1X-05

多階層型ネットワークにおけるブロックチェーンを用いたセキュアなデータ共有手法

安井 貴規 †　　藤田 桂英 ‡

† 東京農工大学大学院　工学府　情報工学専攻　　‡ 東京農工大学大学院　工学研究院　先端情報科学部門

1　はじめに

ブロックチェーンは，Ethereum や Hyperledger のように，利用者がスマートコントラクトを構築するプラットフォームとしても利用されている．ブロックチェーンを使用したサプライチェーンマネジメントの研究も進められており，従来のクライアントサーバモデルより冗長性の高い構成となることで，災害対策としても注目されている [1].

一般的に，サプライチェーンでは，原材料生産者から消費者までのすべての工程を含むとされるが，サプライチェーンおよび付随する処理を単一のブロックチェーンで実現する場合，原料や製造工程など，機密にすべき情報が，小売業者や消費者に流れる状況が想定される．

本論文では，単一のネットワークにおいて複数のノードグループを形成したモデルである多階層型ネットワーク，および，多階層型ネットワークにおいて，公開鍵暗号および共通鍵暗号を用いたデータの共有手法の提案を行う．

2　多階層型ネットワーク

図 1 に多階層型ネットワークの例を示す．本論文では，多階層型ネットワークを次の通り定義する．多階層型ネットワークは，複数のノードグループ，および，複数のノードから構成される論理的なネットワークである．ノードグループは，少なくとも当該ネットワークに存在するノードを 1 つ以上含む．また，複数のノードグループに含まれるノードも存在できる．

多階層型ネットワークは，サプライチェーンや IoT デバイスによるセンサネットワークなど，あるノードの発する情報が，他のノードに伝達される場合に用いることができる．また，情報を受信したノードは，さらに情報を処理，もしくは，ノードが属するノードグループのいずれかに送信することができ，これによって情報の処理および送受信による連鎖が発生する．

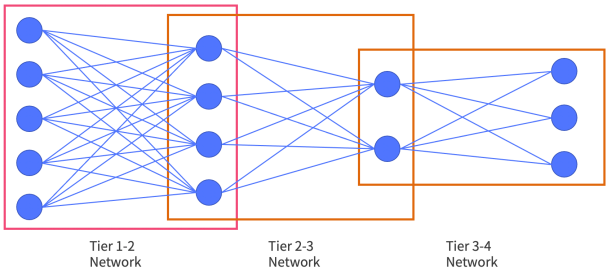

図 1: 多階層型ネットワークの例

3　多階層型ネットワークにおけるセキュアなデータ共有手法

本論文では，ブロックチェーンにおける電子署名アルゴリズムとして Ed25519 を用いた．本モデルでは，ノードグループのマスタを除き，各ノードの保持する Ed25519 秘密鍵と，ブロックチェーンで保持されるデータのみで最新の状態が復元できる．

ノードグループの作成は，GROUP_DECLARE トランザクションの送信により行われる．GROUP_DECLARE トランザクションの送信元アドレスは，以降，ノードグループのアドレスと，ノードグループのマスタを兼ねる．マスタは特殊な権限を持ち，加入の承認など，通常のメンバより多くの行動が可能である．

グループ内の通信は AES (256 bits) による暗号化を行い，鍵はランダムで生成する．AES 鍵の配布には X25519 を使用する．ノードグループへ加入を希望するノードは，ランダムに生成した salt とともに，X25519 公開鍵をノードグループへ送信する．X25519 公開鍵は鍵配布以降も利用されるが，任意のタイミングで更新可能である．

ノードグループからノードが脱退した場合は，AES 鍵の更新を行う．鍵更新はマスタが行い，鍵配布で用いた各ノードの X25519 公開鍵を用いて，新しい AES 鍵を暗号化して，ノードグループ宛に送信する．また，鍵更新以後に加入したノードが鍵更新以前のデータを参照できるように，古い AES 鍵は新しい AES 鍵にて暗号化して送信する．鍵更新により，脱退したノードは，以降のデータの復号が不可能となる．

Secure Data Sharing with Blockchain on Multi-Layer Network
†Department of Computer and Information Sciences, Graduate School ofEngineering, Tokyo University of Agriculture and Technology
‡Division of Advanced Information Technology and Computer Science, Institute of Engineering, Tokyo University of Agriculture and Technology

4 評価

前述のモデルに対して，Python 3.8.6 にて実装したシミュレータによる評価，および，モデルの仕組みに対する評価を行った．

4.1 End-to-End の暗号化および復号化の処理時間

N ノードが参加するネットワークにおいて，L Bytes のデータを送信するとき，AES による End-to-End の暗号化および復号化の処理時間の実験結果を表 1 に示す．なお，今回は，トランザクションの承認を全ノードにて行った．結果から，処理時間は，ノード数 N の影響を強く受けるが，データ長 L の大きさからの影響は小さいことがわかる．ノード数の影響が大きいため，大規模なネットワークに適用する際には，高速にトランザクションを承認できるモデルが必要となる．

表 1: 2 ノードを含むグループでの暗号化および復号化の処理時間 (単位は μs)

データ長 L	$N = 10$	$N = 100$	$N = 1000$
1	2847.341	25087.597	247972.402
10	2833.764	24876.743	246098.119
100	2852.056	24996.903	246828.490
1000	2999.617	25887.116	254812.065
10000	3783.532	29398.363	285550.123

4.2 鍵更新にかかる必要転送量の比較

本モデルにおける鍵更新では X25519 を使用したが，RSA を使用した場合との比較を行った．図 2，図 3 に，それぞれ，転送量と処理時間の比較実験を行った結果を示す．結果から，X25519 は，RSA よりも 1.5 倍程度の処理時間が必要だが，転送量は RSA の 20 %程度となった．

4.3 ノードグループの鍵

ノードグループで使用される AES 鍵は，トランザクションをたどることにより復元可能であるほか，その時点で用いられている鍵の使用が不適切となった場合は鍵を更新できる．

AES 鍵の有効期限については課題が残る．ノードがノードグループから脱退した直後には鍵更新が行われていないため，脱退したばかりのノードも暗号化されたデータを復号することができる．したがって，鍵更新は，ノードが脱退した場合には速やかに行う必要があるといえる．なお，ノードの加入および脱退が多く行われる状況の場合は，一定の期間ごとに鍵更新を行うなど，運用上での工夫が求められる．

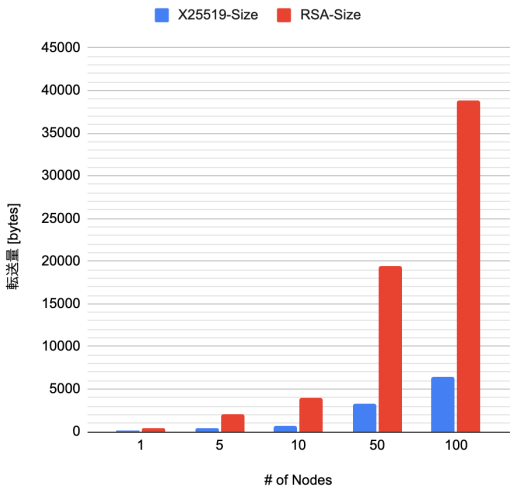

図 2: X25519 と RSA における鍵更新の転送量の比較

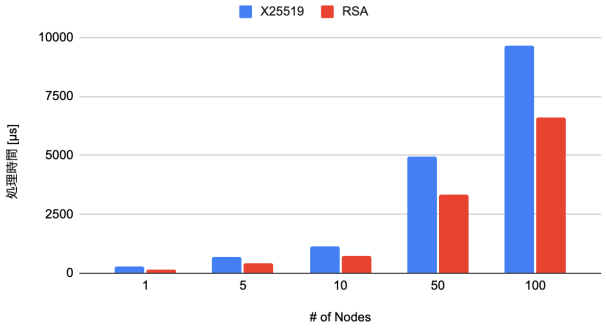

図 3: X25519 と RSA における鍵更新の処理時間の比較

また，短い期間に非常に多くのトランザクションが存在する場合は，鍵更新を行ってから，実際に新しい鍵を用いるまでに時間差が生じることが予想される．時間差の問題については，グループ内で用いられる共通鍵が一時的に複数になる，移行期間を設けることによって解決できる．

5 まとめ

本論文では，多階層型ネットワークのブロックチェーンへの実装，および，ブロックチェーンネットワークにおけるノードグループの形成および暗号化された通信手法を提案した．ノードの保持する鍵数の削減や，鍵配布および鍵更新に X25519 を用いることによる転送量の削減を行うことで，安全かつ軽量なモデルとなった．

参考文献

[1] Celine Herweijer, Dominic Waughray, and Sheila Warren. Building Block(chain)s for a Better Planet. In *World Economic Forum*, 2018.