



Il mondo dei pagamenti digitali: opportunità e insidie della rete nell'era dei Bitcoin

Clara Puce

Divisione Risparmio Gestito e Servizi di Investimento

Banca d'Italia – Sede di Milano



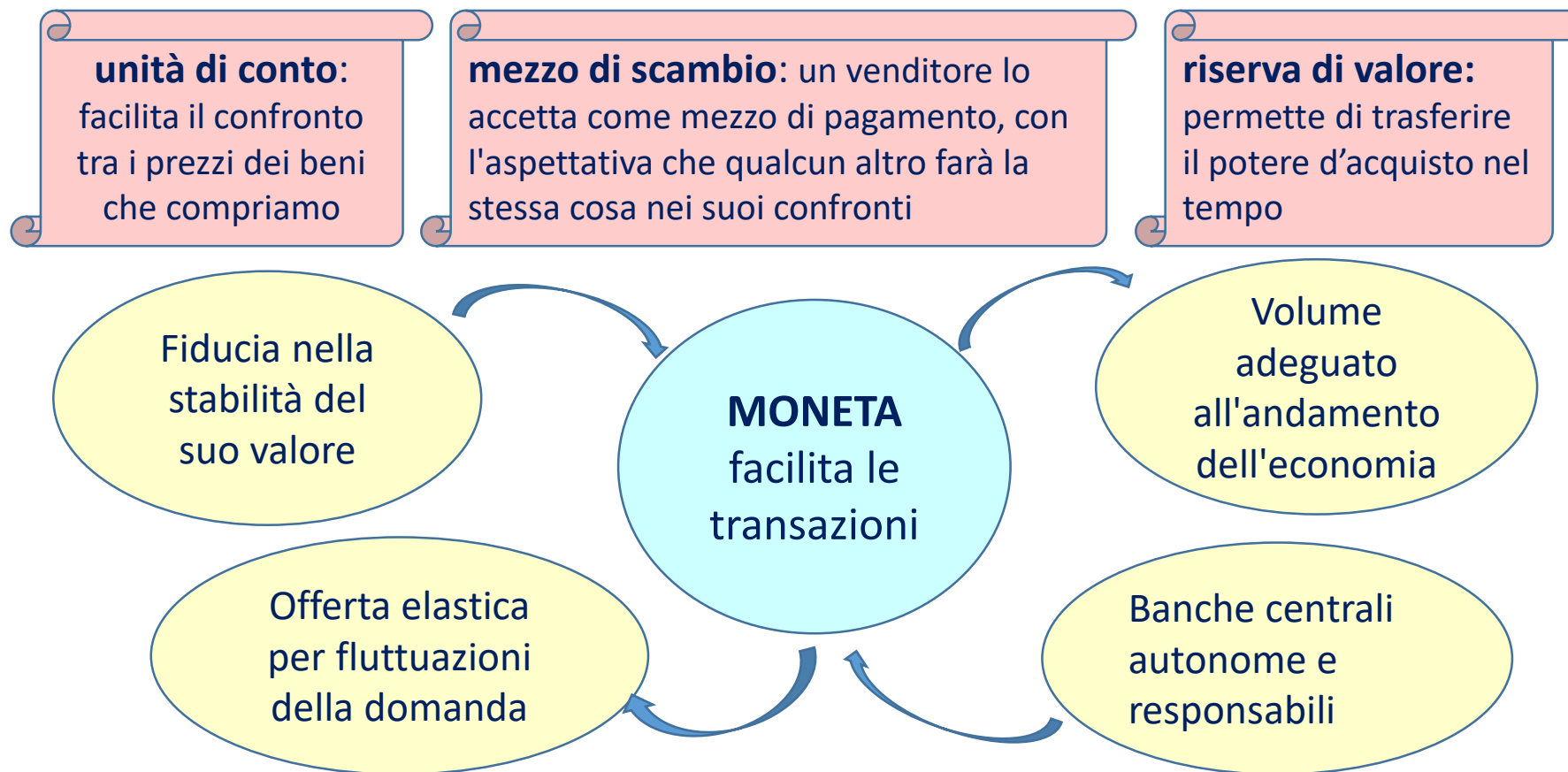
DI COSA PARLIAMO?

- La «moneta» come mezzo di pagamento: le caratteristiche di uno strumento «universalmente» riconosciuto
- Cryptoassets: caratteristiche e utilizzo
- Potenzialità della blockchain e ruolo delle Istituzioni



The good money (la cd moneta «buona»)

Relaz. 2017 – Banca dei Regolamenti Internazionali



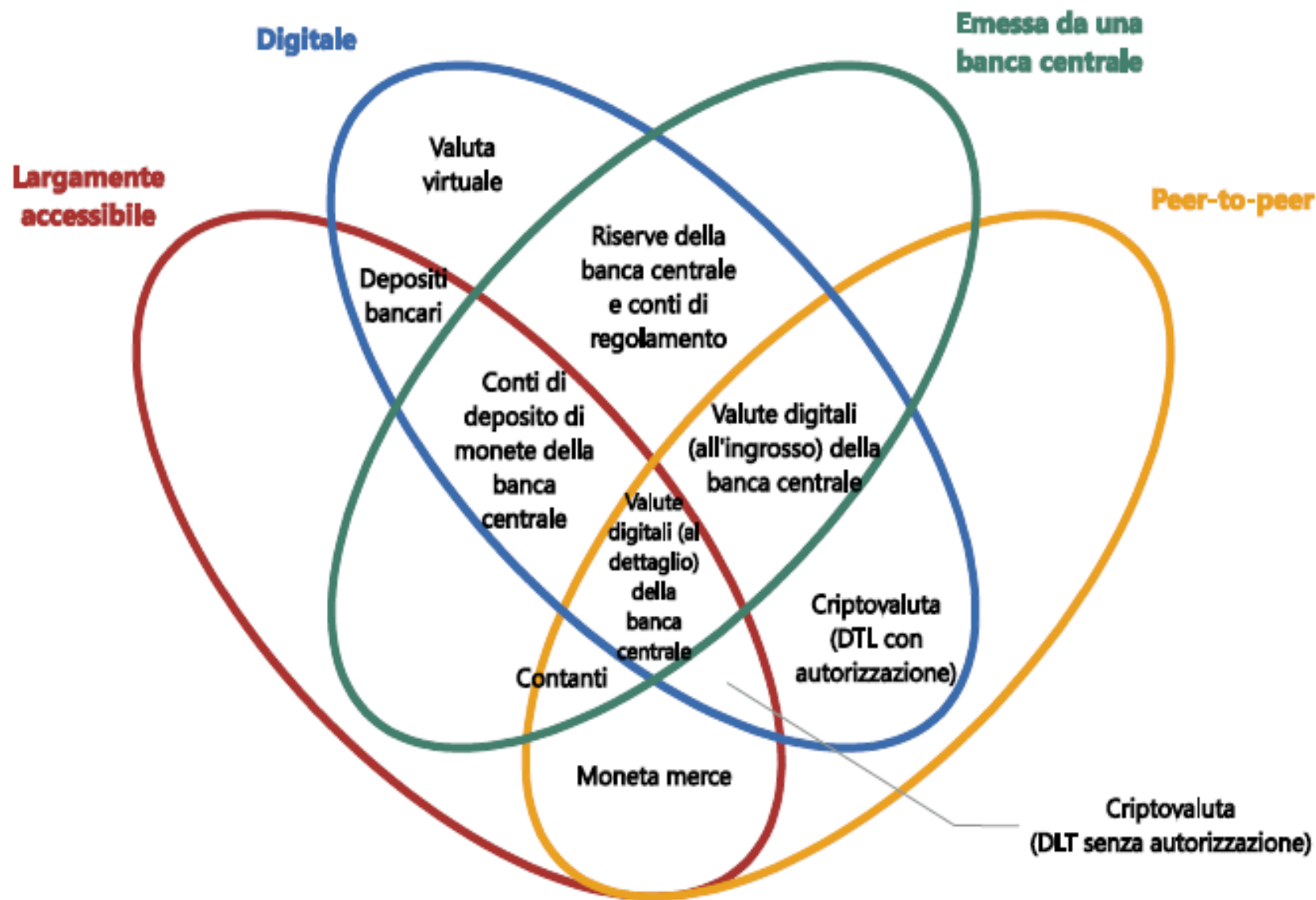
Ma la storia insegna che la moneta può essere fragile, sia che venga fornita attraverso mezzi privati (logica concorrenziale), sia che venga fornita da uno Stato sovrano (logica monopolista).



I primi «attori» della fiducia



Il fiore delle monete: una tassonomia BRI (Relaz. 2017)



Fonte: adattato da M. Bech e R. Garratt, "Criptovalute delle banche centrali", *Rassegna trimestrale BRI*, settembre 2017.



Proprietà chiave della moneta...

Emittente

(una banca centrale, una banca, o nessuno, come quando la moneta prendeva la forma di una merce)

Forma fisica

(monete metalliche, banconote di carta, formato digitale)

Grado di accessibilità

(largo accesso, come i depositi delle banche commerciali, o un accesso più ristretto, come le riserve delle banche centrali)

Meccanismo di trasferimento del pagamento

(peer-to-peer tra privati o tramite un intermediario centrale; attraverso token o conti; rischi di contraffazione o rischi di identificazione della titolarità)



...particolarità delle monete «digitali»...



PROs

- praticità, efficienza, tracciabilità e «legalità»
- pagamenti su dispositivi portatili (cd. **pagamenti di prossimità**): in modalità *contactless* tramite POS con tecnologia **NFC-Near Field Communication**; in tempo reale tra soggetti diversi (**P2P** - *peer to peer mobile payment*); nei paesi a basso tasso di bancarizzazione, i pagamenti poggiano sul credito telefonico

CONs

- sicurezza dei dati (privacy, manipolazione): *skimming, trashing, phishing...*
- prudente gestione delle credenziali di accesso: sottrazione di dispositivi e/o di identità
- disomogeneità di tempi e costi di esecuzione tra gli operatori



... e caratteristiche dei cryptoassets

CARATTERISTICHE

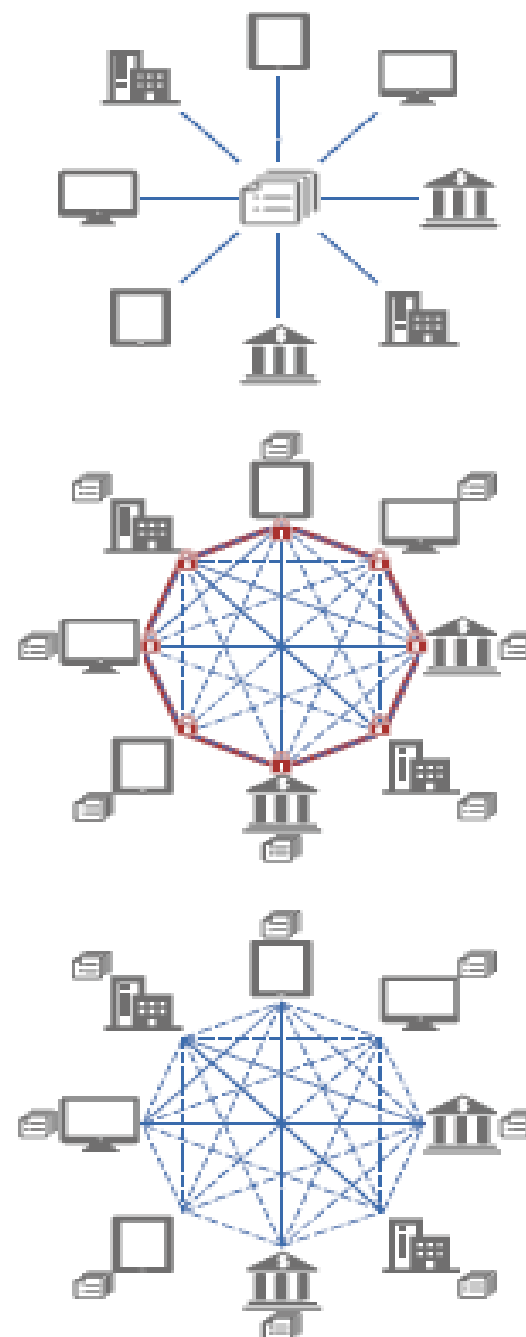
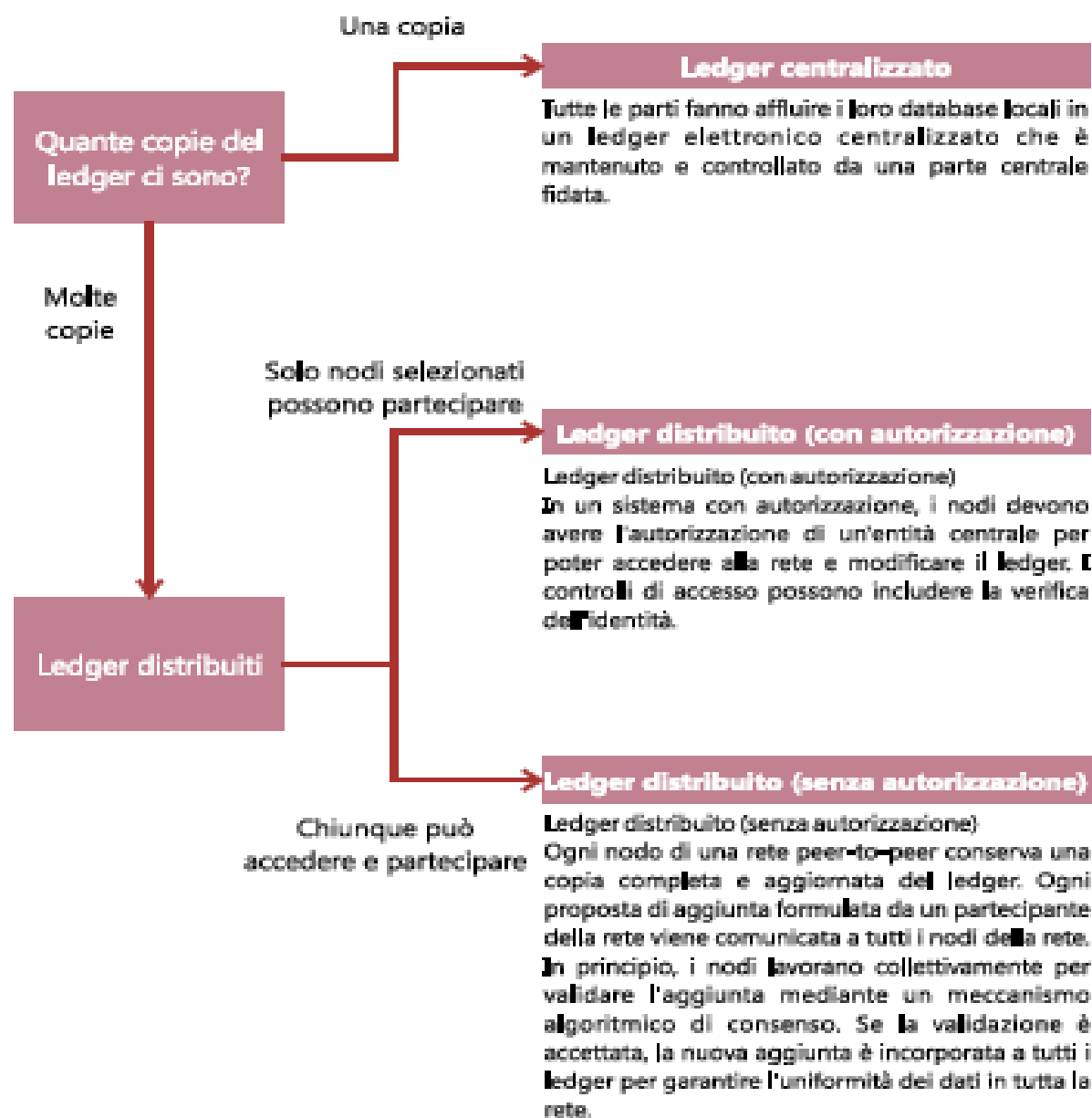
- Sono digitali e fanno affidamento sulla crittografia;
- sono create da un soggetto privato senza attribuzione di passività (non possono essere riscattate);
- valore connesso all'aspettativa che continueranno a essere accettate da altri utenti (come una moneta «merce», ma senza valore intrinseco);
- scambi digitali peer-to-peer, senza bisogno di una controparte centrale

PRESUPPOSTI:

Fiducia in un nuovo sistema completamente decentralizzato:

- Blockchain
- DLT (distributed ledger technology, tecnologia a libro mastro distribuito)
- potenza computazionale controllata da operatori onesti della rete;
- ogni singolo utente può verificare la storia delle transazioni;
- offerta predeterminata dal suo protocollo





...caratteristiche a confronto...

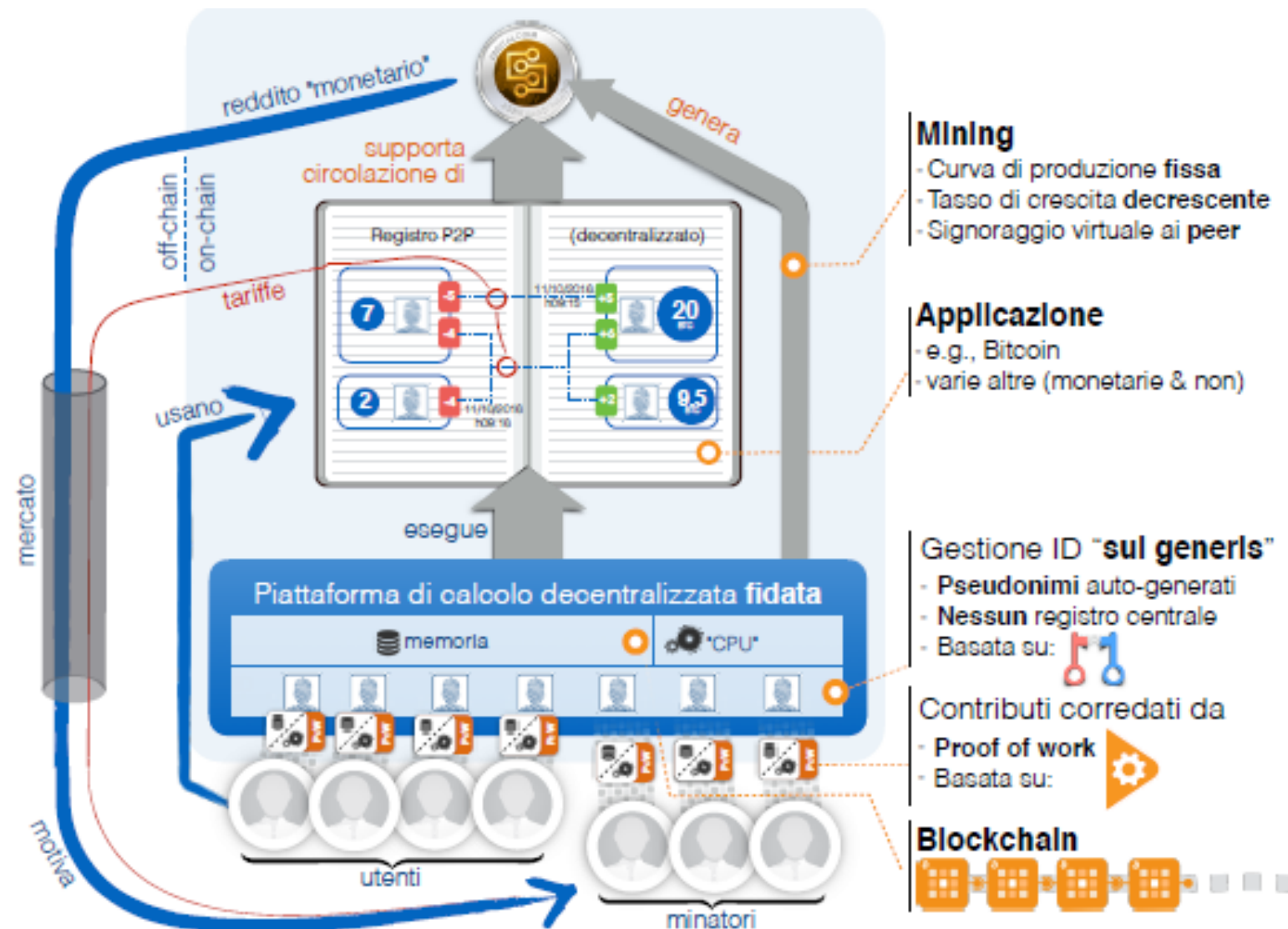
	Moneta elettronica privata basata su un sistema fiduciario	Criptovalute emesse privatamente	
		Con autorizzazione	Senza autorizzazione
1 Conservazione dei saldi/posizioni	Ledger (conti) conservati centralmente da banche e altre istituzioni finanziarie	Conservazione decentralizzata del ledger	
2 Verifica per evitare la doppia spesa	Criterio basato sull'identità	Criterio peer-to-peer: il ledger distribuito può essere verificato per vedere se un'unità specifica di una valuta è già stata spesa	
3 Trattamento delle transazioni	Conti aggiornati dalla banca	Aggiornamento del ledger tramite nodi fidati	Aggiornamento del ledger tramite proof-of-work Regola di seguire la catena più lunga
4 Criterio definitività/regolamento	Regolamento finale tramite banca centrale	Regolamento nella criptovaluta stessa	Criterio probabilistico della definitività tramite la regola di seguire la catena più lunga
5 Elasticità dell'offerta	Politica della banca centrale, ad esempio riguardo il credito infragiornaliero	Il protocollo può essere modificato dai nodi fidati	Determinato dal protocollo
6 Meccanismi per creare la fiducia	Reputazione di banche e banche centrali, vigilanza bancaria, prestatore di ultima istanza, leggi sul corso legale, indipendenza e rendicontabilità della banca centrale, verifiche antiriciclaggio e contro il finanziamento del terrorismo, cybersicurezza	Reputazione delle società emittenti e dei nodi fidati, alcuni dei quali possono essere soggetti a regolamentazione	La proof of work richiede una maggioranza computazionale onesta

Fonti: adattato da H. Natarajan, S. Krause e H. Gradstein, "Distributed ledger technology (DLT) and blockchain", Gruppo della Banca mondiale, FinTech Note, n. 1, 2017; BRI



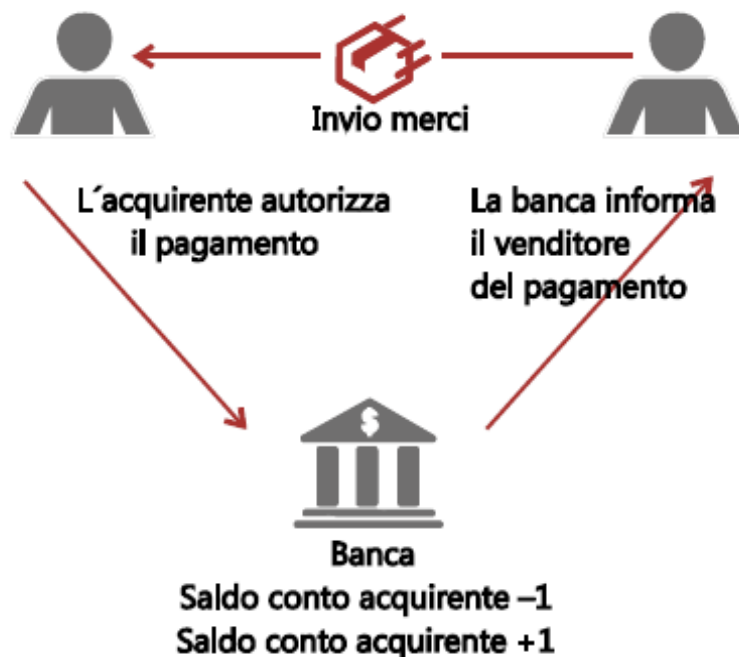
Unpermissioned ledger: Satoshi Nakamoto e la blockchain

Fonte: bankit.art,
dati 2016

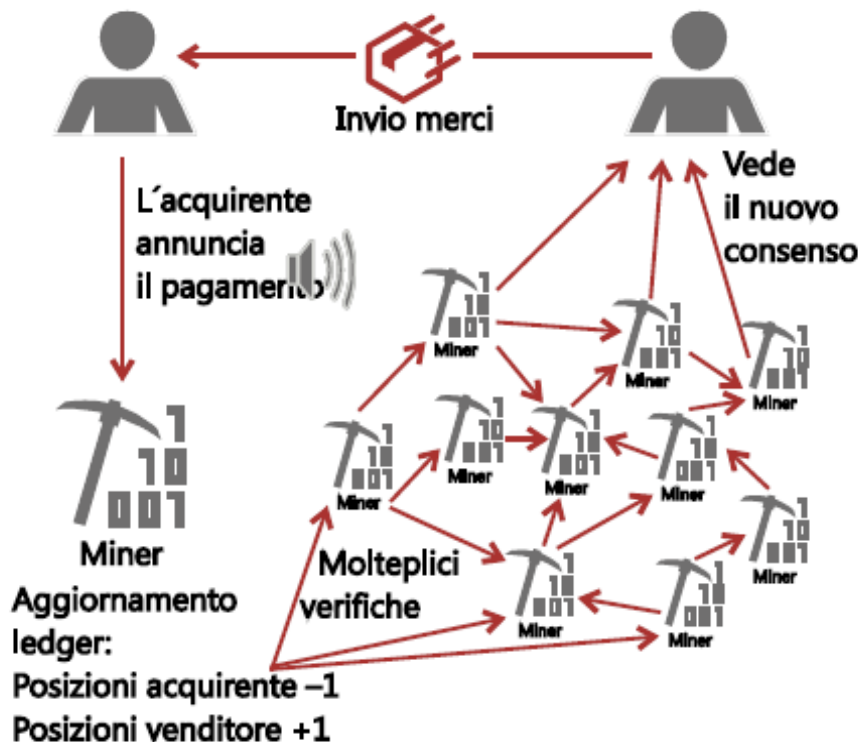


Unpermissioned ledger: la proof-of-work (Rel. 2017 BRI)

Ledger centralizzato



Ledger distribuito



Presupposti:

miner onesti; utenti che verificano la storia di tutte le transazioni; offerta di valuta predeterminata da un protocollo.

Domande:

questo meccanismo è davvero efficiente? è realmente possibile realizzare la fiducia (more untrusted node = trusted node)?



Criptoasset: qualche limite....

La fiducia può evaporare in qualsiasi momento (fragilità del consenso decentralizzato)

Un criptoasset può semplicemente smettere di funzionare (perdita totale di valore)

Un cryptoasset è incline alla congestione ed è oggetto di forti oscillazioni di valore:

- offerta non elastica
- proliferazione
- biforcazione

La scalabilità si presenta, al momento, limitata:

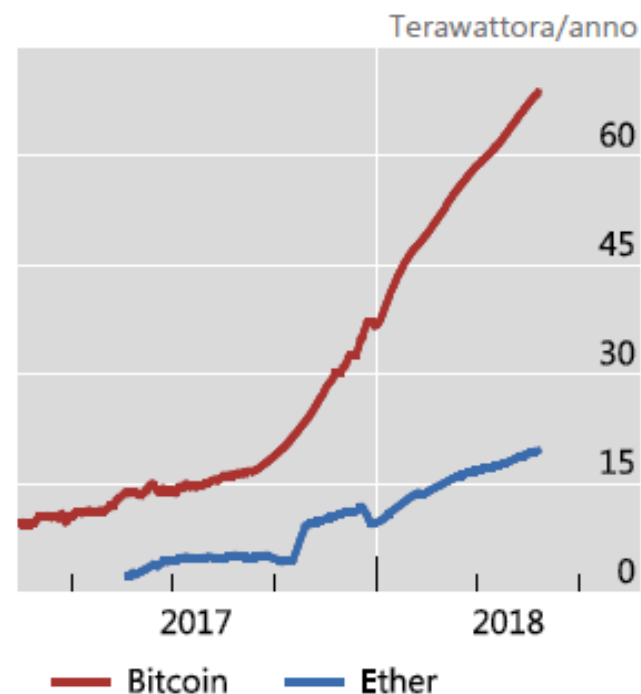
- ogni singolo miner deve scaricare e verificare la storia di tutte le transazioni mai effettuate (informazioni relative all'importo pagato, all'acquirente, al beneficiario e altri dettagli);
- ogni transazione aggiunge qualche centinaia di byte, quindi il ledger cresce notevolmente nel corso del tempo (es. la blockchain di Bitcoin cresce di ca 50 GB all'anno e ha già superato i 170 GB).

Definitività del pagamento?

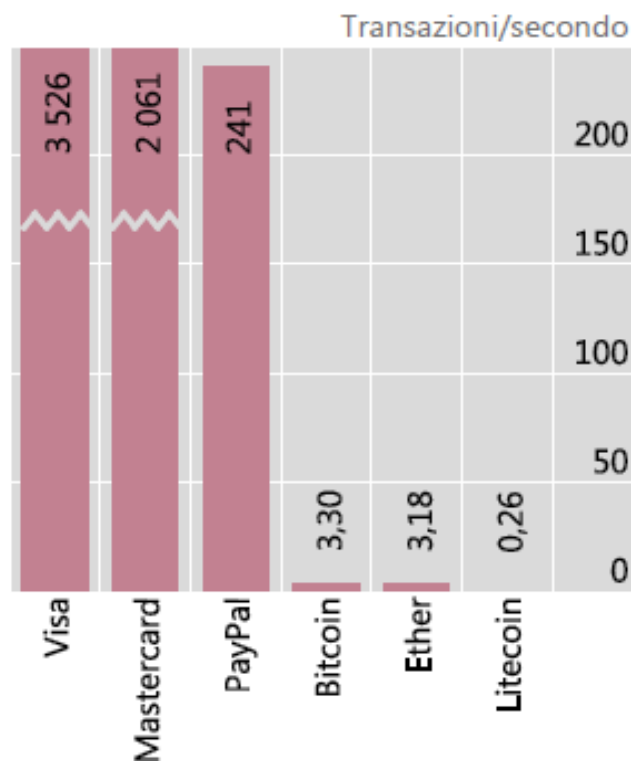


Uno sguardo ai volumi operativi... (Rel. 2017 BRI)

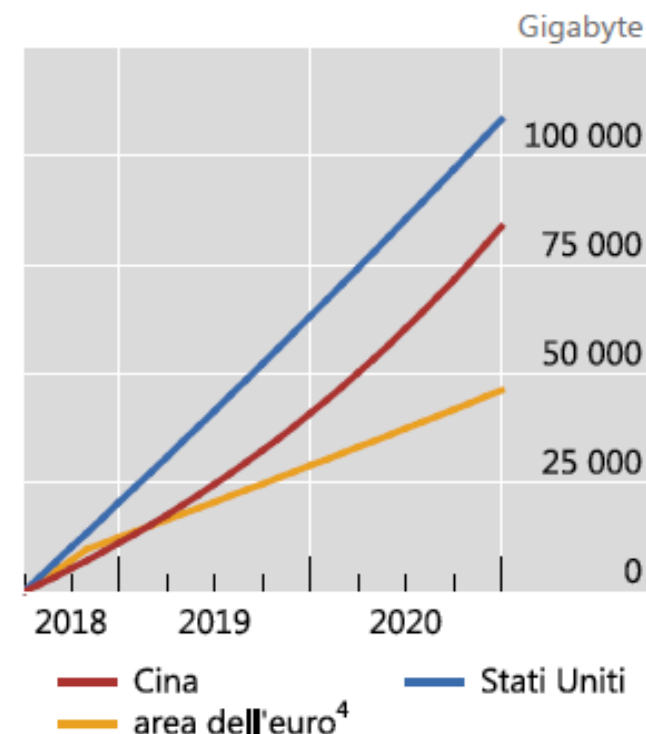
Impiego energetico di criptovalute selezionate¹



Numero di transazioni al secondo²



Dimensioni ipotetiche del ledger per criptovaluta al dettaglio a livello nazionale³



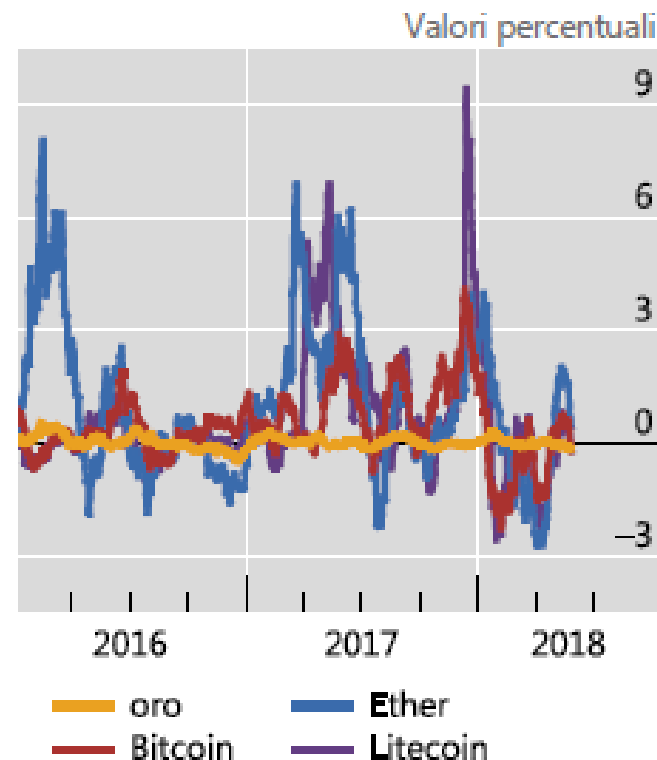
¹ Stimato. ² Dati per il 2017. ³ La dimensione ipotetica della blockchain/ledger qui presentata è calcolata ipotizzando che, a partire dal 1° luglio 2018, tutte le transazioni al dettaglio non in contanti della Cina, degli Stati Uniti o dell'area dell'euro siano elaborate tramite una criptovaluta. I calcoli si basano sulle informazioni relative al numero di transazioni non in contanti tratte da CPIM (2017) e suppongono che ogni transazione aggiunga 250 byte al ledger. ⁴ BE, DE, FR, IT e NL.

Fonti: Comitato per i pagamenti e le infrastrutture di mercato (CPIM), *Statistics on payment, clearing and settlement systems in the CPIM countries*, dicembre 2017; www.bitinfocharts.com; Digiconomist; Mastercard; PayPal; Visa; elaborazioni BRI.

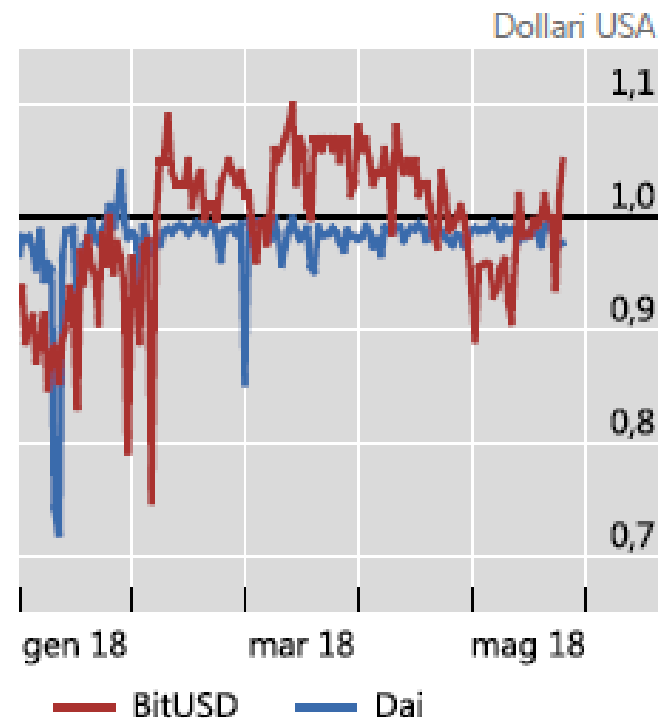


...e uno alla volatilità (Rel. 2017 BRI)

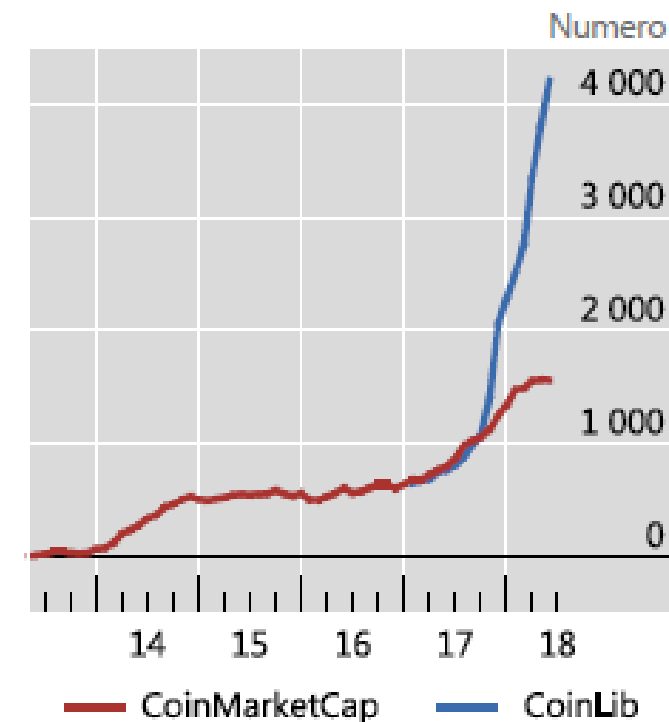
Le principali criptovalute sono relativamente volatili¹



Oscillazioni di valore delle "stable coin"²



Il numero di criptovalute cresce rapidamente³



¹ Medie mobili a 30 giorni dei rendimenti giornalieri. ² Prezzo minimo giornaliero. ³ Con base nelle istantanee mensili di due diversi fornitori. CoinMarketCap include solo le criptovalute con un volume minimo di contrattazioni su 24 ore di \$100 000; CoinLib non ha una soglia.

Fonti: www.bitinfocharts.com; www.coinlib.io; www.coinmarketcap.com; Datastream.



La posizione delle Istituzioni

**QUESTIONI
DA
RISOLVERE**

- Definire la natura giuridica dei cryptoassets (strumento di pagamento vs servizio di investimento)
- Salvaguardare la stabilità finanziaria nel suo complesso (integrità dei mercati e dei sistemi di pagamento, protezione di consumatori e investitori, prevenzione di rischi sistemici)
- Contrastare l'uso illecito di fondi
- Preservare gli incentivi a lungo termine all'innovazione, difendendo il principio "stesso rischio, stessa regolamentazione" (transnazionalità della regolamentazione e interoperabilità dei sistemi)
- Elaborare nuovi strumenti, compresa l'emissione di valute digitali da parte delle banche centrali (central bank digital currency o CBDC): effetti su pagamenti, stabilità finanziaria e politica monetaria

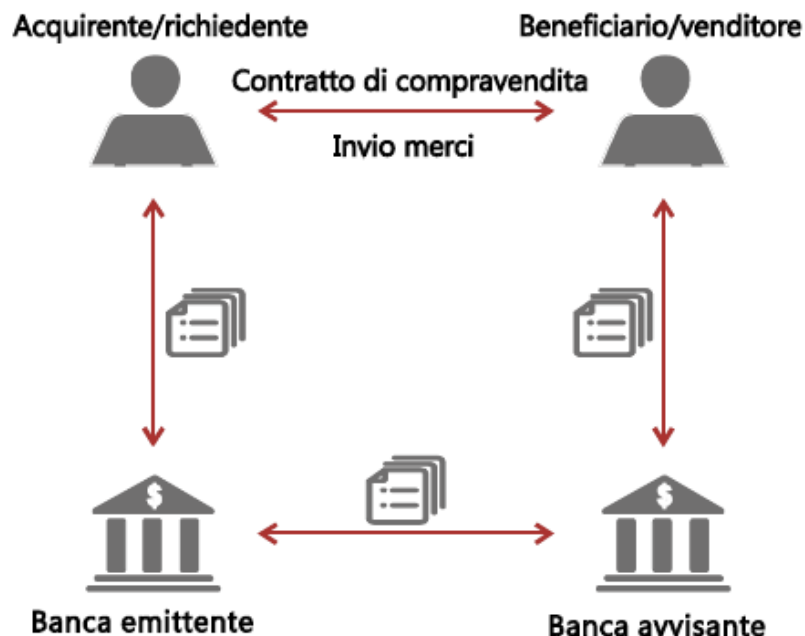


Bitcoin come tecnologia: altri usi per la blockchain

Il credito documentario Relaz. 2017 – BRI

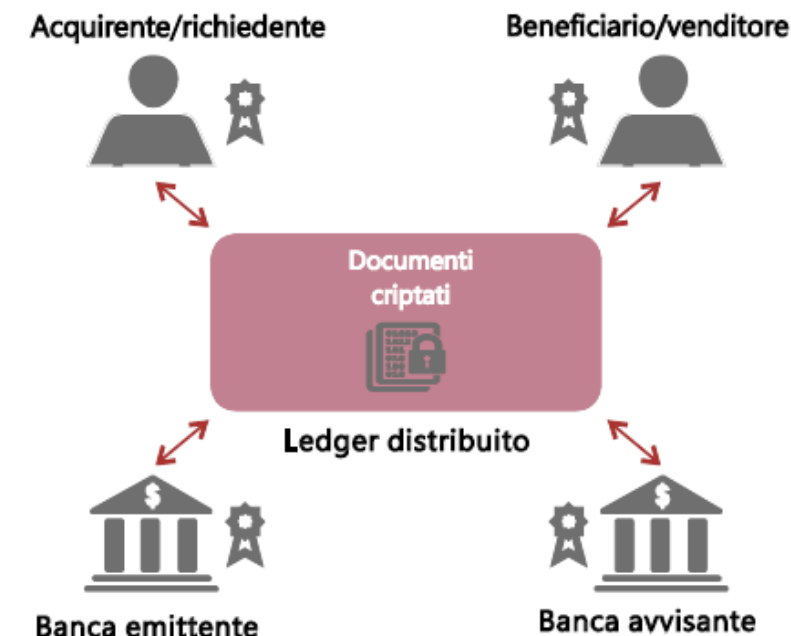
La DLT può essere efficace in contesti di nicchia o in processi amministrativi relativi a transazioni finanziarie complesse, dove i benefici di un accesso decentralizzato superano i costi operativi più elevati dovuti al mantenimento di molteplici copie del ledger.

Sistema attuale



- Lettera di credito
- Documenti
- Pagamento

Basato su DLT



Fonte: adattato da www.virtusapolaris.com.



Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain

Blockchain nel settore universitario e della

ricerca: verifica dei titoli accademici, certificazione criptata dei certificati di studio e meccanismi di trasferimento dei crediti

Blockchain nel settore del diritto d'autore e della proprietà intellettuale in genere:

tracciare, gestire e proteggere la proprietà intellettuale mediante un registro pubblico aperto; valutare la praticabilità di metodi alternativi di pagamento di tali diritti (es. utilizzando criptovalute)

Smart contracts: elaborazione di norme tecniche per l'applicabilità dei contratti intelligenti in un mercato unico digitale; la certezza del diritto può essere rafforzata attraverso il coordinamento giuridico tra gli Stati membri

Blockchain, Pubblica Amministrazione e voto

elettronico: possibilità di concepire una rete blockchain privata (permissioned) condivisa tra gli Stati membri e intesa a memorizzare i dati dei cittadini in modo sicuro e flessibile; utilizzo delle DLT per efficientare i sistemi di votazione elettronica

Regolamentazione delle ICO (offerte iniziali di moneta):

potenzialità ICO come strumento di investimento alternativo per finanziare le PMI e le start-up innovative e accelerare il trasferimento di tecnologie; importante l'inquadramento giuridico, a livello UE, distinguendo tra "security token" e "utility token"



Yves Mersch, Member of Executive Board BCE

Speech at 39th meeting of the Governor's Club Bodrum, Turkey, 14 May 2018

Virtual currencies are a misnomer: they are not money, nor will they become money in the foreseeable future. They lack the official recognition and backing of a public authority.

Authorities should pay close attention to mitigating the potential risks that could stem from a growing VC market and intensify via several channels: consumer spending; collateral valuation; knock-on effects on borrowing and economic activity (not only would investors lack equity to absorb losses, but losses would also spread to creditors); use of derivative contracts could spread the losses more broadly across the economy by allowing other market participants to hold leveraged positions against VCs; a crash could affect the stability of the wider financial system if big banks were to hold huge unhedged exposures to VCs.

The innovation itself is not without virtue. **The underlying technology may, in time, become useful and widespread.** And although we at the ECB don't intend to introduce a central bank digital currency for the foreseeable future, we are actively experimenting with the technologies. **We will be able to cater for changing needs in trusted and stable central bank liabilities that are accessible to the citizens, if and when this becomes necessary.**



Approccio congiunto delle ESAs

Comunicato congiunto del 12 febbraio 2018



Perché l'acquisto di criptovalute è un rischio per i consumatori?

Le criptovalute possono rivelarsi estremamente rischiose e sono di solito sono altamente speculative. Chi acquista valuta virtuale deve essere consapevole del rischio di perdere gran parte del denaro investito, se non addirittura di perderlo completamente, a causa di questo fattori:

- **volatilità estrema e rischio di bolla speculativa**
- **assenza di tutele**
- **nessuna opzione di uscita**
- **non trasparenza dei prezzi**
- **interruzioni dell'operatività**
- **informazioni fuorvianti**
- **inadeguatezza delle «criptovalute» per la maggioranza degli impieghi, compresi investimenti e piani pensionistici**



Fabio Panetta, Membro del Direttorio BI

7 giugno 2018, Università Bocconi

The process of digitization reflects increasing demand for immediacy by individuals, and **is transforming our behaviour, our culture and the structure of the economy.** The advent of digitization is particularly evident in the payment system.

The issuance of CBDCs – central bank digital currencies - could accordingly be seen as a natural consequence of the broader process of digitization of the financial system.

CBDCs have nothing to do with crypto-assets such as Bitcoin. In fact – just like banknotes – a CBDC would be a liability of the central bank and would be backed by its assets. It would be supported by the credibility of the central bank and, ultimately, by the rule of law. For these reasons, the value of a CBDC would not suffer from the excessive volatility that affects crypto-assets.



Roberto Rinaldi, Capo Dipartimento Circolazione monetaria

European Banknote Conference General Meeting, 13-15 giugno 2018

CENTRAL BANK DIGITAL CURRENCIES: POSSIBLE FEATURES

	Existing central bank		Central bank digital currencies		
	Cash	Reserves and settlements	General purpose		Wholesale
			token	accounts	only token
24/7 availability	yes	no	yes	possible	possible
Anonymity vis-a-vis central bank	yes	no	possible	no	possible
Peer-to-peer transfer	yes	no	yes	no	possible
Interest bearing	no	possible	possible	possible	possible
Limits or caps	no	no	possible	possible	possible



Fabio Panetta, Membro del Direttorio BI

7 giugno 2018, Università Bocconi

Questioni aperte:

- **whether the digital currency should be traceable or whether it should be designed to guarantee anonymity.** Cash has always been an incredible instrument: it allows for third-party anonymity in transactions and leaves no trace.
- **whether a CBDC should be remunerated or should pay no interest.** Interest payments would make a CBDC a closer substitute of bank deposits. This would increase the volatility of deposits and, in extreme conditions, could even facilitate a digital bank run. An interest-earning CBDC would reinforce the transmission of monetary impulses to banks, households and businesses.
- **whether CBDCs should be token-based** – whereby each token represents a particular denomination of the currency, like banknotes – **or account-based**, whereby holdings are accounting records. In particular, managing an account-based system with millions of account balances, each potentially changing every day, would require an incredible effort by the central bank. The implementation of a token-based system, instead, would be easier and could be delegated to a private party. In both cases the security and resilience of the CBDC to cyber-attacks must be assured, in order to preserve trust in the currency.



Fabio Panetta, Membro del Direttorio BI

7 giugno 2018, Università Bocconi

If central banks decided to make an asset free of credit and liquidity risk, possibly remunerated, and available to anybody at no cost, their role in the economy would fundamentally change. Are central banks ready to play this new role and to deal with the attendant complexities? In the short term the answer is no: greater investment in new technologies and human capital would be necessary to address the challenges associated with issuing a CBDC.

Many Central Banks are currently engaged in research and technical experimentation with a CBDC. The Riksbank, Bank of England, and Bank of Canada, are actively analyzing the issue. Some have gone even further, such as the Central Bank of Uruguay, which has launched a pilot project. At Banca d'Italia, we are also studying how a CBDC would impact our financial system and monetary policy, and we are working within the Eurosystem on trials using DLT, which might prove useful for a digital currency.

This research contributes to the advancement of the technological frontier, and helps make the financial system more resilient to technological and cyber risks. These benefits are here to stay, independently of whether one day we will live in a world with digital cash.



Riferimenti

- ❖ https://www.bis.org/publ/arpdf/ar2018_it.htm
- ❖ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0373+0+DOC+XML+V0//IT&language=IT>
- ❖ <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514.en.html>
- ❖ <http://www.bancaditalia.it/pubblicazioni/interventi-vari/int-var-2018/Rinaldi-20180615.pdf>
- ❖ https://www.bis.org/publ/qtrpdf/r_qt1809f.htm
- ❖ <https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2018/panetta-07062017.pdf>
- ❖ <https://maltablockchainsummit.com>
- ❖ [http://www.quellocheconta.gov.it/it/pdf/cosa_e_come/Quellocheconta ABC CosaECome Cosa sapere del le valute virtuali.pdf](http://www.quellocheconta.gov.it/it/pdf/cosa_e_come/Quellocheconta_ABC_CosaECome_Cosa_sapere_del_le_valute_virtuali.pdf)
- ❖ http://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali-2018/index.html?com.dotmarketing.htmlpage.language=102&pk_campaign=EmailAlertBdi&pk_kwd=it
- ❖ <https://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.en.html>
- ❖ <https://www.eba.europa.eu/-/esas-warn-consumers-of-risks-in-buying-virtual-currencies>
- ❖ https://www.bancaditalia.it/pubblicazioni/bollettino-vigilanza/2015-01/20150130_I15.pdf
- ❖ https://www.esma.europa.eu/sites/default/files/library/joint_esas_warning_on_virtual_currencies_it.pdf
- ❖ <http://www.bancaditalia.it/media/notizia/fabio-panetta-parla-di-cryptoasset-a-superquark/>





**IL FUTURO
PASSA DA QUI**

#SalonePagamenti2018 #payvolution

Grazie per l'attenzione

clara.puce@bancaditalia.it

