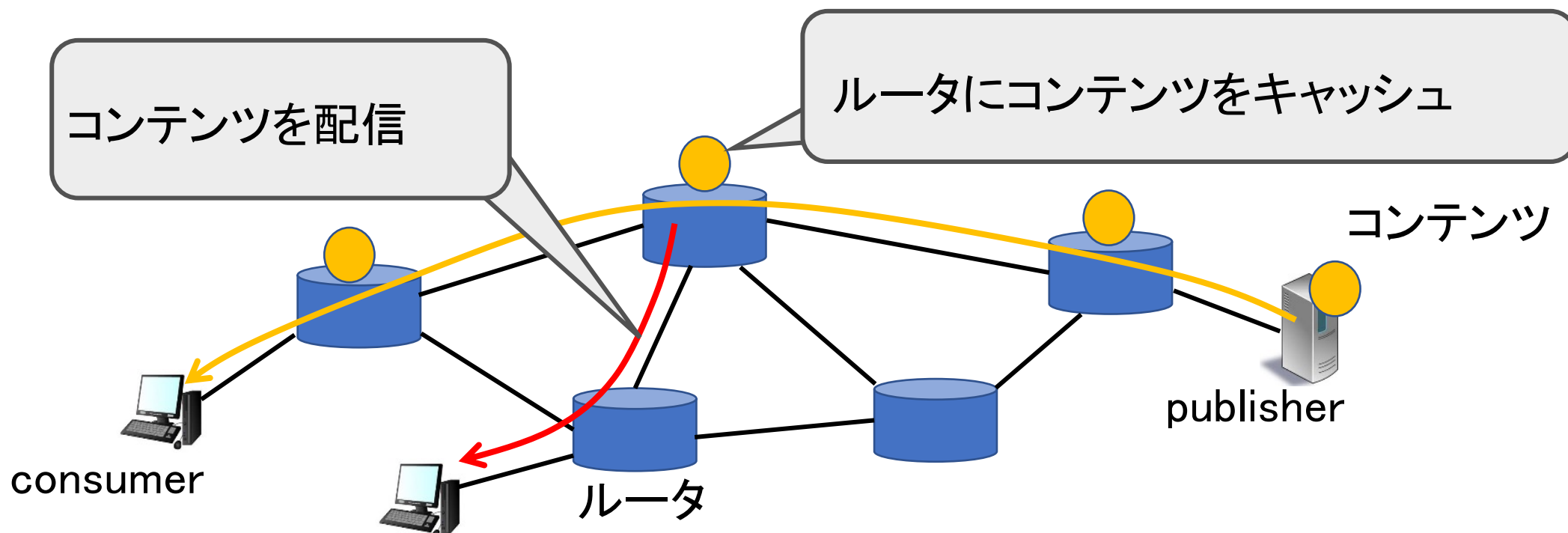


IOTAを用いたICNにおける名前管理方式

1. はじめに

情報指向ネットワーク (ICN: information-centric networking):

- 要求されたコンテンツの名称をもとに配信者(publisher)からコンテンツ要求者(consumer)にコンテンツを転送
- 経路するルータにコンテンツをキャッシュしながら配信



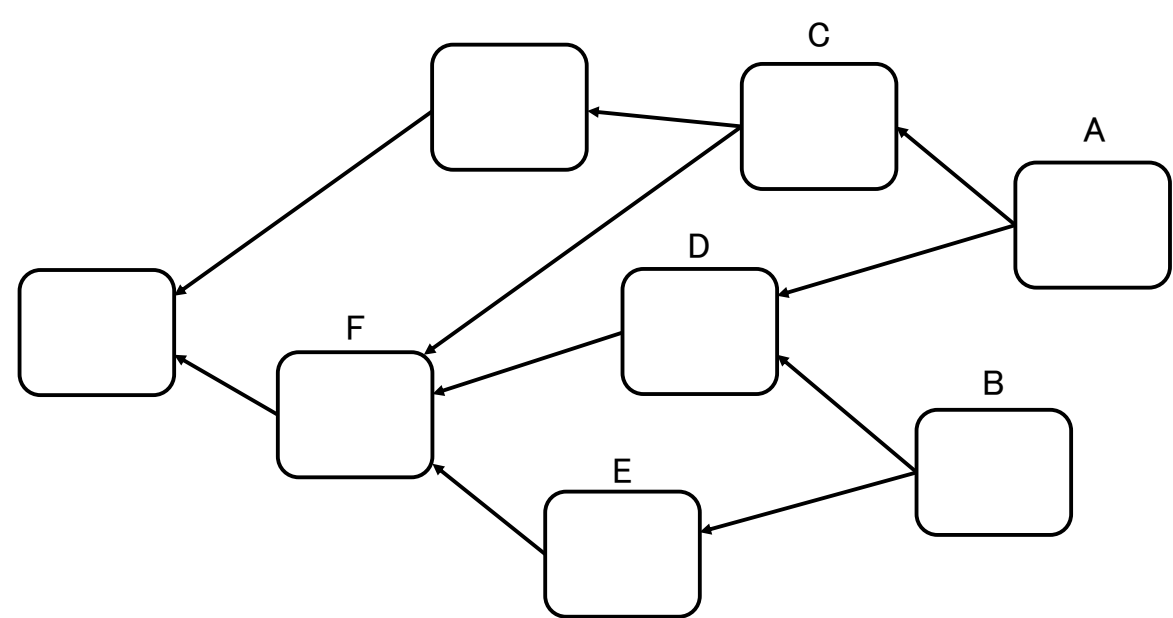
正当なpublisherを騙る攻撃者が、実在するコンテンツ名でfakeコンテンツをアップロードし、キャッシュの機能を低下

→CPA (content poisoning attack)

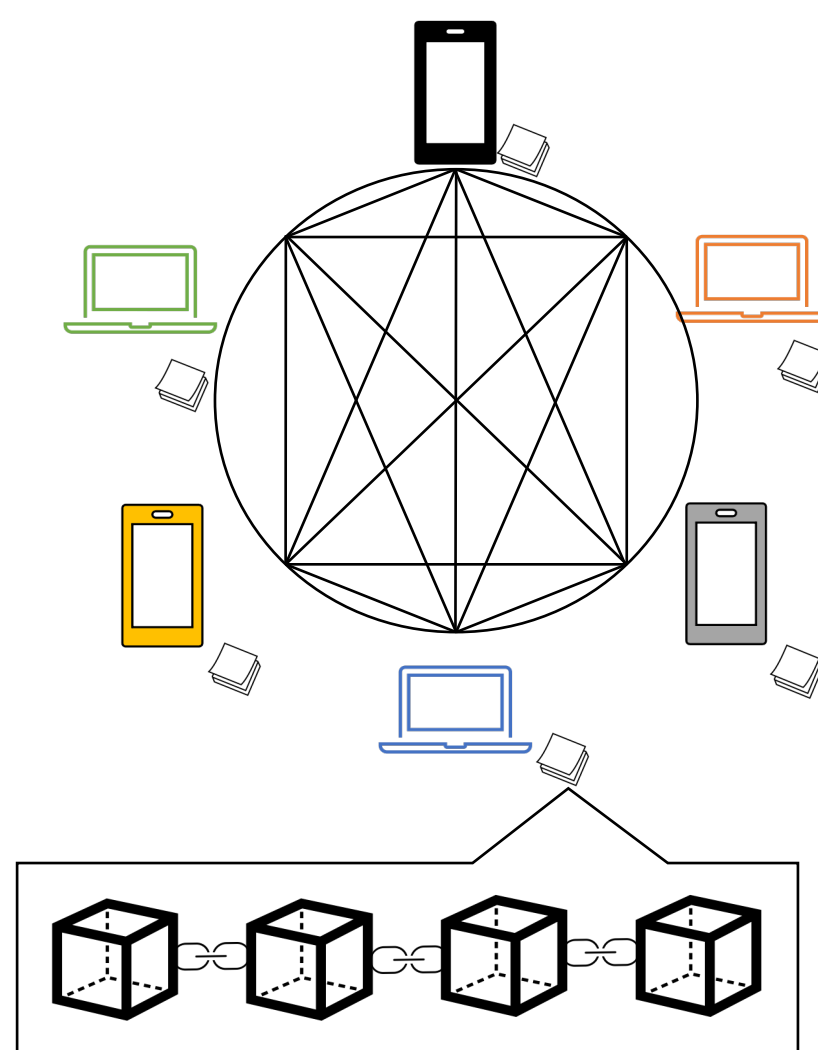
分散型台帳技術のIOTAを用いることで、改ざん困難な形式でコンテンツ名を管理するシステムを提案し、シミュレーションで評価

2. IOTA

- データやプログラムを分散管理できるシステム
- データはトランザクションで保存され、有向非巡回グラフ(DAG: directed acyclic graph)構造をとる
→トランザクションはひとつ前のトランザクションのハッシュ値を保持しているため、データの改変が困難



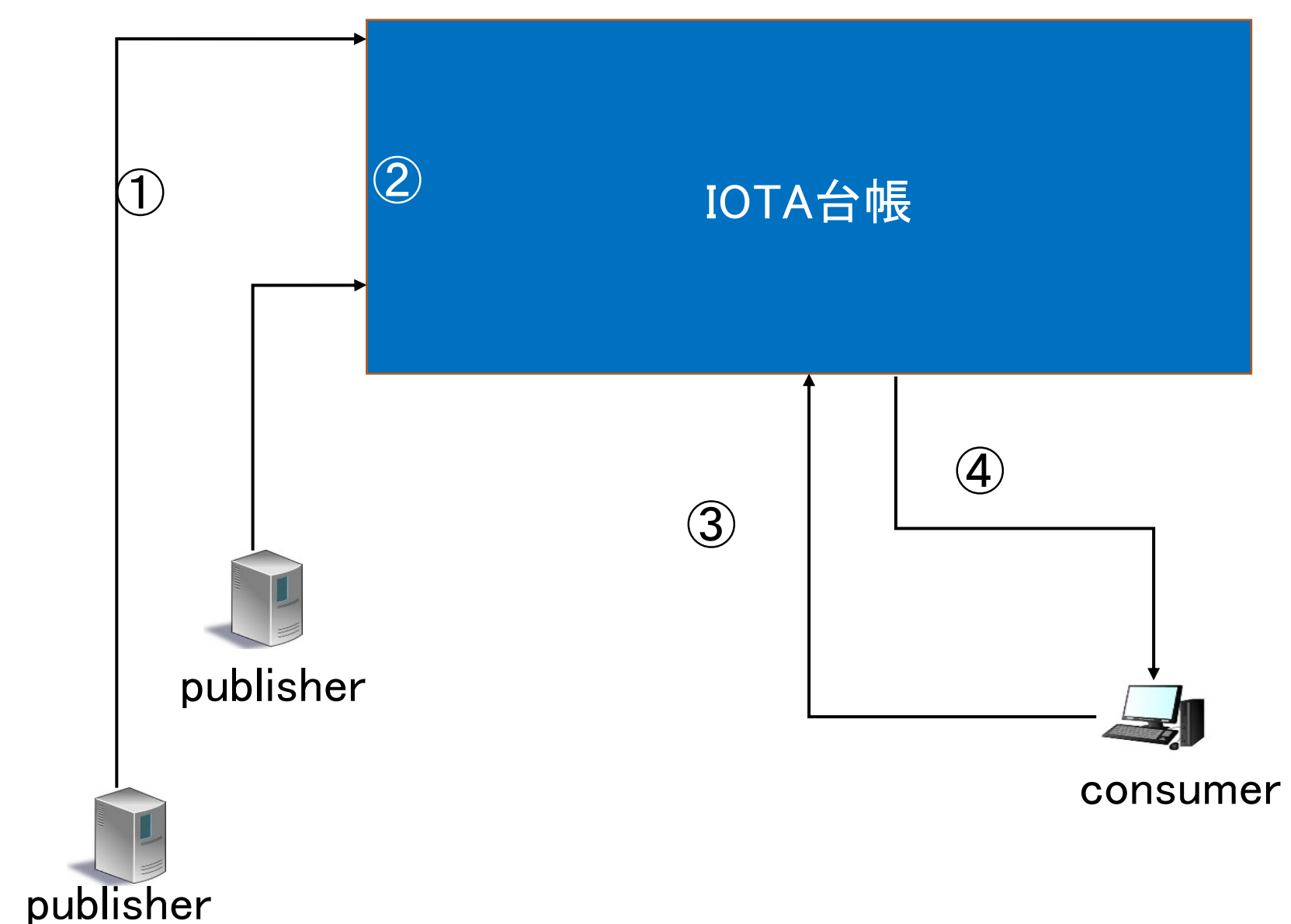
- ブロックチェーンは、分散型台帳の代表例



- デメリット:
 - トランザクションをブロックにまとめ、ブロック毎に管理
 - スケーラビリティ問題
- 承認作業には膨大な量の計算による電力が必要(PoW: proof of work)
- ブロックチェーンの活用例
 - 暗号通貨 (ビットコインなど)

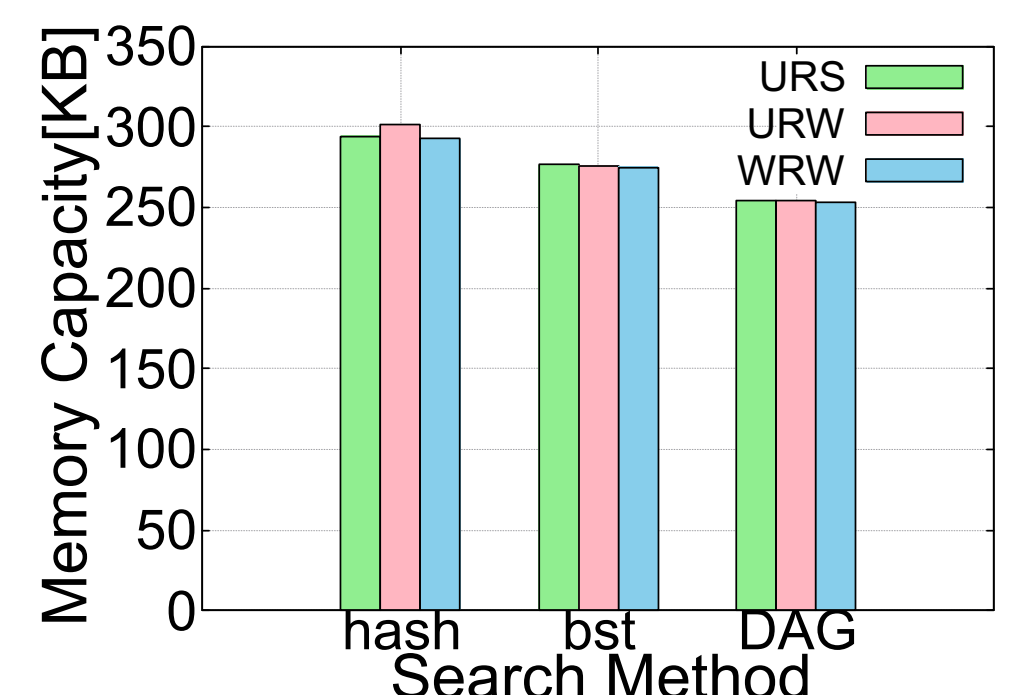
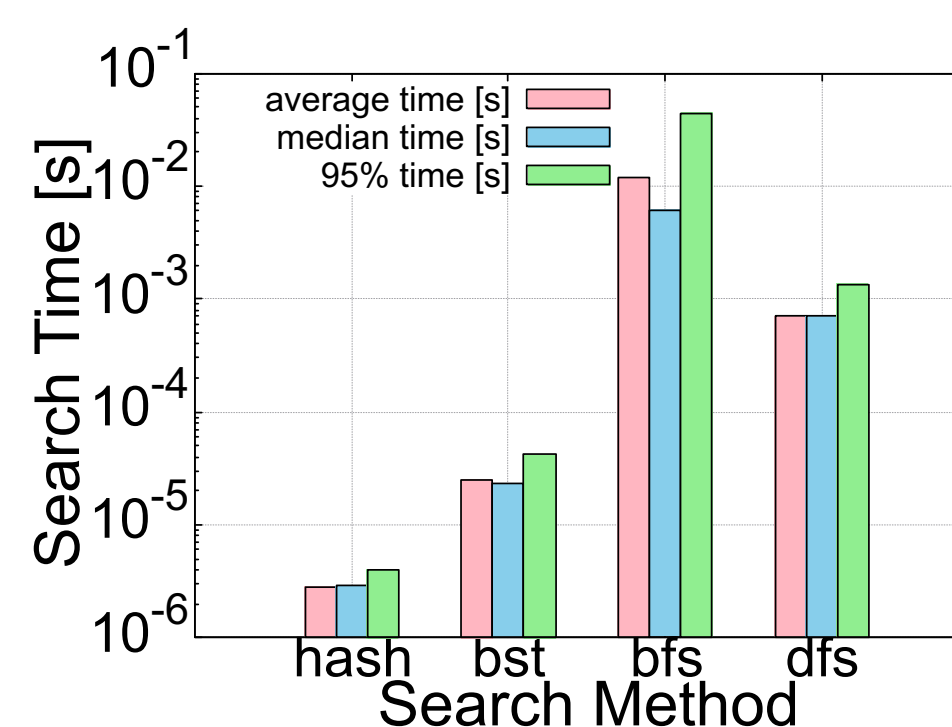
3. 提案手法

- publisherがコンテンツのアップロードに際し、transactionをIOTA台帳に登録
- 重複するコンテンツ名の管理を防ぐため、コンテンツのprefixで台帳内を探索
- consumerがコンテンツのprefixを要求し、コンテンツ名を台帳内で探索
- 発見したコンテンツ名をconsumerに回答
- そのコンテンツ名で要求パケットであるinterestを送信し、コンテンツを要求



4. 性能評価

- IOTA上での検索時間とメモリ量の増加が懸念
- 四つの検索方式間での性能評価
- DAGのtransactionの探索手法
 - ハッシュチェーン法 (hash), 二分探索木 (bst), 幅優先探索 (bfs), 深さ優先探索 (dfs)
- 検索時間 (左)と必要メモリ量 (右)を比較



- 検索時間
 - ハッシュチェーン法が最も少なく、二分探索木、深さ優先探索、幅優先探索の順に大きくなる
- 必要メモリ量
 - ハッシュチェーン法が最も多く、二分探索木、DAG (深さ優先探索と幅優先探索)の順に小さくなる
- 検索時間を抑えたい→ハッシュチェーン法、二分探索木を使用
- メモリ量を抑えたい→幅優先探索、深さ優先探索を使用