監査付き通信路としてのブロックチェーン

(Blockchain as an Audit-able Communication Channel)

鈴木 茂哉, 村井 純

慶應義塾大学 大学院 政策・メディア研究科

慶應義塾大学 SFC 研究所 ブロックチェーンラボ

E-mail: shigeya@wide.ad.jp

2017/7/24 @ 「ブロックチェーンの未来」ワークショップ

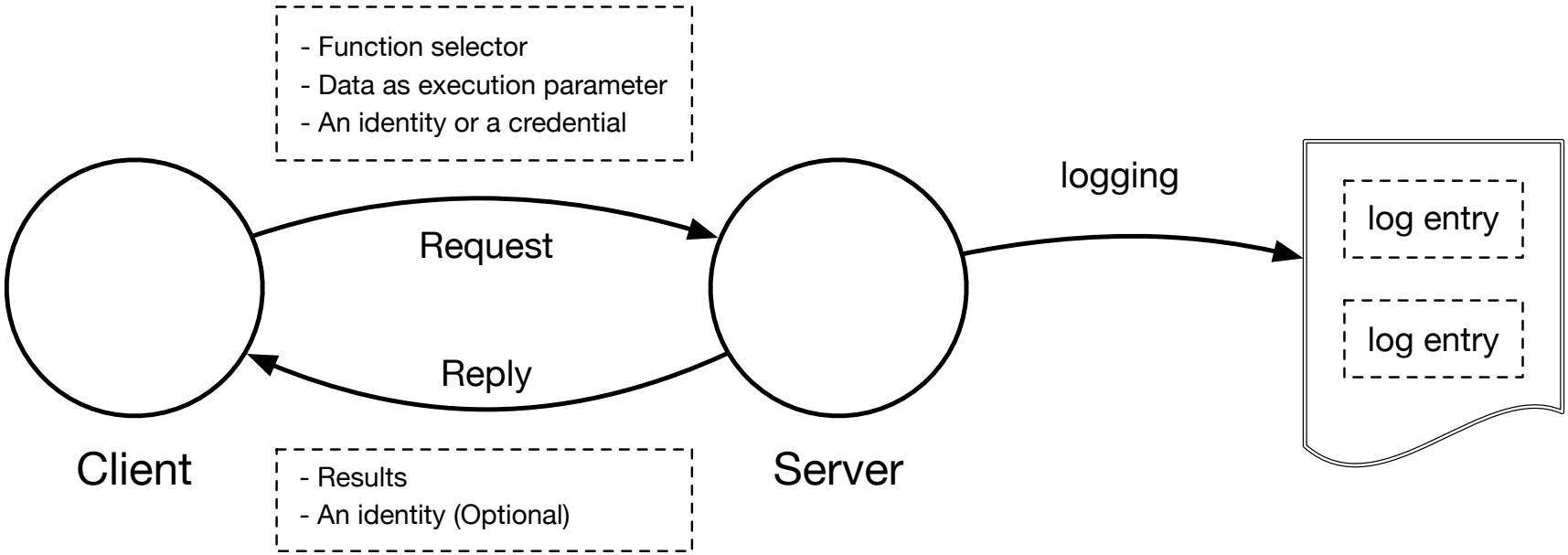
アウトライン

- ログにおける問題
- 提案方式: 監査付き通信路としてのブロックチェーン
- ビットコインブロックチェーンを用いた実装実験
- 今後の発展
- 終わりに

本プレゼンテーションは、下記ワークショップでの発表内容と同一です。詳細については論文をご参照下さい

"Blockchain as an Audit-able Communication Channel,"
Shigeya Suzuki, Jun Murai,
STPSA 2017: The 12th IEEE International COMPSAC Workshop on Security, Trust and Privacy for Software Applications, Trino, Italy, 8 July 2017

クライアント-サーバシステムとログ

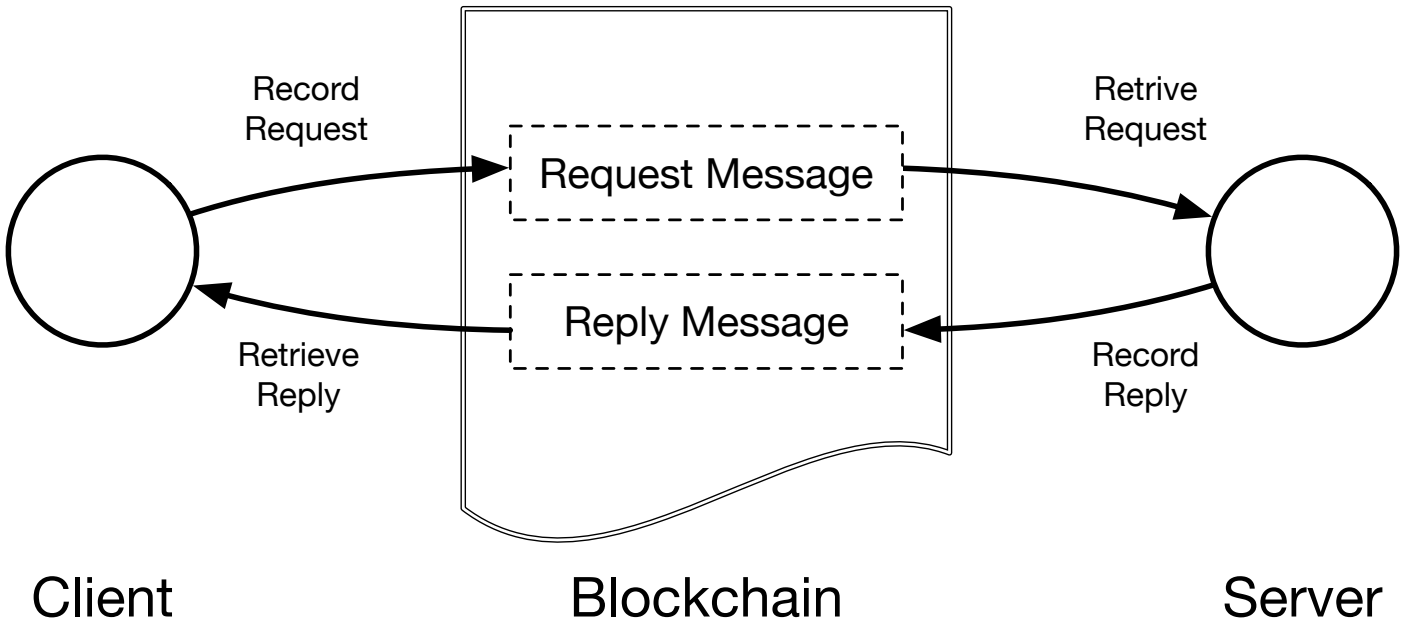


ログ取得に問題

- サーバ上に保管されたログは、以下のような事象で改変されたり、破壊されたりしうる:
  - 攻撃
  - 悪意を持った運用者
  - 運用者の操作ミス

- ログを保管するサーバ全般の問題:
  - ハードウエアの不調

提案方式:
監査付き通信路としてのブロックチェーン



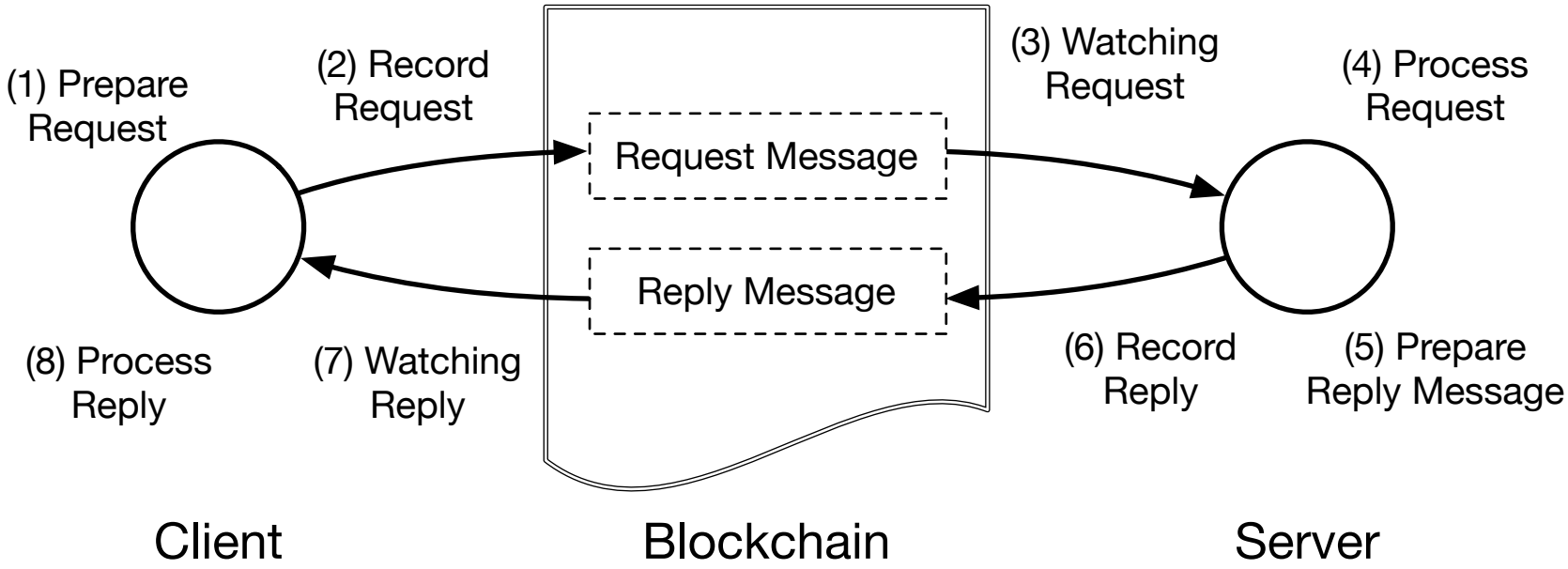
ブロックチェーン技術の通信路への活用

- チェインされたブロックそれぞれへのトランザクション記録
  - 順序づけされた「メッセージ」として
- それぞれのトランザクションに、リクエスト～リプライに必要なメッセージを格納できる
  - メッセージの「ペイロード」
- 参加ノードは、メッセージから、送信者と受信者を識別できる
  - メッセージの送信者と受信者の「アドレス」
- ブロックチェインは、監査者によってアクセス可能である。ただしこれは、公開されているかどうかは関係ない

既存ブロックチェーン技術の本方式への適用可能性

- 以下のメジャーな3種のブロックチェーン技術を適用可能:
  - Bitcoin
  - Ethereum
  - Hyperledger Fabric

提案方式におけるメッセージのやりとり



提案方式の特性

- 可用性が高く、改変に強い、確認可能な監査ログ
- ネットワーク上の位置という視点で、視認性が低い

実装による概念実証

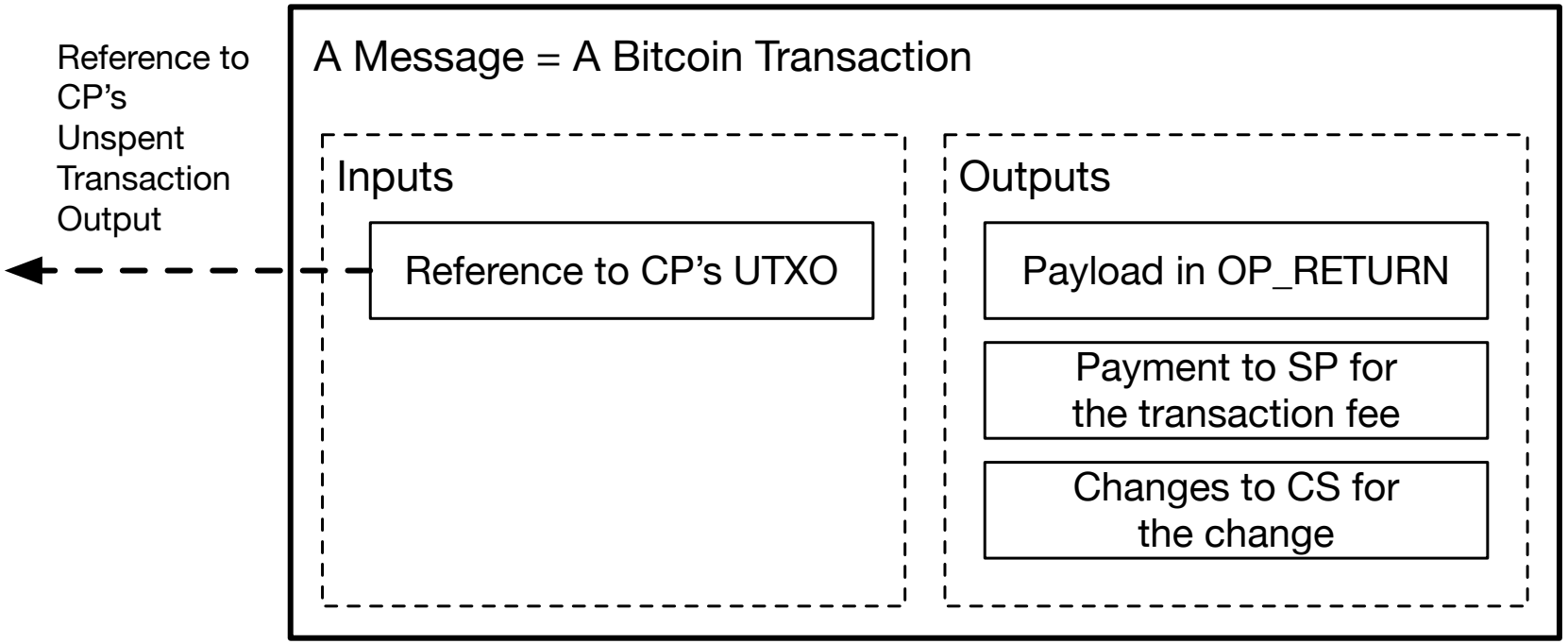
- Bitcoinブロックチェーン上に実装
- TestNet3 テストネットワークを活用してテスト

- Bitcoin アドレスを、送信元・送信先識別子として利用
- トランザクションをメッセージとして用いる
  - トランザクションの支払者を送信者、受取人を送信先とする
- OP_RETURN スクリプトオペコードをペイロードとして用いる

OP_RETURN

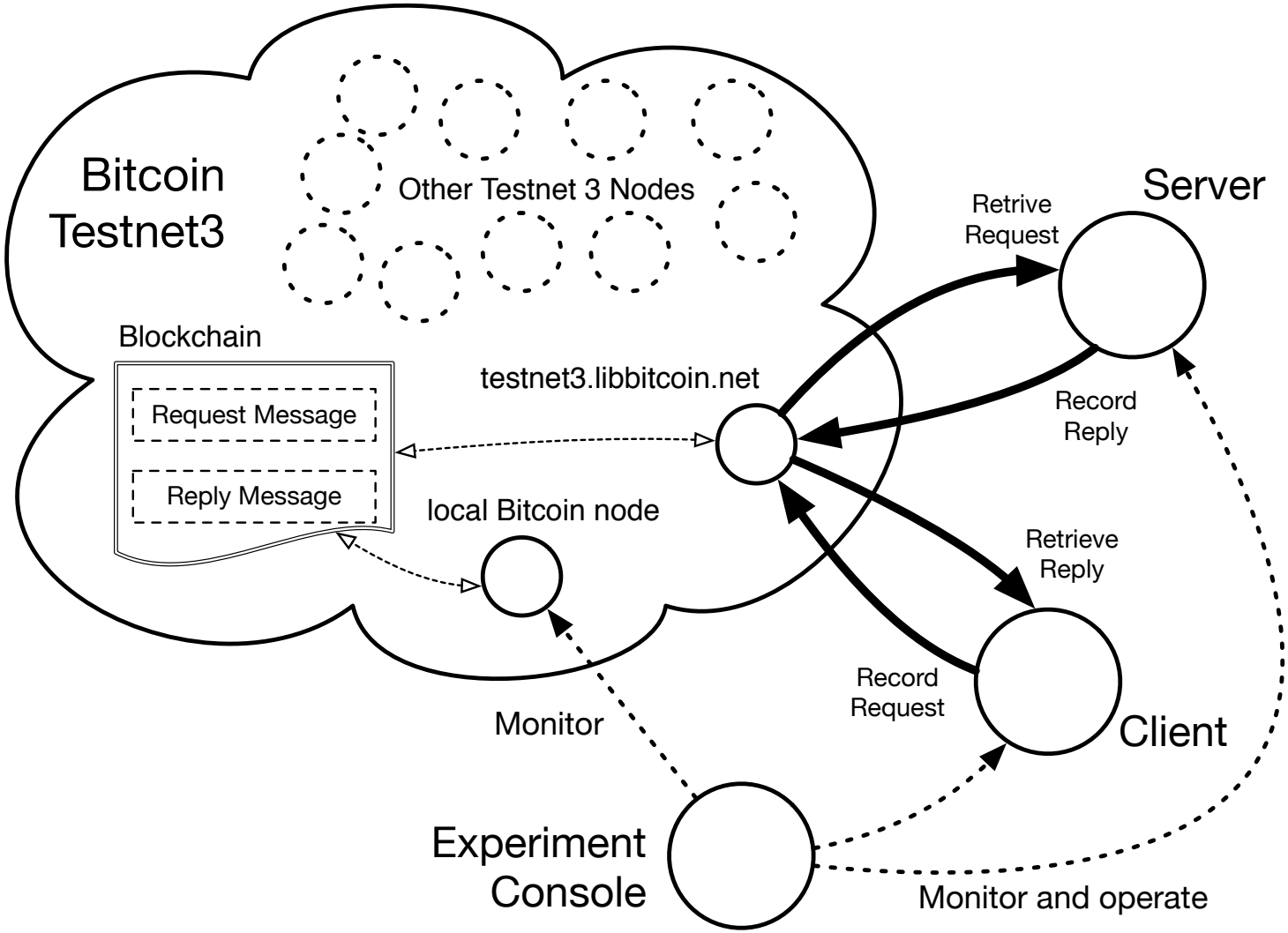
- OP_RETURN スクリプトオペコードを用いると、アウトプットの一つとして、40バイトまでのデータをトランザクションに埋め込める

トランザクションの例



CP = Client Primary Bitcoin Address
CS = Client Secondary Bitcoin Address
SP = Server Primary Bitcoin Address

実験環境



実験結果

- 本方式は、期待通りに動作した

- 一方、Testnet3 がトランザクション展性攻撃の対象となっているため、実験の質を保てていない
  - Transaction ID が変わってしまう
  - ただ、トランザクションは問題無く完了するので、Transaction ID をアテにしない限りは問題なし

- 問題点:
  - メッセージの遅延
  - コスト

評価: メッセージ遅延

- リクエストがBitcoin Blockchainのブロックとなるのに、720 秒 (12 分) かかっている
- リプライがBitcoin Blockchainのブロックとなるのに、 2265秒 (37分45秒) かかっている
- リクエストが入っているブロックと、リプライが入っているブロックの間には一個のブロックが間に入っている

Block Time	Monitor Time	Event
15:59:19 (0)	-	Request Message sent to the network (Transaction ID: 77d15a0b869402e6eacc68ef4df0464bf6f3fd0bc59e5b7ba097bb0b24ce2faa)
16:11:19 (720)	16:11:19 (0)	Request Message confirmation on the block #1119495
16:11:20 (1)	-	Reply Message sent to the network (Transaction ID: bee3f93c0f73eb8ade0c5b4c310d1ba3f06a0ff64357396462794d6d4fc23a8d)
16:49:10 (2265)	16:49:48 (38)	Reply Message confirmation on the block #1119497

評価:コスト

- トランザクションのためのコストとして、コストパフォーマンスを勘案すると、実験時点では 31160 statoshis/メッセージのコストがかかっていた (実験時点では だいたい 0.45USD)
- 7月上旬の時点では、メッセージあたりのコストは倍増し、かつ、Bitcoinの対ドルレートがほぼ倍になっているため、だいたい2USD程度必要となっている

- このコストを許容出来るような用途以外には高すぎる

今後の課題

- 本方式について、もっと詳しく検討する
- Ligtning Networkなどの技術の適用
- 本方式に向いたブロックチェーン自身の開発
- アプリケーションへの応用:
  - 健康情報の保管・取得への活用
  - RFID情報システムへの適用
  - 等

おわりに

- ブロックチェーンを、監査記録のために通信チャネルとして用いる方法を提案

- 概念実証をBitcoinブロックチェーンを用い、動作確認できた
- 二つの問題点: 遅延とコスト
- 遅延を許容するのであれば、適用は可能
- 遅延を緩和する、あるいは、コスト削減のために、本方式で活用しやすいブロックチェーンを開発することもオプション
- これらの問題が解決される前提だが、適用範囲は広い