

# Crittografia in ambito blockchain

Fabio Fiori  
fabio.fiori@quadrans.io

Quadrans è una blockchain pubblica e decentralizzata, nata come fork di Ethereum.

Questa nuova blockchain è stata realizzata per essere applicabile in un contesto aziendale e industriale.

Il primo progetto realizzato è stato relativo alla tracciabilità di filiera.

La Fondazione Quadrans ha come missione quella di favorire lo sviluppo tecnologico di questa nuova blockchain.

A decorative graphic in the bottom right corner consisting of several overlapping, curved lines in shades of blue and green, resembling a stylized arc or a partial circle.

# Crittografia in blockchain

Per definizione, la blockchain è un registro pubblico, decentralizzato, distribuito e immutabile.

Data la natura distribuita e decentralizzata, sono presenti diversi problemi da risolvere, e molti di questi aspetti vengono risolti utilizzando tecniche crittografiche.

Inoltre, visto che è un registro pubblico, non è teoricamente possibile inserire dati “privati” al suo interno, a meno di utilizzare tecniche di cifratura.



Un wallet è il portafoglio digitale per avere accesso alle proprie criptovalute.

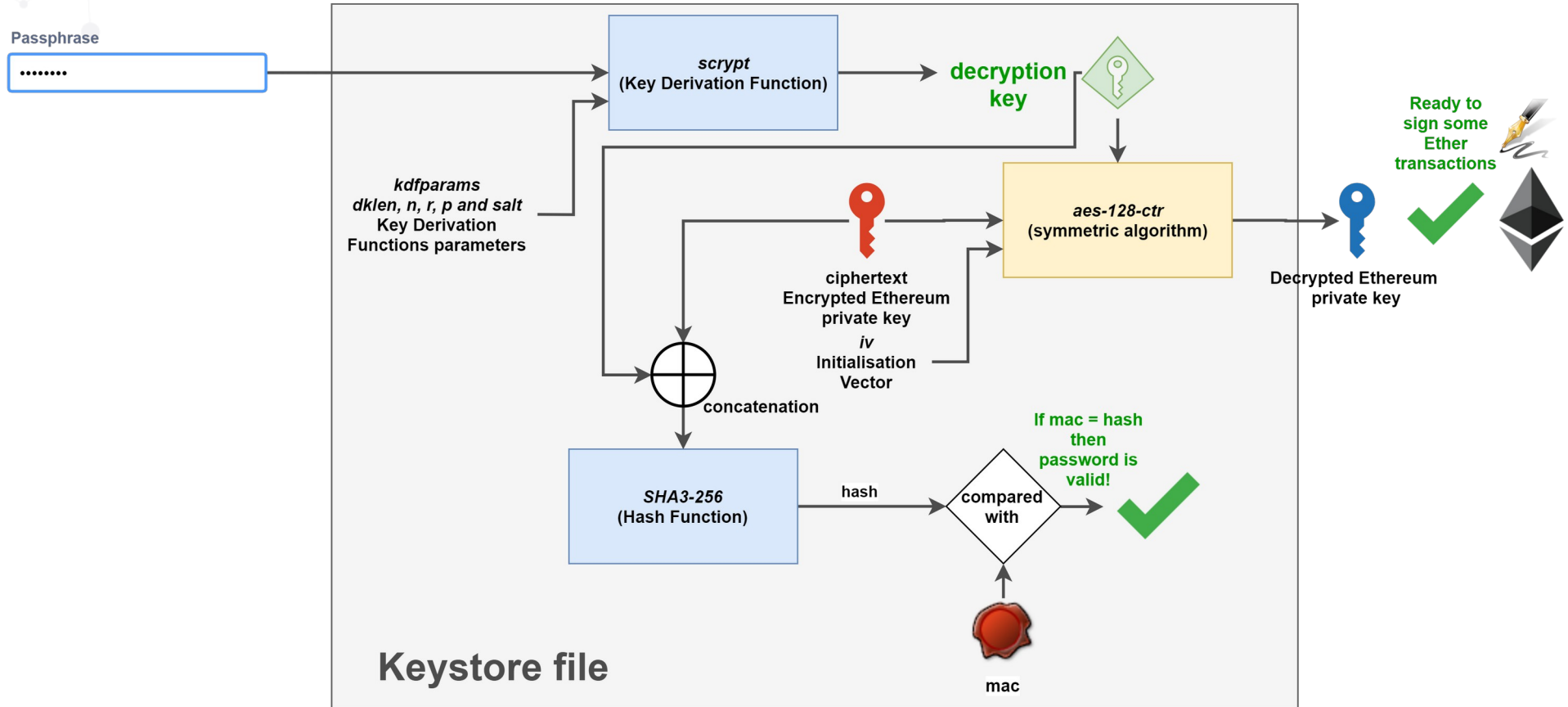
Esistono varie tipologie di wallet, ma di base sono composti da due parti fondamentali: una *chiave privata* e un *indirizzo (chiave pubblica)*.

L'indirizzo viene utilizzato per ricevere i coin, mentre la chiave privata viene utilizzata per firmare le transazioni in uscita da un determinato wallet.

La perdita della chiave privata implica la perdita del wallet stesso.

A decorative graphic in the bottom right corner consisting of several overlapping, curved lines in shades of blue and green.

# Wallet Keystore – Esempio



Un'altro dei problemi principali da affrontare è sicuramente ottenere il consensus in un ambiente dove i vari attori non si conoscono e non esiste un legame di trust tra di loro.

La metodologia scelta deve essere trasparente e equa per tutti i partecipanti, e deve essere resistente ad attacchi di attori malevoli.

Esistono varie tipologie di consensus, come per esempio Proof-of-Work, Proof-of-Stake, Proof-of-Authority, Proof-of-Burn, pBFT, ecc...

BLOCKCHAIN	ALGORITMO
Bitcoin	SHA-256
Litecoin	Scrypt
Ethereum	Now: EtHash Q1 2020(?): PoS
Monero	CryptoNight
Dash	X11
Zcash	Equihash
Peercoin	PoS
Quadrans	Now: Modified PoA TBA: Mixed PoW/PoS

Alcune blockchain, a partire da Ethereum, implementano la possibilità di scrivere “Contratti Intelligenti” da inserire all’interno della blockchain.

Questi contratti permettono di eseguire codice il cui risultato viene scritto all’interno del ledger, ottenendo quindi le proprietà di immutabilità e distribuzione proprie della blockchain.

I contratti contengono una parte computazionale e una di storage, e devono essere deterministici, in quanto devono poter essere eseguiti da tutti i nodi della blockchain.



Gli smart contract implementano nativamente diverse primitive crittografiche e di hash, come per esempio funzioni legate alle curve ellittiche e a SHA 2/3.

È inoltre possibile implementare smart contract che risolvano altre tipologie di funzioni crittografiche, l'unico vincolo da tener conto riguarda la generazione di eventuali numeri casuali.

Inoltre, è possibile utilizzare smart contract in contesti di scambio chiavi in ambiente distribuito.



# Dapp e crittografia

Si definiscono applicazioni decentralizzate (Dapp, o dApp), tutte quelle applicazioni che operano su un sistema computazionale distribuito (ossia un insieme di computer dislocato in parti differenti della Terra).

Le dapp esistono da prima dell'avvento della blockchain, basti pensare a BitTorrent.


Le dapp generalmente sono composte da uno (o più) smart contract e da un'interfaccia utente per rendere il loro utilizzo user friendly.

Una delle operazioni possibili utilizzando le Dapp è quella di utilizzare la blockchain come storage immutabile.

Questo permette di salvare in maniera immutabile le informazioni, ma ci obbliga anche a renderle pubbliche e condivise con tutti.

Questo in alcuni ambiti chiaramente non è possibile, quindi si utilizzano algoritmi di cifratura per proteggere le informazioni.

In Quadrans, per esempio, abbiamo implementato la cifratura con ABE per fornire una soluzione a questo tipo di problema.

Decorative graphic element consisting of several overlapping, curved lines in shades of blue and green, located in the bottom right corner of the slide.

Come è stato visto in queste situazioni, la crittografia gioca un ruolo fondamentale nell'ecosistema blockchain.

Senza la crittografia non sarebbe possibile implementare alcune operazioni chiave all'interno della blockchain, e i campi applicativi su cui applicarla sarebbero molto più ristretti rispetto a quelli attuali.



Grazie

Three overlapping curved lines in shades of green and blue, located in the bottom-right corner of the page.

1. Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, (2008), URL: <https://bitcoin.org/bitcoin.pdf>.
2. Ethereum team, Ethash, (2018), [ethereum/wiki/wiki/Ethash](https://ethereum/wiki/wiki/Ethash)
3. Sompolinsky Y., Zohar A., Secure High-Rate Transaction Processing in Bitcoin, <https://eprint.iacr.org/2013/881.pdf>
4. Lamport L., Shostak R., Pease M., The Byzantine Generals Problem, in ACM Transactions on Programming Languages and Systems, vol. 4, n° 3, luglio 1982
5. Bitcoin.org
6. Castro, M., Liskov, B. (2002). "Practical Byzantine Fault Tolerance and Proactive Recovery". ACM Transactions on Computer Systems.
7. Computing for Good - Ripple's Contribution to Science, [http://www.devtome.com/doku.php?id=computing\\_for\\_good](http://www.devtome.com/doku.php?id=computing_for_good)
8. Meneghetti A., Sala M., Sogorno D., Taufer D., A survey on PoW-based consensus with a new ECDLP-based PoW proposal
9. King S., Nadal S.: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, (2012), URL: <https://peercoin.net/whitepapers/peercoin-paper.pdf>

10. Guo H., Meamari E., Shen C., Multi-Authority Attribute-Based Access Control with Smart Contract, <https://arxiv.org/pdf/1903.07009.pdf>
  11. Schindler P, Judmayer A., Stifter N., Weippl E., Distributed Key Generation with Ethereum Smart Contracts, <https://www.sqi.at/resources/Schindler-2019-CIW-Distributed-Key-Generation-with-Ethereum-Smart-Contracts.pdf>
  12. Quadrans, <https://quadrans.io>
- 
- A decorative graphic in the bottom right corner consisting of several overlapping, curved lines in shades of blue and green, resembling a stylized arc or a partial circle.