"P2P Systems and Blockchains"
Laurea Magistrale in Informatica
Informatica e Networking

13/12/2016

Laura Ricci

"P2P SYSTEMS AND BLOCKCHAINS"

- Prossimo ordinamento della magistrale (se approvato), prevederà 4 curriculum
  - Software: Programming, Principles, and Technologies
  - ICT Solutions Architect
  - Data and Knowledge: Science and Technologies
  - Artificial Intelligence

- "P2P Systems and Blockchains" obbligatorio del curriculum "ICT Solution Architect", ma può essere inserito, sfruttando i crediti liberi, in qualsiasi altro curriculum

- già da quest'anno ampio spazio per la tecnologia distribuita delle blockchains

IL CORSO "P2P SYSTEMS" NEGLI ULTIMI 10 ANNI

P2P file sharing

- file sharing: light weight/ best effort
- persistence and security are not the main goal
- anonymicity is important
  - Napster
  - Gnutella, KaZaa
  - eMule
  - BitTorrent
- Distributed Index: Distributed Hash Tables

P2P Content Publishing e Storage Systems

- persistency and security are main goals
  - Freenet

P2p network	Popular Applications
Ares	Ares Galaxy [12]
BitTorrent	BitTorrent [8], uTorrent [9], Vuze [10], BitTornado [11]
DirectConnect	DC++ [13]
eDonkey2000[1]	eDonkey2000 [14], eMule [15]
FastTrack	KaZaa [16], Kazaa Lite [17]
Gnutella	LimeWire [18], Shareaza [19]
Gnutella2 (G2)	Morpheus [20], Gnucleus [21], Shareaza [19]
Kad Network	aMule [22], eMule [15], MLDonkey [23]
OpenNap	Napster [7]
WPNP	WinMX [24]

P2p application	Brief Description
Freehaven [25]	A system for distributed, anonymous, persistent data storage which is robust against attempts by powerful adversaries to find and destroy any stored data [25].
Freenet [26]	A system which lets you publish and obtain information on the Internet without fear of censorship [26].
Groove [27]	A collaboration software program that helps teams work together dynamically and effectively [27].
Mnet [28]	A shared virtual space onto which you can put, and from which you can retrieve, files. (created from the source code of MojoNation [32]) [28].
OceanStore [29]	An architecture for global scale persistent storage. Scalable, provides security and access control [29].

IL CORSO "P2P SYSTEMS" NEGLI ULTIMI 10 ANNI

- **Voice over P2P**
  - P2PSIP working group
    - definition of a P2P protocol considering NATs
    - minimum involvement of the centralized server
    - exploits Distributed Hash Tables
  - VoP2P: Skype

- **IPTV**
  - video streaming applications
  - PPlive, Ppstream, widely spread in Cina
  - Joost, Soapcast

- **Live audio streaming**: Spotify

- **P2P Dark Web**
  - TOR anonymous network

IL NUOVO CORSO "P2P SYSTEMS AND BLOCKCHAINS"

- **Bitcoin Digital Currency:**
  - cryptocurrency: scambi di valuta diretti
  - non richiede una entità finanziaria centralizzata: costi inferiori
  - transazioni Bitcoin registrate in una blockchain
  - utilizza una rete P2P

- **Blockchains:**
  - una lista di transazioni aggiornata continuamente
  - distributed ledger (libro contabile): un data base si dati replicati, condivisi e sincronizzati memorizzati su nodi geograficamente distribuiti, che memorizzano tutte le tranzazioni avvenute
  - integrità garantita da tecniche crittografiche, che garantiscono che la probabilità di "rompe l'integrità" sia molto bassa.
  - verifica della validità della transazione mediante algoritmi di consenso distribuiti (per Bitcoin il Nakamoto Consensus)

IL NUOVO CORSO "P2P SYSTEMS AND BLOCKCHAINS"

Blockchain (Deloitte Report)

- tagliare il "cordone ombelicale" che lega blockchains e Bitcoin per sfruttarne le caratteristiche in ambiti diversi

- può avere un impatto rivoluzionario in diversi settori: boom di investimenti nell'ultimo trimestre 2015
  - non solo banche, ma anche aziende come Microsoft, IBM, Samsung e Philips

IL NUOVO CORSO "P2P SYSTEMS AND BLOCKCHAINS"

Vantaggi delle blockchain:

- decentralizzazione, replicazione: se uno dei nodi è danneggiato, gli altri continuano a operare saldando la catena, senza perdere alcuna informazione.

- trasparenza: Le transazioni sono visibili a tutti i partecipanti.

- affidabilità: Le informazioni della blockchain non possono essere manipolate. Più attendibilità e meno possibilità di frode. Grande forza di questa caratteristica in ambito contrattuale.

- irrevocabilià: è possibile effettuare transazioni irrevocabili, in modo da rendere la loro traccia più accurata.

IL NUOVO CORSO "P2P SYSTEMS AND BLOCKCHAINS"

Possibili campi di applicazione

- Finanza (banche, intermediari,. gestori,..): transazioni più immediate, più economiche e più sicure. Risparmio in commissioni bancarie (potrebbe toccare i 15-20 miliardi di dollari entro il 2022)
- Media e diritti d'autore: solidità e l'immutabilità della blockchain consentirebbe, di accertare in modo sicuro e attendibile la proprietà intellettuale di musica e immagini.
- Retail: piattaforma di pagamenti alternativa a contanti, carte di credito e di debito per il mercato retail. Ma non solo: anche scambio di contratti in sicurezza, ad esempio acquisto di un'auto eregistrazione passaggio di prorietà.
- IoT: supporto al collegamento collegare molti dispositivi in aree diverse del globo.

"P2P SYSTEMS AND BLOCKCHAINS"

- Lo sviluppo di sistemi secondo la tecnologia P2P è una vera e propria sfida
- Le metodologie classiche proposte per lo sviluppo di sistemi distribuiti di "vecchia generazione" non sono più valide:
  - l'ordine di grandezz di un sistema P2P è diverso rispetto a quello dei sistemi distribuiti classici (milioni di nodi rispetto a centinaio di nodi)
    - algoritmi classici/tecniche classiche "non scalano" su reti di questa dimensione.
  - il fallimento di uno dei nodi non costituisce un evento raro, piuttosto è un evento normale

- Sistemi di queste dimensioni e di questo livello di dinamicità richiedono lo sviluppo di nuovi strumenti/metodologie
  - **algoritmi probabilistici**
  - **analisi statistica di reti complesse**
  - **game theory**: strategia per la cooperazione tra I peer
  - Sviluppo di nuovi modelli computazionale.

"P2P SYSTEMS AND BLOCKCHAINS"

Un pò di slogan per definire la "missione del corso"

- integrazione tra teoria e pratica
- concetti teorici implementati in applicazioni reali
- ad esempio:
  - studio di algoritmi efficienti di routing per `Distributed Hash Tables`
  - teoria del consenso in sistemi distribuiti per blockchains
  - teoria della complex networks