電子情報工学科 (川原研究室)

学生番号	16232066	氏名	服部智哉
論文題目	Ethereum 技術を適用した自律分散アクセス共用網における実現性に関する研究		

1 はじめに

近年，移動型端末の普及により公衆無線 LAN サービスは拡大し，各無線 LAN アクセスポイント (AP) における通信量が増加しているため，AP の稠密設置が予想される．そこで管理者の異なる AP 同士を共用管理することで，データの収容性能を向上させる AP 共用ネットワークが必要とされており，ブロックチェーンを用いた自律分散無線アクセス共用システムが提案されている．

本研究では．上記の無線アクセス共用システムに Ethereum の技術を適用することでより AP が自律的に端末の収容を行う手法の提案を行い，システムに必要なトランザクションやブロックの具体的なフィールドの定義，またこれらを処理フローを定めることで自律分散アクセス共用網の実現性を示す．

2 Ethereum

Ethereum ではトランザクションを状態遷移関数の入力値としてとらえている．あるアカウントの持つ状態 (State) とトランザクションを入力として新しい状態を出力する [1][2]

2.1 スマートコントラクト

スマートコントラクトとは契約を自動的に行う仕組みである．あらかじめ契約をプログラム言語で記すことで条件を満たすトランザクションを入力にプログラムを実行する．プログラム言語で記された契約のことをコントラクトコードと呼ぶ．

2.2 ワールドステート

ワールドステートは，上述のアカウントの状態を考慮することができる．ワールドステートはアカウントのアドレスとそのアカウントの状態の紐付けで構成され，この情報は Merkle Patricia tree と言われるデータ構造に保存される．木構造の根の値をブロックに格納し，木全体はノードが保持する．

3 自律分散無線アクセス共用システム

3.1 システム概要

自律分散無線アクセス共用網では AP をブロックチェーンの全ての情報を持つフルノード，端末を自身の情報のみを保持する SPV ノードと定義する．AP によって P2P ネットワークの構成を行い，端末はネットワークを利用する際にネットワークに参加する．[3]

3.2 オフチェーン

オフチェーンとはトランザクションの交換をブロックチェーンの外で行い，複数のトランザクションの交換を集約しブロックに書き込む技術である，この技術を用いることでトランザクションの認証回数を減らし，リアルタイム性の高い取引が期待できる．自律分散無線アクセス共用システムでは AP 端末間でオフチェーンを構築することで AP への接続をリアルタイムで行うことが提案されている．[4]

4 問題点

自律分散無線アクセス共用システムでは端末が共用システムに参加するたびに AP との間にオフチェーンを構築することが求められる．しかし，これには以下の問題点が存在する．

- オフチェーンを構築する
  - オフチェーンの構築にコストを要するため AP に接続する度にオフチェーンの構築を行うことは現実的ではない．
  - オフチェーンでは集約された取引が不明瞭になる．
- トランザクションに取引の過程を保存している
  - 現在のノードの状態を確認するためには過去のブロックをすべて確認する必要がある．

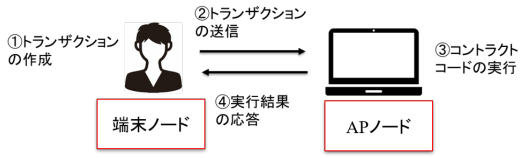

図 1: システム概要図

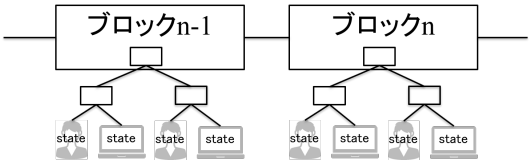

図 2: ワールドステート

5 Ethereum 技術の適用

上記で述べた問題点を解決するため Ethereum 技術をシステムに適用しシステムの考え方，このシステムに必要なトランザクション，ブロック，それらを処理するフローを提案することで実現性を示す．

5.1 端末認証，接続の自動化

スマートコントラクトを適用することで，端末をトランザクションの生成を行うノード，AP を端末から受信したトランザクションを入力とし自身の保持するコントラストコード（プログラム）実行するノードとする．コントラクトコードに端末の認証や接続を行うプログラムを記すことでそれぞれの動作を自動的に行うことができる．動作が自動であるため AP の作成する情報は明確であり，ブロックに格納する必要がない．これにより，トランザクションの認証回数を減らすことができるためオフチェーンを構築する必要がない．

5.2 ノード情報の保持

ワールドステート適用し，自律分散アクセス共用網に接続しているノードの情報を AP が保持をする．AP が他のノードの情報を保持することで，端末を他の AP へ変更する際など他の AP へ情報を問い合わせる動作を行う必要がなく自身の保持しているステートを確認することで対応することができる．これによりトランザクションを受信した AP が自律的に端末の割振りを行える．

6 まとめ

本研究では，先行研究の問題を解決する手法を Ethereum 技術を用いることで提案し，そのために必要となるトランザクション，ブロック，またそれらの動作フローを定義することで自律分散アクセス共用網における実現性を示した．今後は大規模ブロックチェーンを構築した際に生じるネットワークの影響などを調査する．

参考文献

[1] AkiraMAEGAWA,WhitePaper ethereum/wiki GitHub https://github.com/ethereum/wiki/wiki/%5BJapanese%5D-White-Paper.

[2] DR. GAVIN WOOD, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER, https://ethereum.github.io/yellowpaper/paper.pdf.

[3] 青山寛樹，川原憲治”ブロックチェーン技術を適用した自律分散無線アクセス共有網の検討”, 電子情報通信学会 2019 総合大会，2019 年 3 月発表.

[4] 樋野貴文，川原憲治”ブロックチェーン技術を適用した自律分散無線アクセス共用網における AP-端末間チャネル構築方式に関する研究”，九州工業大学 2019 卒業論文，2019 年 2 月発表.