



Blockchain e il mondo della finanza

g.bertoni@securitypattern.com

Disclaimer

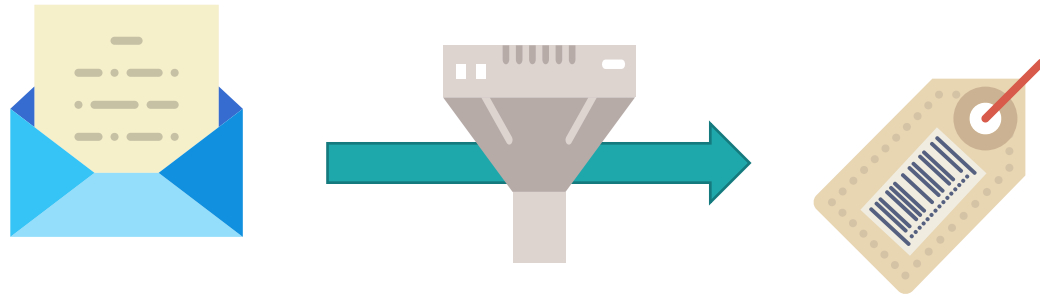
- Il contenuto di questo webinar non costituisce sollecito all'investimento in criptovalute o blockchain

Market cap

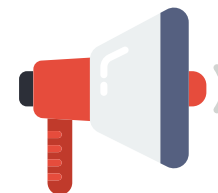
#	Name	Market Cap	Price	Volume (24h)
1	 Bitcoin	\$92,117,966,235	\$5,223.63	\$17,379,465,716
2	 Ethereum	\$18,846,273,506	\$178.51	\$9,679,011,289
3	 XRP	\$14,885,695,326	\$0.356184	\$1,591,050,089

Funzione di Hash

Funzione crittografica che trasforma un messaggio di lunghezza arbitraria in un digest di lunghezza fissa



Crittografia a chiave asimmetrica



Generazione Firma digitale



Messaggio

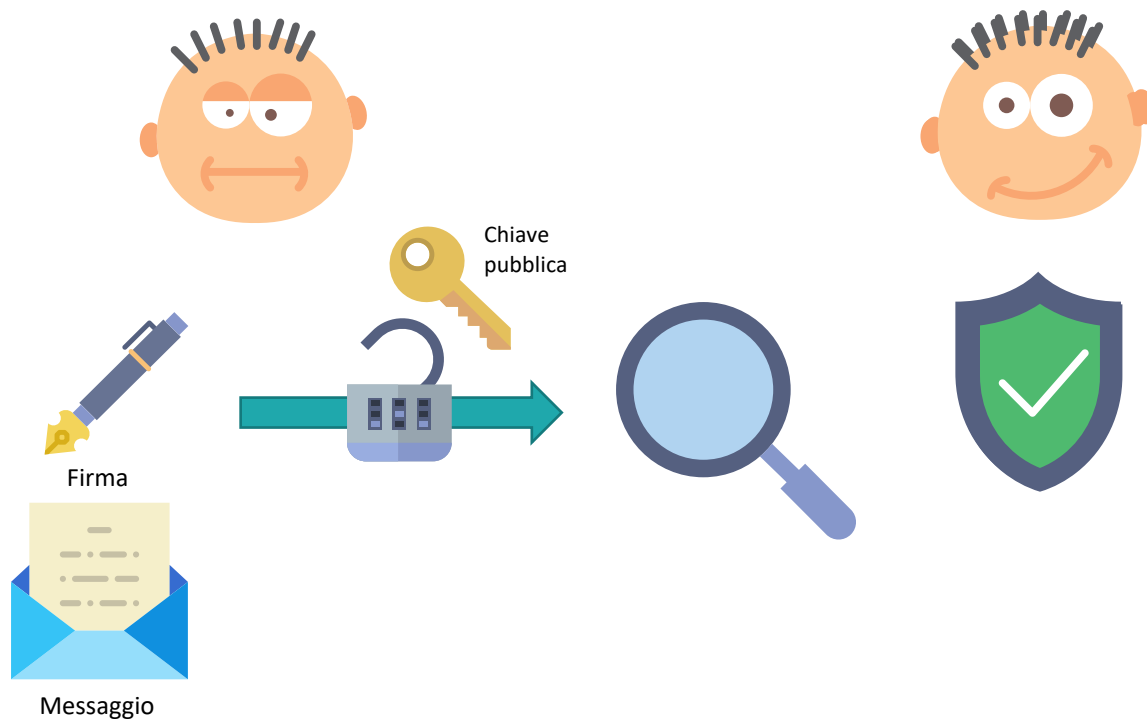


Chiave
privata



Firma

Verifica Firma digitale



CRS e CNS



Mercato auto usate

- Come funziona la compravendita di auto usate tra privati?



Procedura in Italia

- Procedura di vendita
 - Modifica del Certificato di Proprietà
 - Autentica della firma del venditore
 - Registrazione al PRA
 - Emissione nuovo certificato

- Il Pubblico Registro Automobilistico (PRA) permette di:
 - Evitare le truffe:
 - Vendere auto non propria
 - Vendere la stessa auto due volte
 - Emettere certificati di proprietà in caso di smarrimento



Registro centralizzato

- Autenticazione del venditore
- Tracciamento della transazione
 - Registrare il nuovo proprietario, il ricevente della transazione
- Ente centrale gestore del registro





Bitcoin

- Bitcoin è stata la prima moneta basata su blockchain
 - Satoshi Nakamoto 2008
- Sistema digitale, distribuito e **decentralizzato**
- Resistente al ***double spending***
- L'emissione della moneta è programmata e non alterabile

Centralizzato vs Decentralizzato

- In un sistema **centralizzato** l'utente effettua una procedura di registrazione
 - Iscrizione ad un social network, richiesta indirizzo email...
 - Tipicamente sottoscrive un regolamento
- In un sistema **decentralizzato** la partecipazione non richiede approvazione
 - La generazione delle credenziali, del portafoglio bitcoin, sono autonome senza sottostare ad approvazione
 - Il software è accessibile a tutti e permette di interagire con il sistema

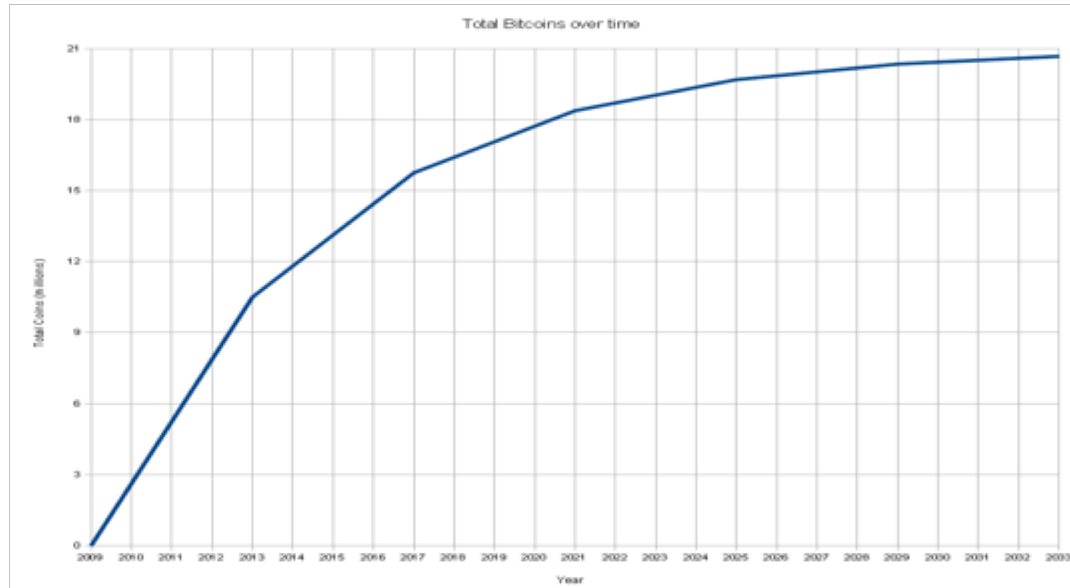
Esempio di creazione portafoglio bitcoin

Monete

- Moneta merce
 - Uso di un metallo (es. oro) per la produzione di moneta
- Moneta legale
 - Nel 1971 gli Stati Uniti passarono definitivamente alla moneta a corso legale, abbandonando la convertibilità in oro
- Politiche monetarie delle banche centrali

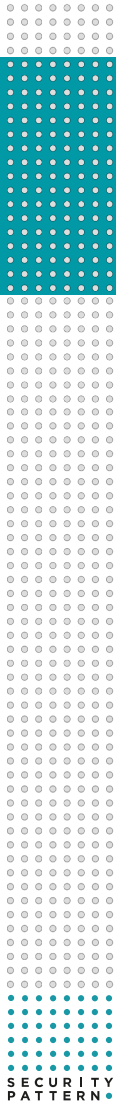
Moneta Decentralizzata

- Supply programmata -> 21 M Bitcoins



Ingredienti

- Utenti
 - Scambiano beni o servizi
 - usano moneta digitale come controparte dei pagamenti
- Registro
 - Libro digitale dove si registrano le transazioni tra gli utenti
 - E si possono leggere gli stati patrimoniali
- Nodi
 - Computer collegati ad internet
 - Mantengono copie del registro
 - Aggiornano il registro



Ruolo degli utenti

- Gestiscono un loro portafoglio
 - Ricevere pagamenti
 - Emettere pagamenti
- Le transazioni hanno un costo (fee)
 - L'utente ha facoltà di scegliere l'ammontare per facilitare la registrazione e per agevolare (ricompensare) i nodi che effettuano una registrazione

Transazione

- Un utente vuole trasferire dei bitcoin ad un altro utente
 - Entrambi devono possedere un indirizzo bitcoin
 - Il pagante deve avere abbastanza fondi
 - Il pagante compila la transazione e la firma
 - Broadcast della transazione ai nodi per registrarla su blockchain

Wallet (portafogli)

- Lo stato del portafoglio di un dato indirizzo è disponibile a tutti attraverso la blockchain
- I wallet hanno due compiti
 - costruzione della transazione
 - Mantenimento della chiave privata

Wallet

- Vari tipi di Wallet
 - Software wallet,
 - App: per mobile o per PC
 - Web: exchange
 - Hardware wallet
 - Paper wallet



Exchange



- Servizi internet che premetto il cambio tra monete e criptomonete
 - Tassi di cambio e commissioni
- Molti exchange permettono la gestione di un wallet online per facilitare l'accesso agli utenti al proprio portafoglio
 - La gestione dei portafogli da parte degli exchange richiede una particolare cura

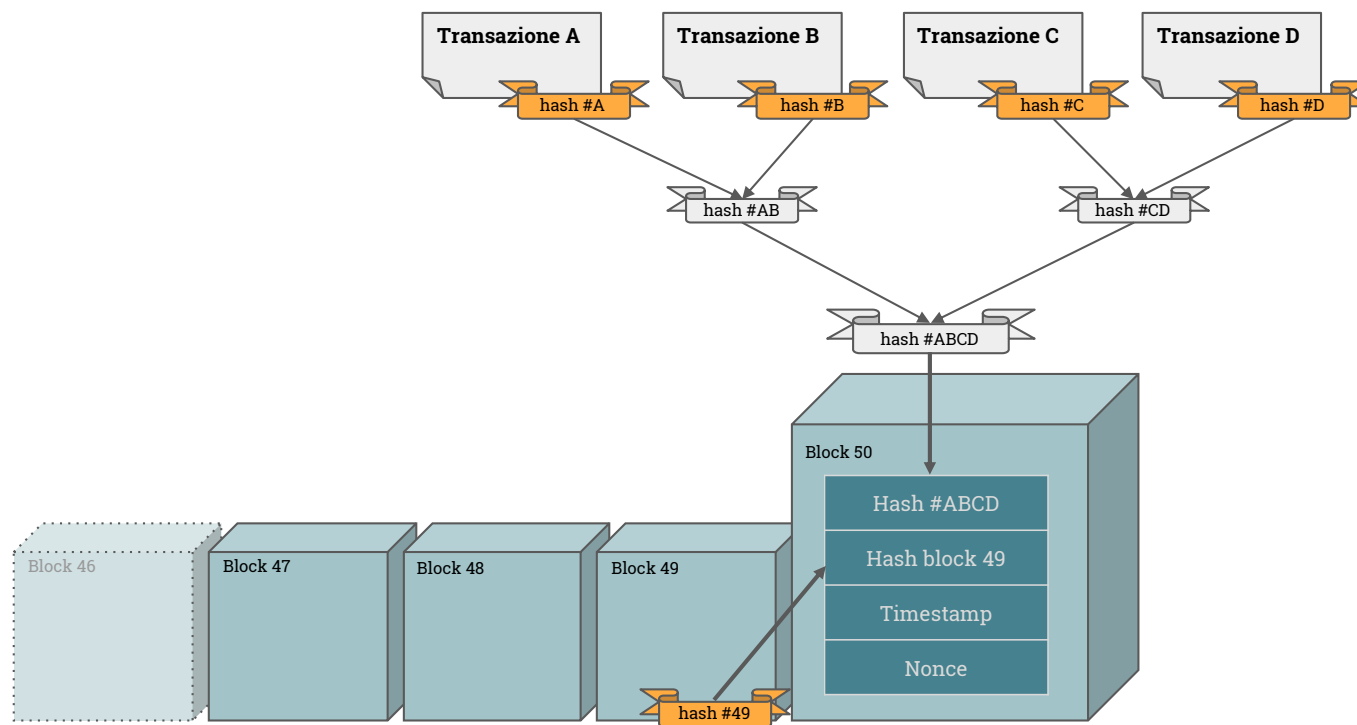
Multisignature

- I portafogli sono gestiti nelle forme base da un utente, che attraverso la propria chiave crittografica firma le transazioni
 - Se si perde la chiave, portafoglio bloccato
- È possibile adottare schemi di firma multipla
 - le transazioni devono essere approvate da più utenti/entità, anche a schemi a soglia, n -su- m

Chi registra le transazioni

- La rete dei nodi ha il compito di mantenere il registro aggiornato
 - Registrare le nuove transizioni
- C'è un incentivo ad essere un nodo
 - Guadagnano bitcoin!
 - I volontari sono i miner

Blockchain

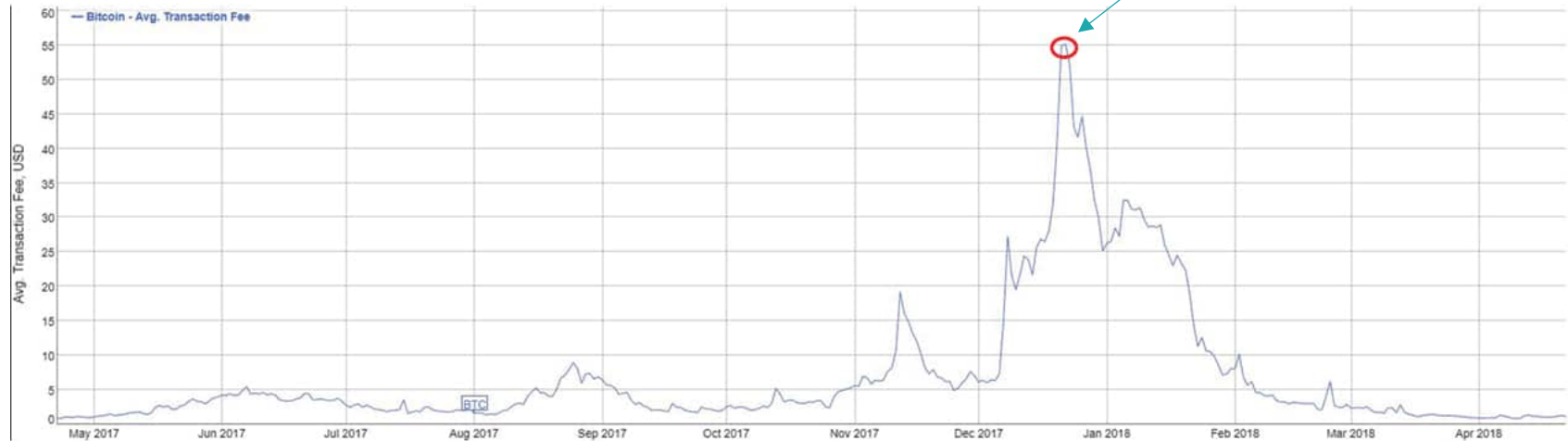


Algoritmo di Mining

- La generazione di un nuovo blocco comporta la soluzione di un «puzzle» crittografico
- La soluzione si basa su potenza di calcolo
 - Più si è potenti maggiore la probabilità di essere il vincitore
 - e quindi di generare il nuovo blocco
 - e quindi di ricevere la ricompensa
 - attualmente circa 12.5 BTC ogni 10 minuti (circa 70 k\$)
 - Il reward continua a diminuire
 - quando tutti i bitcoin saranno emessi, non ci sarà più reward

Bitcoin Fee

55 US\$



Source: <https://bitinfocharts.com/>

Proof of Work

- La soluzione del puzzle crittografico è una dimostrazione di aver speso tempo ed energia per risolvere il problema
 - Diventa la base dell'algoritmo di consenso
 - Il primo che risolve il problema, lo comunica alla rete
 - La rete verifica immediatamente la soluzione, le transazioni incluse, e accetta il blocco generato se i controlli sono corretti

Hashrate bitcoin



- Potenza di 45,867,201 TH/s indice del coinvolgimento dei nodi
- consumo elettrico stimato pari a 40-50 TWh per year
- Italia nel 2017 ha consumato 320 TWh

Decentralizzazione

- Ogni nodo che partecipa potrebbe essere malevolo
- L'algoritmo di consenso non deve permettere ad una minoranza di far deviare il sistema dal comportamento voluto
- Comportamento voluto:
 - corretta registrazione delle transazioni

Attacco del 51%

- Se qualcuno riesce a prendere il controllo del 51% della potenza di hashing può far deviare la blockchain
 - I nodi malevoli decidono arbitrariamente quali transazioni registrare
- Permette di effettuare due transazioni quasi simultanee ma registrarne solo una
 - Ad esempio cambiando verso due exchange diversi la criptovaluta

Attacco del 51%

- A gennaio 2019 si è verificato un attacco 51% sulla blockchain Ethereum Classic (ETC)
 - L'attaccante ha noleggiato potenza di calcolo
- L'attaccante è riuscito ad effettuare alcune transazioni di ***double spending***
 - gli exchange hanno scoperto i tentativi di truffa e bloccato le transazioni
- ETC era tra le 20 monete con maggiore capitalizzazione

Alternative al Proof of Work

- Proof of stake: il protocollo di decisione per la generazione del nuovo blocco decide in base alla quantità di moneta o al tempo di possesso
 - Diminuire il consumo d'energia
 - Premiare chi mantiene depositi nella blockchain

DLT, Blockchain...

- Distributed Ledger Technology (DLT), Blockchain, Permissioned Blockchain, Permissionless blockchain, Hybrid Blockchain
- ????

Permissioned blockchain

- Punto di dibattito tra gli esperti
- È una blockchain?
 - Non ci sono i miner
 - Ci sono nodi qualificati in grado di registrare le transazioni
 - Non è un vero sistema decentralizzato
- Tra i più usati Hyperledger, supportato da Linux Foundation

Stable coin

- Collaterale con moneta tradizionale
 - Promessa di pagamento
- Primo stable coin Tether (USDT)
 - Market cap 2B\$
 - Il vantaggio è quello di usare l'infrastruttura Bitcoin per trasferimento di fondi
 - Cambio fisso con il dollaro per non avere la volatilità delle cryptomonete

HSBC FX Everywhere

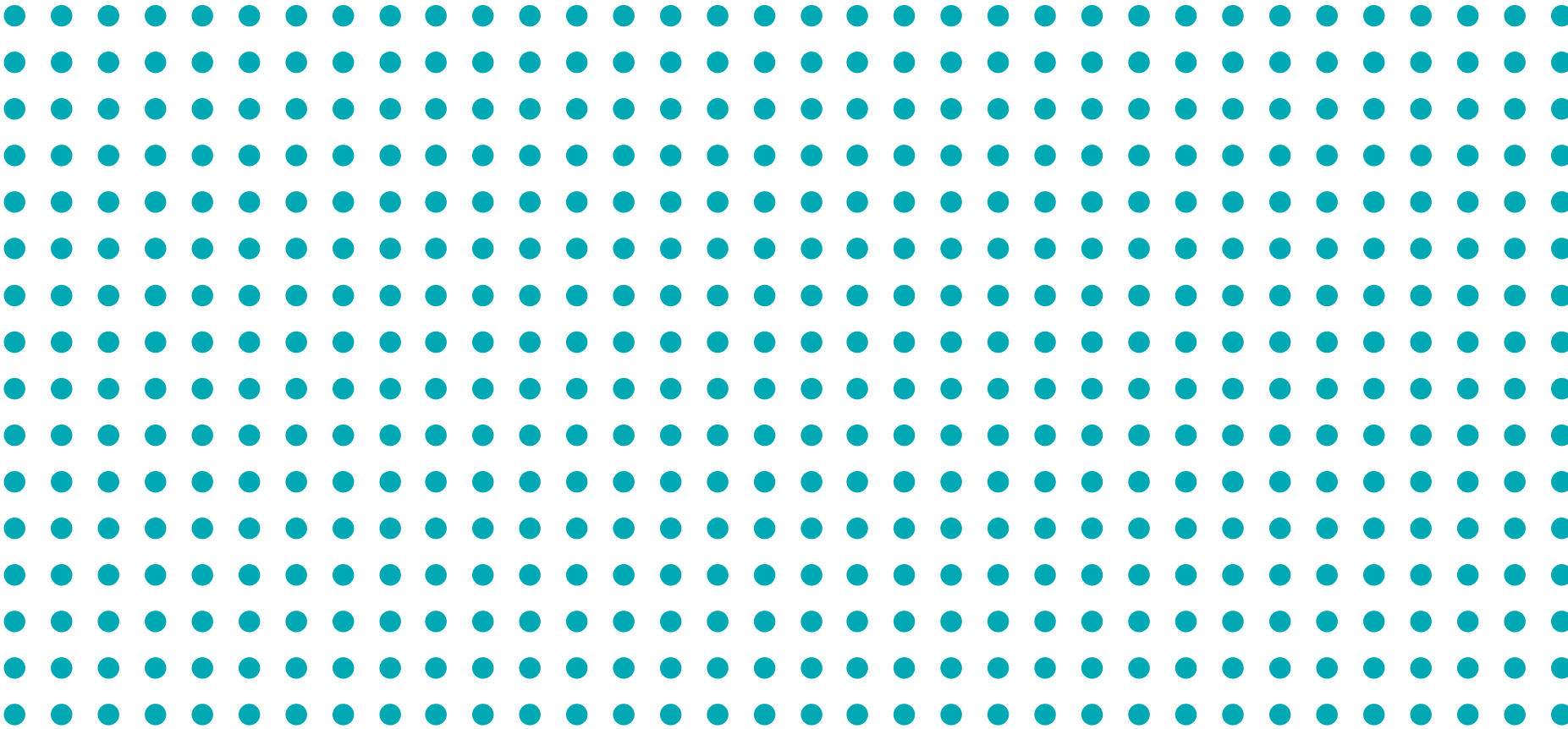
- **HSBC ha effettuato più di 3M di transazioni pari a \$250 B sulla piattaforma DLT chiama HSBC FX everywhere**
- <https://www.hsbc.com/media/media-releases/2019/fx-everywhere>

Come vedere la blockchain?

- Infrastruttura digitale, decentralizzata e distribuita per il tracciamento delle transazioni
- Non esiste un ente centrale che mantiene lo stato
 - Chiunque può partecipare
 - La partecipazione genera ricompensa!
- Le trascrizioni in blockchain diventano rapidamente immutabili

Riassunto

- Bitcoin
- Decentralizzazione
- Transazioni, Wallet, Registrazione
- Mining
- Stable coin, DLT



Smart Contract e Applicazioni

Blockchain 2.0

- Tra le evoluzioni più significative ricordiamo Ethereum introdotto nel 2015
 - Ether è la cryptovaluta di Ethereum
- Con la blockchain Ethereum sono stati introdotti gli **smart contract**

Programmare le transazioni

Blockchain 2.0

- Ethereum estende il concetto di nodi della rete con l'introduzione del concetto di macchina virtuale (Ethereum Virtual Machine)
- I nodi non solo gestiscono il registro ma eseguono anche gli smart contract

Smart Contract

- Il codice degli smart contract è scritto in un linguaggio di programmazione
 - come il software per i PC, smartphone, cloud...
- Ma una volta rilasciati sulla blockchain rimangono lì per sempre
 - Se non programmati per interrompersi o per terminare
- L'esecuzione dei programmi su blockchain ha un costo, chiamato **gas**, dipendente dalla complessità del programma
 - Senza gas lo smart contract non si aziona

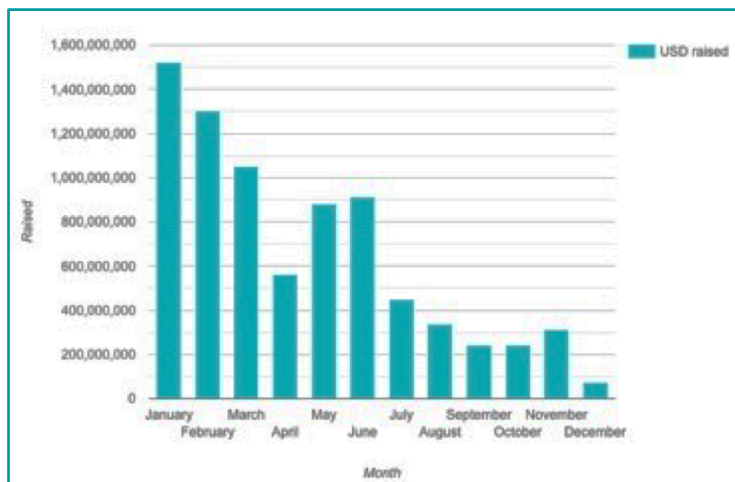
Token ERC20 e Smart Contract

- Ethereum Request for Comment (ERC), è un insieme di migliorie rispetto all'originale blockchain Ethereum
- ERC20 è uno standard che definisce i tokens e il loro utilizzo attraverso smart contract
 - I token sono oggetti digitali con regole definite dagli smart contract
 - Sono stati largamente utilizzati per far partire nuove iniziative

Uso dei Token

- Le ICO (Initial Coin Offer) hanno fatto largo uso dei token costruibili su Ethereum
 - Emissione di «gettoni» per raccolta di capitali e finanziamento di nuove blockchain o nuove iniziative su blockchain

Initial Coin Offer (ICO)



Raccolta attraverso ICO nel 2018,
fonte <https://www.icodata.io/stats/2018>



Raccolta attraverso ICO 2017-2018,
fonte Token Data

Crowdfunding

Nome	Categoria	Piattaforma	Raccolto in M\$
EOS	Blockchain	Ethereum	4,000+
Filecoin	Blockchain	Ethereum	257
Tezos	Blockchain	Independent	232
Star Citizen	Video Game	Indipendente	216
Sirin Labs (SRN)	Mobile Phone	Ethereum e Bitcoin	158
Bancor Protocol	Blockchain	Ethereum	153
TheDao	Blockchain	Ethereum	150

Fonte Wikipedia

Tipi di Token

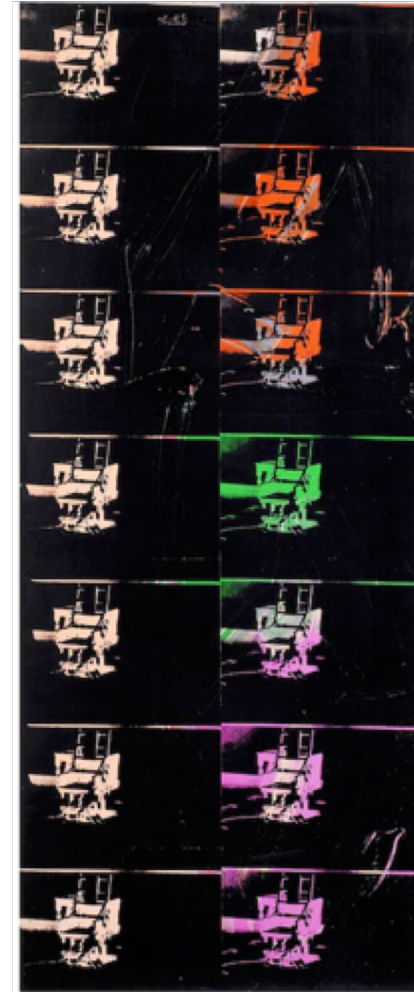
- Utility Token vs Security Token
 - Howey Test, 1946 SEC versus Howey
- Utility token è uno strumento per accedere ad un servizio o all'acquisto di un bene
 - In molti casi è una sorta di crowdfunding
- Security Token è un investimento finanziario

Tokenizzazione

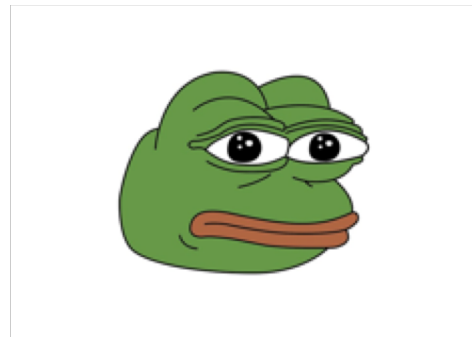
- La procedura di creare quote di un asset (immobile, opera d'arte, quote societarie...) e renderle disponibile su blockchain
 - Initial Coin Offer -> Security Token Offer
- A differenza della ICO, le STO partono con un forte concetto di strumento regolamentato
- Prospettiva di creare un mercato secondario di Security Token

Art-Tech

- La nuova frontiera di arte e tech
- «14 Small Electric Chairs» A. Warhol
- Il 31.5% venduto per 1.7 M\$, asta gestita da smart contract nel 2018



Rarepepe

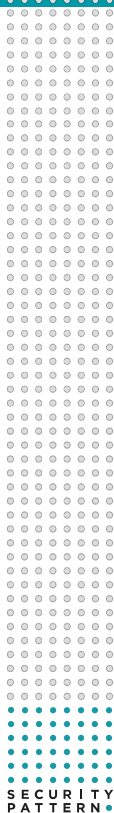
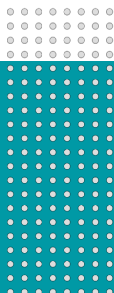


- Meme su blockchain
- I creatori di carte decidono la tiratura dell'arte digitale
- Le carte possono essere trasferite tra utenti, come se fossero figurine
- Carta unica Homer pepe
 - scambiata per 350k pepecash
 - al momento dello scambio 39k\$



Cosa sono le DAO

- **Decentralized Autonomus Organization (DAO):** entità che operano in maniera autonoma e decentralizzata
 - Gli smart contract codificano le regole e le procedure decisionali
 - Ogni azione e decisione di una DAO è programmata attraverso il codice
 - Chiunque può verificare il codice
- **Eliminare l'autorità centrale**
 - Riduzione dei costi
 - Maggior controllo e trasparenza



Come nasce una DAO



Scrittura degli smart contract:

- Definizione dei processi decisionali e regole di gestione dell'organizzazione



Viene definita una fase iniziale di finanziamento necessaria alla raccolta dei fondi che la DAO dovrà gestire:

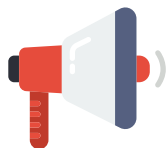
- Le persone interessate a partecipare alla DAO, versano dei fondi
- In cambio ricevono una quantità di token proporzionale al loro investimento



Al termine della fase di finanziamento la DAO può cominciare ad operare



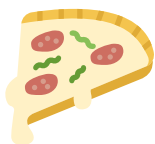
Come opera una DAO



Chiunque può fare delle proposte alla DAO su come investire/spendere i fondi raccolti



Chi possiede dei token può votare e approvare le proposte ricevute



Se una proposta raggiunge il quorum, i fondi richiesti vengono trasferiti all'indirizzo al richiedente

Filosofia

Le DAO non possiedono i soldi degli investitori

Gli investitori possiedono i token della DAO,
I token danno il diritto di voto

«The DAO»

- All'inizio di maggio 2016, alcuni membri della comunità Ethereum annunciano l'inizio della prima DAO chiamata da tutti «The DAO»
 - Codice della DAO open source



L'attacco a «The DAO»



30 Luglio 2015: Lancio della piattaforma Ethereum



30 Aprile 2016: Lancio di DAO e inizio dell'ICO



28 Maggio 2016: Conclusione ICO

150 milioni di dollari raccolti in 28 giorni, 11.000 contributor, 14% di tutti gli Ether

Il crowd-funding più grande della storia fin ad allora

L'attacco a «The DAO»



12 Giugno 2016: Stephan Tual, uno dei creatori, annuncia la presenza di una debolezza nello smart contract di DAO, ma che i fondi depositati non sono a rischio

17 Giugno 2016: un attacco sottrae 3.6 milioni di Ether (\$50M al momento dell'attacco)

18 Giugno 2016: Il valore degli ether crolla da oltre 20\$ a poco più di 11\$

20 July 2016: la comunità Ethereum decide di eseguire un hard-fork della blockchain Ethereum. Le transazioni fraudolente vengono di fatto annullate, e i fondi sottratti vengono così recuperati e restituiti ai legittimi proprietari

- L'attacco prevedeva che i fondi sottratti fossero «parcheggiati» all'interno di uno smart contract copia dello smart contract della DAO, che manteneva i fondi bloccati per 28 giorni, come per la ICO di TheDAO

Hard Fork

- La comunità decise di cancellare la transazione dell'attaccante e restituire i fondi di TheDAO ai sottoscrittori

ETC vs ETH

- La minoranza dei membri della comunità Ethereum, basandosi sui principi di immutabilità e immodificabilità della blockchain, non condivide la proposta di hard fork
- L'hard fork della blockchain Ethereum determina così una biforcazione:

Ethereum Classic (ETC) ed Ethereum (ETH)

Assicurazioni

- Usando la tecnologia degli smart contract è possibile creare delle assicurazioni automatiche
- Il sottoscrittore effettua un pagamento verso lo smart contract specificando l'evento da assicurare
- Se l'evento accade, lo smart contract paga il rimborso
- In generale chiamate «parametric insurance»

Assicurazione voli

- AXA ha attivo Fizzy
 - Smart Contract su Ethereum
 - AXA paga il rimborso su carta di credito e gestisce la raccolta degli orari d'atterraggio
 - Codice dello smart contract disponibile*
- In generale chiamate «parametric insurance»

* <https://etherscan.io/address/0xe083515d1541f2a9fd0ca03f189f5d321c73b872#code>

Oracoli

- L'esempio precedente fa vedere come sia necessario portare informazioni dal mondo reale (orario d'atterraggio) alla blockchain
- Questi portatori d'informazione vengono chiamati oracoli
 - La sicurezza dell'informazione costituisce un punto chiave

Scalabilità

Numero di transazioni al secondo gestibili:



Bitcoin **7**



Ethereum **20**



VISA **24000**

<https://usa.visa.com/run-your-business/small-business-tools/retail.html>

Problema della Scalabilità

- L'aumento dei nodi nella blockchain riduce la scalabilità
 - Ogni singolo nodo deve processare ogni singola transazione
 - Un aumento dell'efficienza complessiva dei nodi non aumenta il numero di transazioni gestite
 - Piuttosto aumenta il lavoro da fare a parità di transazioni

Blockchain Trilemma

Termine coniato da Vitalik Buterin per indicare il problema della **scalabilità** nelle blockchain.

Si possono avere contemporaneamente solo 2 di queste 3 proprietà:

- Sicurezza
- Decentralizzazione
- Scalabilità

Bitcoin & Ethereum

- Bitcoin e Ethereum sono state create con l'obiettivo di essere decentralizzate e sicure
 - Entrambe sacrificano la scalabilità
 - Decentralizzazione e sicurezza sono realizzate senza compromessi

EOS

- Nuove blockchain superano il problema della scalabilità sacrificando la decentralizzazione
- Esempio: EOS, che si basa su **Delegated proof of stake**
 - Essenzialmente si delega il compito di mantenere il registro a un limitato gruppo di nodi

Approcci misti

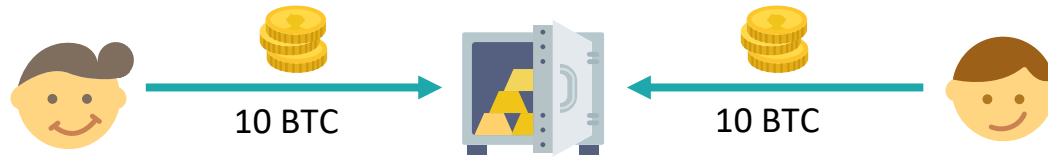
- A seconda dei casi applicativi, un diverso mix di priorità delle 3 proprietà è preferibile
- Esistono numerose soluzioni alternative che cercano di estendere la blockchain principale
 - Mantengono il vantaggio della solidità di Bitcoin e Ethereum
 - Permettono di adattarsi a diversi casi d'uso e sacrificare solo in contesti limitati questa solidità

Bitcoin: Lighting Network

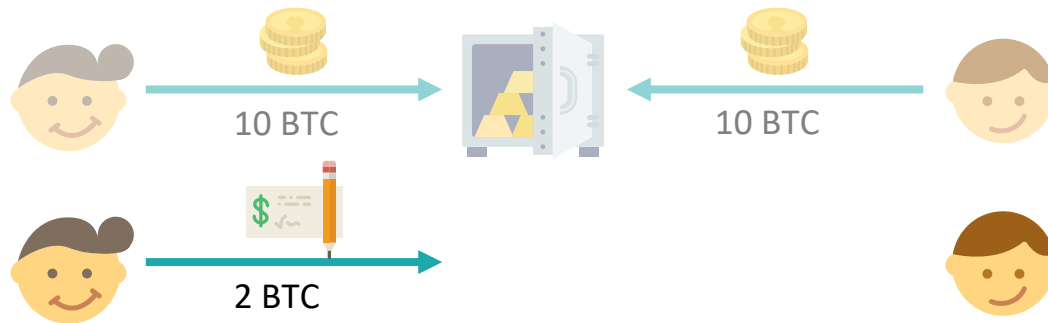


- Creare un secondo livello sopra la blockchain principale
 - La maggior parte delle transazioni vengono gestite off-chain (nel livello 2)
 - Solo il «saldo» finale viene registrato sulla blockchain principale (nel livello 1)

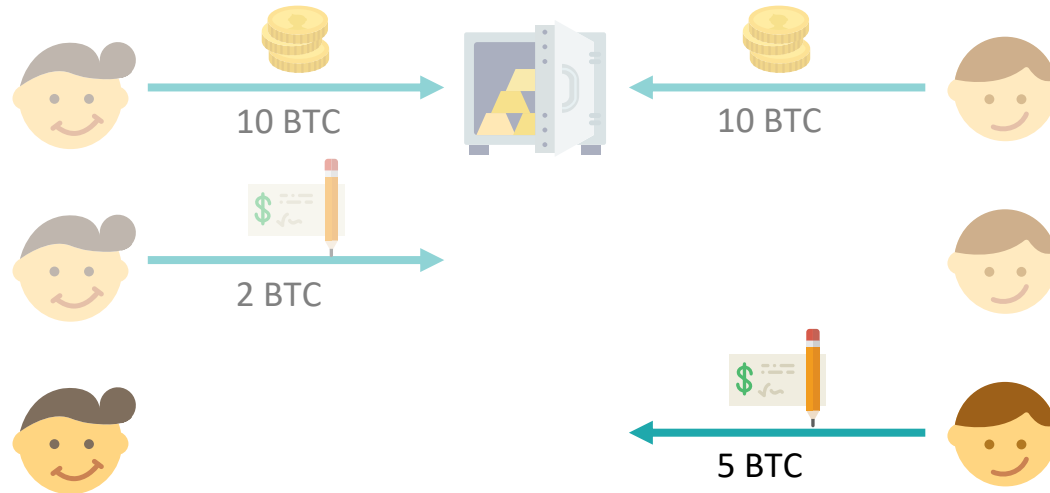
Esempio



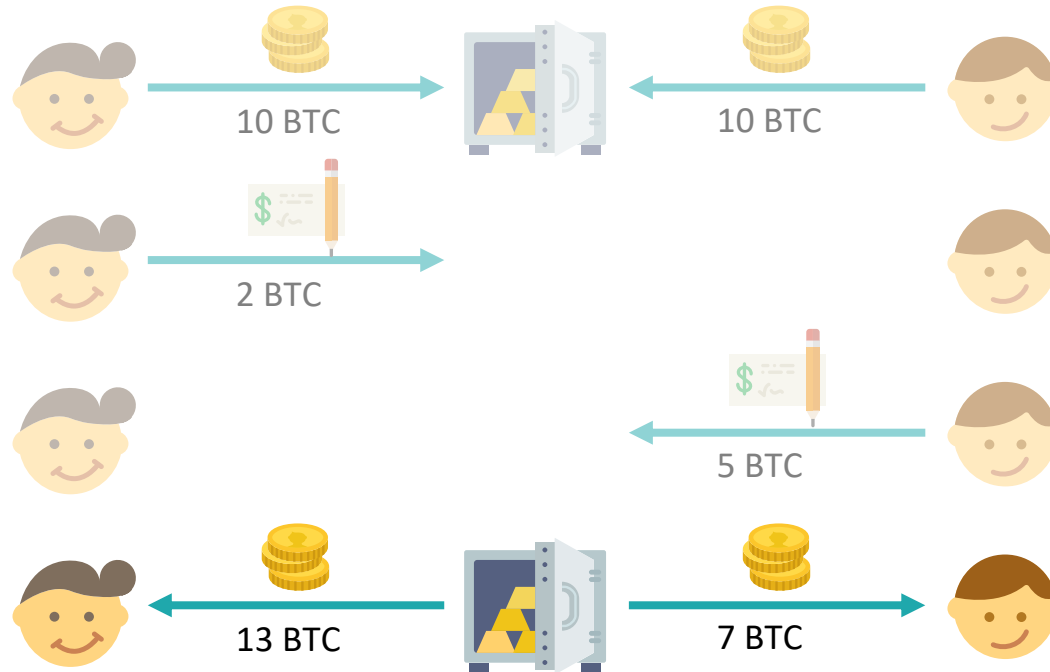
Esempio

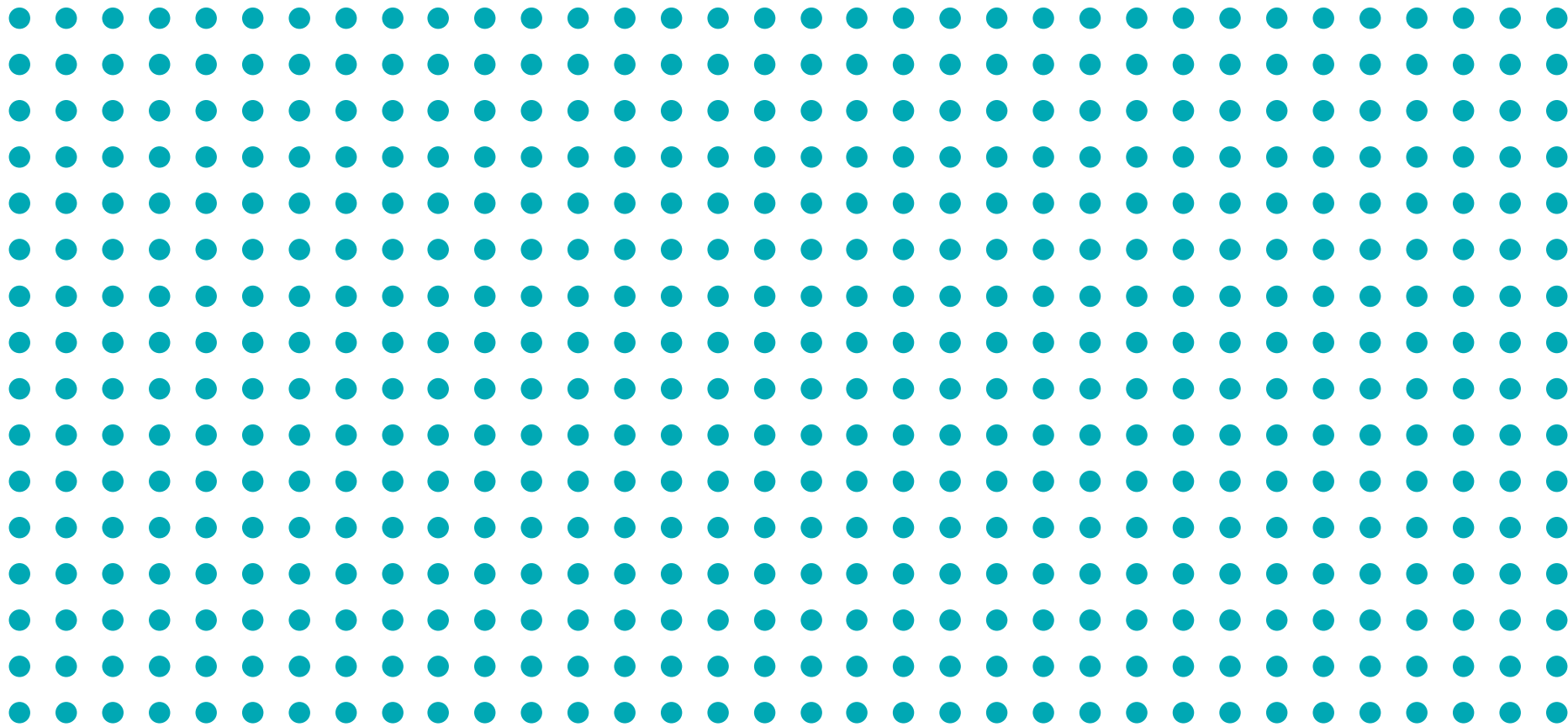


Esempio



Esempio





Aspetti Normativi



Valuta Virtuale

Autorità Bancaria Europea

«Rappresentazioni digitali di valore che non sono emesse da una Banca centrale ovvero da una Autorità Pubblica, né sono necessariamente collegate ad una valuta avente corso legale, ma che, alternativamente, vengono utilizzate da una persona fisica o giuridica come mezzo di scambio o sono detenute a scopo di investimento, e che possono essere trasferite, archiviate e negoziate elettronicamente»

EBA Opinion on Virtual Currencies, 4 luglio 2014.

Banca d'Italia

- Avvertenza sull'utilizzo delle cosiddette “valute virtuali”
Gennaio 2015
 - Carenza di informazioni.
 - Assenza di tutele legali e contrattuali.
 - Assenza di forme di controllo e vigilanza.
 - Assenza di forme di tutela o garanzia delle somme “depositate”.

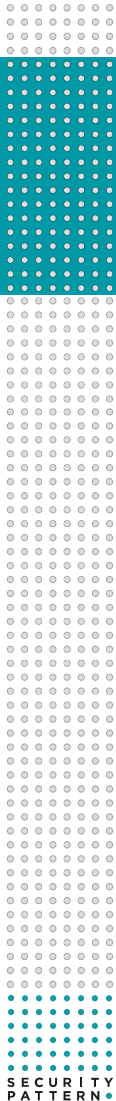
Banca d'Italia

- “Rapporto sulla stabilità finanziaria n. 1/2018” del 27 aprile 2018 ha elaborato una prima definizione di criptoattività:

“attività di natura digitale il cui trasferimento è basato sull’uso della crittografia e sulla Distributed Ledger Technology”

Banca d'Italia

- Ha affermato:
 - nonostante le criptoattività siano comunemente individuate come “valute virtuali” non svolgono le funzioni economiche della moneta
 - non integrano la moneta da un punto di vista giuridico e legale;
 - non conferiscono diritti di carattere economico (es: cedole e/o dividendi);
 - non rappresentano passività di un ente emittente.



Agenzia delle entrate

- Con riferimento ai bitcoin che, a fine esercizio, sono nella disponibilità della società si ritiene che gli stessi debbano essere valutati secondo il cambio in vigore alla data di chiusura esercizio
- *Risoluzione N.72 02/09/2016*

Imposte per i privati

- I privati cittadini devono pagare le imposte, sempre soltanto sulle eventuali plusvalenze, solo se superano 7 giorni consecutivi di detenzione di Bitcoin per un controvalore superiore a circa 51mila Euro.

Decreto Semplificazioni

- Il decreto Semplificazioni introduce:
 - definizione normativa delle tecnologie basate su registri distribuiti (blockchain) e degli smart contract.
 - memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produca gli effetti giuridici della validazione temporale elettronica.
 - Attribuisce all'AgiD il compito di realizzare, con **linee guida**, le condizioni tecniche perché la validazione temporale abbia valore legale.

Sandbox

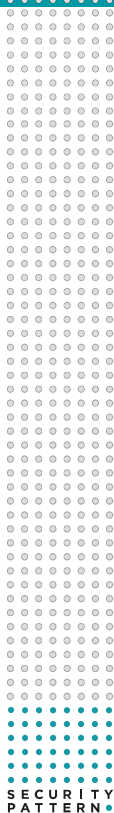
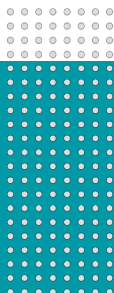
- In alcuni stati sono state create delle «bolle normative» per impedire che una lacuna normativa blocchi l'innovazione tecnologica
 - La sandbox viene monitorata attivamente del regolatore per capire le lacune normative e preparare le norme

Capitale sociale in Bitcoin

- Nel 2015 è stata costituita Oracolize s.r.l.
 - Prima società in Italia con capitale versato in Bitcoin, equivalente a 10000 euro
 - Portafoglio bitcoin gestito dall'amministratore, ricevuto transazione dai soci
- Se il valore del capitale in bitcoin scende al di sotto di 1/3 del capitale sociale, va reintegrato

Diniego dell'aumento di capitale

- Vi è stato un caso di diniego da parte di un Notaio di un aumento di capitale
 - Le criptovalute, stante la loro volatilità «non consentono una valutazione concreta del quantum destinato alla liberazione dell'aumento di capitale sottoscritto»
- Il socio ha fatto ricorso
 - Decreto di rigetto n. 7556/2018 del 18 luglio 2018 il Tribunale di Brescia,
 - Corte d'Appello di Brescia, Sez. I, 30 ottobre 2018

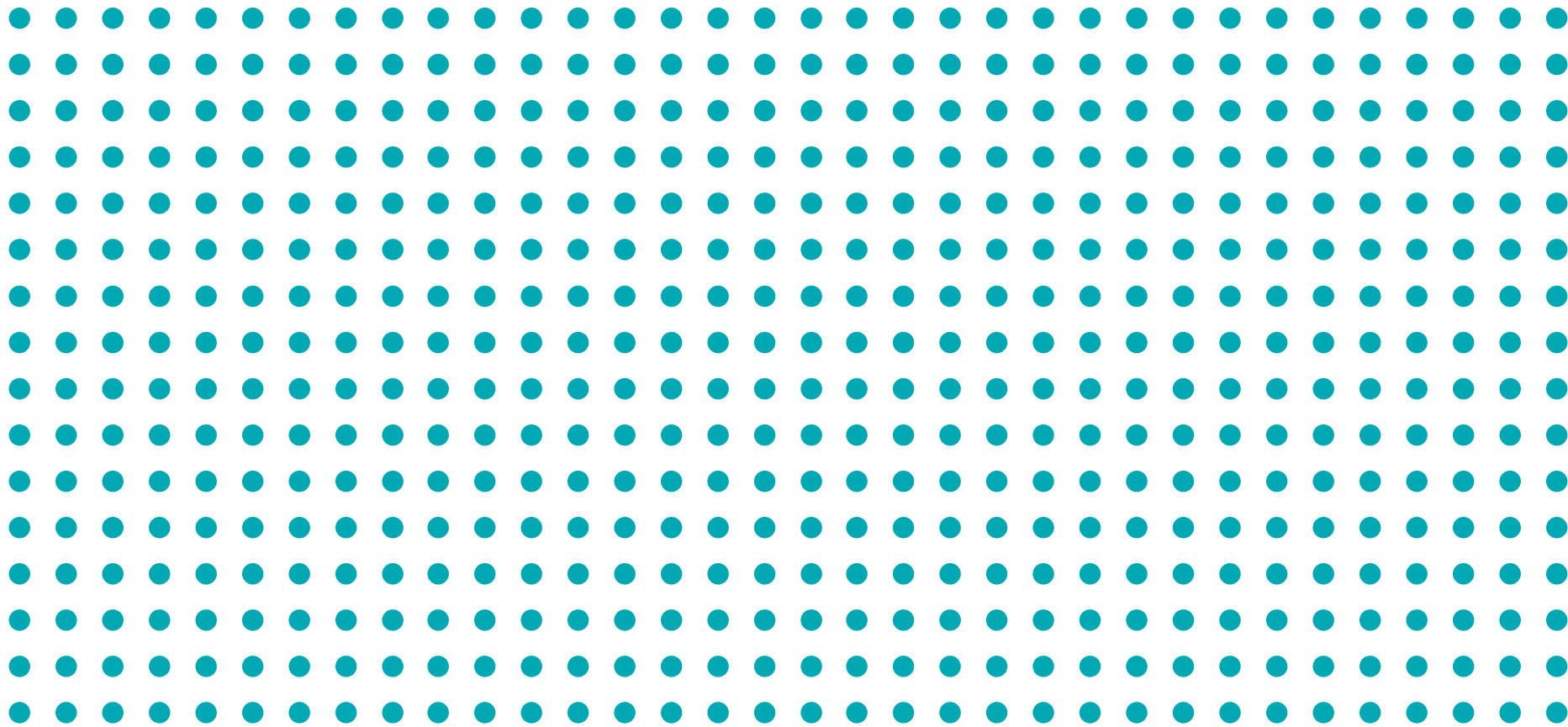


Diniego dell'aumento di capitale

- Corte d'Appello di Brescia, Sez. I, 30 ottobre 2018
«Il Collegio ritiene opportuno evidenziare preliminarmente che in questa sede non è in discussione l'idoneità della categoria di beni rappresentata dalle c.d. 'criptovalute' a costituire elemento di attivo idoneo al conferimento nel capitale di una s.r.l., bensì se il bene concretamente conferito nel caso di specie (la valuta virtuale denominata ONE COIN) soddisfi il requisito di cui all'art. 2464, comma secondo, c.c.»

Conclusioni

- Le criptomonete, la blockchain e i registri distributi sono stati una grossa novità negli ultimi anni
- Nuovo paradigma con grandi potenzialità in diversi campi applicativi
- Gli aspetti di sicurezza sono centrali per il successo delle applicazioni



Thank you!

hello@securitypattern.com

