大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

トップエスイー ソフトウェア開発実践演習

ビザンチン故障検出器を用いたブロックチェーンシステムのアカウンタビリティの強化

NEC ソリューションイノベータ　堀口 直也

ブロックチェーンの課題

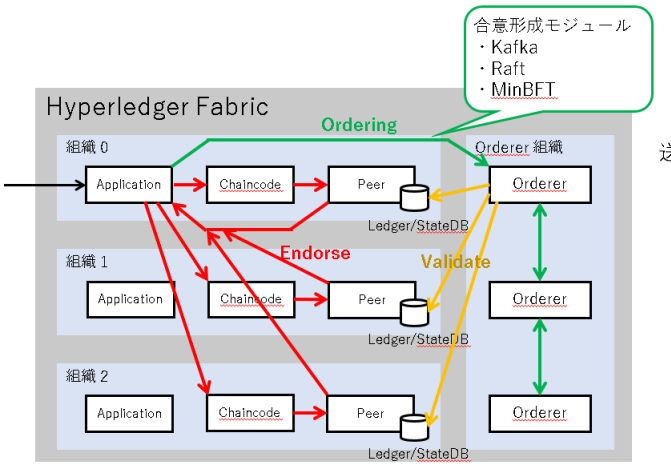
ビザンチン故障耐性を持つ合意形成アルゴリズムは，コンソーシアム型のブロックチェーン基盤への適用が期待されているが，実際に参加ノードにビザンチン故障が発生したときに，その原因や故障箇所の特定が困難でアカウンタビリティに欠けるという課題があった．

提案する解決策

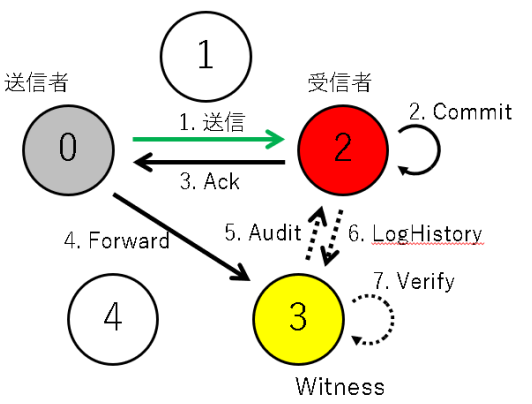
アプリケーション非依存で eventually strong completeness と eventually strong accuracy を持つ故障検出アルゴリズム PeerReview を適用することで，合意形成アルゴリズムにアカウンタビリティを付与する．

課題・提案手法の概要

- ブロックチェーン＝分散台帳技術＝改ざん耐性を持ち，非中央集権的な分散トランザクション処理基盤
- 現状，合意形成が成立していさえすれば処理に支障がないとして，ビザンチン故障は無視される．
- 実運用では障害発生時に責任の所在を明確にすることが重要で，故障検出器により，正常ノード間で検証できる形でビザンチン故障を検出可能
- MinBFT上にPeerReviewを実装して評価した．



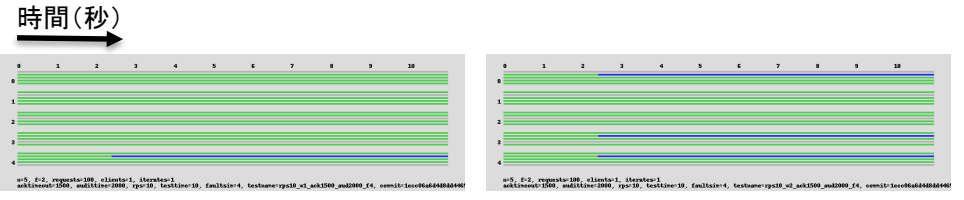
Hyperledger Fabric の合意形成



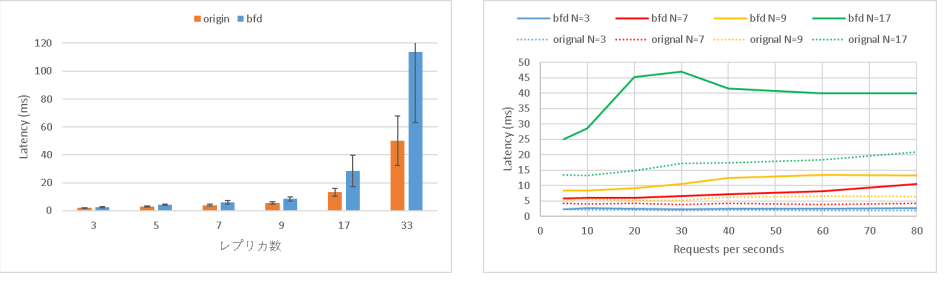
PeerReviewの正常系処理

評価結果と結論

- 故障検出器により，複数ノードが共謀するようなビザンチン故障のケースを検出できるようになる．
- 従来のノード間メッセージに加えて故障検出用のメッセージが増え，オーバーヘッドは増大する．
  - クラスタサイズに応じて遅延が 10%-120% ほど増大
  - クラスタがタイムリーにさばける秒間リクエスト数は下がる(N=17だと40→20)
- Hyperledger Fabric の典型的な設定では Ordering に投げられるブロックの合意形成要求はせいぜい数RPSのため，故障検出器が利用可能な範囲に抑えることが可能である．



共謀がある場合のビザンチン故障の検出例．
ノード0, 1が共謀してノード4を選択的に無視する場合，witnessが1ノード（左図）だと故障をうまく検出できないが，2ノード（右図）にすると全ての正常ノードがノード1の故障を検出できる．



故障検出器の性能インパクト