Financial applications of blockchains and distributed ledgers

Lipton Alexander, Treccani Adrien

<table>
<thead>
<tr>
<th>Cursus</th>
<th>Sem.</th>
<th>Type</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ing. finance</td>
<td>MA1, MA3</td>
<td>Opt.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Language</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credits</td>
<td>2</td>
</tr>
<tr>
<td>Withdrawal</td>
<td>Unauthorized</td>
</tr>
<tr>
<td>Session</td>
<td>Winter</td>
</tr>
<tr>
<td>Semester</td>
<td>Fall</td>
</tr>
<tr>
<td>Exam</td>
<td>During the semester</td>
</tr>
<tr>
<td>Workload</td>
<td>60h</td>
</tr>
<tr>
<td>Weeks</td>
<td>14</td>
</tr>
<tr>
<td>Hours</td>
<td>2 weekly</td>
</tr>
</tbody>
</table>

Remarque
Special schedule: see the IF website http://sfi.epfl.ch/mfe/study-plan

Summary
This course provides an introduction to distributed ledger technology, blockchains and cryptocurrencies, and their potential applications in finance and banking.

Content
The course covers the basics of cryptography and its applications to cryptocurrencies; historical examples to centralized cryptocurrencies; foundations of modern decentralized cryptocurrencies; Byzantine fault tolerant consensus; mechanics of Bitcoin platform including storage, mining, wallets, etc.; alternative platforms, including Ethereum; smart contracts; potential applications of decentralized ledgers in finance and their pros and cons.

Keywords
Electronic Money, Cryptocurrencies, Distributed Ledger Technology, Blockchain, Bitcoin, Ethereum, Smart Contracts

Learning Prerequisites
Recommended courses
Introduction to Finance

Important concepts to start the course
Cryptography, Databases, Payment Systems

Learning Outcomes
By the end of the course, the student must be able to:
- Use basic cryptographic concepts including private/public keys, signatures, hash functions, Merkle trees
- Distinguish pros and cons of centralized versus decentralized databases
- Demonstrate several historical examples of electronic money
- Quantify alternative approaches to Byzantine fault-tolerant consensus including proof of work, proof of stake, etc.
- Characterize the basic setup of Bitcoin, including storage, mining, and payments
- Implement the best practices in key management, including multi-signature schemes and multi-layer wallets
- Argue the limits of privacy with distributed ledgers and possible solutions, such as channeling, coin-joining,
confidential transactions and zero-knowledge proofs

• Analyze some of the potential applications of distributed ledger technology to finance and banking
• Elaborate inherent scalability limits of distributed ledgers and potential solutions with channeling, horizontal scaling and second-layer, off-chain transactions
• Implement some basic operations with Bitcoin
• Assess / Evaluate differences and commonalities between Bitcoin and Ethereum
• Implement basic smart contracts

Teaching methods
Lectures, exercises, homework

Assessment methods
30% Homework assignments
30% Coding exercises
40% Final paper

Supervision
Office hours Yes
Assistants Yes
Forum No

Resources
Bibliography

Ressources en bibliothèque
• Bitcoin and Cryptocurrency Technologies / Narayanan