used.



# WHY DIGICASH FAILED?

- The main problem with DigiCash was that it was hard to persuade the banks and the merchants to adopt it.
- Since there weren't many merchants that accepted Ecash, users didn't want it either.
- It didn't support user-to-user transactions.
- It was really centered on the user-to-merchant transaction. So if merchants weren't on board, there was no other way to bootstrap interest in the system.
- Bitcoin allows user-to-merchant and user-to-user transactions.
- The support for user-to-user transactions probably contributed to Bitcoin's success.
  - There was something to do with your bitcoins right from the beginning: send it to other users, while the community tried to drum up support for Bitcoin and get merchants to accept it.

# ACHIEVING SCARCITY

- To create a free-floating digital currency that is likely to acquire real value, you need to have something that's scarce by design.
- In the digital realm, one way to achieve scarcity is to design the system so that minting money requires solving a computational problem (or puzzle) that takes a while to crack.
- It was first proposed by cryptographers Dwork and Naor as a potential solution to email spam back in 1992.
- A similar idea was later discovered independently by Adam Back in 1997 in a proposal called Hashcash.
  - Bitcoin uses essentially the same computational puzzle as Hashcash, but with some minor improvements.
- Why did Hashcash never catch on?
  - Spam wasn't a big enough problem to solve.

# B-MONEY AND BITGOLD

- Bitcoin combines the idea of using computational puzzles to regulate the creation of new currency units with the idea of secure time-stamping to record a ledger of transactions and prevent double spending.
- **b-money**: invented by Wei Dai in 1998.
  - Anyone can create money using a hashcash-like system.
  - There's a P2P network, like in Bitcoin.
  - Each node maintains a ledger, but not a global ledger like in the Bitcoin.
- **Bitgold**: invented by Nick Szabo in 2005.
- **b-money and Bitgold were informal proposals**
  - b-money was a post on a mailing list and Bitgold was a series of blog posts.
  - Neither took off, or was even implemented directly.
  - Unlike the Bitcoin white paper, there wasn't a full specification or any code.



# IMPORTANCE OF DIGITAL CASH

**The 1990s**

**David Chaum and anonymous ecash**

*“The difference between  
a bad electronic cash system  
and well-developed digital cash  
will determine whether  
we will have a dictatorship  
or a real democracy”*



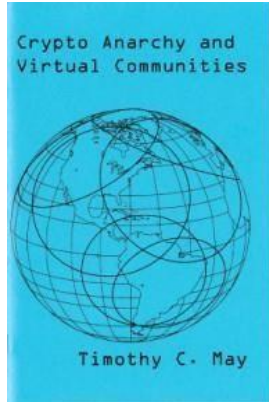
(attributed to Chaum)

# LIBERTARIAN DREAMS

- The existing financial system was viewed as one of the greatest threats to individual privacy.
- With the advance of technology in the 1980s and 90s, the Cypherpunk movement came into being.
- A group of activists formed the “Cypherpunk Mailing List” to exchange information on privacy, cryptography and online liberty.
- Started by **Timothy May**, Eric Hughes, St. Jude and John Gilmore.
- Cypherpunk Manifesto:  
“Privacy is necessary for an open society in the electronic age.”



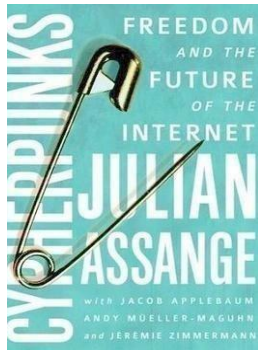
# CYPHERPUNKS AND CRYPTO-ANARCHISTS



<https://news.bitcoin.com/introduction-cypherpunk-tale/>

# NOTEWORTHY CYPHERPUNKS

- **Jacob Appelbaum:** A core member of Tor project
- **Julian Assange:** WikiLeaks founder
- **Adam Back:** inventor of Hashcash
- **Philip Zimmermann:** original creator of PGP
- **Nick Szabo:** inventor of Bitgold
- **Bruce Schneier:** well-known security author
- **Hal Finney:** cryptographer, main author of PGP 2.0
- **Satoshi Nakamoto**





# BITCOIN, THE 2008 MYSTERIOUS BIRTH

- In the three months of August to October, 2008:
  - In the middle of Financial Crisis, **Bitcoin.org** was registered (Aug 18)
  - Sep 12 to 16 (Fri to Tue), Financial Armageddon
    - The Domino of Bankruptcies reaching Huge Banks (Lehman and Merrill) (Fri)
    - Bank of America bought Merrill Lynch for \$50 billion (Sun),
    - US and Britain do NOT support Barclays to buy Lehman (Sun),  
Lehman Brothers filed for **the largest bankruptcy in American** history (Mon),
    - Then to Stop the Domino, the **U.S. Government** established the \$700 billion Troubled Asset Relief Program to Support AIG and other huge companies (Tue)

# SATOSHI NAKAMOTO

- **Satoshi Nakamoto** is the anonymous creator of Bitcoin who wrote a nine-page white paper that brilliantly combined all previous efforts to create a self-sustaining digital money.

## 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.



## 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.



- It's completely **decentralized**, with no central server or trusted parties, because everything is based on **crypto proof** instead of **trust** ...

# WHO IS SATOSHI NAKAMOTO?



**Nick Szabo**  
The inventor of  
Bitgold



**Dorian Nakamoto**  
systems engineer on classified  
defense projects and computer  
engineer for technology and  
financial information services  
companies



**Hal Finney**  
An early Bitcoin user and  
received the first bitcoin  
transaction from Satoshi  
Nakamoto.

# WHO IS SATOSHI NAKAMOTO?

- **Craig Steven Wright**
- Australian computer scientist
- Gizmodo published a story with evidence obtained by a hacker who supposedly broke into Wright's email accounts
- Claimed that Satoshi Nakamoto was a joint pseudonym for Craig Steven Wright and computer forensics analyst David Kleiman, who died in 2013.



## Here's All the Evidence That Craig Wright Invented Bitcoin



Kate Knibbs

12/09/15 11:10am • Filed to: BITCOIN



29.8K



49



5



Sommer

Okay. So any questions about any of that? Do you need to change - -

McMaster

No, it's good for another 15 minutes.

Sommer

Okay. Good. This is going to make riveting listening.

McMaster

Well, the Aus transcript person is going to love it.

Sommer

Excellent. I always - you know, my students sometimes hate my lectures and just cannot understand why it is unless they're suffering from, you know - -

McMaster

Insomnia?

Sommer

Sleep deprivation.

Wright

I did my best to try and hide the fact that I've been running bitcoin since 2009 but I think it's getting - most - most - by the end of this I think half the world is going to bloody know.

# WHY MAINTAIN ANONYMITY?

## ➤ Just for fun:

- Many people write novels anonymously, and there are graffiti artists like Banksy who maintain their anonymity.

## ➤ Legal worries:

- Two U.S. companies, Liberty Reserve and e-Gold, ran into legal trouble for money laundering.
- In 2006, one of the founders of Liberty Reserve fled the United States
- E-Gold's founders stayed in the US, and pled guilty to the charges.
- The guilty plea was registered right before Satoshi set up the Bitcoin website

## ➤ Personal security:

- We know that Satoshi has a lot of bitcoins from his mining early on, and due to Bitcoin's success these are now worth a lot of money.

# GENESIS BLOCK

**THE TIMES**  
 Sunday January 3 2009 Timesonline.co.uk No 65123 £1.50

**Eat Out from £5**  
 More than 900 great restaurants, including four Gordon Ramsay favourites from £15

**Israel prepares to send tanks and troops into Gaza**

**Chancellor on brink of second bailout for banks**  
 Billions may be needed as lending squeeze tightens

**99p**

**Salmon Rushdie I Won't Marry Again**

**Giant Killing? Guide to the FA Cup Third Round**

## Block 0<sup>2</sup>

Short link: <http://blockexplorer.com/b/0>

Hash<sup>2</sup>: 00000000019d6689c085ae165831e934f1763ae46a2a6c172b3f1b60a8ce26f

Next block<sup>2</sup>: 00000000839a8e6886ab5951d76f411475428afc90947cc320161bbf18eb6048

Time<sup>2</sup>: 2009-01-03 18:15:05

Difficulty<sup>2</sup>: 1 ("Bits"<sup>2</sup>: 1d00fff)

Transactions<sup>2</sup>: 1

Total BTC<sup>2</sup>: 50

Size<sup>2</sup>: 285 bytes

Merkle root<sup>2</sup>: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce<sup>2</sup>: 2083236893

Raw block<sup>2</sup>

## Transactions

Transaction <sup>2</sup>	Fee <sup>2</sup>	Size (kB) <sup>2</sup>	From (amount) <sup>2</sup>	To (amount) <sup>2</sup>
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGeF1tTL5SLmv7DivfNa: 50

- Genesis block mined Jan 3, 2009
- The **coinbase** of the genesis block references a story in the Times of London newspaper involving the Chancellor bailing out banks
- Bitcoin's libertarian roots
- First bitcoin transaction on Jan 12, 2009 with **Hal Finney**

# MILLION DOLLAR PIZZA

- **Laszlo Hanyecz** made the first documented purchase of a good with bitcoin when he bought two Domino's pizzas from **Jeremy Sturdivant** for 10,000 BTC.
- Laszlo had made contributions to Bitcoin's source code in the past.
- World's first ever Bitcoin transaction for a tangible asset.
- To commemorate the transaction, May 22 is dubbed **Bitcoin Pizza Day**.



The pizzas bought by Laszlo



# SILK ROAD



Welcome [redacted]  
messages(0) | orders(0) | account(\$0.00) | settings | log out

search | (0)

## Shop by category:

[Drugs\(1819\)](#)  
Benzos(176)  
Cannabis(417)  
Dissociatives(49)  
Ecstasy(187)  
Opioids(162)  
Other(242)  
Psychedelics(232)  
Stimulants(216)  
[Apparel\(5\)](#)  
[Books\(188\)](#)  
[Collectibles\(2\)](#)  
[Computer equipment\(3\)](#)  
[Digital goods\(147\)](#)  
[Drug paraphernalia\(62\)](#)  
[Electronics\(9\)](#)  
[Fireworks\(2\)](#)  
[Food\(11\)](#)  
[Forgeries\(51\)](#)  
[Home & Garden\(1\)](#)  
[Jewelry\(1\)](#)  
[Lab Supplies\(9\)](#)  
[Medical\(13\)](#)  
[Money\(122\)](#)  
[Packaging\(1\)](#)  
[Services\(49\)](#)  
[XXX\(52\)](#)



Ibogaine HCL 2 grams

**\$146.45**



Barcode Manipulation  
scam keeping...

**\$0.59**



Metal Chamber Pipe

**\$1.78**



HEROIN (AFGHAN) PURE  
STRAIGHT...

**\$18.08**



\_Grape Wreck\_  
"Premium"

**\$3.04**



250mg 2C-E (4-ethyl-  
2,5-dimethoxyphenethyla

**\$19.83**



Ephedrine Hcl 48mg - 100  
Tablets

**\$17.72**



==== Party Time ==== 2x  
110mg...

**\$3.14**



One Kilogram Crystal  
Methyloine

**\$435.22**

## News:

- Who's your favorite?
- Acknowledging Heroes
- A new anonymous market **The Armory!**
- **State of the Road Address**

# SILK ROAD

- On February 2011, Silk Road opened for business: a Bitcoin marketplace, launched an illicit marketplace for drug deals, called the eBay for drugs.
- On October 2013, the FBI shut down Silk Road, seizing 3.6M dollars worth of bitcoin
- **Ross Ulbricht**, the founder of Silk Road, is currently serving a life sentence without possibility of parole.



# MT. GOX

- In 2010 **Mt. Gox** was established in Tokyo
  - The biggest bitcoin exchange during the beginning stages of bitcoin.
  - CEO: Mark Karpeles, a computer geek with little experience in the financial world.
- 2011: Mt. Gox suffers a significant breach of security that required the site to be shut down for seven days.
  - The breach compromised the Mt. Gox database with a leak of the user table that contained usernames, email addresses, and passwords of 60,000 accounts.
- 2014: Mt. Gox is handling 70% of transactions
- 2014: Mt. Gox loses over 850,000 bitcoins in a theft that went unnoticed for years and declared bankruptcy in April 2014



Mark Karpeles

# BLOCKCHAIN HISTORY

**SATOSHI NAKAMOTO**  
begins working  
on the concept

**Oct 2008**  
Bitcoin  
whitepaper  
published

**May 2010**  
First real world  
transaction is  
10,000 BTC for  
2 pizzas

**Feb 2011**  
Bitcoin  
reaches  
parity with  
the US dollar

**2011/2012**  
Fraud & illicit  
behavior gains  
momentum.  
Silk Road opens.  
Mt.Gox is  
hacked and shut  
down for 7 days.  
Governments  
warn of terrorist  
financing & FBI  
report leaked.

**May 2013**  
First Bitcoin  
ATM debuted  
in San Diego

**Apr 2014**  
Attacks on  
exchanges  
leads Mt.Gox  
to collapse.  
Bitcoin price  
craters

**Dec 2014**  
NY regulator  
proposes lighter  
rules for Bitcoin  
companies

2007

2008

2009

2010

2011

2012

2013

2014

2015

**Dec 2009**  
First Bitcoin  
transaction in  
block #170

**Aug 2008**  
Bitcoin.org is  
registered

**Jul 2010**  
Mt.Gox is  
established  
as an  
exchange

**Jun 2012**  
Block 181919  
is largest with  
1,322  
transactions

**Jun 2012**  
Coinbase, a  
bitcoin wallet,  
founded in San  
Francisco

**Aug 2013**  
NY State  
Dept. of  
Financial  
Services  
subpoenas  
22 bitcoin  
companies

**Nov 2013**  
Bitcoin  
reaches over  
\$1,000 after  
market  
perceives US  
Senate  
hearings were  
positive

**Sep 2014**  
PayPal  
announces  
Bitcoin  
integration

**Aug 2015**  
Bloomberg  
Markets magazine  
Blythe Masters  
feature on  
blockchain &  
financials.  
Suddenly,  
blockchain is hot.

