IoT 機器連携のための暗号通貨交換システム

○島田貴矢　時間浩彰　大谷雅之（近畿大学）

cryptocurrency exchange system for IoT equipment cooperation

* T. Shimada, H. Tokima, and M. Otani (Kindai University)

Abstract－ When linking IoT devices, it is expected to use cryptocurrency so that IoT devices can freely cooperate without authentication. When the cryptocurrency is different by the IoT device, the trouble of management and exchange of the currency owned by the user becomes a problem. In this research, we construct a cryptocurrency exchange system to realize highly convenient IoT device linkage. The system to be constructed has the following two functions. (i) The function of having a cryptocurrency exchange list, selecting a suitable exchange and converting the sent cryptocurrency to the cryptocurrency of the destination device. (ii) In the currency exchange network, the function to calculate the route with the least exchange loss of the cryptographic currency. We conducted experiments by simulation environment and actual currency exchange, and verified the validity of the proposed system.

Key Words: cryptocurrency, optimal route, IoT

1　はじめに

近年，IoT 技術が注目されており，電化製品の遠隔操作や，自動車の自動運転システムなど，幅広い分野で利用されている．これらは，IoT デバイス(以下デバイス)が互いに連携するために，各デバイスが独立に動作しながらも，他のデバイスと連携可能な状態となっている．これらのデバイスが誰でも自由に連携できるよう設定されている場合は，悪質なユーザのデバイスと接続し情報を不正に取得されることや，乗っ取られる場合がある．実例として，「Mirai」に感染した IoT 機器が増え続け，それらを使った大規模な DDoS 攻撃により，GitHub や Twitter などの大手ウェブサイトがダウンしたこと [1]などがあげられる．その他にも，様々な手段を用いて DDoS 攻撃を行うために遠隔操作されるという事例が多くある．一方で，認可済みデバイスのみ接続を許可する設定では，接続先の情報やデバイスによって異なる認証鍵をデバイスへインストールする必要があり，時間や手間を要する．

このような問題に対し，認証なしで IoT デバイスを自由に連携できるよう，ブロックチェーン技術を用いる暗号通貨の利用が注目されている．ブロックチェーン技術は，誰でも参加することでき，すべての参加者がシステムの機能を担う P2P 機能を利用しているため，中央管理者を必要とすることなくシステムを維持することができるだけでなく，取引の履歴が公開されおり，改ざんすることができない [2]．これらの技術により，ブロックチェーンでは取引全体の安全性かつ透明性を保証することができる．

IoT デバイス同士の連携に暗号通貨を導入する場合，利用している暗号通貨が異なるデバイス同士は連携できないという問題がある．これらのデバイス同士を連携するには，暗号通貨を取引所などで交換し，利用する必要がある．暗号通貨取引所ではプログラムなどから取引するための API があるため，自動的に交換するプログラムを書くことが可能である．しかし，取引所ごとに交換時の手数料や価格に差がある場合に交換差損が発生することがある．一方，暗号通貨の交換差損を低減するための方法として，アービトラージ（裁定取引）戦略がある．アービトラージは，株式や有価証券・為替市場などで行われている取引戦略で，ある銘柄が異なる市場で異なる価格で販売されている場合に，価格の安い方で購入し，高い方で売るということを同時に実行することで差益を得る手法である．アービトラージは暗号通貨市場においても利用されているが，暗号通貨では，2 通貨間で直接交換する場合を対象にしていることが多く，3 通貨以上の通貨を経る交換について考慮する例は少ない．

そこで，本研究では，利便性の高い IoT システムを実現するため，ユーザの所有する暗号通貨に依存せずに動作する IoT システムの開発を目指す. そのために，暗号通貨取引所リストを有し, 適した取引所を選択し，送付された暗号通貨を送付先の機器の暗号通貨に変換するシステムと，暗号通貨間の取引をネットワークと捉え，ネットワーク最適化手法を用いて差損を最小化する通貨交換経路を算出するシステムの開発を行う．

2　関連研究・前提知識

暗号通貨を用いた IoT システムの連携の先行研究として, Ethereum を利用した例がある [3]. この研究では，占有グリッドマップの分散管理を Ethereum のプライベートネットワークでのブロックチェーンを用いて実現する方式を提案している．実験として，ユーザ定義のプログラム（コントラクト）を実行し，操作の応答時間について計測が行われている．結果としては，ブロックチェーンでは，トランザクションがブロックに取り込まれて検証されるまで確定しないため，リアルタイム処理には適さないとしている．

また, IOTA を利用した例では, 電気自律走行車の充電に IOTA と MQTT と GPS を利用する方法が提案されている [4]．現環境では IOTA のプラットフォームが未発達であるため，実現することは困難であるとしているが, IOTA が発展すると, 現在のミクロ経済に革命をもたらす可能性があるとしている．これらの通貨だけでなく，その他の通貨を利用したシステムやサービスの構築も進んでいる．このことから，暗号通貨を用いて多種類の IoT デバイスの制御やシステムを利用するには，それらに対応した暗号通貨を所持しなければ

ならないため，管理が容易ではなくなることが予想される．そのため，暗号通貨の管理を容易にし，利便性を高めるため，所持する暗号通貨を送付先の機器に対応する暗号通貨に変換するシステムが求められている．

しかしながら，暗号通貨交換においては，取引所間の送金手数料や通貨交換における手数料などが発生するため，一般に交換すればするほど差損が発生するという問題がある．これを軽減する方法として，株式や有価証券・為替市場などで利用されているアービトラージ戦略がある．アービトラージは，価格の安い方で買い，高い方で売るということを同時に行う手法だが，暗号通貨のように多数の取引所があり，その間の価格差が発生しやすい問題では，利益が得やすいというメリットがある．逆にデメリットとしては，暗号通貨市場はボラティティ(価格の変動率)が大きく，価格差が予想しにくいという点や，交換している間に価格変動が起こるなどの問題がある．そこで本研究は，1 つの取引所で通貨交換を行うために 3 通貨以上で行い，仮想通貨交換における差損を低減するシステムの構築を行う．

3　実装システム

3.1 暗号通貨交換システムと送金システム

送付された暗号通貨を送付先の機器の暗号通貨に変換するために，各取引所で公開されている取引用APIを利用する．しかし，各取引所によって，同じ動作をさせる場合であっても，動作する関数名や与える引数異なる．そのため，それらを共通化する共通APIを作成し，そのライブラリを作成する．そして，板情報を用いて，交換後に得られる通貨量を計算によって求めるシミュレーションシステム，実際に通貨交換を成行注文により行うシステム，実際に交換後の通貨を送金するシステムの3つを開発する．これらを開発することで，所有する暗号通貨を容易に変換し利用することが可能になると考える．

本研究で実装する暗号通貨交換システムで利用する取引所はBinance，Zaif，OKExの3つとし，取り扱う通貨は基軸通貨を含めた4種類とする．共通化する取引所の名称と取り扱う暗号通貨一覧を Table 1に示す．交換対象の通貨はETH(Ethereum)とし，これを利用してIoTデバイスを制御するものとする．これは，Ethereumは分散アプリケーションプラットフォームとして発展しており，IoTデバイスの制御が容易であるためである．

これら3つの取引所が公開，または推奨するJavaでのAPI[1][2][3]の板情報を取得する関数，成行注文を行う関数，送金を行う関数の3つを共通化する．そして，これらの機能をスマートフォンなどの機器で動作可能とするために，Web上で実行することができるように実装する．そのために，作成したJavaプログラムをJarファイルにまとめ，Node.jsでのexec関数で実行するように設計し，htmlファイルと組み合わせる．

Table 1 cryptocurrency list

Exchanges	Binance	Zaif	OKEx
cryptocurrency1	BTC	BTC	BTC
cryptocurrency2	ETH	ETH	ETH
cryptocurrency3	BNB	XEM	OKB
cryptocurrency4	IOTA	JPY	IOTA

3.2 最適な暗号通貨経路の導出

本研究では，暗号通貨取引を，暗号通貨をノード，暗号通貨間の交換比率を重みと見なした，重み付き有向グラフと定義する．暗号通貨の交換差損を最小化するためには，このグラフの最大経路を求める必要がある．暗号通貨取引においては，経路の長さは，各辺の重みの積算である．最大経路や最小経路を求める問題においては，重みを経路長とみなし，その和を経路長とすることから，そのままでは経路探索のための手法を利用できない．そのため，本研究では，各辺の重みを対数に変換することで，重みの積算を和算として扱えるようにした．また，最大経路を求める問題は，逆に言えば，各辺の重みの符号を逆にして，最小経路を求める問題であると言える．元の重みが正の場合，負の値になるため，各辺の重みが負の場合でも利用できる最短経路計算アルゴリズムが必要になる．そこで，本研究では，グラフの最短経路探索手法として，ベルマン・フォード法 [3]に着目した．ベルマン・フォード法は，元々重み付き有向グラフにおける単一始点の最短経路を解くためのアルゴリズムである．ベルマン・フォード法は，閉路がないグラフであれば，負の重みをもつ経路も取り扱える手法である．そこで，閉路を持たない仮想通貨グラフを対象として，ベルマン・フォード法を用いて最大経路を探索することにした．

そこで，１つの取引所の取引データを利用し，ベルマン・フォード法と全探索法のそれぞれの手法で最大経路を算出する．全探索法はベルマン・フォード法と比べるために比較する．具体的には，暗号通貨取引所の一つである Binance の取引データを用いて，ETH，IOTA，および Binance の基軸通貨である，BTC と BNB の４種類の暗号通貨間の交換最適化を行う．この４種類の通貨はそれぞれに通貨交換を行っている．Fig.1 に Binance の 4 通貨の交換グラフを示す．

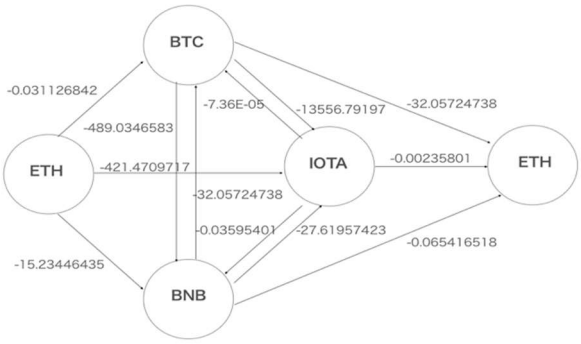

Fig. 1: Cryptocurrency exchange graph (Binance)

[1] Binance の JavaAPI: https://github.com/binance-exchange/binance-java-api

[2] Zaif の JavaAPI: https://github.com/nyatla/JZaif

[3] OKEx の JavaAPI: https://github.com/okcoin-okex/open-api-v3-sdk/tree/master/okex-java-sdk-api

本研究では，プログラムで実装する前に，ベルマン・フォード法を使用し，交換差損が最小化されるのか手計算で確認を行う．確認方法としては，取引所の Binance である時間の ETH，IOTA，BTC，BNB のそれぞれの値を取得し，手数料を含めて計算を行い，交換差損が低減するのか確認を行う．取引所一つでは確認が足りないため，Zaif でも確認を行う．Zaif では，BTC，JPY，XEM，MONA の 4 通貨を使い，Binance と同様に計算を行い，確認を行う．Fig. 2 は Zaif での 4 通貨間の交換グラフを示す．2 つの取引所でベルマン・フォード法の確認を行った後，Fig. 1 の Binance で公開している Java での API の板情報を取得し，ベルマン-フォード法と全探索法の 2 種類のアルゴリズムをそれぞれプログラムとして実装する．

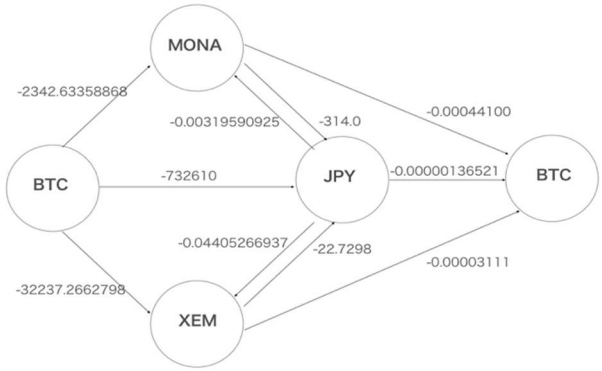

Fig. 2: Cryptocurrency exchange graph (Zaif)

4 結果・考察

4.1 通貨交換シミュレーション

通貨変換シミュレーションシステムの実行結果を Fig. 3 に示す．

Fig. 3: Simulation of currency exchange.

Fig. 3 は交換元暗号通貨を XEM，変換に利用する暗号通貨を Zaif，変換元暗号通貨量を 100 として実行した結果を示す．変換後に得られる ETH 量と手数料のみでなく，交換の際に経由する BTC に変換する際に得られる BTC 量と手数料を表示した．この結果から，本シミュレーションを用いることで，実際に交換すると得ることができる ETH の量を容易に予測することが可能である．これにより，次節で述べる成行注文を行うシステムを利用する際に入力する交換元通貨量の目処を立てやすくする．

4.2 成行注文による通貨交換システム

実際に成行注文を行うシステムを，交換元通貨を XEM，交換に利用する取引所を Zaif，交換に利用する XEM の量を 100 として実行した．動作前のウォレットを Fig. 4，動作後のウォレットを Fig. 5 に示す．

BTC	0.00343575
XEM	100.788
MONA	0
ETH	0.000078

Fig. 4: Before currency exchange Wallet.

BTC	0.00343765
XEM	0.788
MONA	0
ETH	0.0381399

Fig. 5: After currency exchange Wallet.

Zaif での XEM は一度の交換で ETH にすることは不可能であるため，BTC を経由して ETH に変換している．本システムと同時に 4.1 節で示したシステムを動作させたが，本システムでは 0.0380619 を取得しているが，4.1 節でのシステムでは 0.0381229 となり，0.000061 の誤差が生じた．この誤差は，BTC から ETH に変換する際，少数第 5 位以下の値は取引で利用することができないことが原因である．以上のことから，本システムを利用することで，シミュレーションシステムと多少の誤差が生じるが，容易に通貨交換を行うことを可能にした．

4.3 送金システム

送金システムを利用し，Binance から Metamask のアドレスに 0.1ETH 送金するシステムを動作させた．動作後の Binance の送金履歴を Fig. 6，受け取り後の Metamask のウォレットを Fig. 7 に示す．

Completed	ETH	0.09

Fig. 6: Binance's withdraw history.

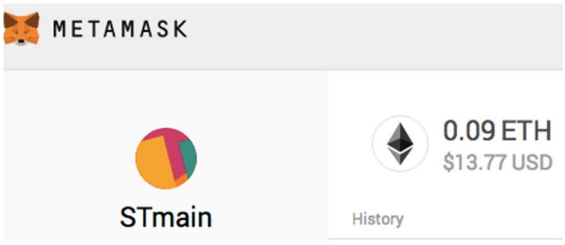

Fig. 7: Metamask's wallet after receiving.

送金したい量を 0.1ETH としたが，実際に送金できたのは 0.09ETH である．この誤差が生じた理由は，送金額から手数料である 0.01ETH を引いて送金しているためであると考えられる．Zaif と OKEx では，総金額からではなく，送金側のウォレットから手数料が引かれた．このことから，取引所によって，発生する手数料を引く部分が異なると考えられる．そのため，API を共通化させるだけでなく，それぞれの取引 API 以外の特徴も考慮し，制御する必要がある．

以上のことから，送金 API を共通化するだけでは全ての取引所で正確な量を送金することは達成できなかったが，容易に送金を行うことができた．4.2 節と本節の結果から，これらを組み合わせたシステムの実装によって，所持する暗号通貨を提案システムに支払うことで，自動で送付先に適した通貨の種類に変換し，支払いを完了することが可能になると考えられる．これは，暗号通貨で制御可能なデバイスを多種類制御する場合であっても，所持する暗号通貨に縛られることなく，容易に制御を可能にするため，利便性の高いシステムであるといえる．

4.4 暗号通貨経路探索の分析

プログラム実装前に，2 つの取引所から通貨交換の値，手数料を取得し，ベルマン・フォード法で手計算を行い，交換差損の低減を確認した．その後，ベルマン・フォード法を実装し，全探索法との分析を行った．その結果を Table 2 に示す．Excecution time はプログラム実行を 10 回行い実行時間の平均時間を比較したものである．全探索法の場合はすべての経路で計算するため，実行時間に差が出た．また，path は 1 回実行することに，通るパス数である．全探索法のパス数はすべてのパスを見るため，ベルマン・フォード法に比べるとパス数が多くなる．この分析から，全探索法よりもベルマン・フォード法が適していると考える．

Table 2 Result of analysis

	Execution time	path
Full search algorithm	2118.73214ms	14
Bellman-Ford algorithm	729.140134ms	12

また，暗号通貨価格の分析として Zaif の取引所から通貨取引の値の最小値，最大値，平均値それぞれ 24 時間計測を行った．時間計測した理由として，暗号通貨の価格は時間ごとに変動するため，交換する際に変動した価格で交換する可能性がある．そのため，24 時間の計測を行った．計測したところ，取引所の値は最小値，最大値ともに大きく変動することはなく，暗号通貨価格が安定していると考えられる．しかし，頻度は少なくても価格変動は起こっているため，シミュレーションと同じ結果にならない可能性がある．その結果を Table 3 に示す．

以上から，4 種類の暗号通貨を使い経路探索アルゴリズムのベルマン・フォード法で計算を行い，複数の通貨交換をすることで，交換差損が低減できた．

Table 3 Currency Trading

	MIN	MAX	AVERAGE
BTC→JPY	699000	699295	699170
BTC→MONA	5934.07186813780	5934.0718681378	5934.0718681378
BTC→XEM	68518.5870371056	68518.5870371056	68518.5870371054
JPY→BTC	0.0000014300	0.0000014306	0.0000014301
JPY→MONA	0.0088407168	0.0089196518	0.0088551197
JPY→XEM	0.0987252692	0.0988121779	0.0987412952
MONA→BTC	0.0001542300	0.0001542300	0.0001542300
MONA→JPY	110.5000000000	111.2000000000	111.1519607843
XEM→BTC	0.0000145000	0.0000145000	0.0000145000
XEM→JPY	10.1100000000	10.1101000000	10.1100421569

5 おわりに

実装したシステムを利用することで，通貨交換を行うと得られる通貨量の予測と通貨の交換，そして，送金を容易に行うことを可能にした．これらのシステムを組み合わせることで，自動で送付先の IoT デバイスに適した暗号通貨に交換差損を最小にしながら変換し，利用対象の IoT デバイスへの支払いを実現できると考える．しかし，実際に通貨交換を行うシステムと送金システムでは期待した量の結果を得ることができない事例が発生する可能性がある．そのため，いかなる状況であっても，期待する結果を得ることができるシステムを開発することが必要となる．さらに，利用することができる取引所と暗号通貨を拡張することを今後の課題とする．

また，暗号通貨の交換差損を低減するための経路探索アルゴリズムとしてベルマン・フォード法を実装し，交換差損が低減されることを可能にした．暗号通貨の交換差損を低減するための経路探索アルゴリズムはシミュレーションのみで評価しており，実際の通貨交換で実験を行っていない．そのため，最適な経路を求めても，交換の時に通貨の値が変動する可能性があるため，通貨交換の時間を考慮し，シミュレーション通りに交換差損が低減するシステムを開発することを今後の課題とする．

参考文献

1) 情報界のトピックス，情報管理，巻(**59**), 4 号, p.645-646, doi: https://doi.org/10.1241/johokanri.59.645, 2016 (参照 2019-01-26).
2) 野口悠紀雄．「ブロックチェーン革命 － 分散自律型社会の出現」．日本経済新聞出版社. pp.21-23. 2017.
3) 渡辺陽介．「ブロックチェーン技術を用いた占有グリッドマップの分散サービス化」. DEIM Forum 2018, 2018.
4) Strugar, D. Hussain, R. Mazzara, M. Rivera, V. “M2M Billing for Electric Autonomous Vehicles”. arXiv:1804.00658, 2 Apr 2018.
5) Dimitri P. Bertsekas, “A Simple and Fast Label Correcting Algorithm for Shortest Paths”. Networks. Vol.23, pp.703-709. 1993