PROGETTO UCAL

UNIVERSITÀ DELLA CALABRIA

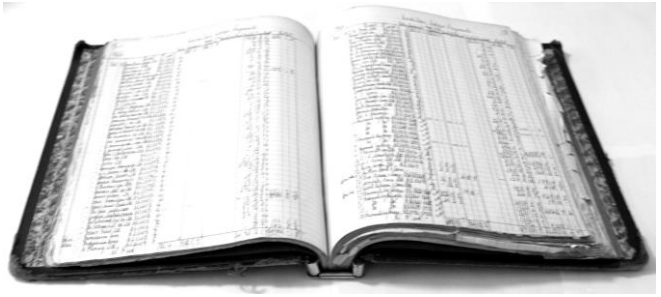
FONDAMENTI DELLA TECNOLOGIA BLOCKCHAIN E SUI PROBABILI SVILUPPI
Utilizzo di smart contract e dei metodi crittografici per la certificazione

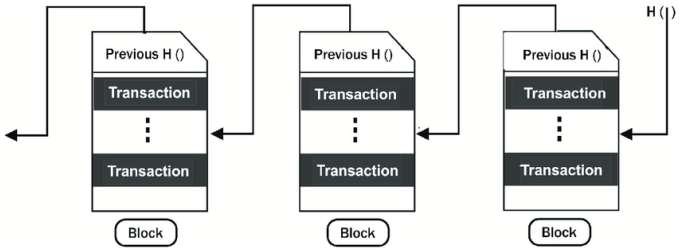
GIANFRANCO D'ATRI

Lunedì, 21 Maggio 2018

LE ORIGINI

Sistema di archiviazione sicuro





- *Inventata nel 1991 per garantire "data certa" (timestamp) in un archivio digitale*
- *Utilizzata per il Bitcoin nel 2008 per garantire la non duplicabilità di una transazione monetaria*
- *Basata sulla concatenazione dell'informazione tramite algoritmi crittografici (da cui "crittovalute"*

ORIGINE DELLA MONETA BITCOIN

Tecnologia	Tipo moneta
METALLO analogico	"SCAMBIO " .
METALLO discreto	CONIATA
CARTA	CARTACEA
SCRITTURA CONTABILE	FIDUCIARIA
ELABORATORE DIGITALE	DIGITALE
INTERNET	ELETTRONICA
BLOCKCHAIN	CRITTOVALUTE (BITCOIN
Blockchain 2.0	*functional money*

SISTEMA GENERALIZZATO DI ARCHIVIAZIONE E GESTIONE DI RELAZIONI DIGITALI

Obiettivo:
Efficienza Gestione dell'Informazione

Passato → *Centralizzazione*

Dal ~2010 → *Decentralizzazione*

Costi ridotti della tecnologia informatica:

- *Intero database di 1 crittovaluta circa 500GB su computer personale*
- *Connessione alla rete a banda larga diffusa tra popolazione mondiale*
- *Disponibilità diffusa di dispositivi personali collegati alla rete*

COS'E' LA TECNOLOGIA BLOCKCHAIN

Cosa e' una blockchain XCoin

LEDGER + MECCANISMO DI PREMIO

Ledger = Archivio di scritture non cancellabili o modificabili. Cambia solo per aggiunte di nuove scritture.

Meccanismo Premiale = Scrittura speciale che registra l'assegnazione di una quantità di XCOIN

Solo "incidentalmente" legato all'uso monetario!

Gli Attori (di una qualsiasi blockchain)

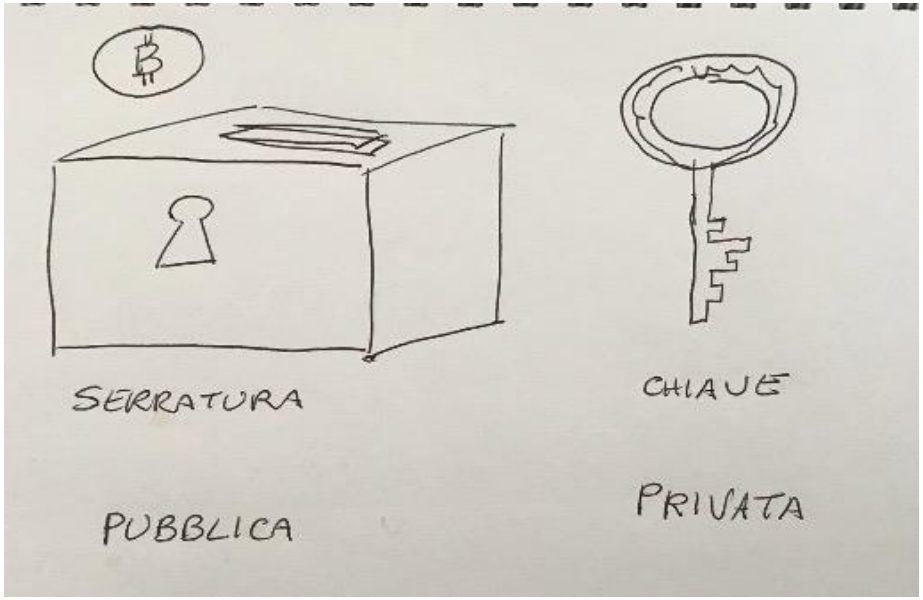
- *Proprietario* → Controlla - *indirizzi privati* - *indirizzi pubblici* } *Chiavi*
- *Minatore* → *Proprietario speciale, tiene attivo un software standard che "aggiunge" scritture*
- *Utilizzatore* → *Detiene accesso indiretto al funzionamento della blockchain*

Come funziona?

- *Ogni minatore conserva una copia del ledger*
- *I proprietari pubblicano in rete le scritture richieste*
- *Un minatore alla volta, con cadenza regolare aggiunge un blocco di scritture ammissibili alla sua copia del ledger*
- *Al "primo" minatore spetta il premio : e' individuato secondo un protocollo condiviso (es. PoW, PoS,…)*
- *Il conflitto tra piu' minatori dichiaratisi primi e' risolto tramite il consenso "a maggioranza del 51%"*
- *Tutti i minatori aggiornano conformemente la loro copia*

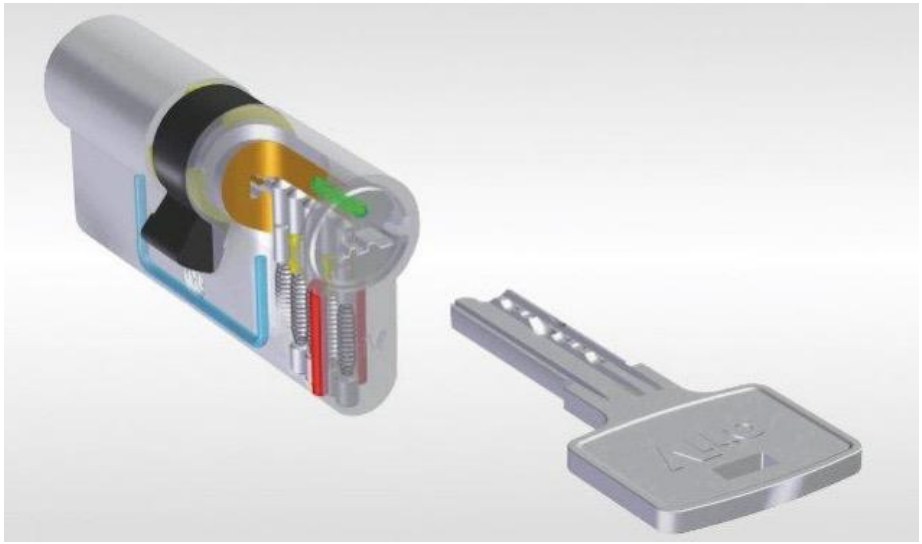
Crittografia a chiave pubblica

- *Combinazione di una chiave privata e una chiave pubblica*
- *Chiave privata: un numero compreso tra 1 to 2^256-1*
- *Chiave pubblica: deriva dalla chiave privata applicando funzioni matematiche irreversibili (algoritmi di crittografia)*



- *Reversibile*

Dalla serratura e' possibile riprodurre la chiave



- *Irreversibile*

Dalla serratura non e' possibile riprodurre la chiave

Indirizzo Blockchain

E’ l’identificatore di di un soggetto che opera sulla blockchain, è generalmente rappresentato come una stringa alfanumerica di lunghezza variabile in base alla rappresentazione scelta.

Ogni indirizzo pubblico e’ una rappresentazione di una chiave pubblica

Esempi di indirizzi blockchain

Indirizzi Ethereum: 40 caratteri alfanumerici lowercase

- *EIPs/55* 0xc2d7cf95645d33006175b78989035c7c9061d3f9

0xC2D7CF95645D33006175B78989035C7c9061d3F9

- *Indirizzi Bitcoin : 25-42 caratteri alfanumerici*
  - *P2PKH primo carattere sempre 1*

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

  - *P2SH primo carattere sempre 3*

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

  - *Bech32 primi caratteri sempre bc1*

bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq

Punti di debolezza

- *Indirizzi e transazioni sono pubbliche (ancorche' non associate ad un utente specifico)*
- *Possesso token legato a conoscenza della chiave privata*
- *Conservazione e trasmissione delle chiavi necessita' di regole di governance*
- *Dimensione degli archivi (ledger) enorme (centinaia di gigabytes) influenza usabilita' della catena (ie. tempi di verifica transazione)*
- *Immutabilità e ininterruttibilità e non manipolabilità, sono subordinate alla concreta distribuzione delle risorse fra soggetti indipendenti e incorrompibili, ma la categoria "minatori" e' in genere indeterminata e solo parzialmente verificabile*

BLOCKCHAIN E NOTARIZZAZIONE

Notarizzazione

Transazioni sulla blockchain come proof of existence di un determinato file ad un certo momento temporale -> utilizzo del time-stamping intrinseco

- *Impossibile manipolare, retrodatare o postdatare il file -> Inserimento, quale "causale" della transazione, il codice hash* del file di cui si intende provare l'esistenza ->*

- *Costo marginale pressoché nullo*

- *Indipendente da ente fiduciario terzo*

** Codice hash = una funzione di pochi byte che riconduce con sicurezza ad un file*