2018 年度未踏ターゲット事業

アニーリングを用いた

ブロックチェーンの高速化技術の開発

1. 背景

現在のビットコインブロックチェーンはスケーラビリティの問題に直面している。このスケーラビリティの問題によってビットコインブロックチェーンは実社会の求める取引ニーズに対応できていない。

例えば、クレジットカード会社である VISA の取引処理数は約 4000 件(毎秒)と言われているのに対して、ビットコインの取引処理数は約 7 件(毎秒)である。

上記のようなスケーラビリティ問題の解決策として提示されたのがオフチェーン技術である。このオフチェーン技術を利用したネットワークの１つが Lightning Network である(以降 LN)。

2. 目的

アニーリングマシンを使うことで、より効率的に LN の経路探索を行える手法を開発する。

3. ソフトウェア開発内容

アニーリングマシンによって LN のトランザクションの経路探索を行うための手法を開発した。開発した手法は二段階に分かれている。最初に各トランザクションに対して経路の候補を 3 経路作成する。次にアニーリングマシンを用いてこの候補の中から最適な経路を選択する。

ここからは、アニーリングマシンを用いて最適な経路を選択する手法について説明する。まず、LN においてトランザクションの経路が満たすべき条件は以下の２つである。

⑴チャネルにはキャパシティが存在し、これ以上の金額のトランザクションが経由することができない
⑵送出したノードからコインを受け取るノードまでの経路はただ１つ

LN のネットワークに参加するユニークなコンピューターは通常ノードと呼ばれ、このノード間で送金を行うことをトランザクションと呼ぶ。このトランザクションが辿る経路が各ノード間に繋がれたチャネルである。チャネルが扱える取引数量がキャパシティである。

チャネルを通過できるトランザクションの総量は双方向の支払いチャネルの作成時に定められ、この総量を超えての送金は行えない。

また、トランザクションは始点から終点まで 1 つのルートのみしか辿ることができない。トランザクションの経路探索をアニーリングマシンによって行うため、以上の 2 つの制約を、二値変数 xを用いて定式化を行ない、ハミルトニアンを作成した。ここで xはトランザクション数×候補経路数の二値行列であり、i番目のトランザクションがj番目の経路を利用するときx_{ij}=1 となり、そうでない時はx_{ij}=0 となる。

⑴の制約を以下のハミルトニアンによって表現する。
全てのチャネルに対してそのチャネルを通る容量がキャパシティよりも大きいとペナルティが発生する。また、正の整数であるキャパシティ容量を最小のビット数で表現するために対数エンコーディングを利用した。

キャパシティコストのハミルトニアン

$$H_{capacity\_cost} = \sum_{k\in C}(\sum_{s\le N_k} z_s 2^s - \sum_{i\in T}\sum_{j\in route\_list[i]} A_i x_{ij})^2$$

A_i ： i 番目のトランザクション金額

$route\_list[i]$ ： i 番目のトランザクションのルートの集合

P_k ： C 内の k 番目のチャネルのキャパシティ金額

N_k ： P_k を表現するために必要となるビット数

S ： 0から N_k までのキャパシティ金額を表現するビット数

z_s ： 二値変数

C ： チャネルの集合

T ： トランザクションの集合

⑵以下はルート制限のハミルトニアンであり、各トランザクションでは 1 つのルートのみ選択される。

ルート制限のハミルトニアン

$$H_{const} = \sum_{i \in T} (\sum_{j \in route\_list[i]} x_{ij} - 1)^2$$

T : トランザクションの集合

$route\_list[i]$: i 番目のトランザクションのルートの集合

トランザクションはノードを経由するたびに手数料が課されるので、出来るだけ短い経路が選ばれ、課される手数料を少なくすることが好まれる。トランザクションの経路の距離を短くするためのハミルトニアンを $H_{distance\_cost}$ として導入する。ここで言及したトランザクションの距離とは経由するチャネルの数を指す。

距離コストのハミルトニアン

$$H_{distance\_cost} = \sum_{i \in T} \sum_{j \in route\_list[i]} D_j x_{ij}$$

T : トランザクションの集合

$route\_list[i]$: i 番目のトランザクションのルートの集合

D_j : j 番目のルートのトランザクションの距離

キャパシティコストのハミルトニアン、ルート制限のハミルトニアン、距離コストのハミルトニアンを踏まえ、以下のハミルトニアンを生成した。

$$H = H_{capacity\_cost} + \alpha H_{distance\_cost} + \beta H_{const}$$

今回は富士通デジタルアニーラによってこれらのハミルトニアンによって定義される経路探索問題を、擬似的に生成したグラフ上でトランザクションの経路を探索する問題として解いた。グラフ構造は Python のライブラリである NetworkX2.2 を用いて生成。ノード数は 2000、チャネル数は 20000 と設定した。各チャネルのキャパシティのレンジは 200～900 とし、1 つのノードにおおよそ 15～30 ほどのチャネルがランダムに配置されるように設定した。

また、トランザクションの数は 4、各トランザクションの金額のレンジは 200～600 とした。各トランザクションには異なる 3 つのルート候補を用意した。チャネルの手数料に平均 0.1、標準偏差 1 の乱数を掛け合わせたものを手数料の重みとしたグラフにおける最短経路をダイクストラ法によって求め、これをルートの候補とした。

なお、パラメーターの α には 2 を、β にはキャパシティコストのハミルトニアンでトランザクション金額の二乗分の金額が含まれ出力が大きくなることもあり、対称性を持たせるためにトランザクション金額の平均値の二乗に 100 を掛け合わせたものをパラメーターとして設定した。

上記の経路探索問題を富士通デジタルアニーラの FujituDAPTSolver モード number_iterations1000000, number_replices100 で計算した結果、解は通信時間を含め、10 秒で得られた。

また(1),(2)の制約に加えて短い距離の経路を解として得ることができた。要したビット数は 361 ビットであった。

4. 新規性・優位性

LN のグラフを模したグラフ問題をアニーリングマシンで解くことができた。また、扱っているトランザクションの数は少ないものの、現在の LN の開発のトップランナーでもある LND という開発チームのもつネットワークの約 2 倍の規模のグラフを解く足掛かりを掴めたことで将来的な LN のルーティング問題のアニーリングマシンの応用可能性が示せた。

5. 期待されるユーザー価値と社会へのインパクト

Lightning Network の Web サイト内[1]では数百万、数十億の同時トランザクションの処理が可能とのように述べられているが、ネットワーク内でのトランザクションが活発になり特定のチャネルへのトランザクションの集中などが起こる可能性を考慮すると、トランザクションの成功確率を高めネットワークでのトランザクション件数の最大化を目指す必要がある。

将来のデータ量増加に伴って問題になると言われている LN のルーティング問題において、アニーリングマシンの応用可能性が示せたことはインパクトがあると考える。

参考文献

[1]Lightning Network 「Lightning Network 」< https://lightning.network/#intro > （最終アクセス 2019 年 3 月 1 日）

6. 氏名（所属）

藤崎勇哉（フリー）
三上功太（東京大学）
藤崎拓深（横浜国立大学）a