UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

"Bitcoin, Blockchain and their new frontiers"
12, 13 Maggio 2016 - Trento

Docenti: Prof. Massimiliano Sala, Prof. Antonino Alì, Prof. Jack Birner

Assistenti: Dr. PHD A. Tomasi, Dr. PHD F. Pintore, Dr. PHD M. Calderini, Dr. PHD M. Piva

Day 1

10.30 - 10.50 - Chunk 1: Introduzione e richiami sulle primitive crittografiche:
chiave privata e pubblica, funzioni hash, firma digitale.

10.50 - 11.10 - Chunk 2: **Prof. Massimiliano Sala**
Introduzione alle valute e crittovalute.
I vantaggi della decentralizzazione.

11.10 - 11.30 - Chunk 3: **Prof. Massimiliano Sala**
Introduzione al Bitcoin, con statistiche, e ai relativi Wallet.

11.30 - 11.50 - Pausa

11.50 - 12.10 - Chunk 4: **Prof. Massimiliano Sala**
Le transazioni Bitcoin ed un'introduzione allo script Bitcoin.

12.10 - 12.30 - Chunk 5: La tecnologia fondante della Blockchain.
Confermare e validare le transazioni.
Il Mining e le possibili proof-of-work.

12:30 - 14:00 - Pranzo

14.00 - 14.20 - Chunk 6: Approfondimento sullo script Bitcoin e la sua sintassi.

14.20 - 14.40 - Chunk 7: Funzionalità evolute dello Script:
pay-to-hash script, multisignature e proof-of-burn.

14.40 - 15.00 - Chunk 8: **Prof. Massimiliano Sala**
Problematiche generali di sicurezza del Bitcoin:
double spending, soft fork e hard fork.

15.00 - 15.20 - Pausa

15.20 - 15.40 - Chunk 9: La gestione delle credenziali e chiavi nei Wallet.
Cold wallet vs. hot wallet.
Gli indirizzi Bitcoin all'interno dei Wallet.

15.40 - 16.00 - Chunk 10: L'intermediazione di denaro nella rete Bitcoin:
I Bitcoin-Exchange e i Payment Processors.

16.20 -16.20 Pausa

16.20 - 16.40 - Chunk 11: Dettagli sul mining:
Mining pool e Bitcoin farm.
Client alternativi.

16.40 - 17.00 - Chunk 12: Attacchi al protocollo Bitcoin:
51% attack, il problema dei Generali Bizantini.

Cena sociale presso Agritur Ponte Alto
La partecipazione alla cena è importante in quanto momento privilegiato per discutere informalmente del fenomeno Bitcoin e della tecnologia Blockchain.

Day 2

AULA 1 - PERCORSO TECNICO

9.00 - 9.20 - Chunk 13: Protocollo di firma DSA su gruppi abeliani e su campi finiti.

9.20 - 9.40 - Chunk 14: Un'introduzione alle curve ellittiche per l'uso crittografico.
La curva *bitcoin curve.*

9.40 - 10.00 - Chunk 15: Protocollo di firma ECDSA, basato su curve ellittiche.
Il suo utilizzo nel sistema Bitcoin.

10.00 - 10.20 Pausa

10.20 - 10.40 - Chunk 16: Approfondimento sulle funzioni hash.
Proprietà crittografiche delle funzioni hash.
Le funzioni hash standardizzate e le loro caratteristiche.

10.40 - 11.00 - Chunk 17: *Hash pointer*, *Merkle tree* e loro utilizzo nel sistema Bitcoin.

11.00 -11.20 Pausa

11.20 - 11.40 - Chunk 18: Crittovalute alternative.
LiteCoin, Ripple e varianti.

11.40 - 12.00 - Chunk 19: Crittovalute con elevato livello di anonimicità:
il caso di Monero e le sue varianti.

AULA 2 - PERCORSO GENERALE

9.00 - 9.40 - Prof. Jack Birner: Trust in cryptocurrencies?

9:40 - 10:20 - Prof. Jack Birner: Sociological aspect of the cryptocurrencies

10:20 - 10:40 Pausa

10:40 - 11:10 - Chunk 20: Come contrastare la pseudo-anonimicità nel sistema Bitcoin.

11.10 - 12.00 - Prof. Antonino Ali: Breve excursus legislativo su Bitcoin e cryptocurrency a livello internazionale

12:00 - 13:00 - Pranzo

13.00 - 13.20 - Chunk 21: Un'applicazione avanzata della BlockChain: Factom.

13.20 - 13.40 - Chunk 22: La blockchain e gli smart contract.

13.40 - 14.00 - Chunk 23: Un'evoluzione dell'e-voting con la blockchain.

14.00 - 14.20 - Pausa

14.20 - 14.40 - Chunk 24: Il cloud decentralizzato usando la Blockchain.

14.40 - 15.00 - **Chunk 25:** Synereo: un social network distribuito.