# ライトニング・ネットワーク
# 特徴と仕組み

2021/10/12

小川裕也
ogw_yuya

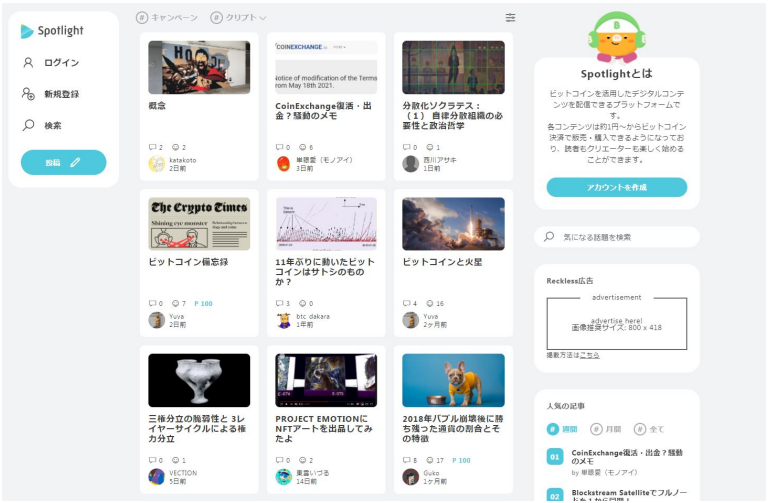
# 自己紹介

## 金融系SIer

地銀・信金向けの業務系システムやインフラ構築

## フリーのエンジニア

ビットコイン・LNのサービス開発 **spotlight.soy**

# 目次

# LNの特徴

1. LNの特徴
2. LNの仕組み
    a. ビットコインの問題
    b. ペイメントチャネル
    c. マルチホップペイメント
3. まとめ

# ライトニング・ネットワークとは

ビットコインのスケーリング問題を解決するために考案された技術
ブロックチェーンへの書き込みを抑え、オフチェーンでの取引をする

| # | 項目 | オンチェーン（ブロックチェーン） | オフチェーン（LN） |
|---|---|---|---|
| 1 | 少額決済 | 294 satoshi | 0.0001 satoshi |
| 2 | 送金速度 | 最低10分 | 数秒 |
| 3 | 処理性能 | 7件／秒 | 無限大（P2P送金） |
| 4 | 手数料 | 最低でも300 satoshi | ゼロ～ |

# ライトニング・ネットワークの指標

1. ロック金額
    - **3,000BTC**
2. ノード数
    - **20,000ノード**以上（ビットコインノードは13,000ノード）
3. 取引高
    - **10~100BTC／日**（オンチェーンは10~20万BTC／日と比べると約0.1%）
    - **数万件 ??? ／日**（オンチェーンは20~30万件／日）
4. 運用益
    - **0~5%**（送金の中継をすることで手数料を得る）

# ライトニング・ネットワークの指標

Lightning Network Explorer (acinq.co)

# ライトニング・ネットワークの活用(LApps)

少額決済、高速送金、低手数料な特徴を生かし、IoTとの連携に相性が良い

- Blockstream サテライト
  - 少額課金でデータを衛星経由で配信
- Blocksat reader
  - サテライト配信されたデータを使った掲示板
- Nemopeed
  - 少額課金で金魚に餌やり
- Lightning Crush
  - ブロック崩しゲーム。クリア報酬として1satoshiからリアルタイムで受け取れる

# LNの仕組み

1. LNの特徴
2. LNの仕組み
    a. ビットコインの問題
    b. ペイメントチャネル
    c. マルチホップペイメント
3. まとめ

# ビットコインの問題

- 送金時間が遅い（最低10分）
- 手数料が高い

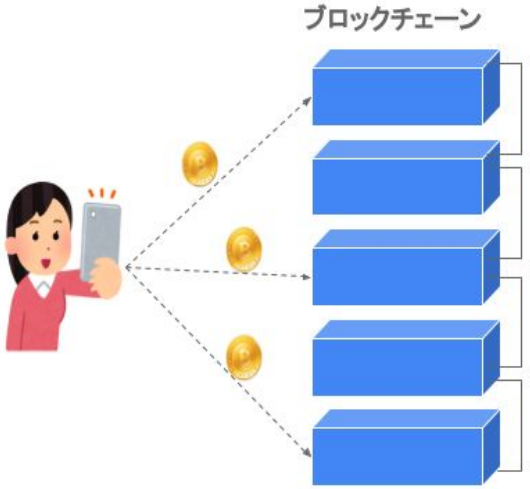
## 1. リソースが限られている

ビットコインのブロックチェーンには以下の制限がある

- 10分に1ブロックの生成
- 1ブロックのサイズは1MB

## 2. 送金ごとのデータ書き込み

- ビットコインの送金は、ブロックチェーンへのデータ書き込み
- データを書き込む際に手数料を払う



# ライトニング・ネットワーク

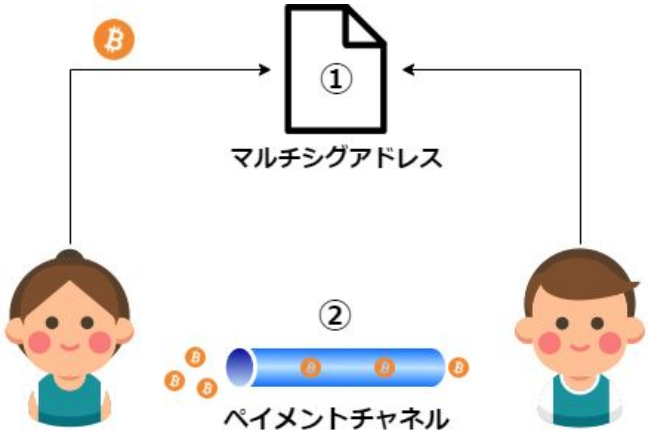
ライトニングネットワークでは、**ブロックチェーンへのデータ書き込みを極力少なくし** 、オフチェーン取引と言われる、**当事者間のみで送金データの送受信** をします。今回はLNの2つのコア技術について紹介します。

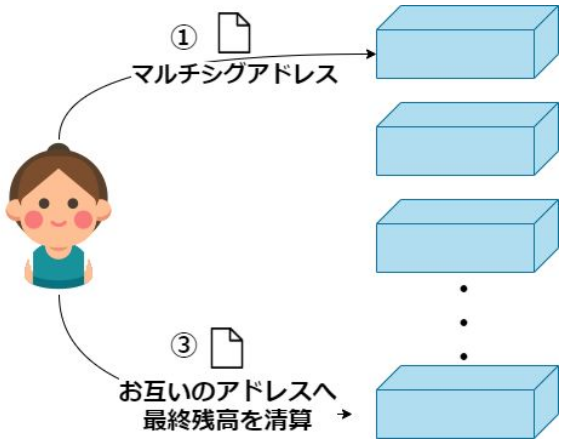
- ペイメントチャネル
- マルチホップペイメント

# ペイメントチャネル

ペイメントチャネルとは、オフチェーン取引をするために 2者間で作る台帳
この台帳は2者間でしか共有されず、送金ごとの内容はブロックチェーンへ書き込まない

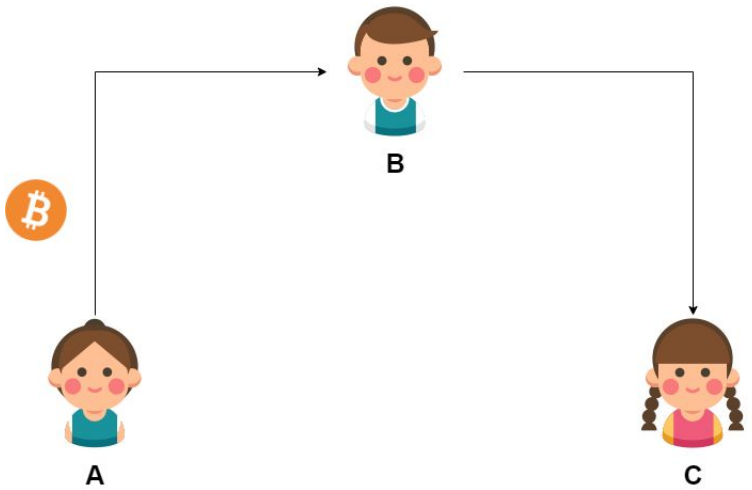
1. マルチシグアドレスを生成し、BTCを預託（ブロックチェーン書き込み）
2. 当事者間で送金（プレ署名）
   a. 送金毎に署名はするが、ブロードキャストはしない
3. マルチシグアドレスから最終残高をお互いのアドレスへ送金（ブロックチェーン書き込み）



# マルチホップペイメント

第三者へも送金をしたいけど、それぞれペイメントチャネルを作る？
中継者への信頼
トラストレスに送金を中継するための仕組みが HTLC（Hash TimeLock Contract）



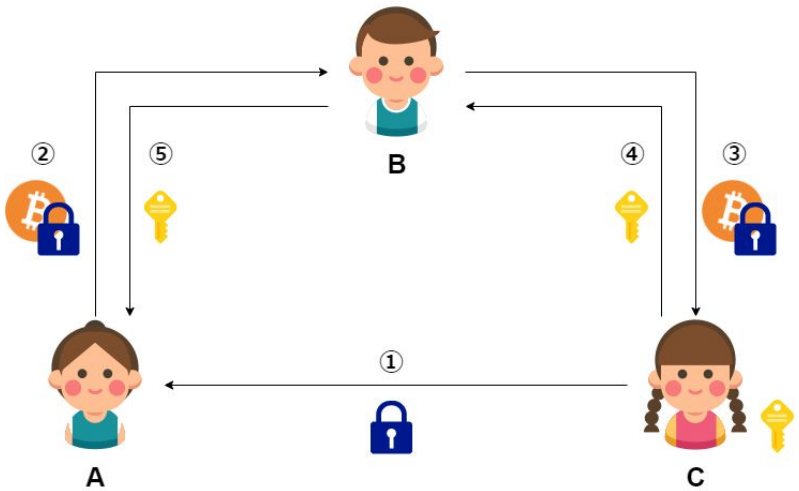

HTLCの例

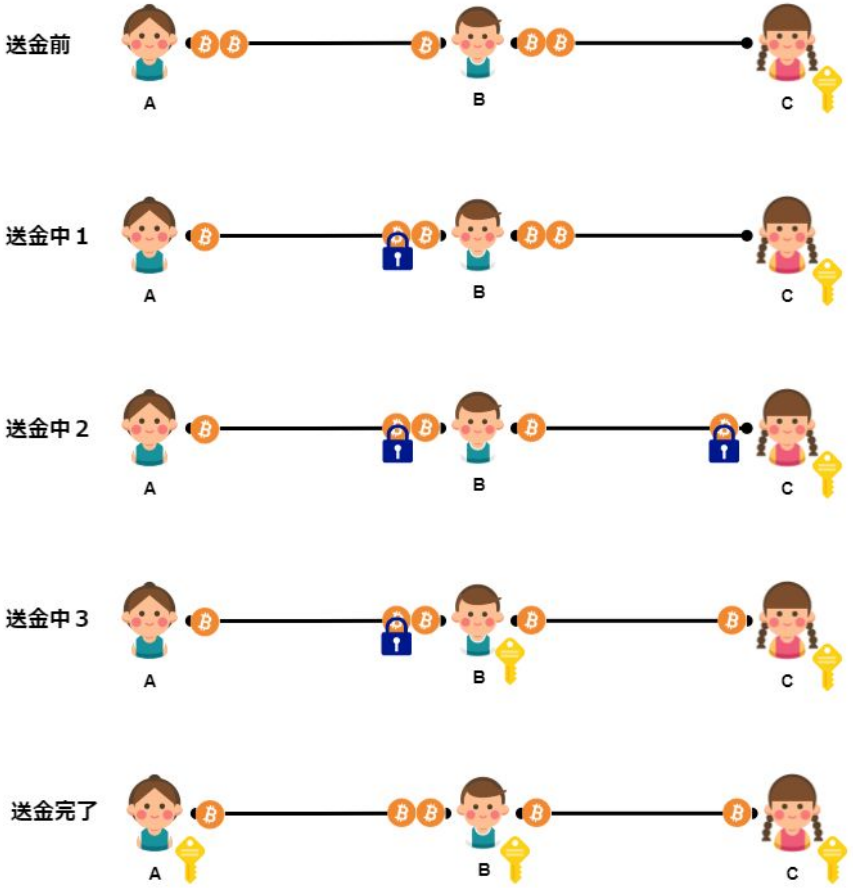
```
# To remote node with revocation key
OP_DUP OP_HASH160 <RIPEMD160(SHA256(revocationpubkey))> OP_EQUAL
OP_IF
    OP_CHECKSIG
OP_ELSE
    <remote_htlcpubkey> OP_SWAP OP_SIZE 32 OP_EQUAL
    OP_NOTIF
        # To local node via HTLC-timeout transaction (timelocked).
        OP_DROP 2 OP_SWAP <local_htlcpubkey> 2 OP_CHECKMULTISIG
    OP_ELSE
        # To remote node with preimage.
        OP_HASH160 <RIPEMD160(payment_hash)> OP_EQUALVERIFY
        OP_CHECKSIG
    OP_ENDIF
OP_ENDIF
```

lightning-rfc/03-transactions.md at master · lightningnetwork/lightning-rfc (github.com)

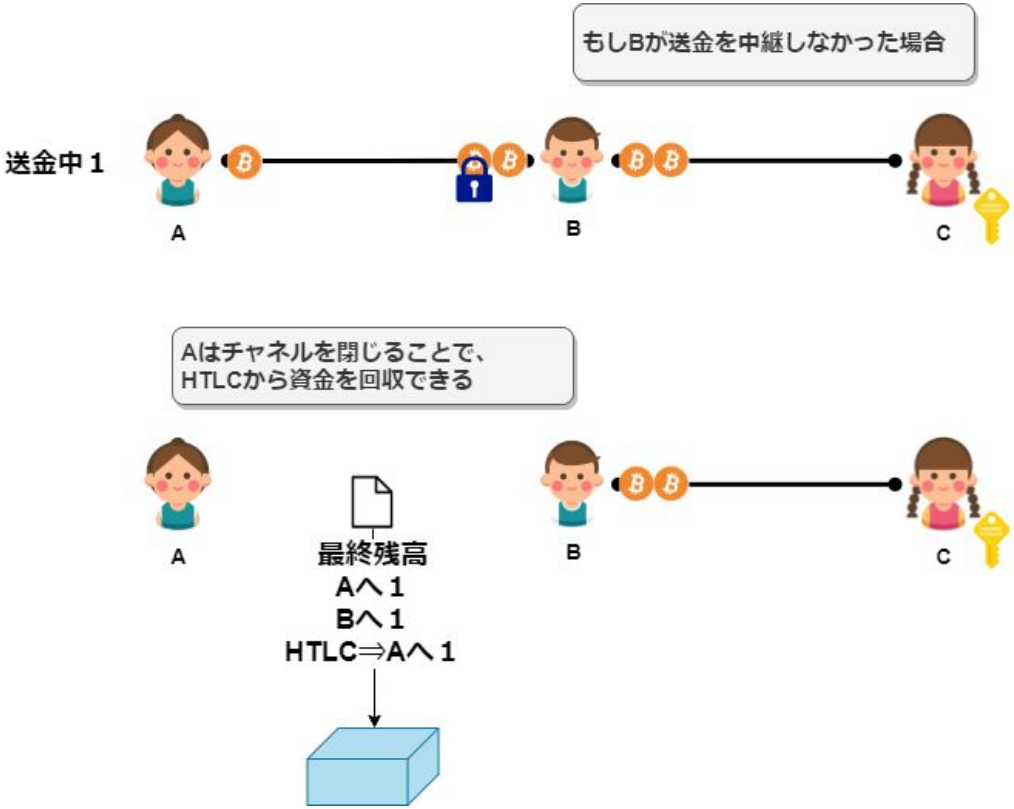
# マルチホップペイメント

1. Cは鍵とそのハッシュ値を作成して、ハッシュ値のみ Aへ送信
2. Aはそのハッシュ値でビットコインをロックした HTLCを作り、Bへ送信
3. Bも同様なHTLCを作り、Cへ送信
4. Cは鍵を使ってHTLCを解除してビットコインを受け取る
5. Bは4で受け取った鍵を使って HTLCを解除してビットコインを受け取る




送金前
A
B
C
送金中１
A
B
C
送金中２
A
B
C
送金中３
A
B
C
送金完了
A
B
C

# マルチホップペイメント



# まとめ

1. LNの特徴
2. LNの仕組み
    a. ビットコインの問題
    b. ペイメントチャネル
    c. マルチホップペイメント
3. まとめ

# まとめ

ライトニング・ネットワークはブロックチェーンへの書き込みを最低限に抑え、
オフライン取引を可能にする技術

- ペイメントチャネル
  - マルチシグとプレ署名による2者間のオフライン取引

- マルチホップペイメント
  - HTLCを使うことでトラストレスに中継者を経由してチャネル間の送金

ご視聴ありがとうございます