

BLOCKCHAIN E IMPRESA

Firenze, 28 marzo 2018

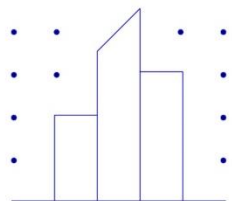
Enrico Corradini
Gianluca Zanini

*Tecnologie e
persone per*
**ASCOLTARE
INNOVARE
FARE**

inspiring innovation

VARGROUP

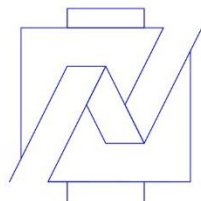
Numeri che **trasferiscono valore**



fatturato

240Mln

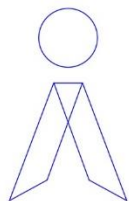
al 30.04.2017



crescita

+6,4

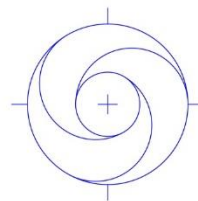
2017/ 2016



collaboratori

1600

2017



breakdown

business technology solutions

47%

managed & security services

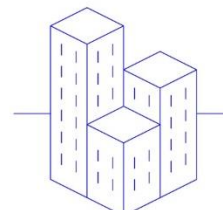
18%

business & industry solutions

30%

digital transformation

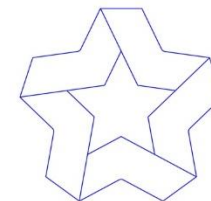
5%



sedi

23

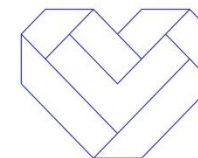
italia



competenze

796

certificazioni



esperienza

44

anni



VAR GROUP & SESA

Var Group è una società controllata al 100% dal Gruppo SeSa, leader in Italia nella distribuzione di soluzioni IT a valore per le imprese, dal 2013 presente sul Mercato Telematico Azionario di Borsa Italiana con una capitalizzazione di circa 250 Mln €.

Mln € di ricavi

1271,5

ricavi consolidati
al 30.04.2017
rispetto al 2016

+3,4

Mln € di utile netto

27,1

Certificazioni che garantiscono la competenza dei nostri consulenti.



Collaborazioni **Eccellenti**

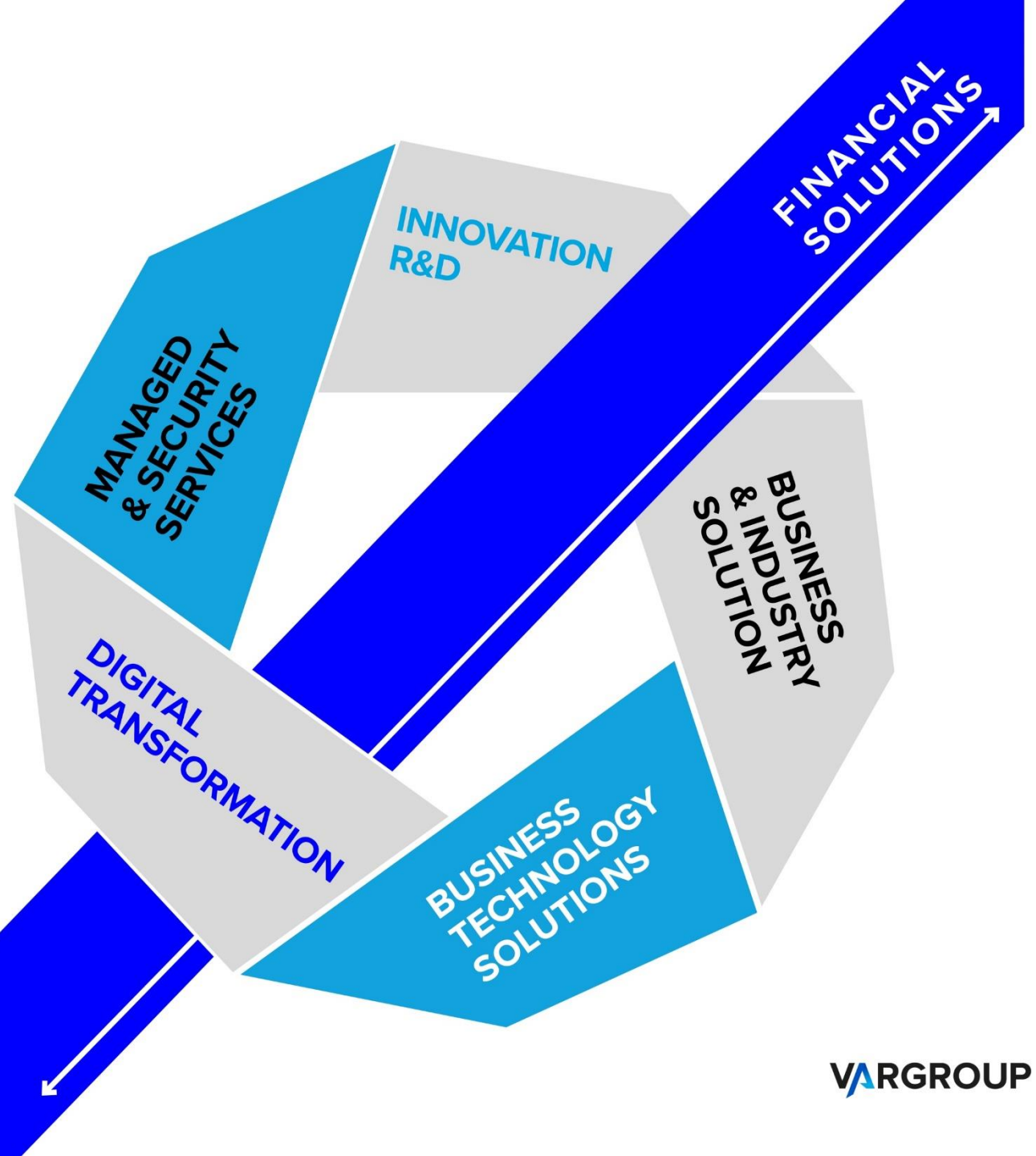
Var Group collabora costantemente con i più importanti brand del mondo ICT internazionale.

La stretta relazione con ognuno di questi permette di modellare soluzioni tecnologicamente evolute e subito pronte per sostenere la competitività.

// **IBM**
// **MICROSOFT**
// **CISCO**
// **HEWLETT PACKARD ENTERPRISE**
// **SAP**
// **DELL EMC**
// **HP**
// **LENOVO**
// **ORACLE**
// **APPLE**

Soluzioni **Competenze** *Persone*

L'offerta Var Group trae la sua forza dall'integrazione del lavoro di Business Unit focalizzate su aree specifiche del mercato IT.



Servizi e soluzioni all'avanguardia per la sicurezza a 360 gradi delle aziende, grazie a esperienza pluriennale, personale certificato, utilizzo delle migliori tecnologie. La **Cyber Division di Var Group rappresenta l'unico centro privato in Italia ammesso al FIRST** - la rete di protezione globale per contrastare minacce emergenti e promuovere un ambiente globale più sicuro - assieme a player come Nasa, Apple e Google.



SOC

Per il monitoraggio H24x7x365 e la sicurezza delle reti aziendali.



Sala forense

Per indagini su crimini e incidenti informatici e il recupero di documenti eliminati.



Training

Per formare figure esperte in indagini digitali e per un'efficace security awareness in azienda.



R&D

Laboratorio a Tel Aviv per lo sviluppo di sistemi di sicurezza all'avanguardia.

Servizi e soluzioni all'avanguardia per la sicurezza a 360 gradi delle aziende, grazie a esperienza pluriennale, personale certificato, utilizzo delle migliori tecnologie.

La **Cyber Division di Var Group** rappresenta l'unico centro privato in Italia ammesso al **FIRST** - la rete di protezione globale per contrastare minacce emergenti e promuovere un ambiente globale più sicuro - assieme a player come Nasa, Apple e Google.

Cybersecurity

Security

- ✓ SOC - Security Operation Center
- ✓ Security Assessment (PT, VA, Wi-Fi, Social Engineering)

Digital Forensic

- ✓ Digital Forensic Analysis
- ✓ Malware Analysis
- ✓ Data Recovery

Cyber Intelligence

D3Lab offre servizi di Anti-Phishing e Cyber Intelligence integrando i servizi di Cyber-Security di Yarix.

- ✓ Anti-Phishing
- ✓ Brand Monitor
- ✓ Early Warning
- ✓ Recupero Carte di Credito

Training

Per formare esperti in indagini digitali e per un'efficace Security Awareness in azienda.

- ✓ Pillole Security (con Giunti O.S. Psychometrics per erogare formazione tramite Moodle)
- ✓ Analisi Forense (certificazione X-Ways)
- ✓ Security Awareness

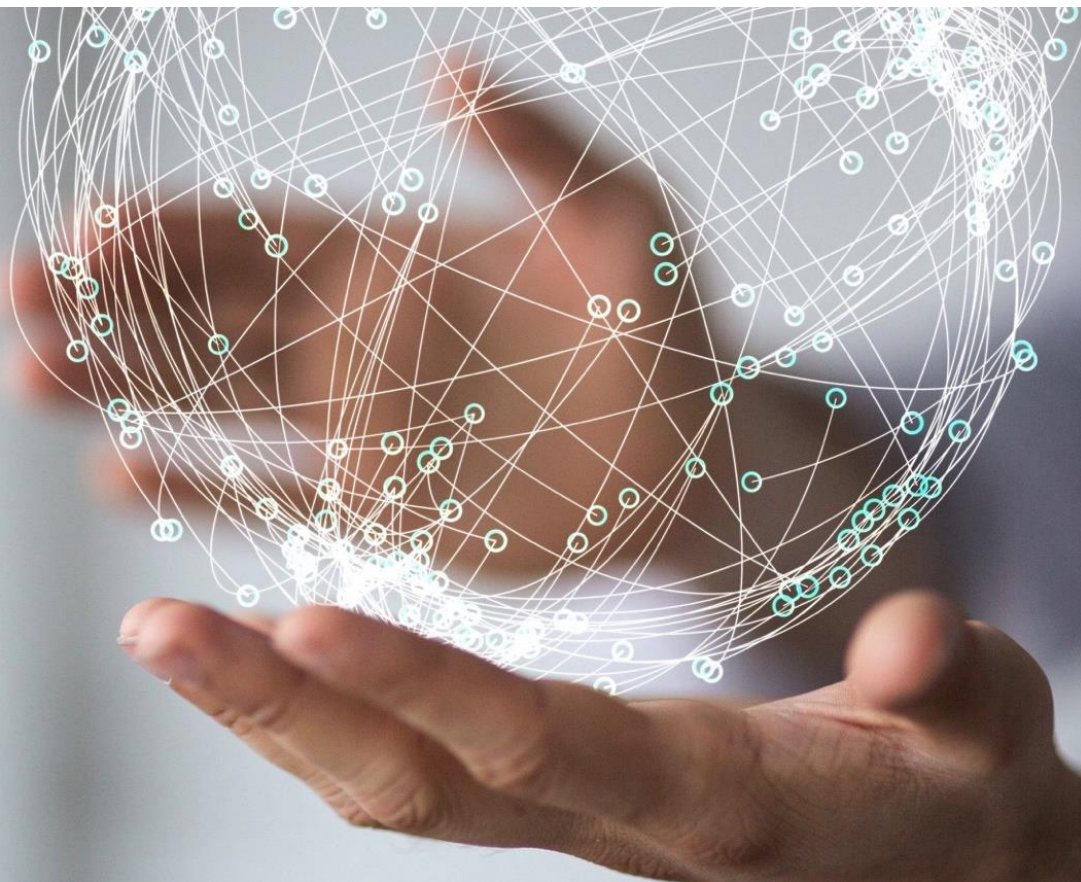
Privatamente e **Block IT**, partecipate da Var Group e la sua Cyber Division Yarix, costituiscono team specializzati in servizi di consulenza professionale in ambito **Privacy, GDPR, PCI-DSS e Servizi Blockchain** a completamento della Data Protection.

Legal Compliance

- ✓ Privacy (DLG 196/2003)
- ✓ GDPR (General Data Protection Regulation - Regolamento UE 2016/679)
- ✓ Compliance ISO 27001
- ✓ PCI-DSS (Standard per la sicurezza delle transazioni con carta di credito)

Blockchain

- ✓ Soluzioni Blockchain (tecnologia all'avanguardia nel mondo dei pagamenti digitali, ad esempio, alla base dello scambio di molte crypto-valute)



BLOCKCHAIN

Implicazioni di Cybersecurity

Cybersecurity e Blockchain

Il vero grande terreno di innovazione delle Blockchain è rappresentato dalla necessità delle aziende tradizionali di trovare **un nuovo modello per gestire in modo più sicuro, affidabile e veloce le operazioni** (o transazioni) **e le relazioni tra gli attori delle filiere.**

L'identity management nelle soluzioni IoT, per esempio, necessita in maniera sempre più forte di appoggiarsi a strutture informatiche in grado di garantire l'identità di ciascun apparato coinvolto.

Quanto un dato registrato su Blockchain è sicuro?

Cosa una Blockchain può garantire in termini di sicurezza?

1

Un dato o una transazione, una volta scritto su un blocco di una Blockchain, è immutabile.

Una volta confermato dalla “rete”, ovvero, dai partecipanti alla validazione dei blocchi (i nodi della B.C.), nessuno lo può più modificare.

2

L'immutabilità di un dato su una Blockchain è considerata certa per l'enorme **difficoltà**, per l'enorme **dispendio di risorse informatiche e tempo** che servirebbe ad un malintenzionato per invalidare un numero elevato di nodi della catena.

3

Inoltre, per poter sostituire un valore in un blocco, oltre ad invalidare buona parte della rete della Blockchain, il malintenzionato dovrebbe avere una potenza elaborativa tale da poter creare nuovi blocchi prima che la rete stessa ne crei altri.

I dati di una Blockchain sono sicuri poichè “il gioco non vale la candela”:

- ✓ **Una Blockchain è di per sé inattaccabile** principalmente per il principio che lo sforzo e l’investimento (anche economico) necessario ad hackerare anche un solo blocco di dati è pressoché insostenibile.
- ✓ **Per capire dove una Blockchain** (o meglio i dati e le transazioni in essa registrati) **può essere attaccata e risultare vulnerabile** è necessario prima di tutto analizzare le componenti che formano l’ecosistema delle Blockchain stesse.

Un progetto basato su Blockchain vede principalmente quattro macro elementi che interagiscono tra loro:

1 - PEER

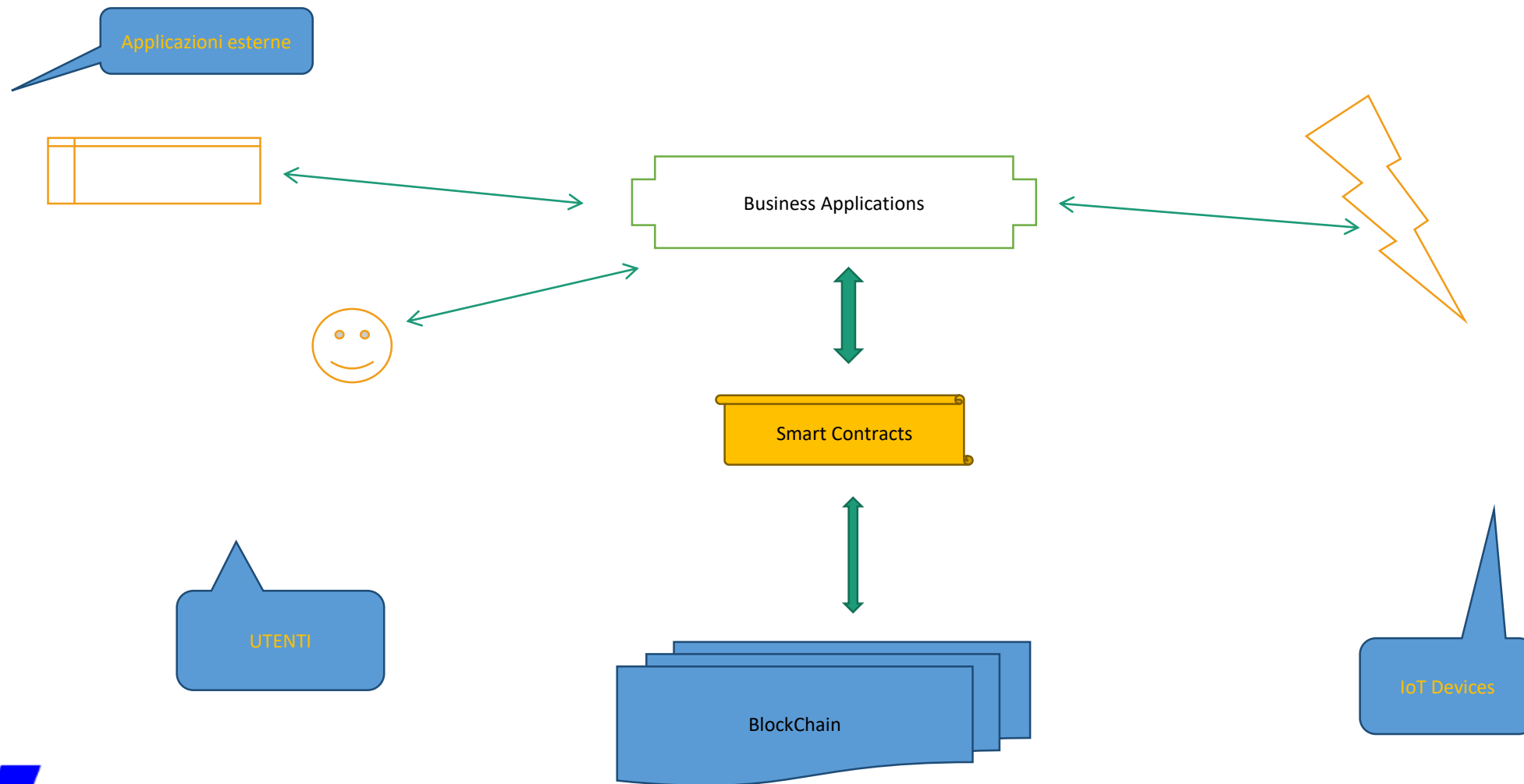
(utenti, applicazioni esterne che eseguono accessi alla Blockchain per fornire dati, eseguire transazioni o ricevere dati, IoT Devices, etc.)

2 - BUSINESS APPLICATIONS

(Web Application di Front-End, Back-End Application, Mobile Application etc. che colloquiano con la Blockchain tramite le API di comunicazione con gli Smart Contracts)

3 - SMART CONTRACTS

4 - LA BLOCKCHAIN



1 - Peer

- ✓ **Gli utenti, le applicazioni esterne e i device IoT sono passibili di attacchi informatici**, malware e furti delle chiavi private
- ✓ **La possibilità di imbattersi** in uno di questi problemi è direttamente proporzionale al servizio che i peer utilizzano
- ✓ **Statisticamente** è più probabile su servizi legati alle transazioni relative alle criptovalute

2 - Business Application

Le Business Application sono un punto molto delicato e hanno bisogno di essere sicure dal punto di vista:

- ✓ **infrastrutturale** (apparati di rete, Firewall, Firewall applicativi, IDS, IPS, Hardening dei servizi Web e degli Application Server etc.)
- ✓ **applicativo** (Codice privo di bug quali XSS, SQL o Command Injection, Session replication etc.)

3 - Smart Contracts

- ✓ Grande potenza delle Blockchain dopo l'immutabilità dei dati che, se non gestiti opportunamente, possono diventare il vero e proprio "tallone di Achille" di tutto l'ecosistema.
- ✓ Gestiscono in modo inconfutabile e preciso, tutte le regole che i PEER devono seguire, tutte le "leggi" e tutte le possibilità che un PEER ha di accedere ai dati in una Blockchain.
- ✓ Sono dei veri e propri contratti scritti tramite linguaggi di programmazione da parte di tecnici informatici e a prova di errore, ovvero in termini "umani", non devono poter essere interpretabili (per poter garantire tutta la filiera delle informazioni che vengono gestite dalla Blockchain).

1 - Peer
2 - Business Application



Vedono come contromisure le analisi di sicurezza passive ed attive di qualunque sistema critico (Penetration Test, Vulnerability Assessment infrastrutturali ed applicativi periodici, bug fixing dei sistemi e del codice, SOC, etc.).

3 - Smart Contracts



È necessario avere competenze di sicurezza e legali assolutamente specifiche sulle tecnologie legate alle Blockchain che diano la garanzia di una corretta trasposizione di un contratto legale vero e proprio nel suo equivalente software.

Sono tanti gli esempi di Smart Contracts scritti male dal punto di vista tecnico che hanno portato progetti promettenti a fallire miseramente. Per citarne alcuni:

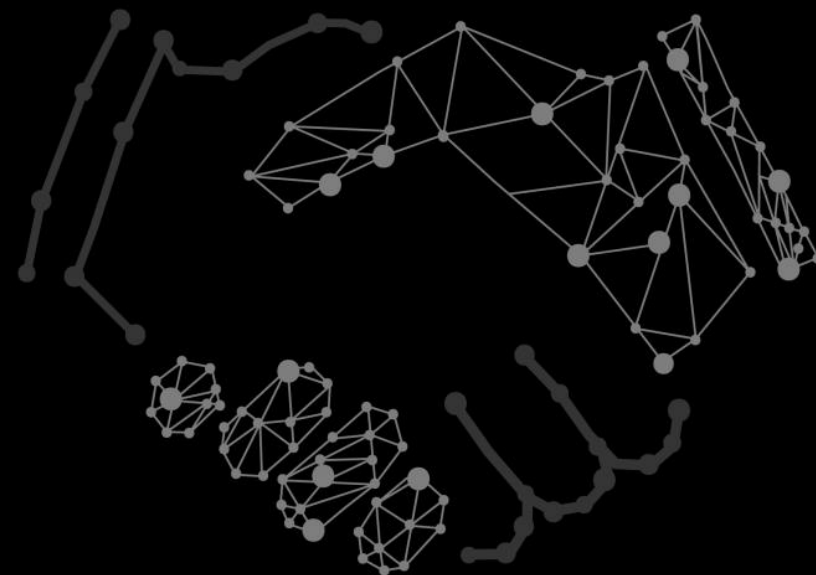
THE “PAYOUT INDEX WITHOUT THE UNDERSCORE” [PONZI](#) (“FIREPONZI”)

Per una dichiarazione errata di una variabile ha permesso di aggirare le clausole contrattuali, permettendo l’accreditamento fraudolento di 1000 Ethereum (poco meno di mezzo milione di Euro).

“GOVERNMENTAL'S 1100 ETH JACKPOT PAYOUT IS STUCK BECAUSE IT USES TOO MUCH GAS”

Ha permesso di frodare ben 1100 Ethereum (poco più di mezzo milione di Euro) al portafoglio del gestore del servizio a causa di una dichiarazione errata dei tempi di gestione delle cancellazioni dei movimenti già confermati.

E gli esempi possono continuare, il tutto perché non sono state gestiti correttamente i controlli di sicurezza legati al codice degli Smart Contracts.



4 - Blockchain

Una Blockchain è di per sé sicura, ma è importante, in un progetto saper scegliere il tipo di Blockchain da utilizzare:

- ✓ **Blockchain pubblica** (come per esempio BitCoin o Ethereum).
In questo tipo di Blockchain tutti i partecipanti alla rete possono vedere il registro e i dati in esso contenuti. Non esiste quindi la possibilità di gestire permessi e modalità di accesso restrittive.
- ✓ **Blockchain privata** (come Hyperledger prodotta dalla Linux Foundation e adottata in Hyperledger Fabric di IBM).
Si tratta di una Blockchain Permissioned, dove è possibile gestire profili e Access Control List.

In base alla tipologia di informazioni che si vogliono gestire nella Blockchain e ai target del progetto, la scelta migliore, per diminuire la superficie di rischio è quella legata alle Blockchain private. Una ulteriore scelta è quella di utilizzare nodi segregati all'interno di un cloud autenticato, come BlueMix di IBM.



A graphic illustration of a blockchain network. It features a central, glowing blue cube-like structure composed of interconnected lines and nodes, resembling a complex geometric or molecular model. The word "BLOCKCHAIN" is written in a bold, blue, sans-serif font across the center of this structure. The background is dark, with faint, glowing blue lines extending outwards from the central structure, suggesting a global or distributed network.

BLOCKCHAIN

Insieme a Yarix, Cyber Division Var Group e leader nel mondo della Cyber Security, **abbiamo sviluppato la nuova strategia che unisce sicurezza perimetrale, preventiva, applicativa e Blockchain Compliant**, creando così un'offerta globale per garantire la sicurezza dei progetti basati su Blockchain, introducendo le regole di controllo SMACIAS ^(tm) (SMArt Contract Is A Software) da noi create in base alle molteplici esperienze sui controlli di sicurezza eseguiti sugli Smart Contracts.

GRAZIE!



www.vargroup.it

DISCLAIMER COPYRIGHT 2017 VAR GROUP S.p.A. Questo documento è redatto a scopo puramente informativo e non costituisce alcun elemento contrattuale con Var Group S.p.A. Esso contiene solo strategie, sviluppi e funzionalità delle soluzioni commercializzate dal Gruppo e non fornisce alcuna garanzia implicita o esplicita di alcun tipo. Tutti i marchi appartengono ai rispettivi proprietari. Nessuna parte di questa pubblicazione può essere riprodotta o trasmessa in qualsiasi forma o per qualsiasi scopo senza la preventiva autorizzazione di Var Group S.p.A.

