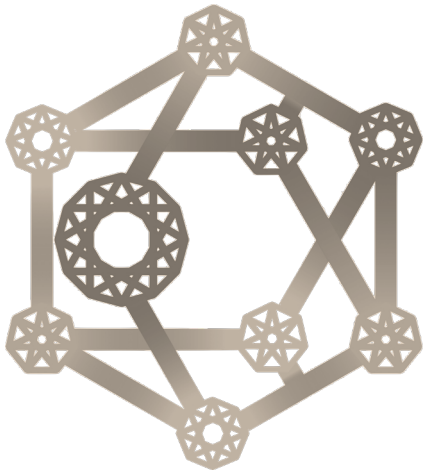


高性能で軽量な

国産公衆ブロックチェーン基盤構成技術

東京電機大学 情報システム工学科
情報ネットワーク研究室 小川猛志
Information network laboratory
https://www.inl.aj.dendai.ac.jp/

概要

- 暗号通貨やデジタル資産(NFT)の流通基盤としてブロックチェーン技術が注目されている
  - 2022年9月: **Bitcoin52兆円,Etherium23兆円**[1]
- 既存技術では重要な技術課題が解決できておらず，持続的な発展が困難

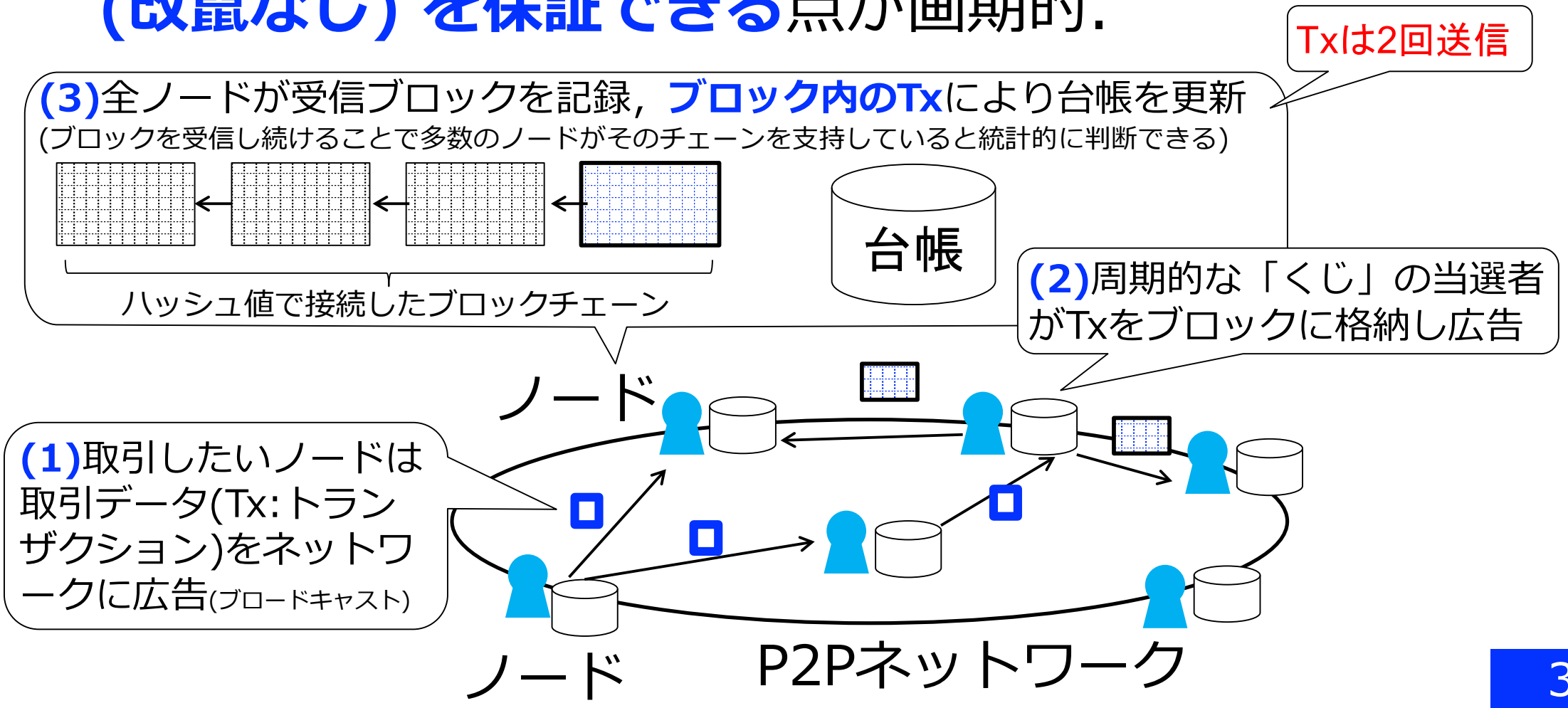
  ①低い取引処理性能，②多量のデータ量，

  ③消費電力とセキュリテイの両立
- それらを**抜本的に解決する技術を発明**，今後長期的に世界の暗号通貨の基盤となる可能性のある，新ブロックチェーン基盤を開発中.
- 発明の特徴とその応用例を紹介します。

[1] https://cc.minkabu.jp/pair, 2022.9.23参照

公衆ブロックチェーン技術とは？

- 不特定多数の利用者(ノード)が全員利己的でも安全に利用可能な，**分散型台帳技術**
- 集中サーバなしで，各ノードが保持する**台帳の同一性(改竄なし)を保証できる**点が画期的.



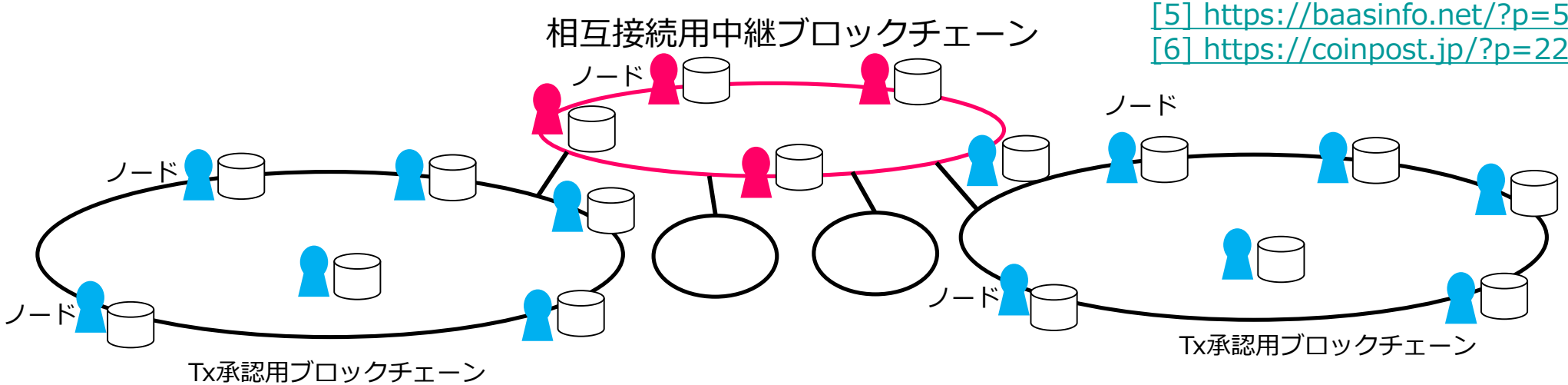
①処理性能問題と解決技術

- Tx承認処理性能の上限は「1ブロックで承認できるTx数」÷「平均ブロック間隔」で決定.
  - Bitcoin: 1ブロック=約4,000Tx, 平均生成間隔10分⇒最大**約7 Tx/s**,
  - Etherium:1ブロック= 約300Tx, 平均生成間隔約15秒⇒最大約**20 Tx/s**[2]
- ブロックサイズを大きくしたりブロック間隔を短くすると合意形成が不安定になる.
- 既存の電子取引のTx承認処理は集中サーバで実現されているが，それらに比べて大幅に小さい
  - Paypay:**63Tx/s**[3]，クレジットカード:**400Tx/s**[4] (国内)
- 今後の発展には**100倍以上の性能向上が必要**.

[2] https://etherscan.io/chart/tx
[3] https://about.paypay.ne.jp/pr/20210412/01/
[4] https://www.j-credit.or.jp/information/statistics/download/dynamicsurvey_creditcard_list.pdf

競合技術：階層型マルチチェーン

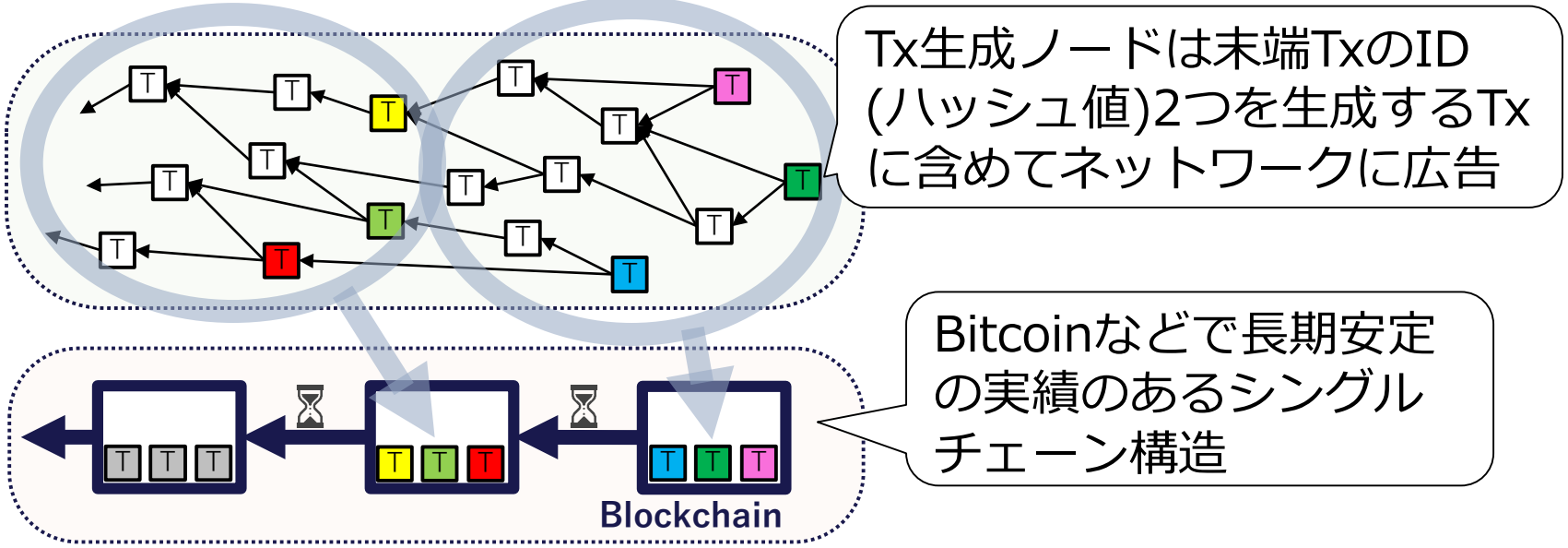
- ブロックチェーンを複数に分割し，各チェーン間の通信を特別なブロックチェーンが中継することで，全体のTx承認処理性能を改善する方法が研究されている.
  - Etherium:64分散[5]，Polkadot:100分散[6](予定)
- 大幅な方式変更・複雑化に伴い多くの懸念がある.
  - Tx承認権限の集中化･プロトコル複雑化による安全性低下
  - 中継ブロックチェーンによる信頼性と性能の低下
  - 決済承認時間の増大，スマートコントラクトの実現性



[5] https://baasinfo.net/?p=5585
[6] https://coinpost.jp/?p=229046

発明技術：Txグラフ

- Tx間にグラフ構造(Txグラフ)を導入，**ブロックにはTxグラフの末端TxのIDのみ格納**することで，Txグラフ全体の承認を実現[T1]．
- ブロックサイズや間隔の変更不要なため**合意形成に影響なし**．



＊ Blocks are created at regular intervals, creator gets Tx fee

- 1ブロックで大量のTxを承認可能⇒**Tx承認処理性能を大幅UP!**

–シミュレーションの実測で**300Tx/s**，外挿で**最大3,850Tx/sと推定**.

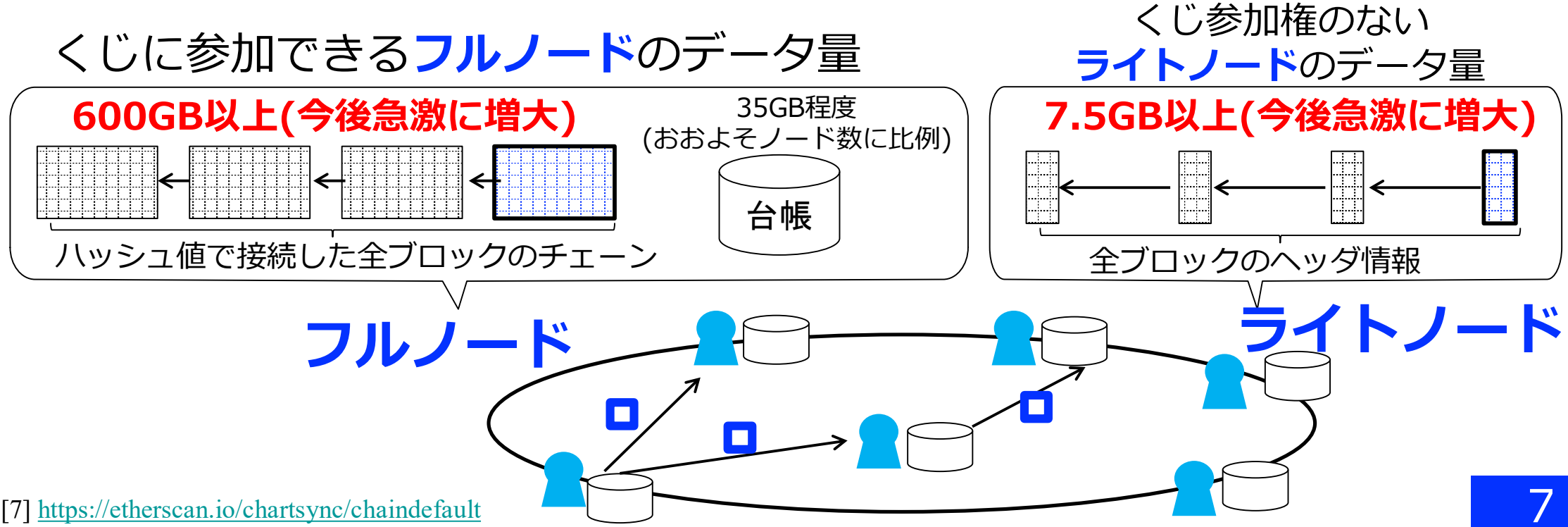
(PC内に仮想的なマシン100台のp2pネットワークを構築して測定)

⇒ **1チェーンで最大 500倍 の性能向上**の見込み

[T1] 島津，小川, "ブロックチェーンにおけるトランザクション処理性能向上技術," 電子情報通信学会論文誌, Vol.J104-B,No.7,pp.613-618,Jul. 2021.

②データ量問題と発明技術

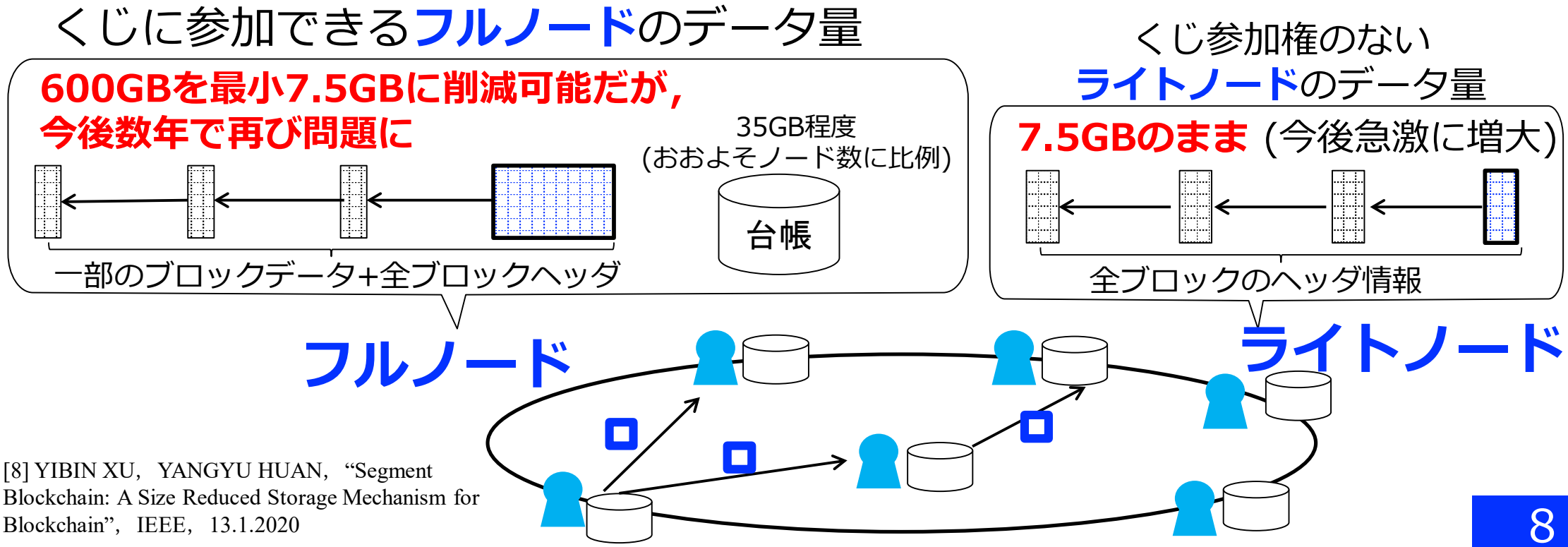
- 従来各ノードは，最初に生成されたブロックから最新ブロックまでの全ブロックデータor 全ブロックヘッダのどちらかを保持.
- イーサリアムの場合，2022年4月時点でブロックデータは**600GB**[7]，ヘッダ部は**7.5GB**以上．今後加速的に増大する見込み.
- 今後，スマートフォンなどの軽量な端末ではブロックチェーンネットワークに参加できなくなる問題がある.



[7] https://etherscan.io/chartsync/chaindefault

競合技術：ブロックデータ分散保持

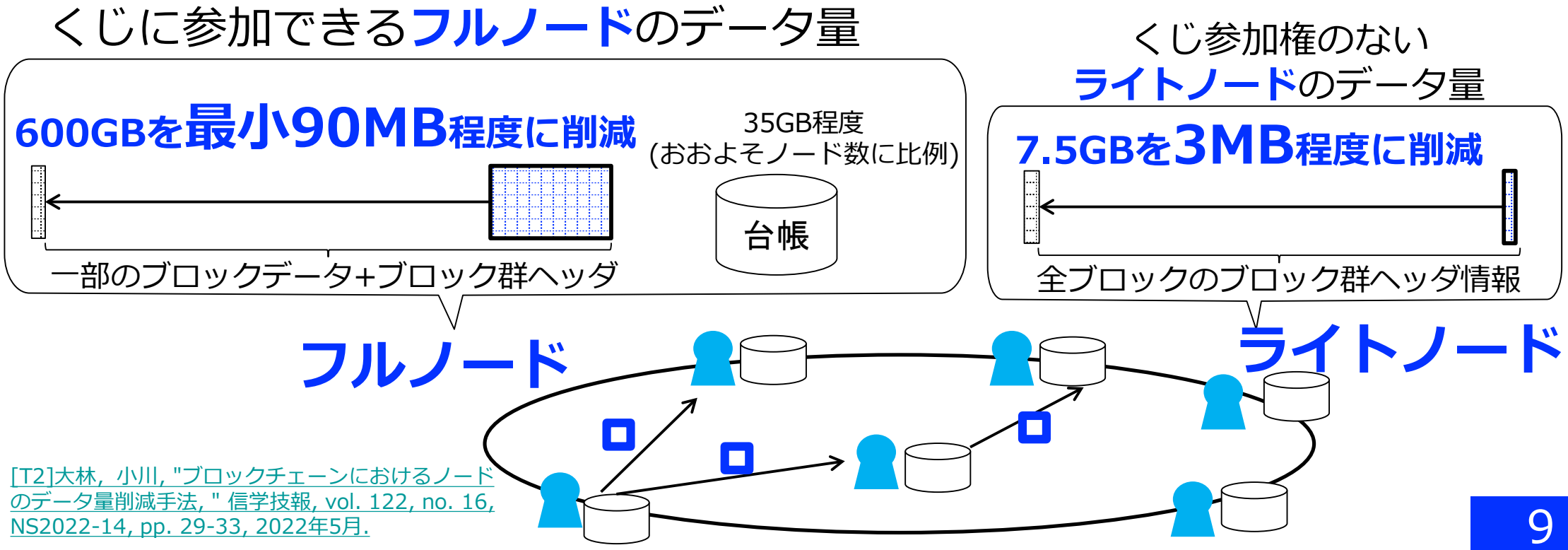
- 各ノードが分散して一部のブロックデータのみ保持する案がある[8]が，他ノードが持つブロックの正当性検証のため全ブロックヘッダの保持が必要
- ライトノードのデータ量は削減できず，フルノードの削減量も不足．**⇒問題解決には至っていない.**



[8] YIBIN XU，YANGYU HUAN，“Segment Blockchain: A Size Reduced Storage Mechanism for Blockchain”，IEEE，13.1.2020

発明技術：ブロック群ヘッダ

- 一定個数(例1,000個)のブロックヘッダを要約したブロック群ヘッダを新たに定義し，ブロックヘッダを廃棄してもブロック群ヘッダを保持していれば，受信ブロックの正当性を判断できる仕組みを発明[T2].
- **競合技術から更に1/100～1/1,000にデータ量を削減！**



[T2]大林，小川, "ブロックチェーンにおけるノードのデータ量削減手法, " 信学技報, vol. 122, no. 16, NS2022-14, pp. 29-33, 2022年5月.

③消費電力/セキュリティ両立問題と発明技術

- 公衆ブロックチェーンは不正のできない「くじ」が必須.
- 従来使用されているくじPoW:Proof of Workは**公正の根拠に事前には計算量が不明な計算問題**を使用.
- くじに勝つ競争の結果，全ノードの消費電力合計が膨大になり，1国の消費電力を既に超過.
  - **Bitcoin:140TWh/年，Etherium:59TWh/年**[9]
  - インドネシア(人口2.4億人):149TWh/年,
  - バングラデシュ(人口1.6億人):36TWh/年[10]

[9] https://digiconomist.net
[10] https://ja.wikipedia.org/wiki/消費電力

競合技術：PoS

- Etheriumは大幅に計算量を削減した新しいくじPoS:Proof of Stakeを採用[11].
- PoSはくじへの参加に掛け金(Stake)を必要とし**公正性の根拠に「高額な掛け金」**を採用.
- 次回のくじの当選確率操作などの不正が可能だが不正発覚時に掛け金を没収することで不正を抑止

⇒ PoWからPoSに移行することでくじに必要な消費電力をほぼゼロに削減できる見込みだが,

十分に不正を抑止できるか安全性が懸念.

[11] https://ethereum.org/en/upgrades/

発明技術：PoL

- PoL: Proof Of Lucky IDは**公正性の根拠に事前には計算結果が不明な各ノードの電子署名**を採用.
- PoWと異なりほぼ1回のくじで勝者が確定
- PoSと異なり多数のノードが結託しても，原理的にくじ当選確率の操作が不可能.
- 今後どのノードが当選するかの予測もできない.

⇒PoW/PoSに代わりPoLを採用することで，

消費電力を大幅に削減しつつ，

PoWと同等の安全性を実現[T3].

[T3] Takeshi Ogawa, Hayato Kima, and Noriharu Miyaho,"Proposal of Proof-of-Lucky-ID (PoL) to Solve the Problems of PoW and PoS," IEEE International Conference on Bitcoin 2018, pp. 1212-1218, Jul.2018.

4. 発明技術の特徴と活用例

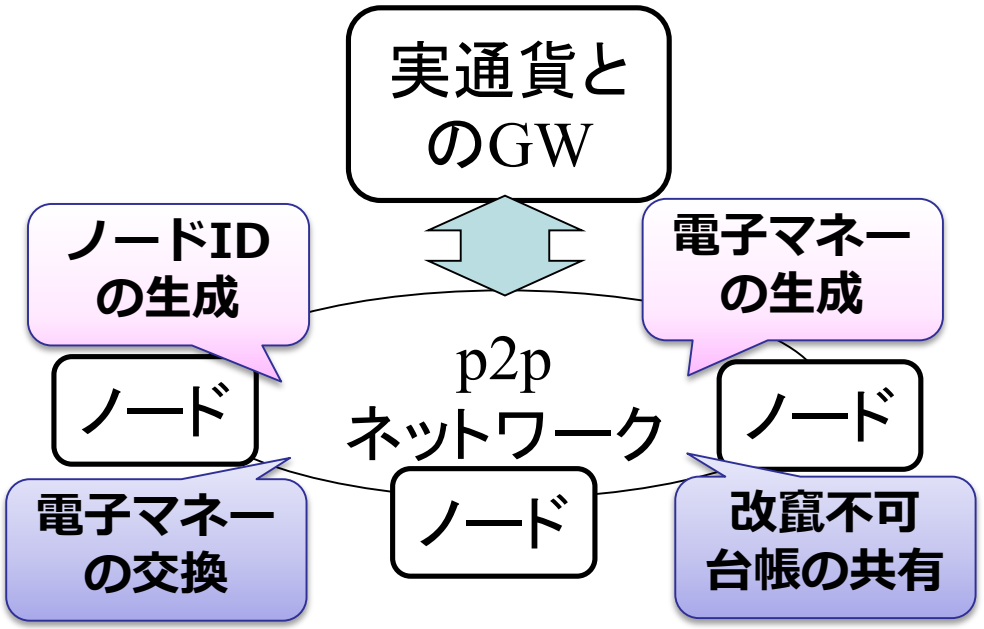
- 競合技術に比べ安全性が高く，プロトコルも単純.
- Etheriumのマルチチェーン対応と異なり，スマートコントラクト対応の課題もなく，NFTサービスの継続も問題ない.
- P2p型マルチチェーンによる更なる高性能化，イーサリアムGASPER[12]に替わる中央集権的でないFinalize手法も開発中.
- 既存のBitcoinやEtheriumに代替する**国産暗号通貨基盤**を実現したい.

[12]https://ethereum.org/ja/developers/docs/consensus-mechanisms/pos/gasper/

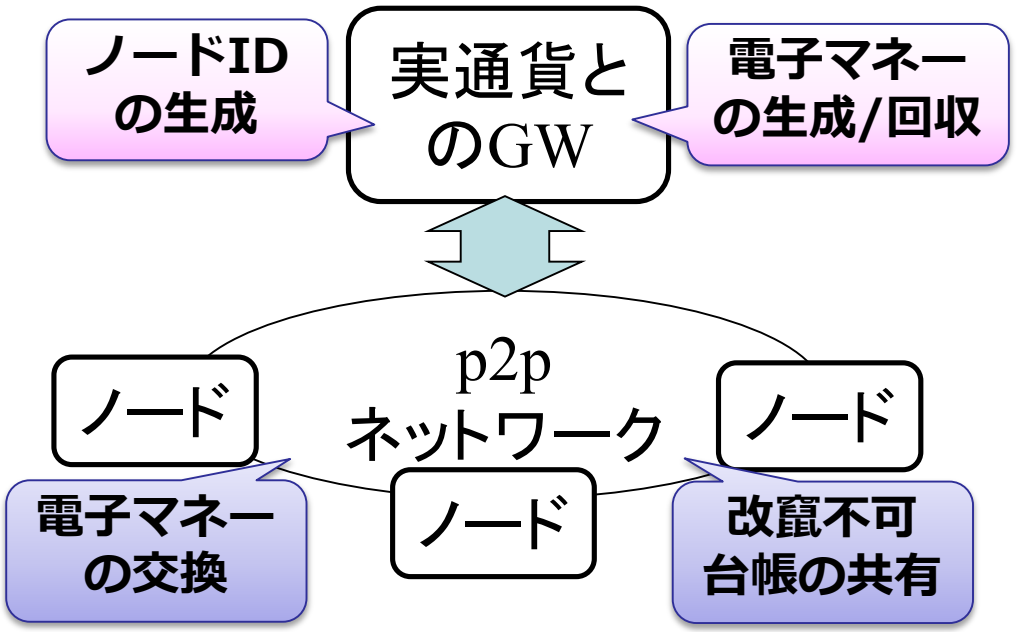
想定する応用サービスの例

- 従来型(Pure-P2P)に加え，現実の現金流通に近いhybrid型も可能であり，CBDC基盤としても有望
- 流通量管理が必要な電子マネー(地域通貨/ポイント等)や電子投票/ランキングではハイブリット型を想定.

従来型(Pure-P2P)



集中/P2Pハイブリット型



5. 企業の皆様への期待

- 提案技術は，今後長期に渡って持続的に発展できる暗号通貨基盤として適用可能と考えています．
- 今後，プロトタイプを開発し，実運用に近い環境での評価が必要であり，現在詳細設計中．
- 研究成果の技術移管，あるいは，共同研究により設計・実装・評価の支援を頂けますと幸いです．

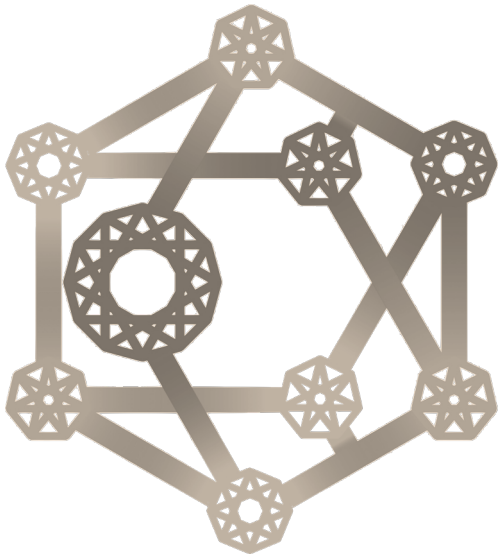
本技術に関する知的財産権

- 発明の名称 : 合意形成システム
- 出願番号 : 特願2022-069495
- 出願人 : 東京電機大学
- 発明者 : 小川 猛志

お問い合わせ先

東京電機大学
研究推進社会連携センター　産官学連携担当

ＴＥＬ　03－5284－5225
ＦＡＸ　03－5284－5242
e-mail　crc@jim.dendai.ac.jp



東京電機大学 情報システム工学科
情報ネットワーク研究室 小川猛志

Information network laboratory

https://www.inl.aj.dendai.ac.jp/