

学生番号	20676124	氏名	服部 智哉
論文題目	Ethereum 技術を適用した自律分散無線アクセス共用網におけるスマートコントラクトに関する研究		

1 はじめに

近年、移動型端末の普及により無線 LAN アクセスポイント (AP) の通信量が増加しており、AP の稠密設置が予想される。そこで管理者の異なる AP 群に対して端末の契約/所属状態によらず接続を可能とする Bitcoin ベースのブロックチェーン技術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 Ethereum 技術を適用することで各ノードが他ノードの情報を保持し、迅速に端末の認証や、端末の接続切替を行う手法を検討する。

2 自律分散アクセス共用網 [1]

Bitcoin は個人に依存しない電子取引システムで、トランザクション (Tx) は UTXO (Unspent Transaction Output: 未使用トランザクション)、すなわち、単変数の授受のみ記録する。[1] では、端末から AP に対する認証要求や切替要求を Tx とし、UTXO を収容端末数として、共用網内の各 AP の端末数を管理していた。そのため、AP の収容端末数を得るには認証されたブロックチェーンにおいて該当 AP に関する Tx を遡る必要があり、端末の接続 AP 切替時に支障をきたす。

一方、Ethereum では、Tx 内に複数の情報を保持可能である。また、各ノードがノードアドレスを基に木構造を構築し、葉ノードにノードの「状態」を格納することでネットワーク内の全ノード情報を保持することができる (State 木)。ノードはそれらの情報を「スマートコントラクト」を用いて遷移させ、反映 Tx をブロックの認証を通して共有することで他ノードに状態変化を反映させる。そこで共用網を構成する AP を上記のノードと定義することで接続端末数などの情報を各 AP が共有し、端末の認証、接続切替のオーバーヘッドを小さくするための Ethereum 技術を適用した AP 共用網を提案する。

3 Ethereum 技術を適用した AP 共用網の検討

3.1 AP の状態定義と Tx の役割

各 AP は共用網内の全 AP の接続端末数や使用帯域、収容端末のリストなどの情報を AP の「状態」として保存する。これらの情報と端末からの端末の接続要求や接続状況を含んだメッセージを基に Tx を生成し、スマートコントラクトを実行する。本研究では、AP の状態を遷移させる「端末の認証」、「端末-AP 間の接続切替」、「共用網への参加、離脱」をスマートコントラクトとして定義をした。3.2 に端末認証手順とそのためのスマートコントラクトについて説明する。

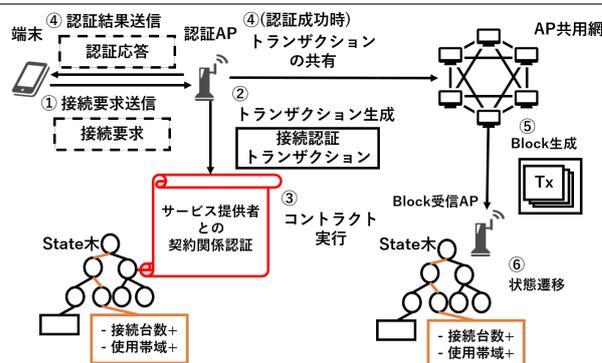


図1. 端末認証手順

3.2 端末認証 (図1)

端末が共用網内の AP と接続し、通信を開始するには共用網内の任意の AP において共用網内のサービス提供者と契約関係にあることを認証する必要がある。以下に任意の AP において端末認証スマートコントラクトを実行し、他ノードに認証情報を共有するまでの手順を示す。端末認証に失敗した場合 5. 以降の手順を行わない。

1. 端末：認証要求メッセージ (端末情報, 認証用情報) を認証 AP に対して送信
2. 認証 AP：認証要求メッセージに含まれる情報と自身の状態情報を含め接続認証 Tx を生成
3. 認証 AP：端末認証スマートコントラクトを実行
 - 入力：接続認証 Tx (端末情報, AP 情報)
 - 処理：サービス提供者との契約関係認証
 - 出力：
 - [成功時] 認証 AP の収容台数や使用帯域の増加
 - [失敗時] 接続認証 Tx や処理の破棄
4. 認証 AP：端末へ認証結果の応答
 - [3. 成功時] 端末と接続, 共用網へ Tx 転送
5. 共用網内の任意の AP：Block 生成/転送
6. Block 受信 AP：該当 AP の状態遷移

4 まとめ

Ethereum 技術を適用した自律分散無線アクセス共有網における端末認証, AP-端末間の接続切替のスマートコントラクトを提案した。今後は提案スマートコントラクトを実装し, 認証, 端末の接続切替のプロセスを実際に確認する必要がある。

参考文献

- [1] 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。

研究業績

服部智哉, 川原憲治, "Ethereum 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 2022 総合大会, 2022 年 3 月発表予定。