



Rotary Club Gemona Friuli Collinare

16 gennaio 2018

Conviviale:

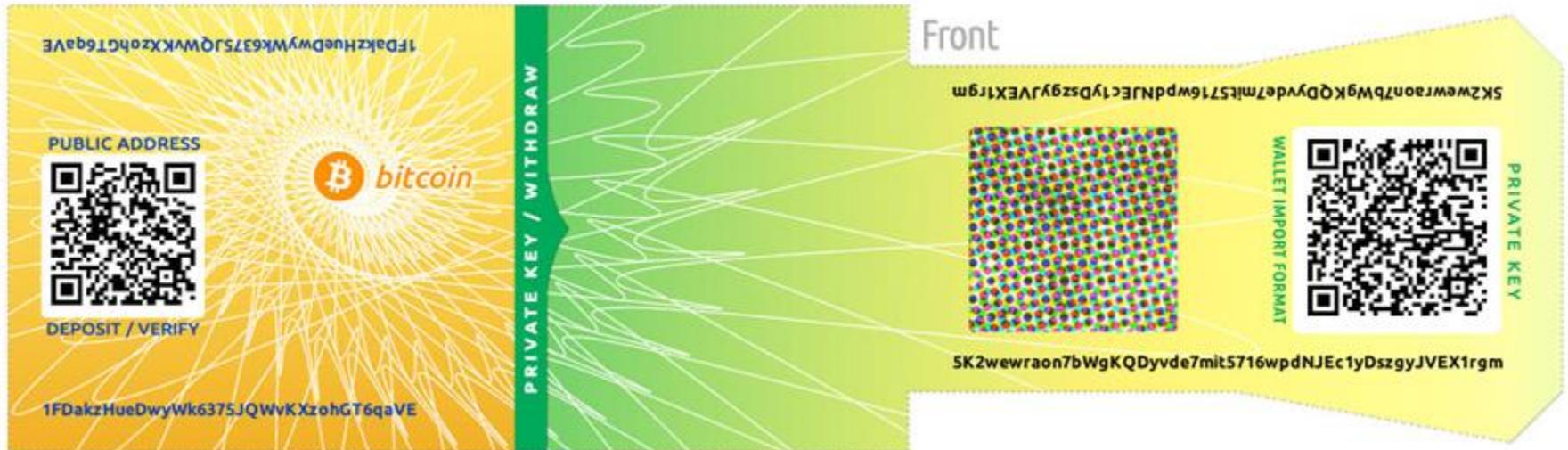
«Bitcoin: moda o valore?»

Relatore:

dr. Oreste Venier,
R.C. Venezia Mestre,

PHF

Cos'è il Bitcoin



Il **Bitcoin** è un **voucher digitale**, protetto dalla **crittografia**, che ha la proprietà di non poter essere duplicato.

Ne esiste in circolazione una quantità comunque limitata e **il Mercato gli ha dato un valore** come ha dato alle monete della Numismatica.

Il Bitcoin tuttavia non esiste in forma fisica (banconote cartacee oppure monete metalliche), quelle proposte sono solo stampe del codice del voucher.



Chi gestisce il Bitcoin?

Il Bitcoin è **decentralizzato**: non esiste una «Banca» oppure un altro Ente centrale che lo gestisce.

I «conti» IBAN vengono **generati** direttamente **dagli utenti**, senza nessun bisogno di intermediazione.

Le **transazioni (ovvero i bonifici)** vengono invece gestite dai **Miners**, un gruppo di «volontari» che gestisce un **archivio pubblico e condiviso** chiamato «**blockchain**».





La Crittografia

Il Bitcoin pone le sue basi sulla **crittografia**: dietro ogni conto Bitcoin vi è una **password** detta **chiave privata**, che l'utente deve **conservare gelosamente**.

Tale **password** è **necessaria** per poter **trasferire i fondi** da un conto all'altro.

Il **trasferimento** avviene apponendo al modulo di richiesta la **firma digitale** con la **stessa password o chiave privata**. Ecco perché è necessario che sia segreta.

Bitcoin Address	Private Key (Wallet Import Format)
	
Public Key 	Private key 
1M3RLrXve5wcT2ZcJu8WXoXjdh4WXcWQA9	5K8BwE76VsatQiRa5wJpGng7758FAz4vLkMxAry8QnyZTdQJxPn

La Blockchain e i Miners

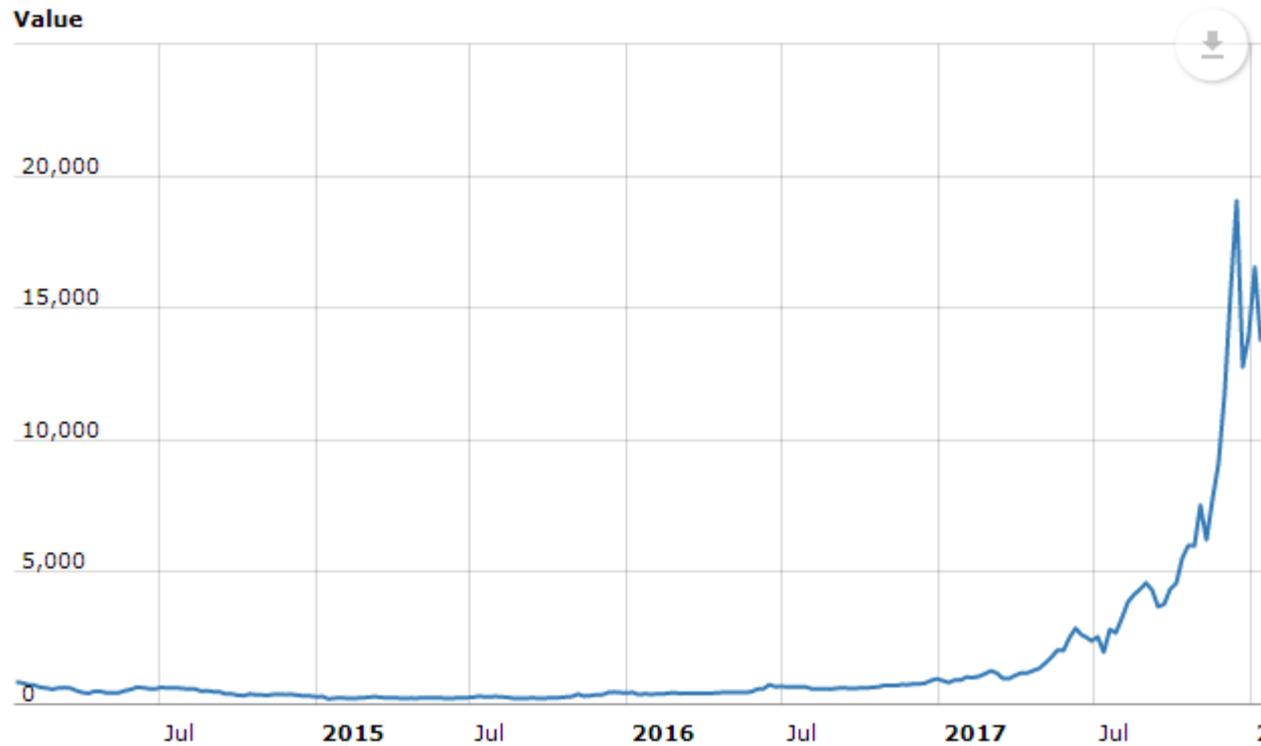
Dietro tutto questo, c'è un esercito di volontari, detti «**Miners**», che provvedono a **validare i bonifici** e a **tenere aggiornato** un enorme **registro** contenente tutte le transazioni.

Questo Registro è **pubblico** e prende il nome di **Blockchain** perché ogni blocco è strettamente legato all'altro da una **continuità di numerazione**, rendendo impossibile imbrogliare.





Il valore del Bitcoin





il Bitcoin come forma di pagamento: le commissioni

Ogni forma di pagamento hai dei **costi**.

Che sia un **bonifico bancario** oppure l'utilizzo di una **carta di credito**, ci sono delle **commissioni da sostenere**, e il **Bitcoin non fa eccezione**.

Fino all'anno scorso, un «bonifico» bitcoin costava **pochi centesimi** di commissione; oggi costa quasi 15 EUR. Questi importi vanno ai Miners.

Ecco perché oggi il Bitcoin non è più molto adatto come forma di pagamento (anche a causa della sua volatilità) e del tutto inadatto per i «micropagamenti» (p.es. il caffè o il giornale), per i quali sono allo studio nuove modalità.





il Bitcoin come riserva di valore: la volatilità e il trading

Il **Bitcoin** invece è adatto come **riserva di valore**. In tal caso, le commissioni incidono meno.

Ci sono vere e proprie **piattaforme di trading**, per poter piazzare ordini di acquisto e di vendita. E' un mercato caratterizzato da forte volatilità.



Come mi procuro dei Bitcoin?

Vi sono veri e propri «Exchange» ovvero ditte che vendono e ricomprano Bitcoin.

Il più noto e comodo per iniziare è **COINBASE**.





Dove tengo i Bitcoin?

Detenere dei Bitcoin significa sostanzialmente detenere la «password» che sblocca i singoli voucher.

Vi sono vari modi, ciascuno con vantaggi e svantaggi, come segue:

Web wallet: servizio web di una ditta esterna simile ad un home-banking. **Vantaggi:** grande comodità anche di accesso. **Svantaggi:** non si ha il controllo del conto.

Software wallet: software (p.es. Electrum) installato su PC o smartphone in cui si conservano le proprie chiavi. **Vantaggi:** si ha il completo controllo del conto.

Svantaggi: se si perdono le chiavi o il PC o telefono viene compromesso, si perdono i Bitcoin.

Hardware wallet: si tratta di una chiavetta USB (come Trezor o Ledger) che contiene internamente le chiavi. **Vantaggi:** le chiavi non risiedono sul PC o telefono ma dentro una chiavetta, meno attaccabile. **Svantaggi:** se si perde la chiavetta e non si ha la password di backup, si perdono i Bitcoin.



I «parenti» del Bitcoin

Il Bitcoin non è l'unica «criptovaluta» esistente.

Ve ne sono in effetti diverse centinaia, ma sono per lo più inaffidabili perché la sicurezza di una criptovaluta è proporzionale a quanti Miners la gestiscono.

Solo il Bitcoin e poche altre sono affidabili. Ecco i rispettivi Market Cap:

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$197.591.184.334	\$11.757,40	\$13.742.100.000	16.805.687 BTC	-15,05%	
2	 Ethereum	\$101.922.134.468	\$1.050,60	\$5.231.780.000	97.013.263 ETH	-21,01%	
3	 Ripple	\$49.657.382.821	\$1,28	\$3.048.670.000	38.739.142.811 XRP *	-30,05%	
4	 Bitcoin Cash	\$32.252.397.153	\$1.906,78	\$1.641.670.000	16.914.588 BCH	-22,85%	
5	 Cardano	\$15.637.238.491	\$0,603124	\$947.277.000	25.927.070.538 ADA *	-27,71%	
6	 Litecoin	\$10.549.809.689	\$192,59	\$816.028.000	54.779.733 LTC	-19,09%	

Grazie per la vostra attenzione!

Risponderò con piacere ad eventuali domande.

