7ZG-06

ブロックチェーン技術を用いた物流への応用
(The Application to logistics using block chain technology)

北川　哲也†　　田中　和明‡
九州工業大学情報工学府†　　九州工業大学情報工学研究院‡

1. はじめに

近年,金融と情報技術を組み合わせたフィンテックと呼ばれる経済活動が高まっており,例としては仮想通貨による決済が挙げられる.決済の取引情報管理はブロックチェーンと呼ばれる技術が採られており,分散管理による情報の共有,ハッシュ値を用いた情報改ざんの検知といった特徴がある.このようにブロックチェーンは情報改ざんへの対策が施された技術であり仮想通貨以外の分野においても適応可能ではないかと考え,ブロックチェーン技術を身近な物流へと適応させる.国をまたぐ長距離における物流では荷物の状態管理を人が一つ一つ記録している.記録は紙媒体で行うので状態管理が多ければ多いほど量は増えていき,人が背負う手間も増えていくという問題点がある.この問題点に対して人による荷物の状態管理を自動で行うとともに紙媒体をデジタル化することで手間を減らすことができる.また,記録,管理の自動化による情報のセキュリティ面に関してはブロックチェーン技術を適応することで向上を図る.本稿ではブロックチェーン技術を物流へと応用するための準備として情報管理構造や改ざんの検知手法を考慮した簡易的な物流・ブロックチェーンモデルを提案する.

2. ブロックチェーン

ブロックチェーンの代表的利用例は仮想通貨による取引情報の管理が挙げられる.ブロックチェーンは複数の取引情報をブロックと呼ばれる形式でまとめ,それらを時系列ごとに繋いだものである.ブロックチェーン自体は一つのサーバで管理する中央集権モデルで管理されておらず複数の管理者によって分散管理されているため管理権限が一つに集中するといったことがなく複数の管理者によるコンセンサス(合意形成)によって取引情報の管理,ブロックの追加、整合性の確認が行われる.また,分散管理によってブロックチェーンは管理されているので中央集権モデルと比較し,サーバの故障によるデータの破損などといったシステム障害に強いという特徴もある.ブロックチェーンを構成するブロックの内容としては複数の取引情報,前のブロックのハッシュ値,タイムスタンプ,ナンスと呼ばれる任意値である.ハッシュ値の生成はブロック自体をハッシュ関数 SHA-256 に入れ,ブロック内のナンスを変えることで提示される条件に合うハッシュ値を見つけ出すことで行われる.ブロック内の取引情報を改ざんしようとすれば条件に合うハッシュ値を見つけ出すためにハッシュ値を再計算しなければならない.ハッシュ値の再計算には膨大な計算量を要するためブロックチェーン自体の改ざんの困難さに起因している.図 1 にブロックチェーンの構成図を示す.

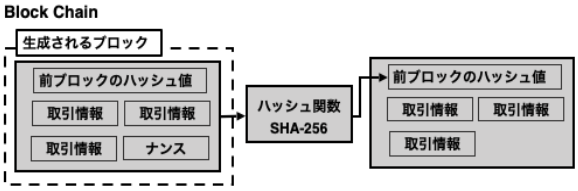

図 1: ブロックチェーンの構成図

3. 提案するモデル

本章ではブロックチェーンを物流へと応用させるための手法を述べる.まず物流において管理する情報としては荷物ごとの温度,温度の記録時刻となるタイムスタンプである.個々の荷物ごとに温度などの情報を数分単位で記録し,一定数の荷物情報が集まれば１つのブロックにまとめ,これらを繰り返していくことでブロックチェーンを荷物に取り付けてあるマイコンに構成していく.従来のブロックチェーンではネットワーク上で数分おきに承認を行うことでブロックチェー

The Application to logistics using block chain technology
Tetsuya Kitagawa† Kazuaki Tanaka‡
School of Computer Science and Systems Engineering†
Graduate School of Computer Science and Systems Engineering‡

ンの整合性を保っているが荷物に取り付けてあるマイコンはオフラインなので常時ブロックチェーンの状態を管理することができない. ゆえに配達道中で荷物のマイコンとサーバの 2 者間で通信(ハッシュ値の交換)を行い, サーバ上にその通信地点での荷物のブロックチェーンが持っている最新のハッシュ値を記録する. 配達後にマイコン上のブロックチェーンからサーバと通信した際に生成されるブロックが所持する前のハッシュ値(送った最新のハッシュ値)とサーバ上にあるマイコンから受け取ったハッシュ値とを照合することで改ざんの有無を検知することができる. また、配達道中のハッシュ値を受け取るサーバもブロックチェーンを持っており, 荷物ごとのハッシュ値を通信して受け取るたびにブロックが生成されていくものとする. 提案するモデルでは配達途中にチェックポイントとなるサーバを複数設置する. 図 2 に物流モデル, 図 3 にハッシュ値の交換, 図 4 に改ざん検知までの流れを示す.

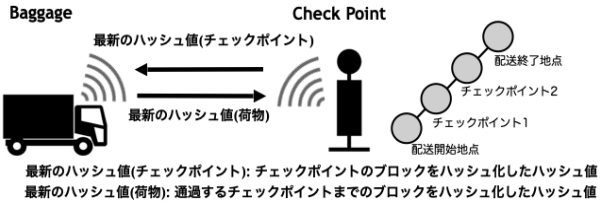

図 2: 物流モデル

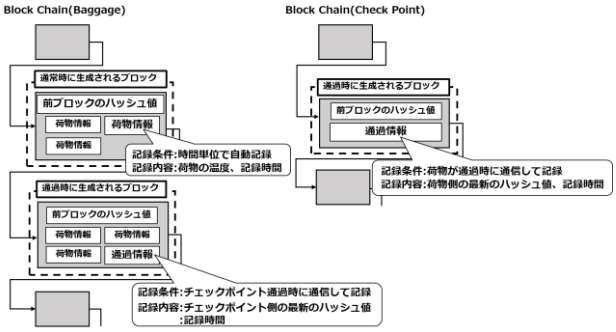

図 3: ハッシュ値の交換

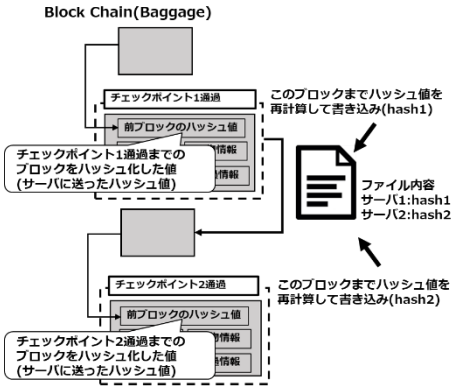

図 4(a):照合用ファイル生成

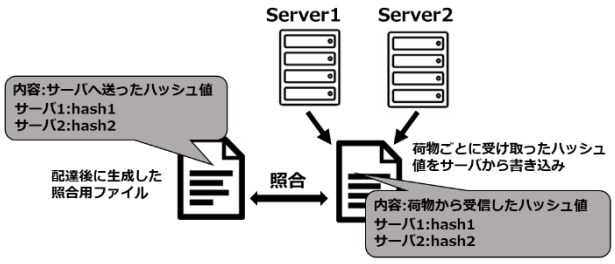

図 4(b):改ざんの検知

4. モデルの実装と課題

提案したモデルの実装に関してサーバとマイコン上のブロックチェーンを模した 2 つのプログラムによりモデルの再現を行なった. 提案したモデルに関して懸念される項目としてはハッシュ値の衝突である. この手法では配達後にブロックチェーンの整合性を確かめる. しかし荷物情報を改ざんして次ブロックに格納している改ざん前の前ブロックのハッシュ値と衝突が起これば改ざんの検知においてハッシュ値の交換によりサーバ側が受け取ったハッシュ値と荷物上の再計算したハッシュ値との照合で改ざんした場合に起こるハッシュ値の不一致が起きず改ざんを検知することができないという課題が出てくる. また, 1 つのブロック内には複数の荷物情報が含まれているのでタイムスタンプや温度などのデータの数も増えることから改ざん可能な部分も増えてしまうためハッシュ値の衝突確率も上がってしまう恐れがある. 対策方法としてはハッシュ値の衝突が起きにくいようにブロックに格納する荷物情報数の制限、荷物情報に含まれるタイムスタンプ・温度の制限を行い, 様々な条件下でブロックを生成しハッシュ値の衝突を確かめていくことで制限を定めていく必要がある.

5. おわりに

本稿ではブロックチェーンを物流分野へ応用することにより人が背負う手間の削減を図った. その準備段階としてブロックチェーンモデルを提案し, 模擬的なブロックチェーンのプログラムを作成し動的なモデルの流れを確認した.

今後の実装に向けてハッシュ関数の衝突を利用した改ざんなどの起こりうる不正行為を見つけ出すとともに対策を考えていくことで詳細的な設計、実装を行なっていく.