2ZC-06

分散型台帳技術を用いたモバイル決済のモデル開発

沈　嘉秋†　　片山英昭‡

舞鶴工業高等専門学校電気情報工学科†‡

1　はじめに

現在，日本国内における電子決済の普及率は20%にも達していない．特に，個人経営の店舗や飲食店といった場所での普及が遅れている．この主な原因として，決済事業者が店舗などから徴収している加盟店手数料であると考えられる．この加盟店手数料の額は決済方法や業務形態により異なる．クレジットカードの飲食店における加盟店手数料は 5%であり，飲食店にとっては大きな負担になることが容易に想像できる．一方，決済事業者は決済システムの構築費用や決済システムを稼働させるためのサーバ，障害発生時の対応といったシステムのランニングコストがかかることがわかる．そのため，システムの維持費用を加盟店手数料という形でとらざるを得ないという現状がある．

手数料などのコストを軽減させるため，本研究では P2P 技術を用いた電子決済サービスのモデル開発を行う．店舗と一般客の間での決済を，極力サーバに頼らず，P2P ネットワーク上で完結させることで，決済事業者にかかるコストの軽減をはかる．

店舗や一般客に決済専用の端末が必要となると，導入コストがかかるため，モバイルネットワークもしくは家庭用のインターネット回線に接続された，一般的な Android OS を搭載した携帯端末を店舗と一般客の両方の決済端末として用いるものとする．

2　決済システムの概要

決済システムのサーバへの依存を減らすために，本システムは P2P ネットワーク上で決済処理を行う仕組みである．ここでは本研究の決済モデルに関して概要を説明する．

一般客は決済事業者から購入した通貨を用いて取引を行う．決済事業者の通貨発行専用のサーバは通貨を発行するとともに，通貨購入客の端末と P2P ネットワークに情報を送信する．取引は P2P ネットワーク上で行われる．P2P ネットワークは一般客と店舗の決済用のスマートフォンによって構成される．本決済モデルの概要図を図 1 に示す．

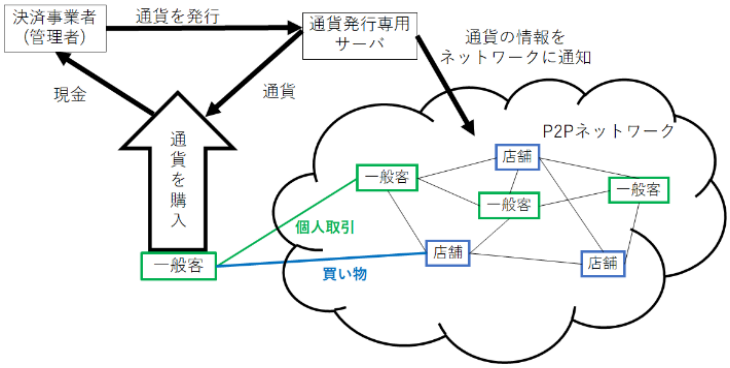

図 1.決済モデルの概要

3　構築するシステムについて

3.1　P2P ネットワーク

モバイルネットワークではキャリアグレード NAT が用いられている．そのため，スマートフォン間で P2P 通信を行うためには，この NAT を越える必要がある．本研究では WebRTC を用いることで，NAT 越えを実現する．WebRTC では，SDP(Session Description Protocol)と ICE Candidate の二つの情報を端末間で交換することにより，NAT を超えて P2P 通信が開始される．この SDP 等を交換する作業であるシグナリングを行うためには，SDP 等を交換するためのサーバが必要になる．このサーバをシグナリングサーバと呼ぶ．本研究では，シグナリングサーバを Google の mbaas(mobile backend as a Service）である Firebase を用いてクラウド上に実装する．通貨などの内容をブロードキャストするためのネットワークを，シグナリングサーバと携帯端末を用いて図 2 に示すように構築することで実装する．またそれぞれの端末間でシグナリングを繰り返すことにより，接続するピアの数を最大で 3 台まで増やす．このことにより，図 3 に示すように，端末の離脱による中継分断に対する耐久性を持ったネットワークの構築を可能としている．

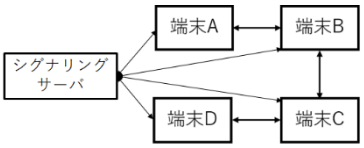

図 2.初期ネットワーク

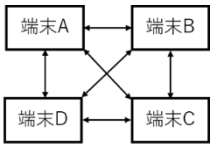

図 3.相互通信

Model Development of Mobile payment with Blockchain
†Yoshiaki Shin, Dep. of Electrical and Computer Engineering, National Institute of Technology,Maizuru College
‡Hideaki Katayama, Dep. of Electrical and Computer Engineering, National Institute of Technology,Maizuru College

Copyright ©2018 Information Processing Society of Japan.
All Rights Reserved.

3.2　分散型台帳技術

分散型台帳技術とは，ブロックチェーンの機能を派生し，共有台帳という特徴だけを抽出して一般化した概念である．すべての端末が共有台帳を持ち，すべての取引が共有台帳に記帳される．台帳はハッシュチェーンという仕組みによって保護されている．ハッシュチェーンの概略を図 4 に示す．ハッシュチェーンは新しく記帳されたデータに前回記帳したデータをハッシュ値に変換したものを含めることで,ハッシュ値の鎖のような構造を作る.これにより台帳の中のデータが改ざんされるとハッシュ値が変化し,データが持つハッシュ値の整合性が取れなくなるので,データの改竄を容易に検知することができる.

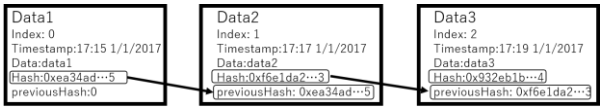

図 4.ハッシュチェーン

3.3　コンセンサスアルゴリズム

複数のノードが同時に異なるブロックを作成した場合，異なるハッシュチェーンが同時に誕生する可能性がある．これは，全てのノードに新しいブロックを生成する権限が与えられていることに起因する．この問題を解決するためには，ブロックを生成する権限をもったノードを一つに限定する必要がある．ブロック生成権をもつノードを確定させる方法として Bitcoin で用いられている POW(Proof of Work)や Hyperledger で用いられている PBFT(Practical Byzantine Fault Tolerance)が挙げられる．POW は各ノードが処理能力を競い合ってブロック生成ノードを確定させている．処理能力を競い合わせるためにはモチベーションを持たせるために報酬を用意する必要があるが，本システムは法定通貨のトークンであるため，新たに報酬を設けるとなると決済事業者への負担となるため望ましくない．

PBFT はブロックチェーンの運営者が指定したリーダーノードのみがブロックの生成権を持つ．PBFT はプライベートなブロックチェーンであり，リーダーノードはあらかじめ選出されている．本システムは不特定多数のノードが参加可能なパブリックなブロックチェーンであるため，稼働時間が最も長いノードを信頼性が高いと評価し，リーダーノードとしている.リーダーノードは 1 秒間隔で生存信号を全ノードにブロードキャストし，他のノードはリーダーノードからの生存信号が途絶えた際には，その次に稼働時間の長いノードを新しいリーダーノードとなる．

3.4　取引の内容

本システムで．は，１取引につき１つのブロックを作成する方法を採用している.ブロックの中にはハッシュチェーンを構築する要素のほかに取引の内容が含まれる．取引の内容は,取引の種類，取引に用いられるトークンの情報，取引の識別子などがある．取引には，決済事業者による新たな通貨のトークンの発行，一般客による支払処理，店舗による受け取りの完了の三種類がある．

4　アプリケーション

3 節で説明したシステムにより，Android アプリケーション作成した．アプリケーションで決済を行っている画面を図 5 に示す．この図において，左が一般客の端末で，中央と右が店舗の端末である．一般客が支払う金額を所有する端末に入力すると決済に必要な情報が QR コードに表示される．店舗側はその QR コードを店舗がもつ端末で読み込むと決済処理が行われる．

図 5.決済処理

5　まとめ

本研究で，手数料などを節減させるため， P2P 技術を用いた電子決済サービスのモデルを行った．また実際に Android 端末上で動作する，分散型台帳技術を用いた決済システムのモデルを開発し，支払いなどが問題なく行われることを確認した．今後は，Windows や Linux 環境でも動作するモデルを作成し，システムへの参加ノードの増加や長期にわたる連続稼働による影響を検証する必要があると考えられる．

参考文献

[1] はじめての Blockchain
https://www.ibm.com/developerworks/jp/cloud/library/j_cl-blockchain-basics-bluemix/index.html
[2] [webRTC for android vol2] 繋げてみる
http://qiita.com/nakadoribooks/items/d046fb68d59c7ffffbc42
[3] 200 行のコードへのブロックチェーンの実装
http://postd.cc/a-blockchain-in-200-lines-of-code/

Copyright ©2018 Information Processing Society of Japan.
All Rights Reserved.