POLIMI Fintech Journey

From Blockchain&Bitcoin to Distributed Ledger Technologies, Smart Contracts and Cryptocurrencies in Finance

Politecnico di Milano

Dipartimento di Matematica

May 9, 2018

IT TUTORIAL

9.00 am - 2.00 pm - Information Technology for DLTs

Daniele Marazzina (Politecnico di Milano), Francesco Bruschi (Politecnico di Milano), Stefano Leone (Deloitte Consulting)

Introduction (Daniele Marazzina)

- DLT and Blockchain
- Mining and blockchain immutability
- Public and Private Blockchains
- Two well-known examples: Bitcoin and Ethereum
- Pseudonymization and cryptography: public and private keys with a view to Distributed Ledger
- Notarization and Hashing

Smart Contracts (Francesco Bruschi)

- What a Smart contract is
- Smart contracts and blockchains: distributed execution and main properties
- Programming languages for writing smart contracts: solidity
- Hello World: how to define a new cryptocurrency
- Problems and perspectives

ICOs vs Kryptokitty (Stefano Leone)

- Fungible and not fungible assets on blockchain (ERC20 vs ERC 721)
- Ethereum scalability issues.

CONFERENCE

2.45 pm - 6.30 pm - Session 1. DLT and Smart Contracts

- Andrea Bracciali (Università di Stirling)

Decentralised governance?

- Massimo Bartoletti (Università di Cagliari)

Models for Bitcoin smart contracts

Albeit the primary usage of Bitcoin is to exchange currency, its blockchain and consensus mechanism can also be exploited to securely execute some forms of smart contracts. These are agreements among mutually distrusting parties, which can be automatically enforced without resorting to a trusted intermediary. However, the existing informal, low-level descriptions, and the use of poorly documented Bitcoin features, pose obstacles to the research in this field. We present a formal model of Bitcoin transactions, which is sufficiently abstract to enable formal reasoning, for instance proving well-formedness properties of the Bitcoin blockchain like the absence of double-spending. We then show how to use our model as a concrete layer upon which designing higher-level specification languages for smart contracts.

- Andrea Visconti (Università degli Studi di Milano)

On the cryptography of DLT

- Stefano Bistarelli (Università di Perugia)

An End-to-end Voting-system Based on DLTs

In this work we re-adapt the Bitcoin e-payment system and propose it as a decentralised end-to-end voting platform (from voters to candidates). We describe the main architectural choices behind the implementation, which consists of the pre-voting, voting, and post-voting phases. The resulting implementation is completely decentralised: it is possible to directly cast a vote in the block-chain without any collecting intermediate-level. All the votes can be verified by anyone reading such a public ledger. We also exploit digital asset coins to directly keep track of votes (through the Open Asset Protocol), and we show the election cost for n voters.

- Claudio Impenna (Bank of Italy)

DLT applications in the financial sector: the regulator's perspective

May 10, 2018

9.30 am - 1.00 pm - Session 2. The economics and the Finance of DLT/smart contracts

- Davide Grossi (University of Groningen)

Incentive Structures behind Consensus in Distributed Ledgers

The talk explores the nexus between Distributed Ledgers Technology and Game Theory. It highlights, through a series of examples, the incentive structures underpinning the correct functioning of consensus protocols for distributed ledgers (e.g., Bitcoin's Nakamoto consensus, Stellar's federated voting), and the sort of game-theoretic foundations such protocols need to rely upon.

- Francesco Bruschi (Politecnico di Milano)

Stretching our oracles farther: making smart contract aware of the world

- Simon Trinborn (Humboldt University)

Investing with Cryptocurrencies - A liquidity constrained investment approach

- Gianna Figà Talamanca (Università di Perugia)

Attention-based dynamics for BitCoin price modeling and applications

We present recent developments about Bitcoin price modeling and related applications. Precisely, we show that market attention, measured either by trading volume or by the volume of Google searches on the topic, affects both the return and the volatility of BitCoin price when the dynamics is described by a discrete time model within the ARMA-GARCH family. Motivated by our findings, we then introduce a continuous time model in order to derive a pricing formula for European style derivatives on Bitcoin. The proposed model is also fitted to historical data of Bitcoin prices and model option prices are computed for some test dates and compared with market prices provided on the trading platform www.deribit.com; the valuation formula we provide does a good job in pricing traded options and outperforms the Black and Scholes price taken as benchmark.

- Giancarlo Giudici (Politecnico di Milano)

The ICO market

In 2017 Initial Coin Offerings (ICOs) allowed startup projects around the world to raise more than $5.3 billion, according to market observers. We analyze the characteristics of these token offerings and the determinants of the fundraising success.

Lunch

2.00 pm Organizing meeting

2.45 pm - 6.15 pm – Session 3. Applications of DLT and smart contracts in finance

- Ferdinando Ametrano (Banca IMI)

Central bank digital cash and private monies

- Giovanni Sartor (Università di Bologna)

On Legal contracts, Imperative and Declarative Smart Contracts and Blockchain Systems

This paper provides an analysis of how concepts pertinent to legal contracts can influence certain aspects of their digital implementation through smart contracts, as inspired by recent developments in distributed ledger technology. We discuss how properties of imperative and declarative languages including the underlying architectures to support contract management and lifecycle apply to various aspects of legal contracts. We then address these properties in the context of several blockchain architectures. While imperative languages are commonly used to implement smart contracts, we find that declarative languages provide more natural ways to deal with certain aspects of legal contracts and their automated management.

- Massimo Morini (Banca IMI)

Transforming Banks

The blockchain buzz is just the tip of an iceberg that will change the foundations of finance. In this talk we start from the reality of negative rates to understand what justifies the rise of digital currencies, then we move to explore how smart contracts allow to decentralize the typical roles of exchanges, depositories, and central counterparty. Finally, we see how very recent advances in cryptography can be used to redesign financial markets.

- Paolo Gianturco (Deloitte consulting)

TBD

- Regulatory authority on financial markets

TBD

6.15 pm - Final remarks