ブロックチェーンによる IoTデータの正真性担保

株式会社ガイアックス　峯 荒夢

自己紹介

峯 荒夢(Aram Mine)

株式会社ガイアックス 開発部 部長

日本ブロックチェーン協会 理事
ISO/TC307 国内審議委員(ブロックチェーンの国際標準化)

2000年 ソニー子会社に入社
2013年 株式会社ガイアックス入社
　RNDの開発マネージャーとして新規技術開発を担当
　2015年よりブロックチェーンを担当


Gaiax

ガイアックス


Top » About us
GAIAX IS A RESPONSIBILITY-DRIVEN COMMUNITY
THAT EMPOWERS PEOPLE TO CONNECT
ガイアックスは、人と人をつなげるため、
ソーシャルメディアとシェアリングエコノミーに注力し、
社会課題の解決を目指すスタートアップスタジオです。

SHARING ECONOMY ASSOCIATION JAPAN

シェアリングエコノミー協会　代表理事

STARTUP STUDIO UNION

協会について　各会員種別のご案内　理事紹介　お問い合わせ

UNITED FRONT FOR FRONT-RUNNERS

スタートアップ創出をなめらかに

100人中93人の失敗者が生まれてしまうのがスタートアップの業界。起業へのハードルを下げ、挑戦すること自体に価値がある世界を目指して

スタートアップスタジオ協会　代表理事

JBA

日本ブロックチェーン協会
Japan Blockchain Association

元代表理事　肥後彰秀
元理事　上田祐司
現理事　峯荒夢

経歴

2016年

情報発信メディア
Blockchain Biz
開設

2017年

ブロックチェーン
国際標準化
ISO/TC307
国内検討委員
就任

2018年

技術評論社
60分でわかる！
ブロックチェーン
最前線
監修

2019年

インプレスR&D社
ブロックチェーン
用語集
著書

2021年

インプレスR&D社
Nuxt.js Firebase PWAではじめる
ブロックチェーン
アプリ開発
著書

LiDAR

NICT Beyond 5G国際共同型プログラム として委託研究に採択

City as a Serviceを支えるデジタルツインを持続可能な状態で自己成長させるエコシステム

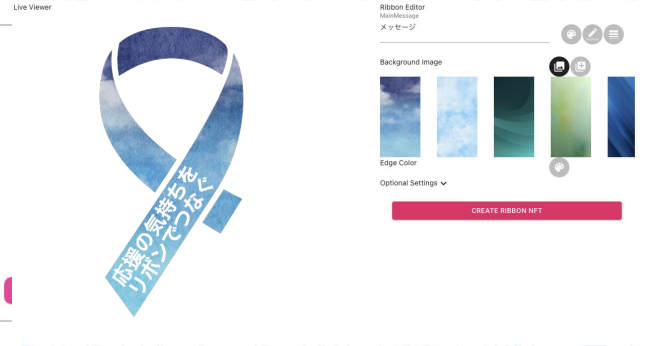
提案者：学校法人早稲田大学（代表提案者）、
学校法人芝浦工業大学
学校法人片柳学園東京工科大学
株式会社ガイアックス
学校法人福岡大学
欧州側共同研究者
イタリア Dipartimento di Ingegneria Elettronica
Universit à degli Studidi ROMA "Tor Vergata"

3次元で物体の形状を測定できるカメラLiDARのデータを改ざんを防止しながら共有できるシステムの開発

Ribbo

NFTのリボンを販売し、寄付を集めるサービス

資金を必要とする個人や団体が作成したリボンを買うだけで、応援ができます



誰でも簡単にリボンがデザインでき、作ったリボンはそのままサイト上で販売できます。
しかも在庫リスクゼロ。

リボンが売れたら、売上は活動資金や寄付として受け取れます。
※一部手数料として差し引かれます。

シェアハウス x DAO

地方創生や学生起業家にむけたDAOシェアハウスを展開

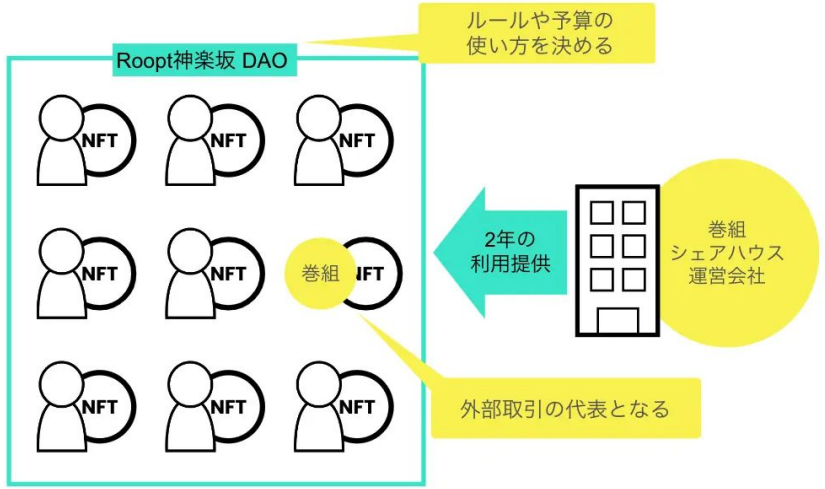
Web3.0による住のアップデートを進める

巻組運営の一軒家をDAOが2年間借上げ、シェアハウスとして自律的に運営

最大240名のDAOメンバー (ベッド10台×24ヶ月分)

魅力的なスペースにするための運営ルールをDAOメンバーが決定

掃除や運用の業務委託、費用や資産購入を投票で都度決定



DAOコンサル

なぜDAOが必要なのか

これまでの経済において、経営者からトップダウンで組織の意思決定を行う株式会社が発展の大きな役割を担ってきました。
これに対して、ブロックチェーンが登場し、DAO（自律分散型組織）という形で、意思決定を中央なしに行えるようになりました。
これにより、民主的に組織を運営することができるようになり、国籍や性別に関係なく気持ち次第でDAOに参加し能力を発揮することができるようになりました。
このサービスでは、企業におけるDAOの立ち上げ、及びDAOによる事業検証をブロックチェーンや組織・コミュニティづくりの知見をもつガイアックスが支援いたします。

コミュニティ運営

Blockchain Biz
Community

ブロックチェーンをスタートアップに使いたい人と、
技術を学びたい人の学びの場であるコミュニティを運営中

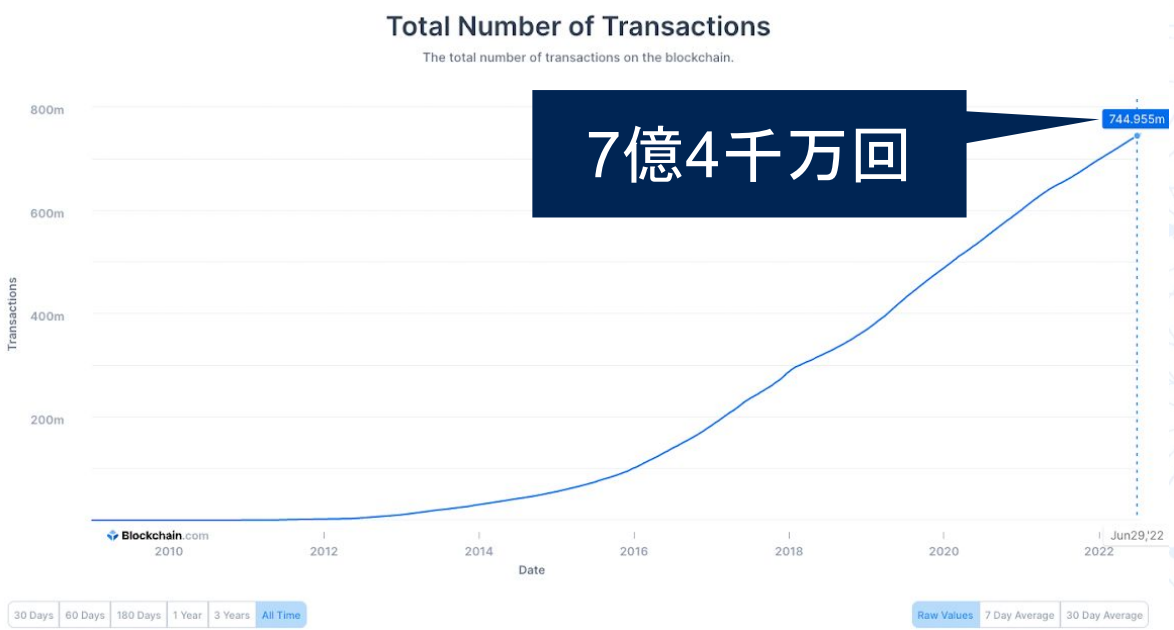
ブロックチェーン

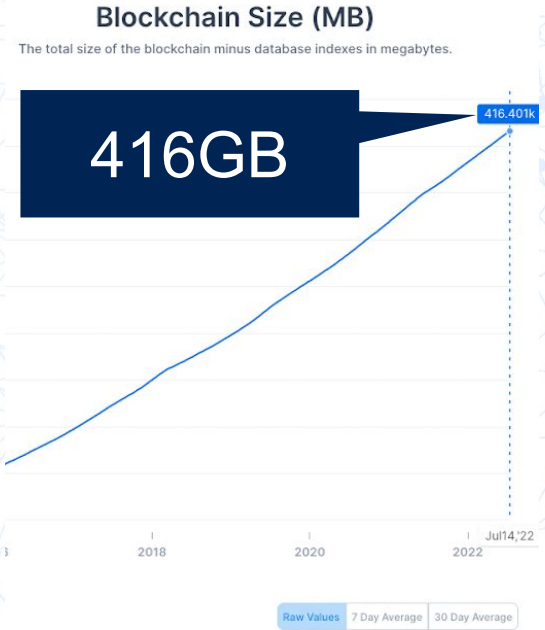

台帳

台帳

ブロックチェーンは、生まれてから現在までの**全ての取引**を記録している台帳

ビットコインでは2009年1月3日に誕生してから全ての取引が記録されている





ブロック

台帳の1ページ

誰から誰にお金や権利が移動したかといった成立した**取引データ**が書いてある

チェーン

台帳のページは、数珠つなぎに1列につながっている

ページは出来上がった順に時系列にならんでいる

このつながり方がチェーンににている

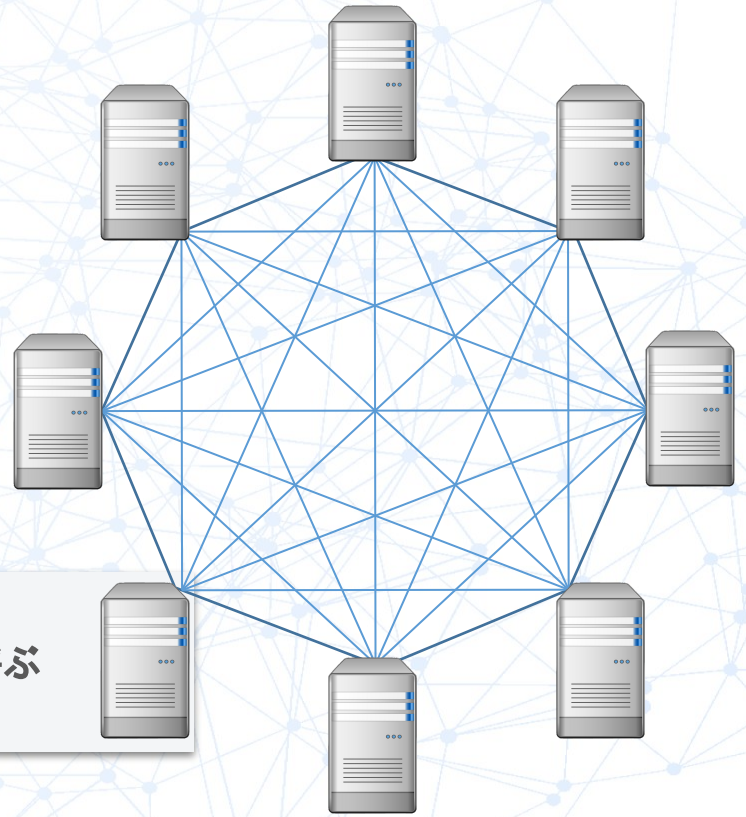
ブロックチェーンのネットワーク

誰でも参加できるネットワーク

みんなでデータを保存している

全員が**すべてのデータ**を持っている

なにかあっても消えない



この1台をノードと呼ぶ

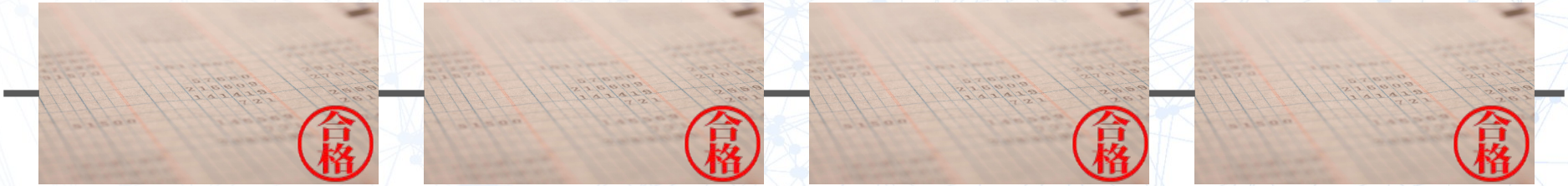
マイニング

各ブロックには合格印が押されている

合格印を押すには、全世界の全ノードが全力で10分間計算させる必要がある

ブロックに記録される取引データに**任意の数字**を加算してハッシュをとり
ターゲット値より小さい数になるまで計算を繰り返している。

※ターゲット値は、過去2週間の結果から算出し、確率的に10分に1度当たるよう自動調整される。

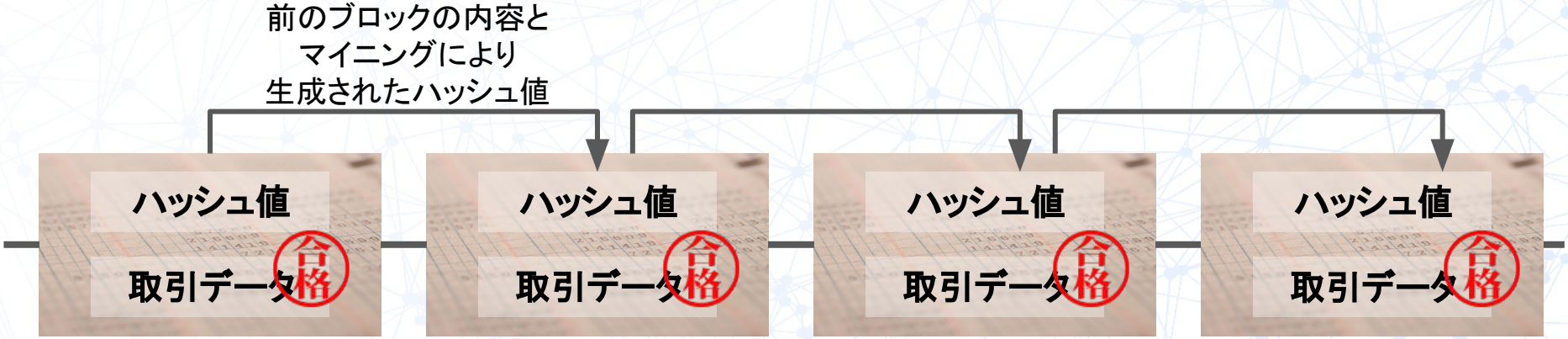


ブロック確定に**多大な計算パワー**を要する

ハッシュチェーン

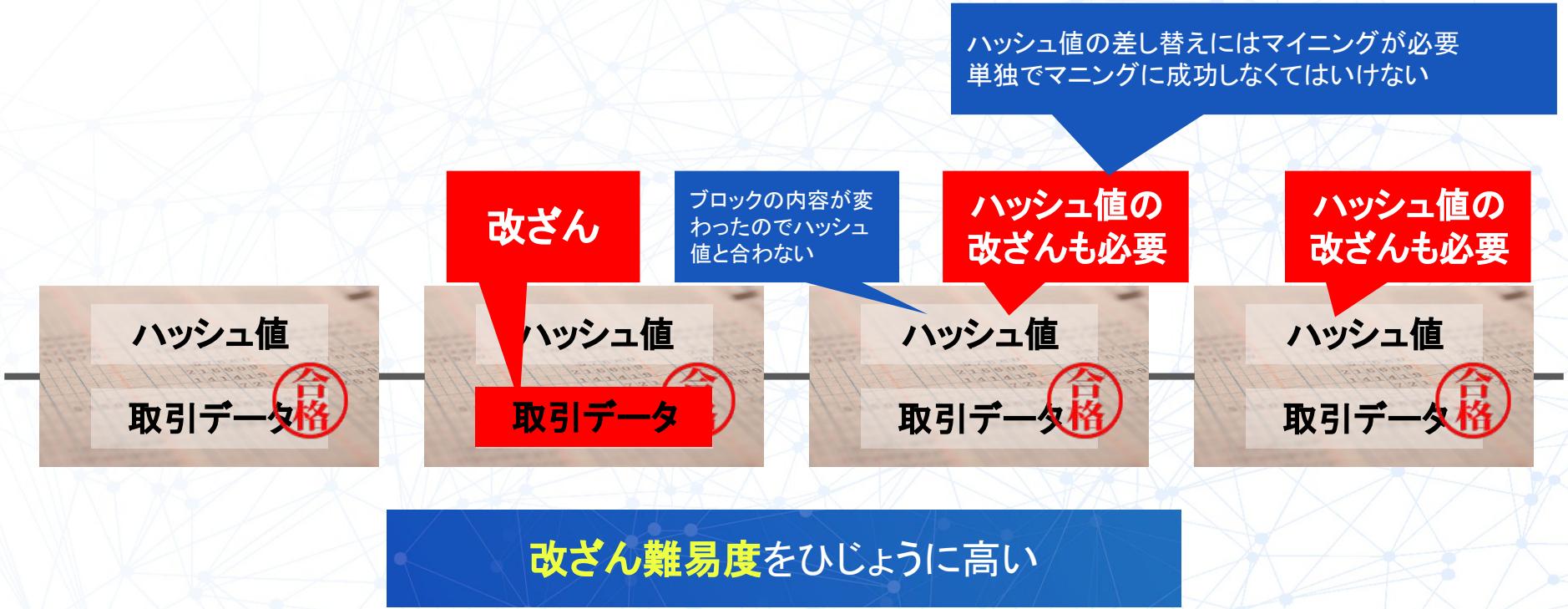
前のブロック全体のハッシュ値を次のブロックに保存

ハッシュ値がチェーン状につながっている



1番最初のブロックから現在のブロックまでハッシュ値につながりの関係がある

データ改ざん耐性


ハッシュ値の差し替えにはマイニングが必要
単独でマニングに成功しなくてはいけない
改ざん
ブロックの内容が変わったのでハッシュ値と合わない
ハッシュ値の改ざんも必要
ハッシュ値の改ざんも必要
ハッシュ値
取引データ
合格
ハッシュ値
取引データ
合格
ハッシュ値
取引データ
合格
ハッシュ値
取引データ
合格
改ざん難易度をひじょうに高い

ブロックチェーンの欠点

改ざん耐性は強いが書き込みが遅い

IoT x ブロックチェーン

データの記録

データを直接ブロックチェーンに記録する

例：東京都千代田区大手町　2022年10月25日 8時 11℃

改ざんできない記録方法

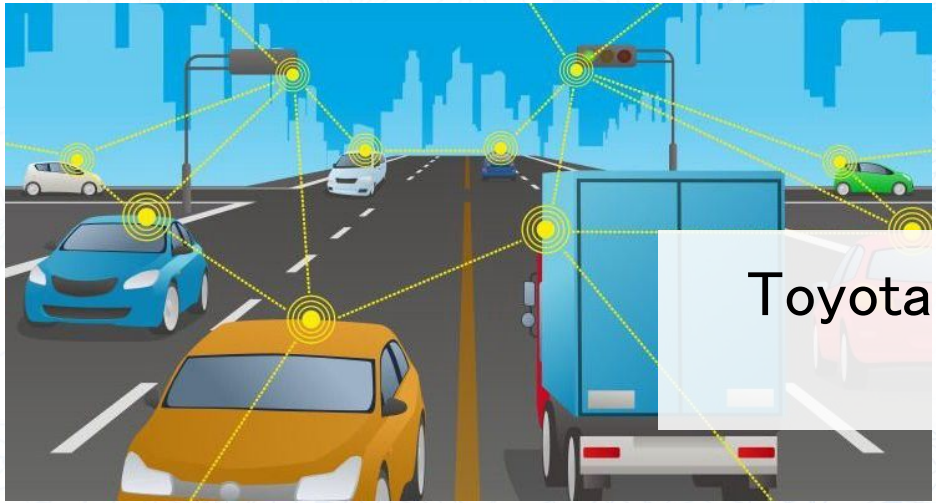
M2M

Filament
21.co
IOTA

センサーがブロックチェーンを通じてデータを自動販売

スマートコントラクトを利用

AI x ブロックチェーン



Toyota Research Institute
BigchainDB

自動運転データをブロックチェーンで管理
データはAIの学習用に活用される

データの共有、権利の管理を利用

その他

輸送ログの保存

・GPS、振動、温度などロジスティックの証拠担保

ファームウェアの改ざん検知

・ファームウェアのハッキングを防ぐ

ブロックチェーンの未来感

AIがM2Mで買ったデータを
AIが加工しM2Mで販売

ほとんど映画の世界ですね

データが改ざんされると全てか崩れる

AIが間違った学習をする
AIが間違った判断をする
命に関わることも起こりえる

IoTデータの正真性担保の例

データの記録

データを直接ブロックチェーンに記録する

例：東京都千代田区大手町　2022年10月25日 8時 11℃

改ざんできない記録方法

ブロックチェーンの課題①

大容量データを書き込めない

ブロックに書き込めるデータは1MBytes(ビットコインの場合)など大きくない

1ブロックの生成時間は10分。すなわち、10分に1MBytesしか書き込めない

制限がきつい

ブロックチェーンの課題②

書き込み速度の遅さ

・ビットコイン　秒間7取引

・Ethereum　秒間12取引

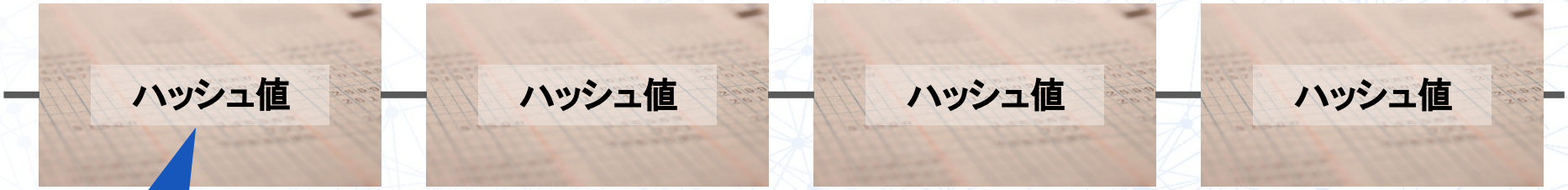
・プライベートチェーン系　秒間数千取引

※いずれも参考値

全てのデータとハッシュ値をブロックチェーン書くには負担が大きい

対策　記録する容量をへらす

ハッシュ値だけブロックチェーンに記録し容量を軽くする



10分間のデータを要約したハッシュ値

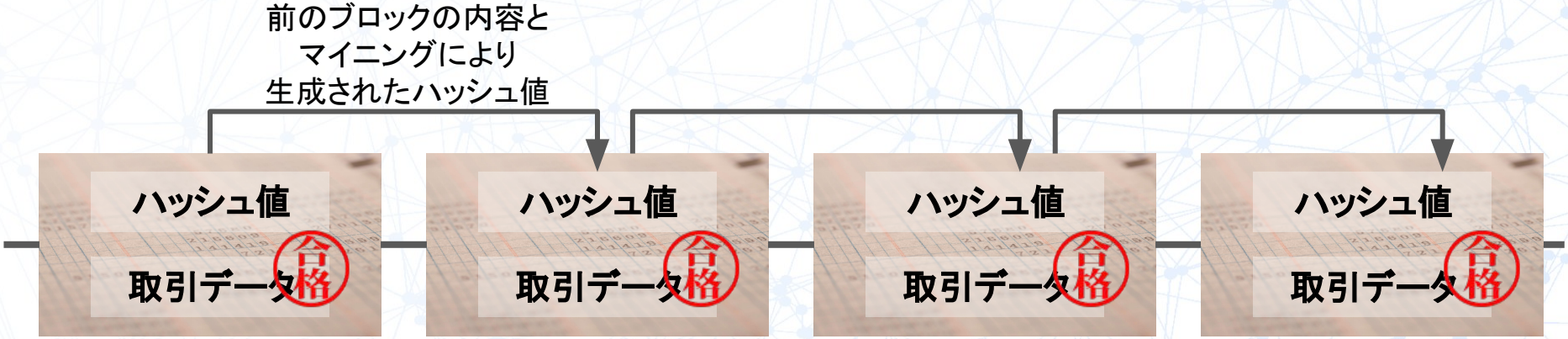
データはブロックチェーンの外のデータベースに記録する
この書き込み方法がブロックチェーンにペッグするという

もう少し発展させる

ハッシュチェーン

前のブロック全体のハッシュ値を次のブロックに保存

ハッシュ値がチェーン状につながっている

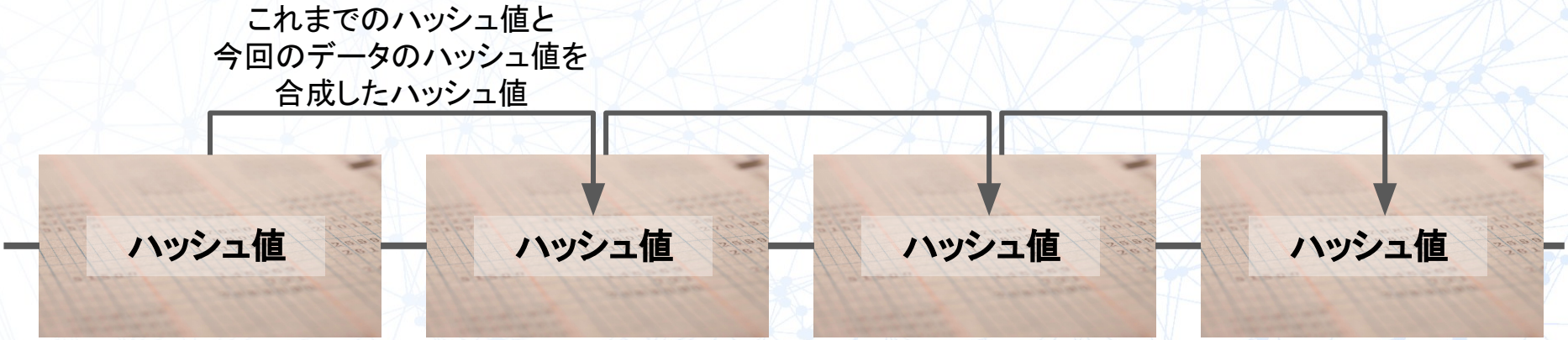


1番最初のブロックから現在のブロックまでハッシュ値につながりの関係がある

IoTのデータのハッシュチェーン

前のブロックのハッシュ値も含めたハッシュをブロックに保存

ハッシュ値がチェーン状につながっている



データの連続性まで担保した形で保存できる

対策2　複数のデータを要約する

データNo	データのハッシュ値	ハッシュスタック	ブロックチェーン への書き込み
324	AAAAAAAA	OOOOOOOO = hash(NNNNNNNN + AAAAAAAA)	
325	BBBBBBBB	PPPPPPPP = hash(OOOOOOOO+BBBBBBBB)	✅ PPPPPPPP
326	CCCCCCCC	QQQQQQQQ = hash(PPPPPPPP+CCCCCCCC)	
327	DDDDDDDD	RRRRRRRR = hash(QQQQQQQQ + DDDDDDD)	
328	EEEEEEEE	SSSSSSSS = hash(RRRRRRRR + EEEEEEEE)	
329	FFFFFFFF	TTTTTTTT = hash(SSSSSSSS + FFFFFFFF)	✅ TTTTTTTT
330	GGGGGGGG	UUUUUUUU = hash(TTTTTTTT + FFFFFFFF)	

いくつかのデータを時系列を含めてまとめたハッシュをブロックチェーンに書き込む

対策まとめ

- 記録する容量を減らす
  - ブロックチェーンの書き込みの負担を減らし高速化を行う
- データの連続性を担保する
  - 時系列にまとめて記録することでブロックチェーンへの書き込み回数を減らす

要約されたデータの検証

データNo	データのハッシュ値	ハッシュスタック	ブロックチェーン への書き込み
325	BBBBBBBB	PPPPPPPP = hash(OOOOOOOO+BBBBBBBB)	✅ PPPPPPPP
326	CCCCCCCC	QQQQQQQQ = hash(PPPPPPPP+CCCCCCCC)	
327	DDDDDDDD	RRRRRRRR = hash(QQQQQQQQ + DDDDDDD)	
328	EEEEEEEE	SSSSSSSS = hash(RRRRRRRR + EEEEEEEE)	
329	FFFFFFFF	TTTTTTTT = hash(SSSSSSSS + FFFFFFFF)	✅ TTTTTTTT

previous_hash: PPPPPPPP
first_data_number: 326
last_data_number: 329
hash: TTTTTTTT

前の書き込みのハッシュ値から
各データのハッシュスタックを計算していき
最後のデータNoのハッシュ値と一致すれば OK

PPPPPPPPを起点に計算していきTTTTTTTTになれば改ざんがないことを証明できる

本方式のまとめ

- **ブロックチェーンでデータの正真性を担保できる**
- **ブロックチェーンの遅さをカバーできる**
  - ただし、改ざん発生時は要約したブロック単位でデータを捨てなくてはいけない
- **生データは一般的なデータベースに普通に保存できる**
  - 改ざんがないことはブロックチェーンで保証すれば良い
    - 改ざんがおきないようにガチガチに固める必要がない
    - コストの低いDBでも改ざんがなくデータを維持できる
- **改ざんが発覚したときは、データの復旧ができない**
  - ハッシュ値からはデータの復元はできないため、改ざん発生時にデータの復旧は行えない

ご清聴ありがとうございました

ブロックチェーンをスタートアップに使いたい人と、

技術を学びたい人のコミュニティに興味が有る方はこちらへ