Dietro il *Bitcoin* ed oltre: una panoramica della tecnologia blockchain e le sue applicazioni

Dayton Marcucci

Direttore Tecnico – HID Global S.p.A.

Introduzione

Gli Inizi - Cypherpunk

“Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.”

- Eric Hughes

9/3/1993, Cypherpunk Manifesto

"La privacy è necessaria per una società aperta nell'era elettronica. La privacy non è segretezza. Una questione privata è qualcosa che uno non vuole che il mondo intero sappia, ma una questione segreta è qualcosa che uno non vuole che nessuno sappia. La privacy è il potere di rivelare in modo selettivo se stessi al mondo. "

Prima di Bitcoin

- ***DigiCash*** *era una società di moneta elettronica fondata da David Chaum nel 1989. Le transazioni di DigiCash erano uniche nel senso che erano anonime a causa di una serie di protocolli crittografici sviluppati dal suo fondatore.*

  -> firma cieca (blind signature)

- ***Hashcash*** *utilizza un sistema di prova del lavoro effettuato (POW) per limitare gli attacchi di spam e denial-of-service (DOS). Hashcash è stato proposto nel 1997 da Adam Back.*

  -> prova di lavoro (proof-of-work POW)

Storia

- 18/8/2008 - viene registrato il nome di dominio web **bitcoin.org**

- 31/10/2008 - ottobre, un link a un documento scritto da Satoshi Nakamoto intitolato ***«Bitcoin: Un sistema di pagamento elettronico peer-to-peer»*** fu pubblicato in una mailing list di crittografia. Questo documento descrive in dettaglio i metodi per utilizzare una rete paritaria (peer-to-peer) per generare ciò che è stato descritto come "un sistema per le transazioni elettroniche senza fare affidamento sulla fiducia".

- 3/1/2009 - la rete bitcoin nacque con Satoshi Nakamoto che estrae il blocco di genesi del bitcoin (blocco numero 0), che aveva una ricompensa di 50 bitcoin. Incorporato nella base di monete di questo blocco c'era il testo:

Bitcoin

Bitcoin è una crittovaluta, una risorsa digitale progettata per funzionare come mezzo di scambio che utilizza la crittografia per controllarne la creazione e la gestione, piuttosto che affidarsi alle autorità centrali. Il 3 gennaio 2009, la rete bitcoin nacque con Satoshi Nakamoto che estrae il blocco di genesi del bitcoin (blocco numero 0), che aveva una ricompensa di 50 bitcoin. Incorporato nella base di monete di questo blocco c'era il seguente messaggio:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”

«The Times 03 / Jan / 2009 Cancelliere sull'orlo del secondo piano di salvataggio per le banche.»

Bitcoin

1. Bitcoin viene considerato come la prima crittovaluta e anche la più popolare. Una crittovaluta è una valuta digitale e decentralizzata che viene costruita utilizzando principi di informatica, crittografia ed economia. La parola «Bitcoin» (con la B maiuscola) si riferisce al protocollo che disciplina questa valuta.
2. «bitcoin» (con la b minuscola) indica le unità di valuta effettive. Per esempio un utente Bitcoin dirà di avere una certa quantità di bitcoin, cosi come diciamo di avere una certa quantità di euro.
3. Bitcoin è l'ispirazione per la tecnologia blockchain, che è la struttura dati sottostante usata nella gestione di questa crittovaluta.

Blockchain

Blockchain («catena di blocchi») è una tecnologia che sta ridefinendo il modo in cui archiviamo, aggiorniamo e spostiamo i dati.

Un blockchain è un registro digitale, decentralizzato e pubblico di tutte le transazioni di una crittovaluta. Costantemente crescenti come blocchi "completati" (le transazioni più recenti) vengono registrati e aggiunti in ordine cronologico, consentendo agli operatori di tenere traccia delle transazioni in valuta digitale senza registrazione dei registri. Ogni nodo (un computer connesso alla rete) riceve una copia della blockchain, che viene scaricata automaticamente.

Ethereum

Ethereum è stato inizialmente descritto in un white paper di Vitalik Buterin, [un programmatore di 19 anni alla fine del 2013 con l'obiettivo di creare applicazioni decentralizzate. Buterin sosteneva che Bitcoin aveva bisogno di un linguaggio di programmazione più potente per lo sviluppo di applicazioni. Non riuscendo a raggiungere un accordo, propose lo sviluppo di una nuova piattaforma che battezzò con il nome «Ethereum», derivato dalla parola ***ether*** *(etere in inglese).*

Ethereum è una piattaforma decentralizzata creata per la gestione dei contratti intelligenti.

Supporta una versione modificata del consenso di Nakamoto tramite transizioni di stato basate sulle transazioni.

Bitcoin vs. Ethereum

UTXO

valuta

linguaggio di programmazione semplice

conto

contratti intelligenti

linguaggio più sofisticato

ICO

Un'offerta iniziale di monete (Initial Coin Offering - ICO) è un tipo di crowdfunding che utilizza crittovalute. In un ICO, una quantità di crittovaluta viene venduta sotto forma di «coin» a speculatori o investitori, in cambio di moneta a corso legale o di altre crittovalute come per esempio Bitcoin o ethereum. I coin venduti sono promossi come unità funzionali future della valuta se o quando l'obiettivo di finanziamento dell'ICO è rispettato e il progetto viene avviato.

***Esempi**:*

- *Bancor ICO – 150 milioni $*
- *Tezos ICO – 200 milioni $*
- *Filecoin ICO – 253 milioni $*

Bancor

TEZOS FOUNDATION

Filecoin

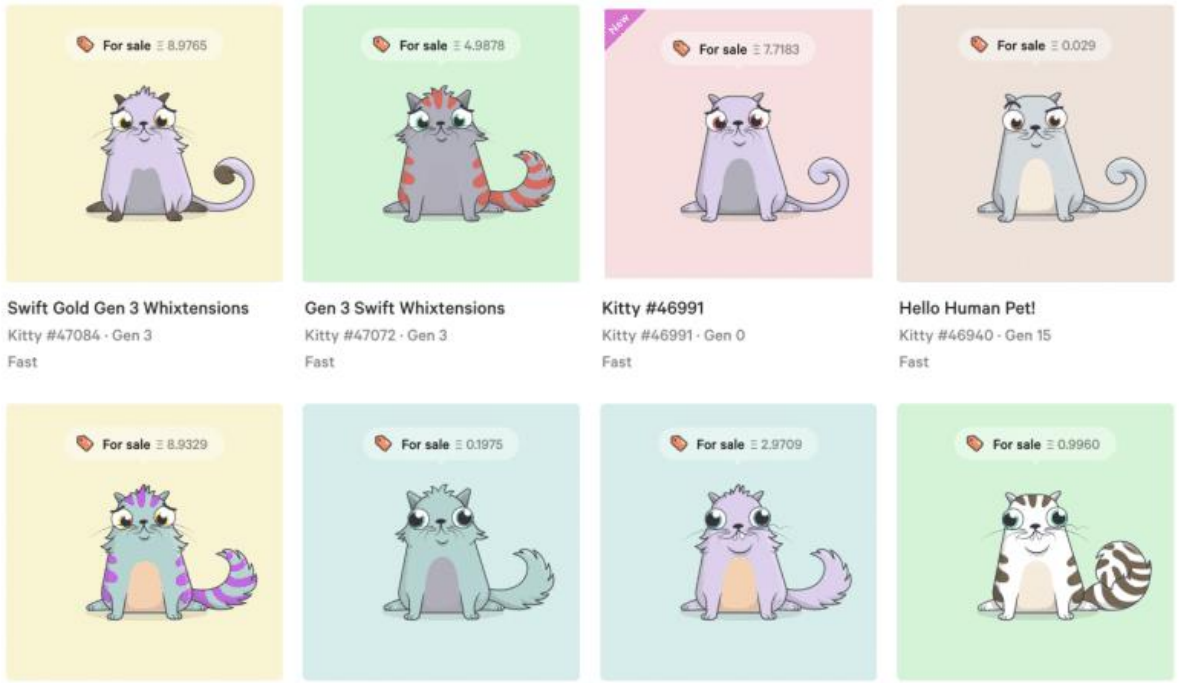
Hacking

Esempi:

- *Mt. Gox – 700.000 bitcoin rubati nel corso di anni*

- *Bitfinex – 120.000 btc rubati nel Agosto del 2017*

Cryptokitties



CryptoKitties è un gioco virtuale basato su una tecnologia blockchain sviluppata da Axiom Zen e Animoca che consente ai giocatori di acquistare, collezionare, allevare e vendere vari tipi di gatti virtuali.

Rappresenta uno dei primi tentativi di implementare la tecnologia blockchain per scopi ricreativi e di collezionismo digitale.

La popolarità del gioco a dicembre 2017 ha congestionato la rete Ethereum, causando il raggiungimento di un massimo storico nelle transazioni e un rallentamento significativo.

La Tecnologia

Hash

Un hash crittografico è un algoritmo matematico che mappa un messaggio di lunghezza arbitraria in dati binaria di dimensione fissa.

```
Nel mezzo del cammin
   di nostra vita
```


```
B027B2C09BD6A323B5043729B0BC1463
5D857E1E5B16337487907292ABEBE48F
```

```
pippo
```


```
A2242EAD55C94C3DEB7CF2340BFEF9D5
BCACA22DFE66E646745EE4371C633FC8
```

```
DMD&b8-kxKTUx4U=6By
GMjtWhMR%%VxrTrZ%!BBN
```


```
4CFFD76B3AA2C2910B82E5C129A79532
AC7D4D9E688217C53B99A2082C671002
```

Hash

Carateristiche:

- **deterministico**

  d = h(m)

- **unidirezionale (resistenza alla preimmagine)**

  difficile calcolare ***m = h'(d)***

- **resistente alle collisioni**

  difficile tovare due messaggi ***m1*** e ***m2*** dove ***h(m1) = h(m2)***

- **resistenza alla seconda preimmagine**

  dato ***m*** è difficile trovare ***m'*** dove ***h(m) = h(m')***

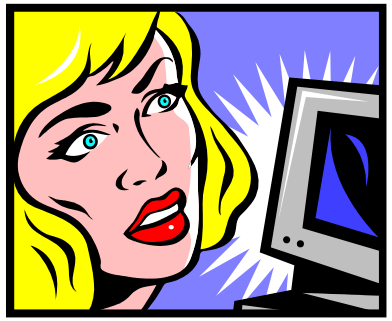
- **valori pseudo-casuali (pseudo random)**

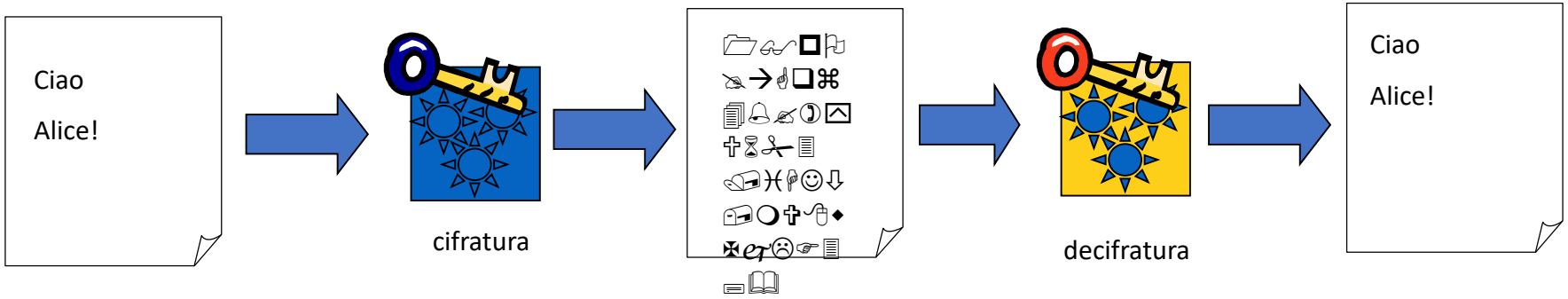
Crittografia a Chiave Pubblica

Mario cifra il messaggio destinato ad Alice con la chiave pubblica di Alice. Alice decifra il messaggio di Mario con la sua chiave privata.

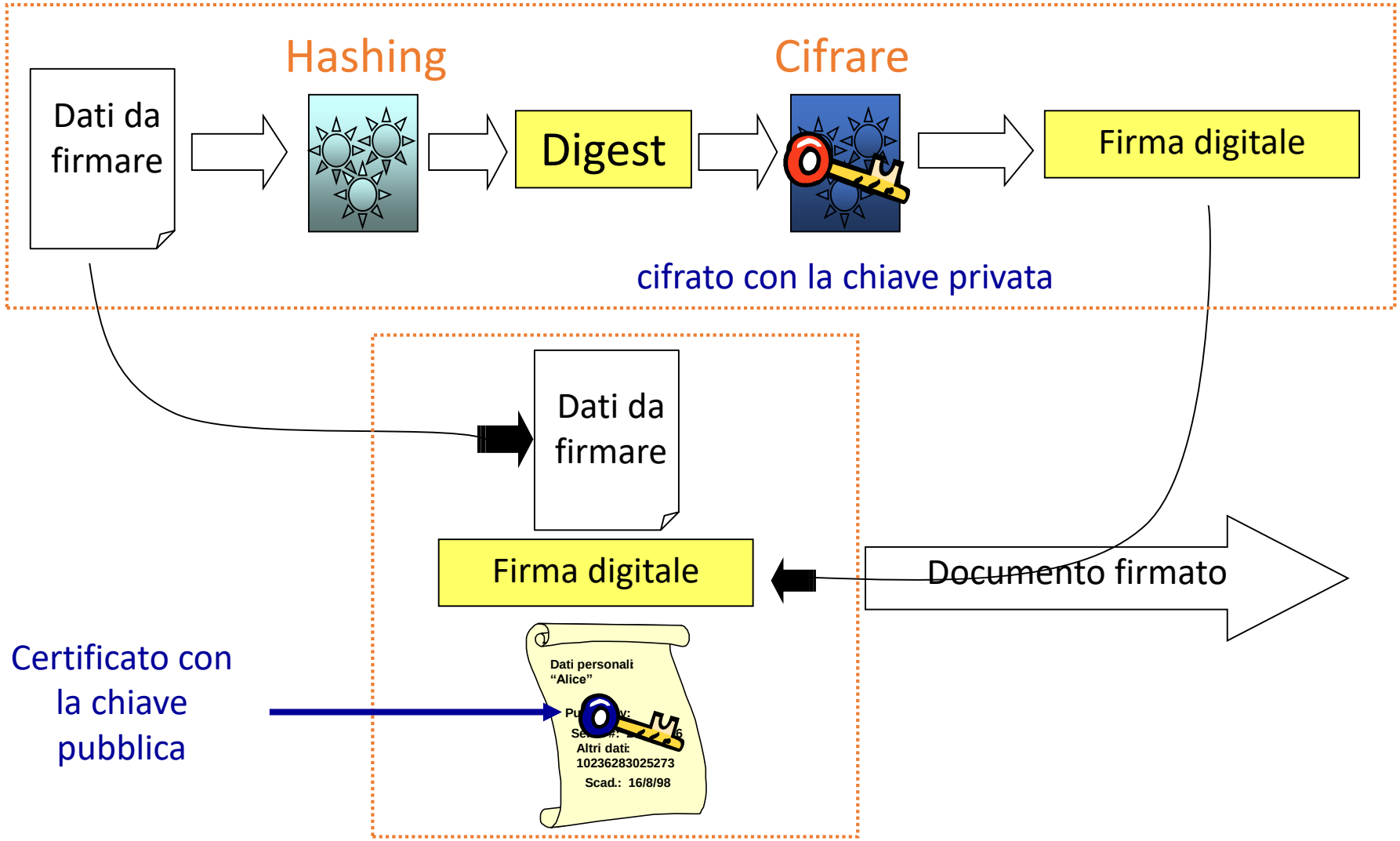
chiave pubblica

chiave privata





Firma Digitale



Componenti

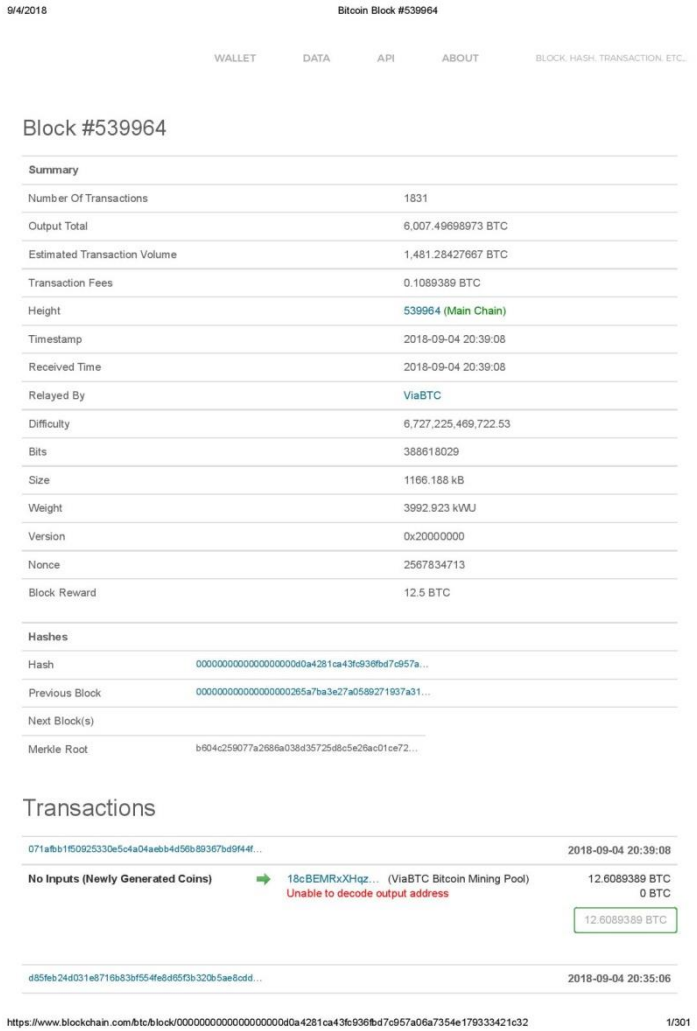
Componenti Chiave

1. Identità
2. Transazione
3. Gestione del registro pubblico distribuito
4. Consenso (ovvero *mining*)

Mining

1. L’intero blockchain viene scaricato
2. Verifica le transazione
3. Creazione di un nuovo blocco
4. Risoluzione dell’hash ottenendo il «nonce» (POW)
5. Trasmissione del blocco alla rete
6. Incassare bitcoin

Struttura di un Blocco



9/4/2018 Bitcoin Block #539964

WALLET DATA API ABOUT BLOCK, HASH, TRANSACTION, ETC...

Block #539964

Summary	
Number Of Transactions	1831
Output Total	6,007.49698973 BTC
Estimated Transaction Volume	1,481.28427667 BTC
Transaction Fees	0.1089389 BTC
Height	539964 (Main Chain)
Timestamp	2018-09-04 20:39:08
Received Time	2018-09-04 20:39:08
Relayed By	ViaBTC
Difficulty	6,727,225,469,722.53
Bits	388618029
Size	1166.188 kB
Weight	3992.923 kWU
Version	0x20000000
Nonce	2567834713
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000000d0a4281ca43fc936fbd7c957a...
Previous Block	0000000000000000000265a7ba3e27a058927 1937a31...
Next Block(s)	
Merkle Root	b604c259077a2686a038d35725d8c5e26ac01ce72...

Transactions

071afbb1f50925330e5c4a04aebb4d56b89367bd9f44f... 2018-09-04 20:39:08

No Inputs (Newly Generated Coins) → 18cBEMRxXHqz... (ViaBTC Bitcoin Mining Pool) 12.6089389 BTC
Unable to decode output address 0 BTC
12.6089389 BTC

d85feb24d031e8716b83bf554fe8d65f3b320b5ae8cdd... 2018-09-04 20:35:06

https://www.blockchain.com/btc/block/0000000000000000000d0a4281ca43fc936fbd7c957a06a7354e179333421c32 1/301

Blocco

- intestazione
- dimensione
- contatore delle transazioni
- transazioni

Wallet

Ogni utente è in possesso di un portafoglio (wallet), un file generato dal client Bitcoin.

Questo *wallet* contiene una serie di coppie chiave privata-chiave pubblica.

La chiave privata è nota solo al proprietario, e serve per effettuare i pagamenti.

La chiave pubblica può essere resa nota, e serve per dimostrare a terzi che si è in possesso della chiave privata.

Dalla chiave pubblica viene estratto un indirizzo, una serie di lettere e numeri lungo solitamente 34 caratteri (minimo 27)

Chiavi e Indirizzi