Bitcoin

una moneta libera

Zio Mc
22 Ottobre 2025

mc@bglug.it

LibreOffice

Cosa andremo a trattare

- Forme di denaro nella storia
- Caratteristiche di una moneta
- La storia cypherpunk della cultura Bitcoin
- Bitcoin e l'inizio della Blockchain
- Il sistema economico corrente (FIAT)
- Come utilizzare Bitcoin
- Spiegazione tecnica del funzionamento di Bitcoin

Forme di denaro nella storia

Il baratto

il primo sistema di scambio, basato sullo scambio diretto di beni e servizi, senza un equivalente universale di valore.

Moneta merce

beni con valore intrinseco (es. sale, grano, bestiame) usati come mezzo di pagamento.

Moneta metallica

introdotta nel VII secolo a.C., inizialmente in forma di lingotti o pezzi grezzi, poi coniate in forme standardizzate.

Moneta cartacea

sviluppata in epoca medievale e moderna, rappresent

Moneta bancaria/fiduciaria (FIAT)

non ha valore intrinseco, ma è accettata perché garantita dalla fiducia nell'emittente (es. depositi bancari, assegni).

Moneta elettronica

forme moderne di denaro, come bonifici, carte di credito, criptovalute, completamente dematerializzate.

Domanda a tutti

Voi scambiereste il vostro Rolex con una moneta emessa da "Pierino"?

no? e perchè?

e lo scambiereste con dei dollari?

e con l'afghani?

meglio ancora in Euro giusto?

Caratteristiche di una moneta

Durabilità

non deve deperire nel tempo, altrimenti perde il valore conservato

Portabilità

deve essere facile da trasportare e scambiare

Divisibilità

deve essere suddivisibile in unità più piccole per pagamenti di importo variabile

Riconoscibilità

deve essere immediatamente identificabile e difficile da contraffare

Scarsità

la quantità disponibile deve essere limitata, per mantenere il valore nel tempo

Stabilità del valore

il suo potere d'acquisto deve rimanere relativamente costante, altrimenti fallisce la funzione di riserva di valore

La storia cypherpunk della cultura Bitcoin

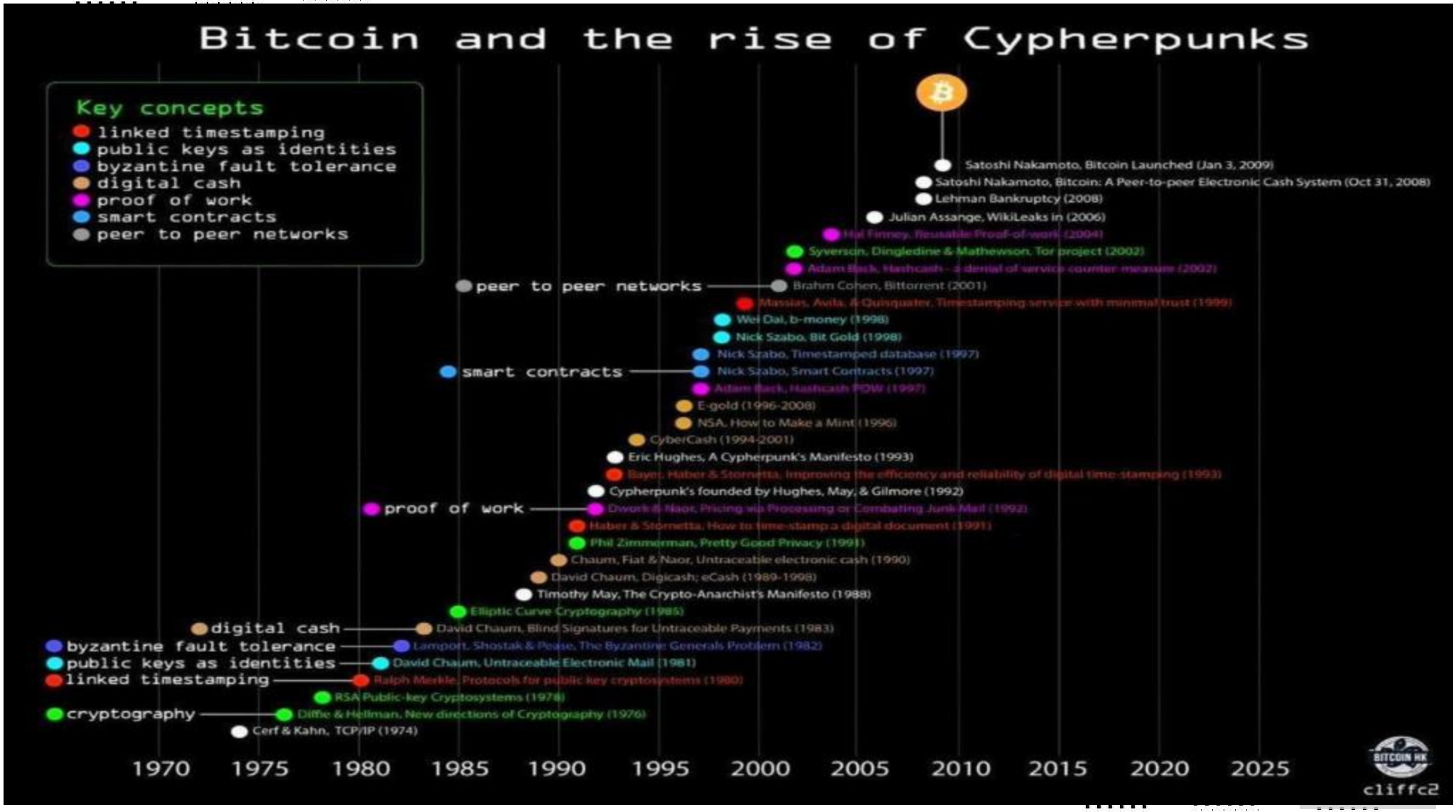
- I cypherpunk sono attivisti nati tra la fine degli anni ’80 e l’inizio degli anni ’90, che promuovono l’uso della crittografia per proteggere la privacy individuale e contrastare il controllo centrale da parte di Stati e corporation.

- Il loro obiettivo era creare sistemi decentralizzati e autonomi, dove le persone potessero comunicare e scambiare valore senza intermediari fidati.

- Il Manifesto cypherpunk (1993) di Eric Hughes sottolinea che “la privacy è necessaria per una società aperta” e che la crittografia è lo strumento per difenderla.

- Dalla comunità cypherpunk nascono molte idee e tecnologie che portano alla creazione di Bitcoin, come il concetto di denaro digitale anonimo e decentralizzato.

- Satoshi Nakamoto, l’ideatore di Bitcoin, è profondamente influenzato da questa cultura: il whitepaper del 2008 e il lancio della rete nel 2009 rispecchiano i principi cypherpunk di autonomia, crittografia e sfiducia verso le istituzioni centrali


Bitcoin and the rise of Cypherpunks
Key concepts
linked timestamping
public keys as identities
byzantine fault tolerance
digital cash
proof of work
smart contracts
peer to peer networks
Satoshi Nakamoto, Bitcoin Launched (Jan 3, 2009)
Satoshi Nakamoto, Bitcoin: A Peer-to-peer Electronic Cash System (Oct 31, 2008)
Lehman Bankruptcy (2008)
Julian Assange, WikiLeaks in (2006)
Hal Finney, Reusable Proof-of-work (2004)
Syverson, Dingledine & Mathewson, Tor project (2002)
Adam Back, Hashcash - a denial of service counter-measure (2002)
peer to peer networks
Brahm Cohen, Bittorrent (2001)
Massias, Avila, & Quisquater, Timestamping service with minimal trust (1999)
Wei Dai, b-money (1998)
Nick Szabo, Bit Gold (1998)
Nick Szabo, Timestamped database (1997)
smart contracts
Nick Szabo, Smart Contracts (1997)
Adam Back, Hashcash POW (1997)
E-gold (1996-2008)
NSA, How to Make a Mint (1996)
CyberCash (1994-2001)
Eric Hughes, A Cypherpunk's Manifesto (1993)
Bayer, Haber & Stornetta, Improving the efficiency and reliability of digital time-stamping (1993)
Cypherpunk's founded by Hughes, May, & Gilmore (1992)
proof of work
Dwork & Naor, Pricing via Processing or Combating Junk Mail (1992)
Haber & Stornetta, How to time-stamp a digital document (1991)
Phil Zimmerman, Pretty Good Privacy (1991)
Chaum, Fiat & Naor, Untraceable electronic cash (1990)
David Chaum, Digicash; eCash (1989-1998)
Timothy May, The Crypto-Anarchist's Manifesto (1988)
Elliptic Curve Cryptography (1985)
digital cash
David Chaum, Blind Signatures for Untraceable Payments (1983)
byzantine fault tolerance
Lamport, Shostak & Pease, The Byzantine Generals Problem (1982)
public keys as identities
David Chaum, Untraceable Electronic Mail (1981)
linked timestamping
Ralph Merkle, Protocols for public key cryptosystems (1980)
RSA Public-key Cryptosystems (1978)
cryptography
Diffie & Hellman, New directions of Cryptography (1976)
Cerf & Kahn, TCP/IP (1974)
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
BITCOIN HK
cliffc2

Bitcoin e l'inizio della Blockchain

18 agosto 2008

Registrazione del dominio bitcoin.org

31 ottobre 2008

Bitcoin WhitePaper viene pubblicato nella Mailing List "Cryptography Mailing List"

3 gennaio del 2009

Blocco Genesi con la frase "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Il Cancelliere sull'orlo del secondo salvataggio per le banche

Blocco genesi

- Satoshi Nakamoto l'ha inserita per datare la nascita della blockchain e per denunciare l'instabilità del sistema finan
- È un manifesto critico contro il sistema bancario centralizzato e una dichiarazione d'intenti per Bitcoin: un'alternati

Bitcoin e l'inizio della Blockchain

7 dicembre 2010

Visa Mastercard Paypal bloccano le donazioni a Wikileaks

11 dicembre 2010

Wikileaks accetta donazioni in Bitcoin

”WikiLeaks has kicked the hornet’s nest, and the swarm is headed towards us.”

23 aprile 2011

Satoshi nakamoto lascia il progetto con il seguente messaggio
”I had a few other things on my mind (as always). [...] I’ve moved on to other things….”

Il sistema monetario attuale (FIAT)

Esempi di transazioni con il sistema attuale

- **Cash:** Mittente, Destinatario (Liberta assoluta)

- **Bonifico:** Mittente, Banca Mittente, Banca Destinatario, Destinatario

- **Carta di credito:** Mittente, Banca Mittente, Banca Destinatario, Destinatario, VISA/MASTERCARD/AMERICANEXPRESS

Vantaggi

Ho un certo lasso di tempo per interrompere la transazinone o in caso di frode c'è quasi sempre un paracadute

Il saldo del mio conto in banca è accessibile ad un numero limitato di persone

Spostare grosse somme di denaro richiede diverse autorizzazioni

Svantaggi

Dipendo dal sistema bancario, senza quello non posso scambiare valore (Fondi congelati Francesca Albanese)

Il 20% della popolazione mondiale non ha accesso al sistema bancario

Il sistema FIAT è pensato per aumentare sempre la massa monetaria in circolazione causando inflazione, se fosse un bene finito questo sarebbe impossibile vedi l'oro

Dovete spendere il prima possibile la moneta o trasformarla in un'altra forma per mantenere il valore (mattone, investimenti)

Non posso inviare denaro a tutti (Russia, Afganistan, Paese remoto dell'africa)

Come utilizzare Bitcoin

Bitcoin è divisibile 1BTC = 100'000'000Sats (1'000Sats ~ 1€)

Ottenere bitcoin (Exchange,P2P,Farsi pagare in Bitcoin,Donazioni)

- bullbitcoin.com
- coinbase.com
- p2p.bitcoinvoucher.bot

Wallet:

- bluewallet.io
- https://phoenix.acinq.co/
- walletofsatoshi.com (modalità non-custodial)

Indirizzo bitcoin (bc1qp6ejw8ptj9l9pkscmlf8fhhkrrjeawgpyjvtq8)

Vantaggi

Non ho bisogno di intermediari #

Chiunque può utilizzarlo #

Il sistema non è inflazionabile max 21M di Bitcoin, oggi abbiamo raggiunto il 95% #

Il sistema non è manipolabile, ed il registro è pubblico #

Svantaggi

Non esiste il paracadute, tu sei il responsabile al 100% dei tuoi fondi se perdi la Seed Phrase hai perso tutto

La transazione non può essere annullata

La velocità di esecuzione della transazione non è istantanea può impiegarci un tempo variabile dai 5 minuti a giornate in base alle FEE

Il sistema L1 non è scalabile a livello mondiale max 5'000TX ogni 10 min (7tx/sec) (Ma abbiamo Lightning Network)

Spiegazione tecnica del funzionamento di Bitcoin

- Blockchain (Hash Precedente)
- Transazione firmata (Pkey)
- Proof of work e ricompensa a scalare da 50BTC ad oggi 3.125
- Dimensione del blocco (7tx/sec)
- Auto adjustment (10Min ogni blocco)
- Bitcoin Node

Domande……

- https://mempool.space (Block explorer)
- https://planb.academy/it/learn-anytime (Corsi e formazione)
- https://bitcoinitaliapodcast.it/ (Podcast molto carino)
- https://bitcoinitalianetwork.com/ (Eventi)
- https://btcmap.org (Esercenti che accettano bitcoin)