″The Blockchain: Theory and Practice″

【講義詳細】
科目名: ″The Blockchain: Theory and Practice″
履修単位: 1 単位(CS5543)
コーディネーター: 片岡広太郎
スポンサー: 株式会社 chaintope
履修期間: 2018 年 9 月 17 日～ 9 月 22 日 (5:30 pm - 8:00 pm)

【概要】
このコースでは、ブロックチェーンの基礎となるメカニズムについて説明し、ブロックチェーンプログラミングを開始するために必要な知識を提供します。ブロックチェーンは暗号通貨を実現するために作られた比較的新しい技術です。P2P によって既存のセキュリティモデルを大きく変える可能性があると期待されており、さまざまな応用事例が生み出されています。

このコースではまず、ブロックチェーンの概要を暗号通貨の背景が生まれたと共に紹介します。その後、ブロックチェーンを使用した最初の暗号通貨である Bitcoin について掘り下げて解説し、基本的な暗号知識、詳細なデータ構造、およびデジタル署名を使用した送金トランザクションを理解します。また、P2P ネットワークを維持するためのブロックチェーンセキュリティやインセンティブデザインなどの重要なトピックについても検討します。ハンズオンでの課題では、学生は Bitcoin ブロックチェーン上でトランザクションを送信するプログラムを作成し、テストネットでの実際の暗号通貨の送金を通じて基本的な理解を深めます。

ブロックチェーンは、まだ開発段階にあり、様々な改良が研究され提案されています。このため、ブロックチェーンの可能性と課題を整理しながら最新のトピックを学習することも目標とします。このコースを修了すると、より高度なトピックに取り組むための必要な知識とプログラミングのブロックチェーンに不可欠なスキルを身に付けることができます。

【参考文献】
[1] Mastering Bitcoin, 2nd Edition by Andreas M. Antonopoulos, ISBN-13: 978-1491954386, O'Reilly Media, 2017.

【タイムテーブル】
1 日目: 5:30 pm - 8:00 pm (2.5 h)
-通貨の進化
-ブロックチェーンの概要
- Docker でのビットコインコアの準備（ハンズオン）

2 日目: 5:30 pm - 8:00 pm (2.5 h)
-ビットコインの構造とノードの役割
-暗号通貨の基本的な使い方
-CLI を使用したビットコインコアの操作（ハンズオン）

3 日目: 5:30 pm - 8:00 pm (2.5 h)
-ブロックの詳細とトランザクション
-アドレス、署名とスクリプト
-簡単なトランザクションの作成 （ハンズオン）

4 日目: 5:30 pm - 8:00 pm (2.5 h)
-セキュリティ:二重支払い、51%攻撃、フォーキング、秘密鍵管理、マルチシグ
-スケーラビリティ
-二重支払いの試行など（ハンズオン）

5 日目: 5:30 pm - 8:00 pm (2.5 h)
-暗号通貨のアップグレード:カラードコイン、レイヤー２
-分散化されたアプリケーションの可能性:イーサリアムなど
-ブロックチェーン上におけるオープンアセットトークンの発行（ハンズオン）

6 日目: 5:30 pm - 8:00 pm (2.5 h)
-ブロックチェーンについての最先端のトピック
-まとめ
-テスト

【課題】
-ビットコインウォレット作成(上級)
-マルチシグウォレット作成（上級）
--一方向性マイクロペイメントチャネル