ブロックチェーン技術の教育への応用可能性

Applicability to Education of the Blockchain Technology

廣瀬　一海
Kazumi Hirose
畿央大学大学院 教育学研究科
Graduate School of Education, Kio University
Email: kazumihirose@hotmail.com

あらまし:ブロックチェーン技術は、従来から考案されていた技術を応用し、改ざんが極めて困難であり、ダウンタイムの無く、非中央集権型のシステムを安価に実現できる、P2P 分散データストアの技術である.近年、スマートコントラクトを実装可能とするプログラマブルなブロックチェーンの登場により、暗号通貨流通以外を対象として、ブロックチェーン技術を応用できる可能性が出てきた.
本稿では、ブロックチェーン技術が単に暗号通貨の流通、価値の保持だけで無く、教育分野においても応用が可能であり、学校教育、生涯教育、遠隔教育などの分野において重要な基盤となりえる事を論ずる.

キーワード：**ブロックチェーン**, Ethereum, Peer to Peer, Bitcoin, **スマートコントラクト**

1. はじめに

Bitcoin は、Peer to Peer を用いた暗号通貨を流通させる分散台帳データストアの仕組みである(1).その後実装が進み、運用を開始、管理者不在であっても、多重支払いを防止し、ダウンタイムが無く堅牢であり、改ざんが極めて困難であり、リコンサイルが不要なシステムがプロトコルのみで実証されている.

現在、これらの特性を活かし、通貨価値流通以外の分野において応用が試みられている．本稿ではブロックチェーン技術であり、且つスマートコントラクトを実装可能である Ethereum に教育分野向けの応用可能性がある事について論じる.

2. ブロックチェーンを構成する技術

2.1 ブロックチェーンと CAP 定理

ブロックチェーンは分散データストアであり、ブリュワーの定理における CAP のいずれかを優先して選択せざるを得ない、P および A を優先しているデータストアである(2).

ブロックチェーンにおける C(Atomic Consistency)は、時間経過より確率として信頼性が向上し、結果整合性が妥当な程度で確保可能であるように考えられたものである.

この為、Bitcoin や同種のブロックチェーンでは、ブロックの投入後から 100 ブロックの進行によって、投入したブロックの一貫整合性が妥当であるとされ、取引は信頼されるものとして扱われている.

2.2 ブロックチェーンを支える既存技術

ブロックチェーン技術は、今まで一般的に扱われてきた、以下に挙げる既存技術を組み合わせる事で実装されている.

1. Peer to Peer
2. Merkle tree
3. Hash 関数
4. ブロックの承認と Proof of Work
5. 電子署名

① Peer to Peer

中央集権型のクライアント・サーバのシステムと比較し、非中央集権型であるブロックチェーンシステムは、Peer to Peer で相互に接続され、それぞれがブロックチェーンデータを保持している.

再起動やトラブルがあったとしても、存在するすべてのノードが停止しない限り、データやブロックチェーンネットワークの健全性が損なわれる事は無い.

② Merkle tree

Merkle tree は、各ブロックのヘッダに格納されたデータのハッシュを格納している.

このようにデータのハッシュ値をツリー上に格納する事で、どのブロックにデータが格納されているかを迅速に確認する事ができる.

③ Hash 関数

各ブロックヘッダは、一つ前のブロックのハッシュ値を保持する事を繰り返す事で、鎖のようにつながっている、これがブロックチェーンと呼ばれる所以であり、過去のハッシュの突合を行えば、そのチェーンの非改ざんであり、一貫整合性が正しいものであると判断ができる．最長のブロック数を保持しているチェーンが常に正しいと解釈するように実装されている.

④ ブロックの承認と Proof of Work

新規にブロックの追加を行う際、各ノードに配られたブロックは、ヘッダに格納された Difficulty の条件を満たす事が出来るまで、Nonce 値を変えながら繰り返し Hash 値を計算する.

条件を満たす Nonce 値が得られたノードは、自ブロックチェーンに追加し、ブロックを他のノードへ配布する.

この仕組みは、Proof of Work といい、Adam Back

により 1997 年に Hashcash の DoS 攻撃対策として考案[3]され、稼働する計算機資源の 51%を上回らない限り改ざんを成功させる事は難しいとされている[4].

⑤　電子署名

各トランザクションは、各ユーザの秘密鍵を用いて楕円曲線 DSA 署名が行われている.

この署名は一つ前のトランザクションに、そのユーザの公開鍵が含まれ、署名を確認する事によってそのトランザクションの関係性が判明する仕組みとなっている.

3.　次世代ブロックチェーン技術や派生技術

前述した特性を持っているブロックチェーン技術を応用・改良したソフトウェアが次々に誕生している.多種多様なソフトウェアが存在しているが、その中でもスマートコントラクトと呼ばれる、手続き行為をプログラムし、その処理を自動化する独自のブロックチェーンシステムの構成を可能とする Ethereum と Eris はブロックチェーン 2.0 と呼ばれ、注目を集めている.

3.1 Ethereum

Ethereum は Ethereum Foundation により、開発が進むオープンソースプロジェクトであり、スマートコントラクトをブロックチェーンネットワークへ展開、運用が可能なブロックチェーン技術である[5].

チューリング完全なプログラミングを可能とする仮想環境である EVM(Ethereum Virtual Machine)を持っており、Solidity というスマートコントラクト記述言語を用いて、プログラマブルなブロックチェーン処理と電子取引を可能としている.

3.2 スマートコントラクト

スマートコントラクトは、契約行為と履行の関係を、ネットワーク上に表現し、不特定多数の人同士にて合意、電子取引を可能にするアイデアである [6].

各ブロックチェーン技術においても、この用語の解釈が異なるが、狭義の意味でのスマートコントラクトは自動販売機のように、当事者に能動的な契約執行権があり、その過程を自動化する事が可能なブロックチェーンネットワークとプログラムコードの複合による仕組みと考える事ができる.

4.　ブロックチェーン技術の応用と期待

このような背景から、ブロックチェーン技術は、以下に挙げる情報の新しい管理形態をもたらすものとして期待されている.

- 貨幣や価値の表現 : 通貨 / クーポン / ポイント / チケット / オークション / 購入記録
- 権利や情報の登録 : 登記 / 遺言 / 出生 / 婚姻 / 転居 / コンテンツ権利 / 賃貸借 / 投票
- 医療記録 : 電子カルテ / 処方記録
- 認証記録 : 製造記録 / 流通過程 / 真正性認証 / 貴金属

4.1 教育分野への応用

前述した情報の管理形態とブロックチェーンの特徴を活用したものとして、以下のような応用が考えられる. いずれも電子署名によるデータの真正性、第三者による検証と透明性、悪意のあるユーザによる改ざん耐性が必要となるデータである.

- 単位取得記録
- 卒業証明書 / 学位証明書 / 成績証明書
- 教員免許

例えば、単位取得記録などは、各大学のコンソーシアムでの単位互換制度、技術資格の取得、インターンシップ、ボランティア活動などを単位認定の対象とする仕組みが存在している.

これらの成果記録をスマートコントラクトで記述を行い、ブロックチェーンネットワークに分散させる事により、低廉なコストでどこからもアクセスが可能となる.

各単位認定機関同士の単位交換と認定に係る業務が署名、単位証明された上で全て自動化できる可能性がある.

また、卒業証明などの発行、証明業務が自動化される事により、証明書発行の業務やシステムは不要となり、各企業や卒業生が必要に応じ証明書を参照する事などが可能になる.

このようにブロックチェーン技術は、単に暗号通貨の流通、価値の保持だけで無く、教育分野においても応用を期待できるであろう.

教育ブロックチェーンの実現は、学校教育だけで無く、生涯教育や遠隔教育など、社会においても重要な基盤となりえる.

我が国における、早期整備と活用について今後に期待したい.

参考文献

(1) Satoshi Nakamoto : Bitcoin: A Peer-to-Peer Electronic Cash System（2008）
https://bitcoin.org/bitcoin.pdf
(2) Seth Gilbert, Nancy Lynch : Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services（2002）
https://www.comp.nus.edu.sg/~gilbert/pubs/BrewersConjecture-SigAct.pdf
(3) Adam Back : Hashcash - A Denial of Service Counter-Measure （2002）
http://www.hashcash.org/papers/hashcash.pdf
(4) LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE : The Byzantine Generals Problem（1982）ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, pp. 382-401
(5) ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER
http://gavwood.com/paper.pdf
(6) Nick Szabo : The Idea of Smart Contracts （1997）
http://szabo.best.vwh.net/smart_contracts_idea.html