

安全で公平な金融システムの実現に資する FinTech フレームワークの提案

目 次

まえがき	……………	大矢野 潤	1
第1部 ブロックチェーン技術の歴史と展望	……………	鎌田 光宣	9
1. はじめに			
2. ブロックチェーンとは			
2-1 ブロックチェーンの定義			
2-2 ブロックの中身 トランザクション			
2-3 マイニング（採掘）			
3. ブロックチェーンを支える技術 その1 ハッシュ関数			
4. ブロックチェーンを支える技術 その2 暗号技術			
4-1 公開鍵暗号			
4-2 電子署名			
4-3 ウォレット			
4-4 送金の流れ			
5. ブロックチェーンを支える技術 その3 分散システム			
5-1 分散ネットワーク			
5-2 合意形成の仕組み			
5-3 パブリック型とプライベート型			
5-4 フルノードと軽量クライアント			
5-5 メモリープールと未承認トランザクション			
6. ブロックチェーンの歴史			
7. ブロックチェーンの課題			
7-1 安全性			
7-2 スケーラビリティ			
7-3 ハードフォーク			

- 7-4 ダブルスペント（二重送金）問題
- 7-5 電力消費
- 8. ブロックチェーンのこれから

第2部 第1章 ブロックチェーンによる分散型台帳技術の解説

… 小林 直人 宮田 大輔 29

- 1. はじめに
- 2. ブロックチェーンとは
 - 2-1 ブロックチェーンに適した情報システム
 - 2-2 ブロックチェーン（ビットコイン）開発の動機
- 3. 取引情報の分散管理
 - 3-1 管理者が1人の場合
 - 3-2 複数人で管理する場合（お互いに信頼できる場合）
 - 3-3 複数人で管理する場合（お互いに信頼できない場合）
 - 3-4 ブロックチェーンとの対応関係
- 4. 要素技術
 - 4-1 一方向性ハッシュ関数
 - 4-2 公開鍵暗号方式を利用した電子署名
 - 4-3 スマートコントラクト
- 5. ブロックチェーンを利用する場合の技術的問題点
- 6. まとめ

第2部 第2章 スマートコントラクトの安全性と公平性の保証

…………… 大矢野 潤 45

- 1. はじめに
- 2. ブロックチェーンとスマートコントラクト
 - 2-1 仮想通貨とブロックチェーン
 - 2-2 スマートコントラクト
 - 2-3 イーサリアム
- 3. 「正しさ」の検証
 - 3-1 プロトコルの正しさ
 - 3-1-1 Needham-Schroeder 公開鍵プロトコル

- 3-1-2 The DAO 事件
- 3-2 スマートコントラクトの持つ「性質」
- 3-3 安全性と活性、公平性
- 3-4 モデル検査
 - 3-4-1 モデル検査の利点と欠点
- 4. モデル検査の実例
 - 4-1 遠隔購入手続き
 - 4-2 Safe Remote Purchase: Solidity
 - 4-3 Safe Remote Purchase: Promela
 - 4-3-1 Promela
 - 4-3-2 Solidity から Promela への変換
 - 4-4 商取引における「公平性」
- 5. おわりに

第3部 第1章 遠隔授業における個人認証技術への期待

…………… 柏木 将宏 69

- 1. はじめに
- 2. 遠隔授業の実施環境と結果について
- 3. 「情報入門」を事例とした遠隔授業の効果について
- 4. LMS における個人認証技術

第3部 第2章 ブロックチェーンの活用事例から見るその技術的側面

…………… 小林 直人 85

- 1. はじめに
- 2. ブロックチェーンの分類と構築プラットフォーム
 - 2-1 パブリック型とコンソーシアム型
 - 2-2 ブロックチェーンの活用事例とその型
 - 2-3 スマートコントラクトとその開発プラットフォーム
 - 2-3-1 イーサリアム
 - 2-3-2 Hyperledger Fabric
- 3. ブロックチェーンの特徴と利用に適した場面
 - 3-1 情報セキュリティの観点によるブロックチェーンの特徴

3-2 ブロックチェーンの利用に適した場面

4. 様々な活用事例

4-1 暗号資産（仮想通貨）

4-2 ブロックチェーンゲーム

4-3 取引履歴やデータの真正性証明

4-4 コンソーシアム型の活用事例

5. まとめ

第3部 第3章 教育目的でのブロックチェーンの応用 …………… 長尾 雄行 103

1. はじめに

2. ブロックチェーン

3. ブロックチェーンの応用

4. ビットコイン

5. イーサリアム

6. イーサリアムのプライベートネットワーク

7. スマートコントラクト

8. 試作システム

9. Dapps

10. おわりに

第4部 FinTech 活用における知覚リスク調査とその啓蒙

— プロジェクト活動報告 — …………… 橋本 隆子 127

1. はじめに

2. 関連研究 — FinTech に対する知覚リスク

2-1 心理的リスク

2-2 セキュリティリスク

2-3 その他の知覚リスク — 金融リスクとプライバシーリスク、パフォーマンス
リスク、時間リスク

3. 大学生を対象とした FinTech に対する知覚リスク調査

3-1 質問内容

3-2 アンケート結果

3-3 アンケートまとめ

4. FinTech 活用に向けた啓蒙活動

4-1 「仮想通貨とブロックチェーン」岩下直行氏（PwC あらた有限責任監査法人
スペシャルアドバイザー）講演報告

4-2 「ブロックチェーンとエネルギービジネス」江田健二氏（一般社団法人エネ
ルギー情報センター理事）講演報告

5. 考察 - FinTech 活用推進のために

5-1 知覚リスク調査からわかる FinTech 活用のためのポイント

6. 結論 - FinTech 活用を目指して

第5部 DX（デジタルトランスフォーメーション）が我が国金融機関に及ぼす影響につ
いて 平井 友行 153

1. はじめに

2. 問題意識

3. DX が従来型の金融の仕組みにもたらすものとは

4. まとめと更なる問題提起