PRIVACY & SICUREZZA

LE LINEE GUIDA DELLA BLOCKCHAIN E DELLE CRYPTOVALUTE

SMARTCONTRACTS . . . A CHE PUNTO SIAMO?

STEFANO BISTARELLI

cini Cybersecurity National Lab

IL SALONE DEI PAGAMENTI PAYVOLUTION

COS'È UNO SMARTCONTRACT

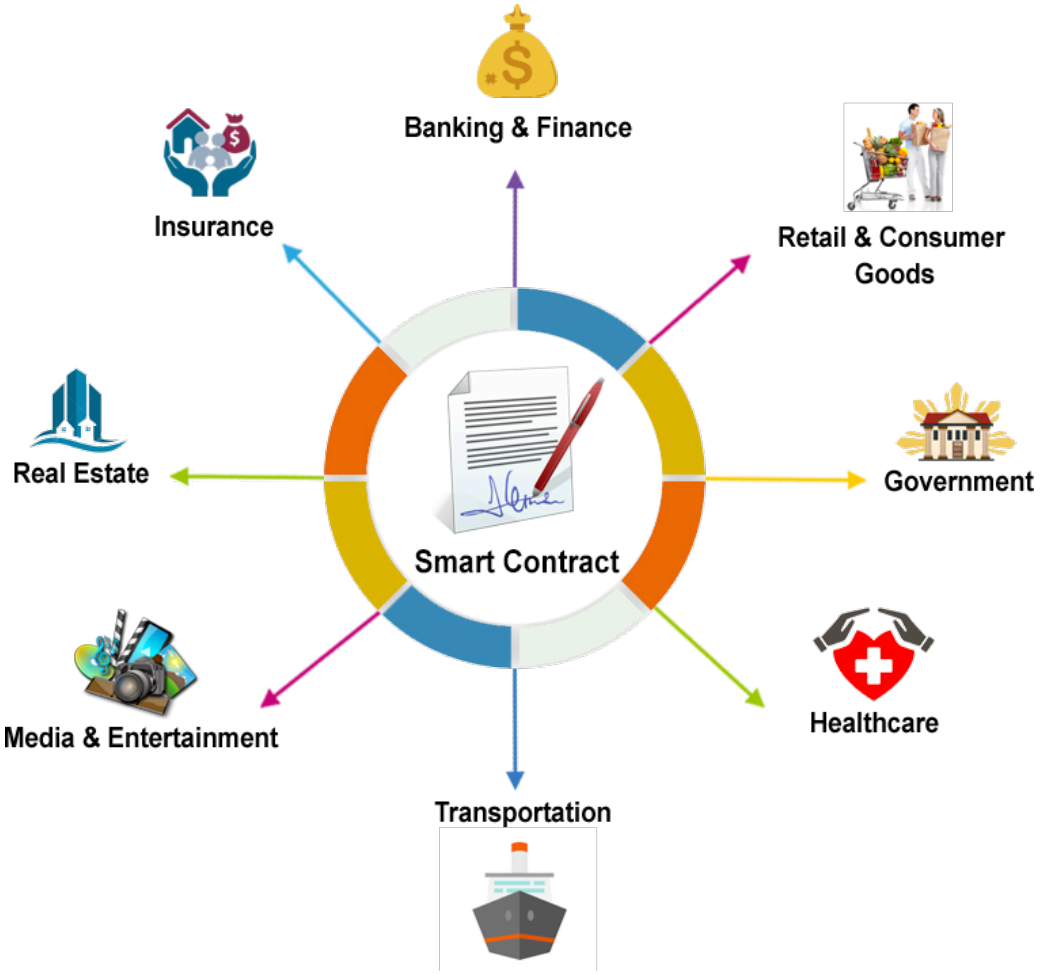
- "contractual type arrangement embedded in software"
- "protocollo informatico in grado di eseguire determinati termini contrattuali"
- "una forma avanzata della funzione "if-then" scritta in un linguaggio informatico" .
- **"[...] a set of promises, specified in digital form, including protocols within which the parties perform on these promises." [Nick Szabo '90]**

- smart contract una sorta di "ibrido" tra codice e contratto, tra informatica e diritto.
  - coniugare la certezza e automaticità di una condizione preimpostata a livello informatico (if-then) con un effetto giuridico che si sostanzia tra due parti contrattuali .

COS'È UNO SMARTCONTRACT IN BLOCKCHAIN

- Quando uno smart contract viene inserito all'interno di una blockchain, a questo particolare "meccanismo" viene aggiunta la caratteristica dell'**immutabilità** e della sua "**distribuzione**"
  - notevoli vantaggi i quali sono legati all'esecuzione pressoché automatica dei termini contrattuali inseriti nello smart contract e
  - la possibilità di avere un "record o prova" di una transazione o di un particolare "fatto" che rimane regi- strato in modo immutabile (o quantomeno la cui falsificazione/ alterazione, per la struttura della blockchain e le regole sul consenso, rende di fatto totalmente anti-economico attuare cambiamenti ex post) .
- legalmente ??

CAMPI APPLICATIVI



ESEMPI

BANKING & FINANCE

Compound

GNOSIS

GOVERNAMENT

ARAGON

computing Power Lend/Borrow

golem

JOB MARKET

Ethlance

DIGITAL IDENTITY

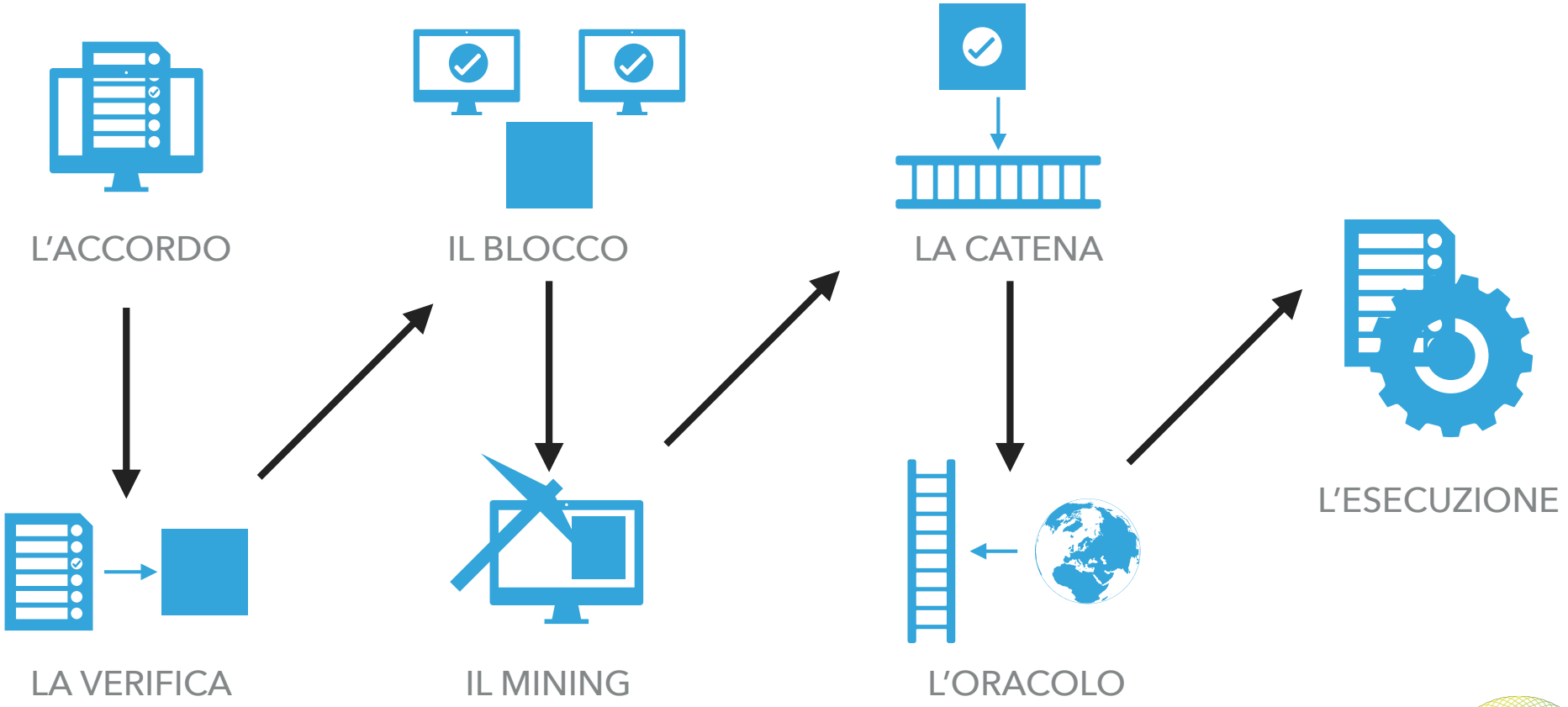
uport

MEDIA & ENTERAINEMENT

CryptoKitties

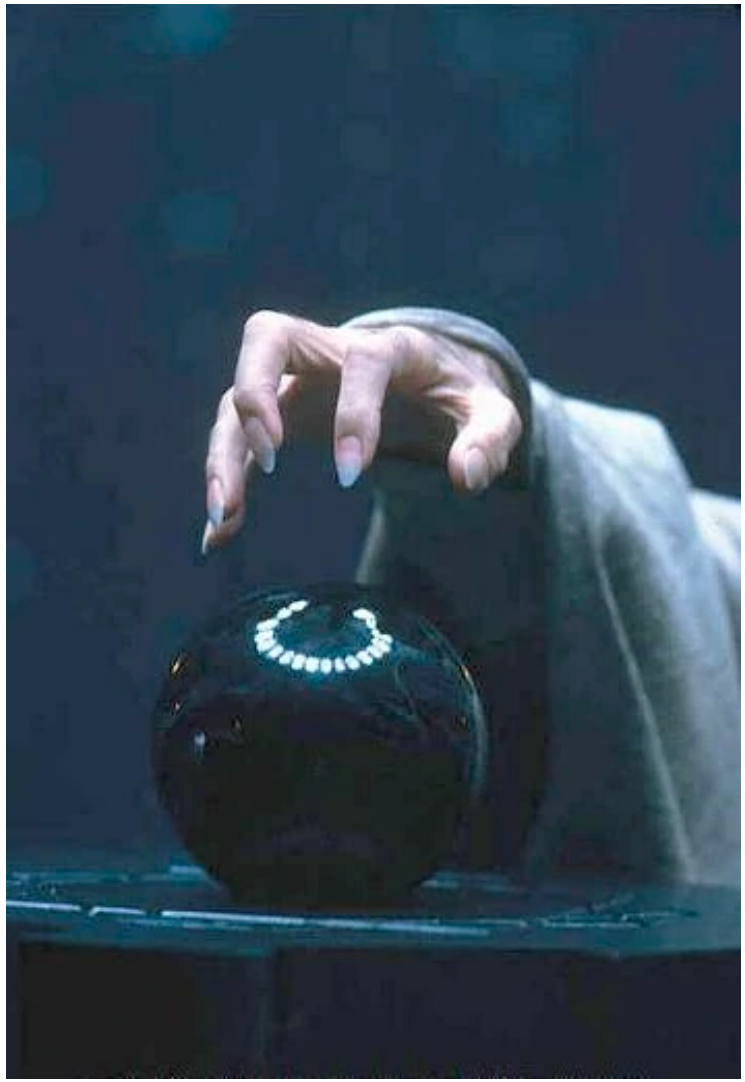
VITA DI UNO SMART CONTRACT (IN CAMPO ASSICURATIVO)

Etherisk



IL SALONE DEI PAGAMENTI PAYVOLUTION

ORACOLI



oraclize

Provable

COS'È UNO SMARTCONTRACT (LEGALMENTE)

Dl 135/2018 convertito dalla legge 12/2019

«Un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse».

SMARTCONTRACT: QUALI PROBLEMI? . . . BUGS

STIME IN ETHEREUM

- 34.200 potenzialmente vulnerabili
- 3,4% degli smart contract totali
- Coinvolgendo circa 4,905 Ether
- Per un valore maggiore di 803.000 €

THE DAO

THE DAO

- primo tentativo di creare un fondo di investimento decentralizzato creato dalla startup tedesca Slock.it.
  - lanciato in rete il 30 Aprile del 2016.
  - I fondi di partenza furono raccolti attraverso una ICO (Initial Coin Offering) per 28 giorni dopo il lancio ed successivamente i finanziamenti raggiunti, oltre $150m con più di 11.000 partecipanti, si sarebbero mossi verso tutte quelle start-up decentralizzate che avrebbero soddisfatto i criteri inscritti negli Smart Contract.
- esisteva però una clausola che era abbastanza arbitraria.
  - riuscì drenare verso di se milioni di ethers con un valore di circa 50 milioni di dollari.
- Il team di Vitalik decise che il protocollo di The Dao doveva essere cambiato, per evitare che ulteriori transazioni di quel tipo venisse eseguite.
  - Il primo hard fork in Ethereum, che genero la differenza tra Ether e Ether Classic.

IL SALONE DEI PAGAMENTI
PAYVOLUTION

GRAZIE PER L'ATTENZIONE

STEFANO BISTARELLI

cini Cybersecurity National Lab