History of Digital Money

Campbell R. Harvey

Duke University and NBER

The beginning

Barter

- Very inefficient.
- Need to match needs of buyers/sellers

The beginning

Coins (Gold/Silver)

- Need metal to start and maintain

https://rg.ancients.info/lion/article.html

The beginning

Promissory Notes/Fiat

- Need trust
- Need to start it off and maintain

Credit

Modern on-line

- Buy something from retailer and given them your card information. The retailer deals with bank, credit card company, etc.
- Paypal is different. It is an intermediary that sits between you and the retailer. You give card details to Paypal and Paypal approves the transaction and settles with retailer. You don’t need to give seller credit card details. Apple Pay is similar in this respect.
- While people hesitant to give card details on line, we do it anyways. Lots of costly fraud.

Credit: My Mastercard

Oct. 14, 2015	J & B AIR LAREDO TX Expand Details	$ 3,910.00
Oct. 14, 2015	J & B AIR LAREDO TX Expand Details	$ 9,257.00
Oct. 14, 2015	J & B AIR LAREDO TX Expand Details	$ 9,257.00
Oct. 10, 2015	J & B AIR LAREDO TX Expand Details	$ 8,900.00
Oct. 10, 2015	J & B AIR LAREDO TX Expand Details	$ 9,414.00
Oct. 06, 2015	IN *J & B AIR CONDITIO 956-3240134 TX Expand Details	$ 3,465.00
Oct. 06, 2015	IN *J & B AIR CONDITIO 956-3240134 TX Expand Details	$ 8,900.00

Credit: My Mastercard

Oct. 21, 2015	IN *SOUTHWEST FLOORING 281-3585678 TX Expand Details	$ 8,500.00
Oct. 21, 2015	IN *SOUTHWEST FLOORING 281-3585678 TX Expand Details	$ 8,500.00
Oct. 21, 2015	IN *SOUTHWEST FLOORING 281-3585678 TX Expand Details	$ 8,500.00
Oct. 21, 2015	IN *SOUTHWEST FLOORING 281-3585678 TX Expand Details	$ 8,500.00

Digital Credit

FirstVirtual 1994

- Similar to PayPal. You give them card details and FV dealt with retailer
- All communication over email. No encryption used.
- Customer had 90 days to dispute charges and retailer only got paid after 90 days!

http://web.stanford.edu/~joelaw/bennpaper/emoney.html#FV

Digital Credit

SET Architecture* 1997

- Avoids user having to send card information to retailers – but avoid having to enroll with intermediary
- Standard developed by Visa/MC/Netscape/IBM/Microsoft/Verisign/RSA

http://www.maithean.com/docs/set_bk1.pdf and https://en.wikipedia.org/wiki/Secure_Electronic_Transaction

Digital Credit

SET Architecture* 1997

- Customer browses website and decides on what to purchase
- Customer sends order and payment information, which includes 2 parts in one message:
  a. Purchase Order – this part is for merchant
  b. Card Information – this part is for merchant's bank only.
- Merchant forwards card information (part b) to their bank
- Merchant's bank checks with Issuer (bank that offers card) for payment authorization
- Issuer send authorization to Merchant's bank
- Merchant's bank send authorization to merchant
- Merchant completes the order and sends confirmation to the customer
- Merchant captures the transaction from their bank
- Issuer prints credit card bill (invoice) to customer

https://en.wikipedia.org/wiki/Secure_Electronic_Transaction

Digital Credit

SET Architecture 1997

- An important innovation introduced in SET is the *dual signature*. The purpose of the dual signature is to link two messages that are intended for two different recipients.
- In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank.
- The merchant does not need to know the customer's credit-card number, and the bank does not need to know the details of the customer's order.
- The customer is afforded extra protection in terms of privacy by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary.
- The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service.

Digital Credit

SET Architecture 1997

- Hashes of the OI and the PI are independently calculated by the customer.
- The dual signature is the encrypted hash (with the customer's private key) of the concatenated hashes of PI and OI.
- The dual signature is sent to both the merchant and the bank. The protocol arranges for the merchant to see the hash of the PI without seeing the PI itself, and the bank sees the hash of the OI but not the OI itself.
- The dual signature can be verified using the hash of the OI or PI. It doesn't require the OI or PI itself. Its hash does not reveal the content of the OI or PI, and thus privacy is preserved.

Digital Credit

CyberCash 1994

- Used SET architecture.
- Digital cash product called CyberCoin which allowed for micro-transactions
- First company to get US approval for exporting encryption
- Killed by Y2K!

Digital Credit

Why Cybercash and SET failed*

- Problem surrounds certificates - a way to securely associate a cryptographic identity (public key) with a real life identity.
- Websites need to obtain certificates from a Certificate Authority like Verisign or Symantec
- CyberCash and SET required not just merchants – but all users get a certificate (very costly process)

*Visa, Mastercard, and American Express use a protocol known as 3-D Secure. Each has their own name for this.

Digital Credit

In mid-1990s, W3C was looking into standardizing financial payments – nothing happened until they announced revisiting in October 2015

W3C

FOR IMMEDIATE RELEASE

W3C Starts Web Payments Standards Work to Streamline the Online "Check-out" Process

Consumers and merchants to enjoy greater choice, security and simplicity in Web payments

---

Read below what W3C Members have to say about Web Payments

Backgrounder | Translations | W3C Press Release Archive

---

21 October 2015 — The World Wide Web Consortium (W3C) launched today the Web Payments Working Group to help streamline the online "check-out" process and make payments easier and more secure on the Web.

The proposed standards will support a wide array of existing and future payment methods, including debit, credit, mobile payment systems, escrow, and bitcoin and other distributed ledger technologies. Standardized APIs (Application Programming Interfaces) will establish a foundation for simplified checkout and payment

Digital Credit

December 12, 2019

https://www.w3.org/TR/payment-request/

Crypto Cash

Cash

- Anonymous
- Transactions can occur off-line
- No intermediary
- But needs to be initially created and endowed

Note

- Bitcoin not completely anonymous
- Need to be on-line

Crypto Cash

Cryptocurrency

- Intuition. I give out pieces of paper that can be redeemed for a certain amount by me. I sign the pieces of paper. People must trust me and my signature needs to be unforgeable.
- This is how currency started in terms of promissory notes
- We could have a digital version but we know you can make perfect digital copies – the so called “double spend” problem
- So you could add not just a signature but a serial number. When a retailer gets the note, you check a ledger for the serial number to make sure it has not already been spent.

Crypto Cash

Cryptocurrency

- Need a central server to keep track of serial numbers. Once, you collect enough notes, you present them to the authority and they issue you fresh serial numbers (you can only spend once)
- Note this is not anonymous like real cash

Crypto Cash

David Chaum – Digital money pioneer, 1983

- Determines way to keep anonymous and prevent double spending
- I issue a note. You pick a serial number (long random number). I sign it and am unable to see the serial number (blind signature)
- Requires central server and every transaction goes through server
- Off-line idea developed in 1988

Crypto Cash

David Chaum – Digital money pioneer, 1983

- Every digital coin issued to you encodes your identity – but no one (not even the bank) can decode it
- When you do a transaction, the recipient requires you to decode part – but not all
- But if you attempt to double spend, the recipient can put the two decoded parts together and determine your identity
- Clunky in that you can't split coins

Crypto Cash

David Chaum – Digicash, 1990

- The cash in Digicash was known as Ecash

Crypto Cash

David Chaum – Digicash, 1990

- Clients anonymous, merchants are not
- No splitting coins so a wallet would have coins of various sizes
- To make an on-line purchase, merchant would have to accept ecash
- When you click on the payment, it takes to you to Digicash website, and open a reverse web connection – i.e. your machine needs to act like a server (need your own IP and the ISP needs to allow incoming connections)
- If connection successful, software would be launched to do transaction
- 100% collateralized based on US dollar

Crypto Cash

David Chaum – Digicash, 1990

- Digicash even had a hardware wallet
- Mondex (acquired by Mastercard) and VisaCash two technologies
- Like cash, if you lose wallet, you lose your money
- If hardware fails or card fails, money is also gone

Crypto Cash

David Chaum – Digicash, 1990

- A number of competing ideas arose
- For example, there was a proposal to give “change” – but this destroyed the anonymity.

Crypto Cash

Why did Digicash fail?

- Hard to persuade merchants to use it
- Did not support user-to-user transactions

Note

- Cryptocurrencies like bitcoin do not distinguish between users and merchants

Crypto Cash

Commodity backed currencies

- E-gold. 100% collateralized by gold
- Digigold fractionally collateralized

However

- Any collateralized currency will fluctuate with the value of the underlying, whether US dollar or a commodity
- What if a digital currency is not tied to any collateral?

Crypto Cash

No Collateral Digital currencies

- Scarcity is essential for a viable currency
- Cynthia Dwork and Moni Naor proposed getting your computer to solve puzzles
- Their application was to eliminate email spam

http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf

Crypto Cash

No Collateral Digital currencies

- Adam Back proposes similar idea hashcash in 1997 (again in the context of eliminating spam)

Note

- Bitcoin “proof of work” has a similar idea to Hashcash

http://www.cypherspace.org/hashcash/hashcash.pdf

Crypto Cash

Why did hashcash fail?

- Spam not that big of a problem
- Anyways, hackers could take over commuters, create hashcash, and then use it to finance email spamming efforts

Note

- Also, there is potentially unlimited currency creation in hashcash – you just need to solve a puzzle. In contrast, bitcoin has scarcity.

Crypto Cash

Ledger

- Blockchain idea goes back at least to 1991 in the context of document dating (Stuart Haber and Scott Stornetta)
- When a new document comes to a server, the server “signs” the document with a time-stamp and a reference (or pointer) to the previous document. The entire history is chained together.
- A later paper suggested using blocks of documents rather than individual documents

https://www.anf.es/pdf/Haber_Stornetta.pdf

Crypto Cash

Ideas close to bitcoin

- B-money by Wei Dai (member of the cypherpunks)
- Anyone can create money (hashing problem)
- Peer to peer network
- Each node maintains a ledger, but it is not a global ledger like bitcoin – just what people think everyone's balance is.

http://www.weidai.com/bmoney.txt

Crypto Cash

Ideas close to bitcoin

- Note there is political aspect to this work, in particular with the cypherpunk group
- Eric Hughes: A Cypherpunk's Manifesto 1993

"*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."*

http://www.activism.net/cypherpunk/manifesto.html

Crypto Cash

Bitgold

- Nick Szabo (had idea in 1998) but began promoting it in 2005
- Closest predecessor to bitcoin
- Szabo may be Satoshi Nakamoto

Crypto Cash

B-Money, Bitgold vs. Bitcoin

- B-money and Bitgold, when you solve puzzle, it creates money
- In Bitcoin system, solving puzzle allows you to win a block (and secure the blockchain) and will lead to minting of new bitcoin

Crypto Cash

Bitcoin: A Peer-to-Peer Electronic Cash System

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

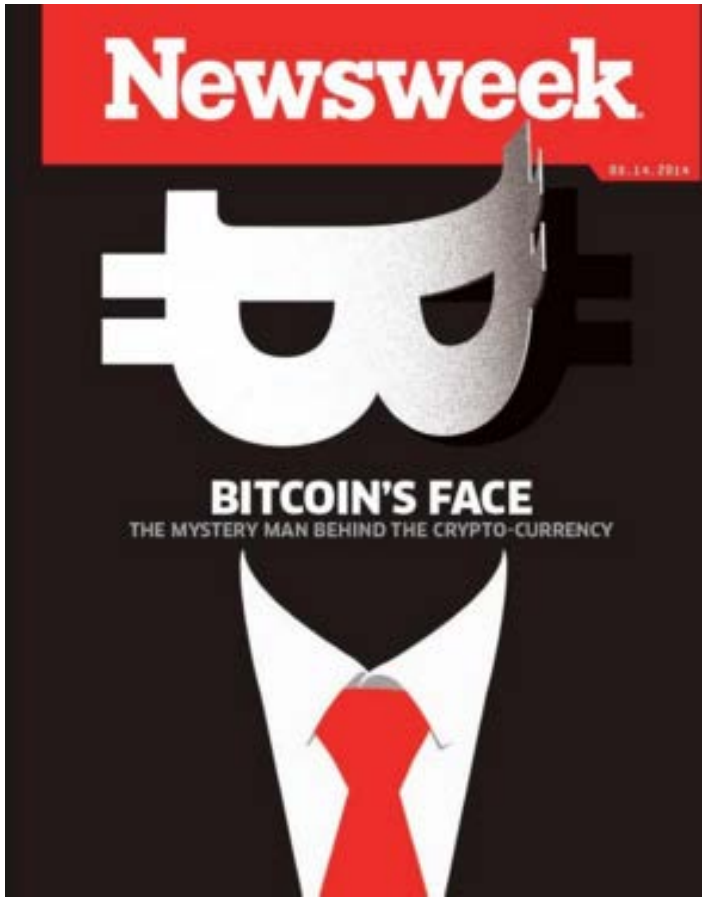
Bitcoin 2008

- Citation list references Adam Back, Wei Dai, Haber and Stornetta
- Satoshi anonymous to today, why?

Crypto Cash

Satoshi Anonymous

- Newsweek's relaunch cover story identified a Satoshi (Dorian) Nakamoto
- Almost immediately discredited



Crypto Cash

Satoshi Anonymous

- December 8, 2015 Wired and Gizmodo identify Craig Wright as Satoshi
- Almost immediately questioned

GIZMODO

This Australian Says He and His Dead Friend Invented Bitcoin

Crypto Cash

Satoshi Anonymous

- Nobel Prize nomination


THE HUFFINGTON POST

INFORM • INSPIRE • ENTERTAIN • EMPOWER

I (Shall Happily) Accept the 2016 Nobel Prize in Economics on Behalf of Satoshi Nakamoto

Crypto Cash

Satoshi Anonymous

- Cypherpunk elan

Crypto Cash

Satoshi Anonymous

- Satoshi has approximately 1 million bitcoin. Currently worth $9 billion
- Note the first real bitcoin transaction was May 21, 2010. Laszlo Hanyecz, a programmer living in Florida, sent 10,000 bitcoin to order some Papa John's pizza.