

# ICO: TRA IL MITO, L'INGANNO E UNA REALTÀ IN CONTINUA EVOLUZIONE

a cura di  
Ing. D. Morea, Ing. M. Aceti



## Introduzione

Project Financing, Crowdfunding, Venture Capital, parole che provengono dal mondo anglosassone, che, da sempre, ha rappresentato il punto zero per il mondo dei capitali e dei mercati finanziari, in generale. Un mondo che, negli ultimi 50 anni, ha iniziato a sfruttare, in modo intensivo, la tecnologia come veicolo e strumento per la creazione e distribuzione di ricchezza.

Si è passati da aziende come General Electric, Ford, Coca Cola, ai prodotti finanziari come le obbligazioni strutturate o gli ETF (Exchange Traded Funds)<sup>1</sup>, per arrivare ai CDO (Collateralized Debt Obligation)<sup>2</sup>.

Parallelamente al suddetto mondo, basato sugli intermediari finanziari tradizionali e certamente sulla logica del profitto nonché della remunerazione degli stakeholder, negli ultimi venticinque anni, anche come risposta agli inevitabili eccessi e crisi finanziarie, alcune figure tecniche come Wei<sup>3</sup> Dai (b-money, 1998), Nick Szabo, Adam Back hanno iniziato a pen-

# ICO: TRA IL MITO, L'INGANNO E UNA REALTÀ IN CONTINUA EVOLUZIONE

a cura di  
Ing. D. Morea, Ing. M. Aceti



## Introduzione

Project Financing, Crowdfunding, Venture Capital, parole che provengono dal mondo anglosassone, che, da sempre, ha rappresentato il punto zero per il mondo dei capitali e dei mercati finanziari, in generale. Un mondo che, negli ultimi 50 anni, ha iniziato a sfruttare, in modo intensivo, la tecnologia come veicolo e strumento per la creazione e distribuzione di ricchezza.

Si è passati da aziende come General Electric, Ford, Coca Cola, ai prodotti finanziari come le obbligazioni strutturate o gli ETF (Exchange Traded Funds)<sup>1</sup>, per arrivare ai CDO (Collateralized Debt Obligation)<sup>2</sup>.

Parallelamente al suddetto mondo, basato sugli intermediari finanziari tradizionali e certamente sulla logica del profitto nonché della remunerazione degli stakeholder, negli ultimi venticinque anni, anche come risposta agli inevitabili eccessi e crisi finanziarie, alcune figure tecniche come Wei<sup>3</sup> Dai (b-money, 1998), Nick Szabo, Adam Back hanno iniziato a pen-



sare a un mondo diverso, basato sulla crittografia e sull'utilizzo di algoritmi per la creazione e distribuzione di moneta, obbligazioni contrattuali ed altro ancora.

I suddetti "nuovi concetti" rimasero puramente teorici fino a quando la sempre crescente diffusione delle infrastrutture tecnologiche, quali internet, gli smartphone, con potenze di calcolo e velocità sempre più

crescenti, hanno fornito le basi per i due eventi fondamentali.

Il primo afferisce alla nascita della prima criptovaluta, nel 2008, il ben noto bitcoin (la b minuscola indica la moneta, mentre con Bitcoin si indica l'infrastruttura tecnologica sulla quale avvengono gli scambi basata sulla Blockchain<sup>4</sup>).

In seguito, con un crescendo d'interesse costituito, inizialmente, di curiosità e leggende



**Dalle criptovalute,  
si è passati  
all'utilizzo degli  
smart contract,  
strumento per il  
finanziamento  
di start up  
tecnologiche ovvero  
di ICO (Initial Coin  
Offering)**



(una moneta per cyberpunk oppure i 10000 bitcoin per una pizza), si è passati, anche attraverso scandali e attività illegali (l'affare SilkRoad ed il furto di 850000 bitcoin dall'exchange MtGox), al secondo evento fondamentale, ovvero la nascita del protocollo Ethereum e della sua criptovaluta associata, l'Ether, per mano di Vitalik Buterin.

Nel protocollo Ethereum, che per scelta progettuale implementa una macchina di Turing completa (presenza dell'istruzione di Loop) ha trovato applicazione il concetto di Smart Contract, che può essere definito come la trasposizione, in formato elettronico, di un contratto che coinvolge parti, prestazioni, costi, modalità di esecuzione, ecc., eseguibile da qualsiasi entità abbia messo a disposizione in modo distribuito un sistema (o nodo) in grado di eseguire la così detta EVM (Ethereum Virtual Machine), sulla quale far eseguire il codice associato allo Smart Contract.

In tal modo, dalle criptovalute, intese, fino a quel giorno, come forma di pagamento alternativa, si è passati all'utilizzo degli smart contract, come strumento per il finanziamento di start up tecnologiche, le quali rispondono al nome di ICO (Initial Coin Offering).

### ICO: definizione, trend, utilizzi

Cos'è una ICO? Essenzialmente, si tratta di una forma di finanziamento indiretto, basata sullo scambio tra un bene in formato elettronico, denominato token, con altre criptovalute (per esempio, ether o bitcoin), secondo un rapporto di cambio predefinito.

Il token, a sua volta, è uno smart contract che può essere



Figura 1: Una parte di smart contract di un token emesso durante una ICO (fonte: Etherscan)

Smart contract: 479 lines of code

Source: Etherscan

Contract Source Code </>

```

456     {
457         return processContribution();
458     }
459
460     /**
461      * @dev handles contribution logic
462      * note that the contribution event is triggered using th se
463
464      * @return tokens issued in return
465      */
466     function processContribution() private
467         active
468         etherCapNotReached(msg.value)
469         validGasPrice
470         returns (uint256 amount)
471     {
472         uint256 tokenAmount = computerReturn(msg.value);
473         assert(beneficiary.send(msg.value)); // transfer the ether
474         totalEtherContributed = safeAdd(totalEtherContributed, msg
475         token.issue(msg.sender, tokenAmount); // issue new funds
476         token.issue(beneficiary, tokenAmount); // issue tokens to
477
478         Contribution(msg.sender, msg.value, tokenAmount);
479         return tokenAmount

```



eseguito o scambiato su piattaforme dedicate (o exchange) consentendo, al suo possessore, un eventuale guadagno (o perdita), in quanto, una volta scambiato in una criptovaluta di base, può essere ulteriormente convertito in valuta così detta fiat (\$, €) a corso legale (Figura 1). Riportiamo a titolo di esempio una parte di smart contract di un token emesso durante una IPO.

Grazie alla potenza del protocollo Ethereum e alla sempre crescente diffusione delle criptovalute, le ICO si sono moltiplicate fino a raggiungere il numero di 1552 (Figura 2).

A questo punto, è possibile definire due aspetti fondamentali: quello legato alle ICO come mezzo di finanziamento alternativo e l'aspetto speculativo, connesso all'andamento finanziario ovvero alla possibilità di

scambio per scopo di lucro.

Analizzando gli andamenti delle 1552 ICO dalla loro emissione ad oggi, è stato verificato quante di queste hanno avuto rendimenti positivi, con i seguenti risultati: su 1552 ICO, soltanto 187 hanno incrementato il loro valore, con una percentuale pari al 12%, con un rendimento medio delle sole ICO positive pari al 2621%, che spazia dall'1,88% al 166780%, con il 70% compreso entro il 500%.

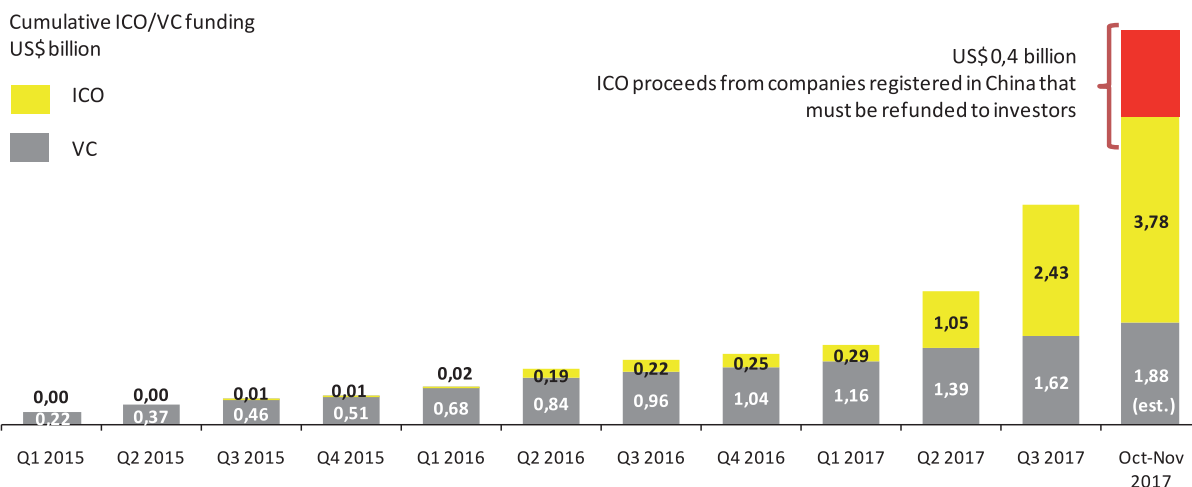
Numeri sicuramente importanti, che tuttavia nascondono i rischi legati alla componente operativa delle ICO, quali hacking, phishing, furti e, in tempi recenti, le richieste di verifica da parte delle autorità di controllo (finanziarie e fiscali in primis).

Le recenti decisioni della SEC (U.S. Security and Exchange Commission) hanno poi porta-

Figura 2 - Venture Capital vs ICO: crescita (in miliardi di \$), in termini di volumi scambiati, dal 2015 al 2017 (fonti: CoinDesk, CB Insights, IFCERT)

### ICO market

**Total ICO proceeds are approaching US\$4 billion and have exceeded venture capital investments in blockchain projects**



Date based on open sources - ICO market is not regulated, there is no standardized reporting and volatility is high (Sources: CoinDesk, CB Insights, IFCERT)



to ad un rallentamento, nel corso del 2018, delle ICO, vista la sempre maggior richiesta di chiarimenti e, con l'applicabilità del così detto Howey Test, molte società vi hanno rinunciato in attesa di maggior chiarezza.

Per mettere in guardia il pubblico statunitense, la SEC ha creato un sito fittizio (<https://www.howeycoins.com/index.html>) che pubblicizza una falsa ICO, nel quale sono riportati i principali meccanismi e schemi per indurre il pubblico alla così detta FoMO (Fears of Missing Out - paura di rimanere esclusi).

Tuttavia, non tutti gli stati sono pregiudizialmente contrari alle

ICO: la Svizzera attraverso la FINMA (Autorità Federale di Vigilanza sui Mercati Finanziari) ha recentemente emanato una raccomandazione che definisce in modo sistematico le tipologie di token che possono essere emesse.

L'interesse delle autorità di vigilanza si è manifestato a partire dagli innumerevoli casi di truffe legate alle ICO, anche di tipo diretto (per esempio, codici all'interno degli smart contract che davano facoltà agli emittenti di cambiare il numero di token emessi, distruggerli o cambiare la durata dell'ICO, non comunicato agli aderenti all'offerta in modo esplicito).



**Nel protocollo  
Ethereum,  
che implementa una  
macchina di Turing  
completa ha trovato  
applicazione il  
concetto di  
Smart Contract**

#### RIFERIMENTI BIBLIOGRAFICI

- Campisi, D., Costa, R., Mancuso, P., Morea, D. (2014), *Principi di Economia Applicata all'Ingegneria - Metodi, Complementi ed Esercizi*, Hoepli.
- Campisi, D., Costa, R. (2008), *Economia Applicata all'Ingegneria - Analisi degli Investimenti e Project Financing*, Carocci.
- Chen, Y. (2018), "Blockchain tokens and potential democratization of entrepreneurship and innovation", *Business Horizon*, in press.
- Morea, D., Jacobone, F. (2017), *Project Financing: elementi di base, profili professionali e modelli innovativi*, Maggioli Editore.
- Morea, D. (2017), *Elementi di Legislazione Tecnica*, Maggioli Editore.

#### NOTE

- <sup>1</sup> Fondi d'investimento ad indicizzazione passiva, che replicano in modo sistematico un indice di riferimento.
- <sup>2</sup> Obbligazione che ha come garanzia (o collaterale) un altro debito, alla base del crollo dei mutui subprime del 2007.
- <sup>3</sup> Wei è la più piccola unità di misura utilizzata nel mondo Ethereum.
- <sup>4</sup> Registro di transazioni in forma distribuita (DLT), sul quale è possibile scrivere ma non cancellare dati.