SCIS2020

 1

DAG技術ベースの暗号資産の匿名性に関する考察

2020年1月31日

（株）IT企画　才所敏明

toshiaki.saisho@advanced-it.co.jp　http://www.advanced-it.co.jp

共　著　者

辻井重男
中央大学研究開発機構

櫻井幸一
九州大学　大学院システム情報科学研究院
＆サイバーセキュリティーセンター
（株）国際電気通信基盤技術研究所

謝辞　本研究の一部は　JSPS科研費 基盤(B) JP18H03240　の支援を受けている。

 2

暗号資産の匿名性に関する研究の動機

インターネットの匿名性の課題を研究テーマとして活動

匿名性は重要だが、特定・追跡性の保証のない匿名性は有害

＊特定・追跡性と匿名性の両立を可能とする
安心・安全な電子メールSSMAX

＊特定・追跡性と匿名性の両立を可能とする
安心・安全なIoTシステムSSIoT

＊特定・追跡性と匿名性の両立を可能とする
インターネットサービスにおける本人認証基盤NAFJP/GAF

悪用される暗号資産の現状

特定・追跡性が保証された匿名性のある暗号資産が必要！

暗号資産の匿名性の現状の把握、2018年に着手

 3

暗号資産の匿名性に関する発表

2019年1月25日　SCIS2019
仮想通貨の匿名性の現状と課題

2019年3月16日　IPSJ第81回全国大会
暗号仮想通貨における匿名化技術の現状と展望

2019年10月22日　CSS2019
匿名暗号資産（Monero/Zcash/Grin）
ブロックチェーンの匿名性に関する考察

DAG系暗号資産についても、匿名性の現状について概略把握
公開されているDAGチェーン上のデータから
利用者の特定・推定に繋がる情報の入手が困難かどうか

 4

DAG技術ベースの暗号資産の匿名性に関する考察

1. はじめに
   - スケーラビリティとDAG系暗号資産
   - IoT向きおよび耐量子性を主張するDAG系暗号資産
2. DAG系暗号資産の特徴
   - タングル型とラティス型
3. DAG系暗号資産のトランザクションの匿名性要件
4. 調査対象DAG系暗号資産の匿名性
   - IOTA、Gbyte、Nano、Hedera Hashgraph
5. まとめ
   - 調査対象DAG系暗号資産の匿名性比較
   - DAG系匿名暗号資産DEROの匿名性概要

4

暗号資産のスケーラビリティ問題

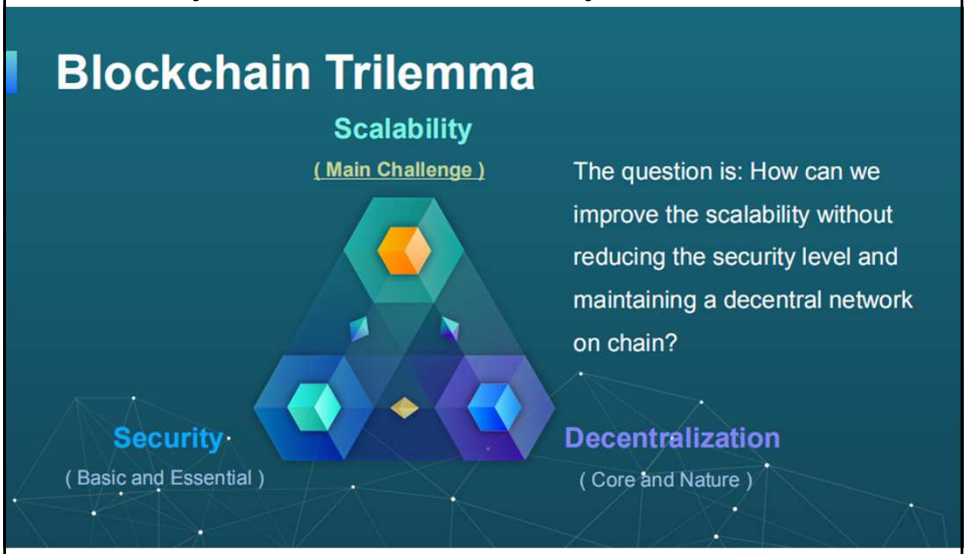
通貨名	公表値	実測値
Bitcoin	ー	7
Ethereum	ー	15
EOS	3990	50
Bitcoin Cash	ー	61
Litecoin	ー	56
VISA		1700

（56K）

（Transactions/second）

下記資料を編集し作成
https://cointelegraph.com/news/who-scales-it-best-inside-blockchains-ongoing-transactions-per-second-race

Scalability trilemma described by Ethereum’s Vitalik



“Solving The Bottleneck Of Blockchain And The Scalability Trilemma Through Sharding”
（Forbs Jan 15, 2019, 06:00pm）

スケーラビリティ向上策

On-Chain Solution		
	Concensus Algorithm	
		Ethereum2.0（PoW－＞PoS）
		EOS（dPOS:21delegates）
		IOTA（coordinator/milestone:22nodes）
	Enlarging Block Size（Reducing Transaction Data）	
		Bitcoin（1M=>2M,Segwit）
	Sharding	
		Ethereum2.0, IOTA, Nano, Hedera Hashgraph
Off-Chain Solution		
		Ethereum（Raiden Network, Plasma）
		Bitcoin（Lightning Network）

IoT向きを主張している暗号資産

順位	名称	記号	時価総額
20	IOTA	MIOTA	¥59,007,350,027
100	Golem	GNT	¥3,460,854,210
121	Waltonchain	WTC	¥2,433,151,549
143	IoTeX	IOTX	¥2,076,967,194
170	Robotina	ROX	¥1,571,508,337
177	Cortex	CTXC	¥1,488,534,667
190	Cindicator	CND	¥1,265,786,490
306	IoT Chain	ITC	¥871,932,031
337	Davinci Coin	DAC	¥709,779,142
356	Nucleus Vision	NCASH	¥628,249,406

2019年11月25日時点の①および②を参考に作成
①All Cryptocurrencies https://coinmarketcap.com/all/views/all/
②最新IoT関連の仮想通貨一覧, 2019 https://www.owl-coin.com/tags/internet-of-things

耐量子性を主張している暗号資産

順位	名称	記号	時価総額
13	Cardano	ADA	¥95,938,478,257
17	NEO	NEO	¥67,039,403,526
20	IOTA	MIOTA	¥59,007,350,027
80	HyperCash	HC	¥5,123,412,789
348	Quantum Resis…	QRL	¥653,283,462
1203	SHIELD	XSH	¥27,912,850
2033	Aidos Kuneen	ADK	¥?

2019年11月25日時点の①および②を参考に作成
①All Cryptocurrencies https://coinmarketcap.com/all/views/all/
②耐量子暗号特性の仮想通貨とその技術概要，2019
https://www.zbaron-newworld.com/entry/2018/03/11/003001
耐量子性の主張の根拠：格子ベース暗号技術/ハッシュベース暗号技術の利用

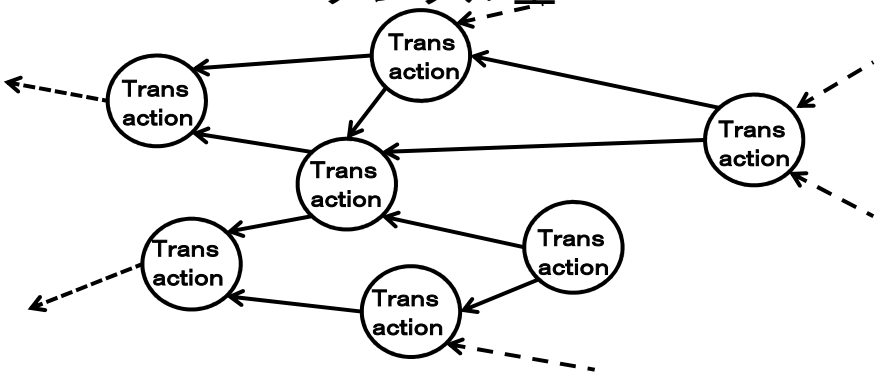
調査の目的

スケーラビリティの良さに特徴があるとされている

現在の主要なDAG系暗号資産が

Bitcoinと比べどの程度の匿名性を維持しているのか

DAG系暗号資産の特徴
タングル型

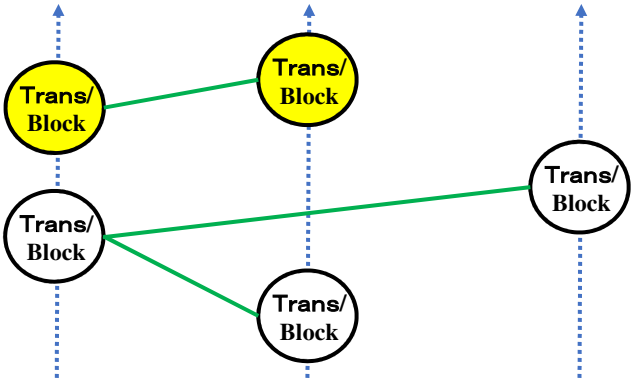


①新たなトランザクションは、既存の複数のトランザクションを承認することによりDAGへ追加され承認の対象となる仕組み（手数料は不要または少額）

②ブロックという概念がなくトランザクション単位の承認のため，ブロック構成・承認のための遅延は発生しない

③暗号資産はトランザクション内に点在するため、2重使用ではないことの確認が必要

DAG系暗号資産の特徴
ラティス型



①ブロックチェーンが複数存在し，資産の取引記録はそれぞれのブロックチェーンあるいは対象となるブロックチェーンに登録

②暗号資産はアカウント（アドレス）ごとに合算され管理

③暗号資産の提供時には指定したアカウントの資産残高が提供資産額以上であることを確認すればよい（2重使用の確認は必要ない）

DAG系暗号資産一覧

順位	名称	記号	時価総額
20	IOTA	MIOTA	¥59,007,350,027
40	Holo	HOT	¥13,149,824,493
47	Nano	NANO	¥10,649,007,809
80	HyperCash	HC	¥5,123,412,789
155	Fantom	FTM	¥1,841,928,035
161	Hedera Hashgraph	HBAR	¥1,692,095,702
188	Constellation	DAG	¥1,282,062,213
260	Obyte	GBYTE	¥1,332,713,823
306	IoT Chain	ITC	¥871,932,031
322	HYCON	HYC	¥780,201,587

2019年11月25日時点の次のサイトの情報より作成
All Cryptocurrencies https://coinmarketcap.com/all/views/all/

調査対象DAG系暗号資産

タングル型

IOTA ：2017年6月にリリース
<100~140 TPS>

Gbyte（Byteball） ：2016年12月にリリース
<20 TPS>

ラティス型

Nano（旧ReiBlocks） ：2014年にベータ版リリース
<70~700+ TPS>

Hedera Hashgraph ：2019年9月にベータ版リリース
<10K+ TPS>

処理性能は、下記資料による期待値
https://masterthecrypto.com/blockchain-scalability-solutions-crypto-scaling-solutions/

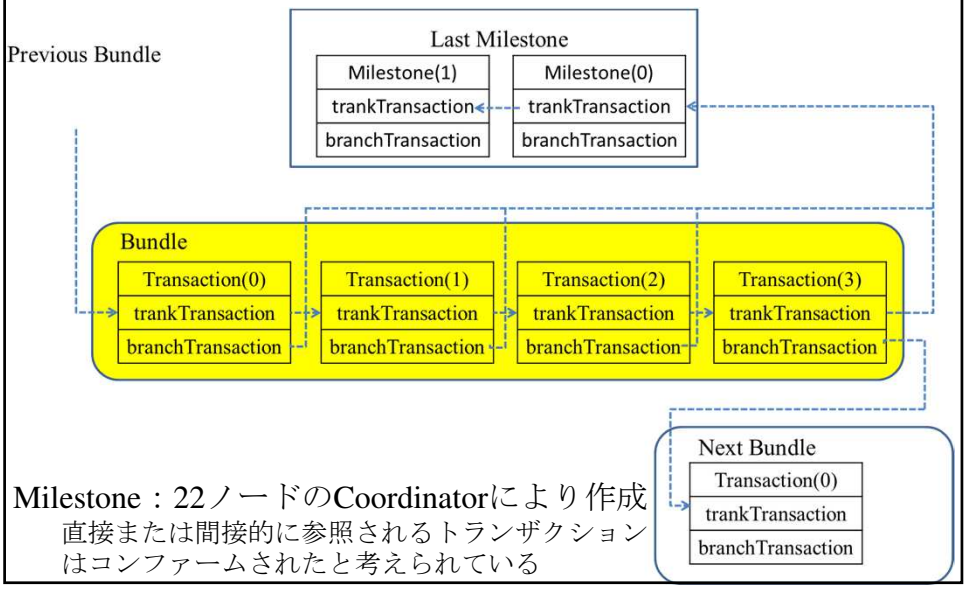
トランザクションの構成（匿名性に関連する情報のみ）

入力欄		出力欄	
入力項目1	使用する資産の位置（提供者のアドレスや金額等の情報が格納されている）	出力項目1	提供先（受取者）の指定（受取者のアドレス）
	指定資産の使用権の証明（公開鍵、署名）		提供額の指定（金額情報）
入力項目2	使用する資産の位置	出力項目2	提供先（受取者）の指定
	指定資産の使用権の証明		提供額の指定
.....		.....	
入力項目n	使用する資産の位置	出力項目m	提供先（受取者）の指定
	指定資産の使用権の証明		提供額の指定

DAG系暗号資産チェーンの匿名性に関する要件

要件名称	要件内容
Pseudonymity of User Identification Information(UII)（利用者識別情報の仮名性）	利用者識別情報（公開鍵、アドレス等）から実在する利用者の実名等の推定が困難であること
Unlinkability of UIIs（利用者識別情報間の非連結性）	複数の利用者識別情報が，同一の利用者に紐づけられていることの推定が困難であること
Untraceability of assets/users between Transactions（トランザクション間の暗号資産/利用者の非追跡性）	受取時の暗号資産（受取者）と提供に使用する暗号資産（提供者）の資産/利用者の対応の推定が困難であること
Untraceability of assets/users within Transaction（トランザクション内の暗号資産/利用者の非追跡性）	トランザクション内の提供資産/提供者と受取資産/受取者の対応の推定が困難であること
Concealment of Amount（移転資産額の秘匿）	暗号資産の提供額・受取額の推定が困難であること

IOTAタングル内の トランザクション/バンドルの繋がり



Milestone：22ノードのCoordinatorにより作成
直接または間接的に参照されるトランザクションはコンファームされたと考えられている

送金バンドルの基本形

	Transaction (0)	Transaction (1)	Transaction (2)	Transaction (3)
sigMF		UTXO使用権を示す署名（前半）	UTXO使用権を示す署名（後半）	
address	受取人アドレス	使用するUTXOアドレス	使用するUTXOアドレス	差額の送金先アドレス
value	送金額	減額する額	0	差額
currentindex	0	1	2	3
lastindex	3	3	3	3

4.DAG系暗号資産の匿名性：IOTA

 19

IOTA DAGチェーンの匿名性評価

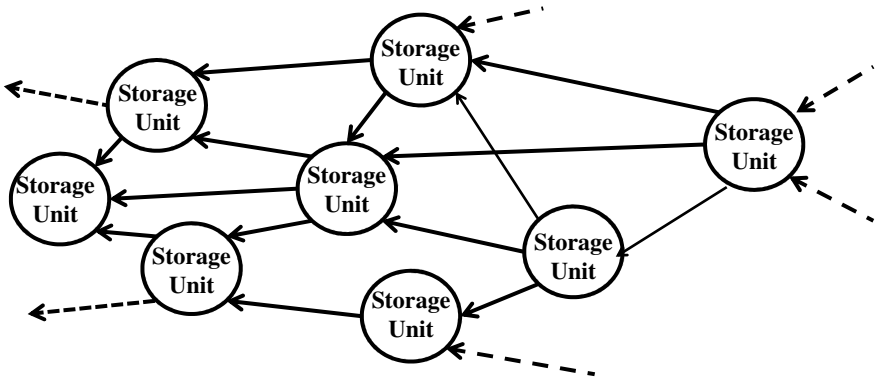
要件名称	評価	評価の根拠
Pseudonymity of UII	○	利用者識別情報であるアドレスは、利用者が選定したランダムなシードと未使用のインデックスから生成される（利用者固有の情報は使用されない）
Unlinkability of UIIs	○	利用者が選定したランダムなシードと未使用インデックスから、毎回異なるアドレスが生成され使用される（同一のアドレスの使用は秘密鍵漏洩に繋がりかねない）
Untraceability of assets/users between Transactions	×	提供に使用する暗号資産は未使用の資産が存在するアドレス（受取時のアドレス）を直接指定している
Untraceability of assets/users within Transaction	×	ワンタイムアドレスといえども、提供者と受取者のアドレスを直接指定している
Concealment of Amount	×	提供額・受取額を直接指定している

4.DAG系暗号資産の匿名性：Obyte

 20

ObyteのDAGchain

Obyte Storage Unit Chain



Witness：ユニットの承認を行う特別なノード
15のWitnessが登録されており、利用者は12のWitnessを選択

4.DAG系暗号資産の匿名性：Obyte

 21

Obyteの資産移転を示すトランザクションのストレージユニット構成

入力欄		出力欄	
入力項目1	使用する資産1を含むストレージユニットのハッシュ値	出力項目1	提供先（受取者）のObyteアドレス1
	使用する資産1を含むストレージユニット内のメッセージインデックス		
	使用する資産1のメッセージ内インデックス		提供額
·····		·····	
入力項目n	使用する資産nを含むストレージユニットのハッシュ値	出力項目m	提供先（受取者）のObyteアドレスm
	使用する資産nを含むストレージユニット内のメッセージインデックス		
	使用する資産nのメッセージ内インデックス		提供額
ストレージユニット作成者達の署名		提供者のObyteアドレス1	認証データ1
		·····	
		提供者のObyteアドレスn	認証データn
ストレージユニットの親ストレージユニットのハッシュ値		親ストレージユニットのハッシュ値1	
		·····	
		親ストレージユニットのハッシュ値k	

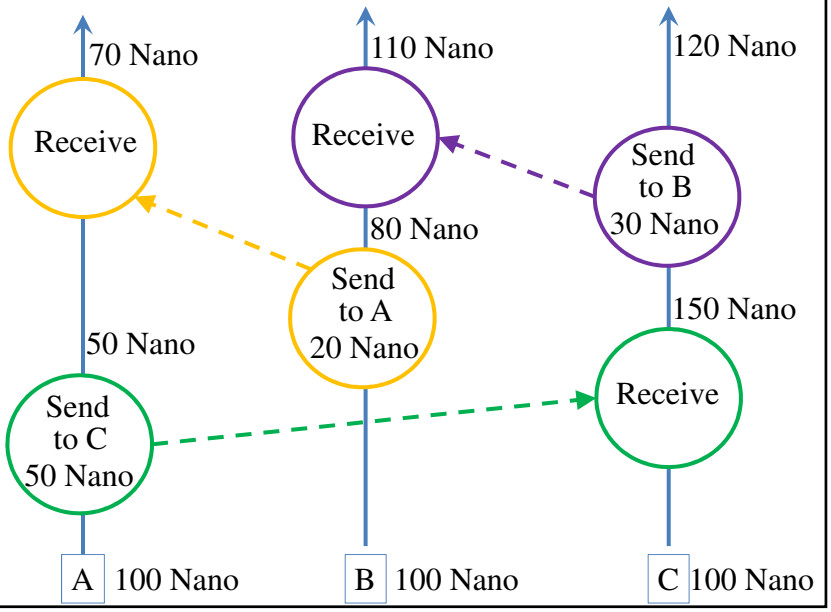
4.DAG系暗号資産の匿名性：Obyte

 22

Obyte DAGチェーンの匿名性評価

要件名称	評価	評価の根拠
Pseudonymity of UII	○	鍵ペアは乱数により生成され、利用者固有の情報は使用されない
Unlinkability of UIIs	○	必要の都度、乱数により生成されたアドレスの使用が推奨されている
Untraceability of assets/users between Transactions	×	トランザクションで使用する暗号資産は、その未使用資産が存在する位置（トランザクションのハッシュ値およびトランザクション内の位置）を指定している
Untraceability of assets/users within Transaction	×	ワンタイムアドレスといえども、提供者と受取者のアドレスを直接指定している
Concealment of Amount	×	提供額・受取額を直接指定している

Nanoのアカウントチェーンの例



Nanoのトランザクション

提供（送信）トランザクション	
トランザクションの型	“send”
提供先のアカウントアドレス	受取アカウントのアドレス
提供アカウントの残高	提供アカウントの今回の送信後の残高
提供アカウントのアカウントチェーンの直前のトランザクション	当該トランザクションのハッシュ値
Nonce（Proof of Work）	条件を満たすNonce（スパム対策）
署名	提供アカウントのトランザクションへの署名

受取（受信）トランザクション	
トランザクションの型	“receive”
受け取る提供（送信）トランザクション	提供（送信）トランザクションのハッシュ値
受取アカウントのアカウントチェーンの直前のトランザクション	当該トランザクションのハッシュ値
Nonce（Proof of Work）	条件を満たすNonce（スパム対策）
署名	受取アカウントのトランザクションへの署名

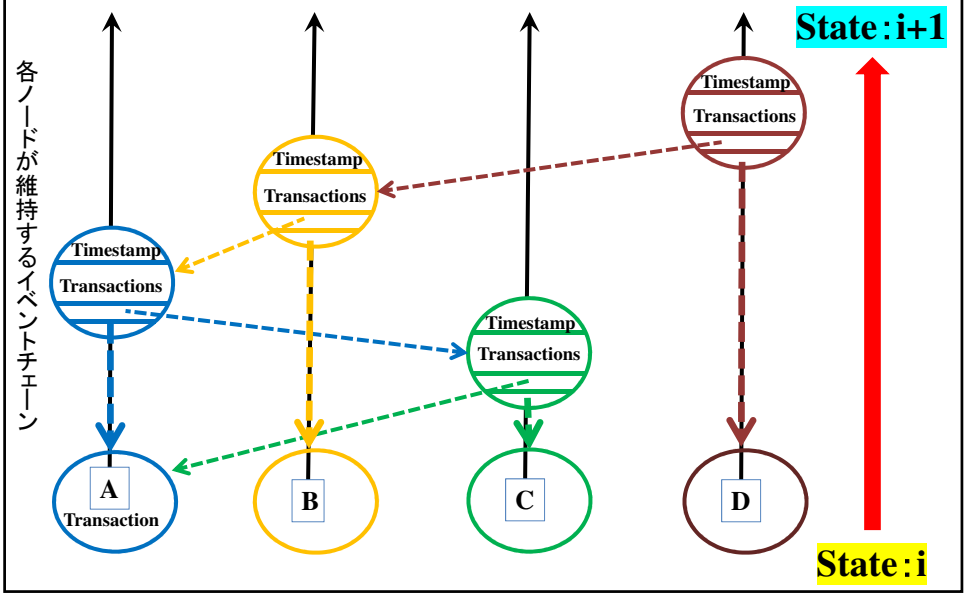
4.DAG系暗号資産の匿名性：Nano

Nano DAGチェーンの匿名性評価

要件名称	評価	評価の根拠
Pseudonymity of UII	○	個々のアカウントに対応する鍵ペア、アドレスは、乱数で生成されるワレットのシードまたは乱数より生成され使用される
Unlinkability of UIIs	△	必要に応じ新たな鍵ペア、アドレスを使用することができるが、一般には資産を合算し管理するアカウントの数はトランザクションの数よりかなり少ないことが想定され、同じアドレスが使用される可能性が高い
Untraceability of assets/users between Transactions	×	暗号資産は個々のトランザクションで管理されるわけではなく、利用者のアカウントに合算され管理される。提供に使用する場合、そのアカウントアドレスを直接指定している
Untraceability of assets/users within Transaction	×	提供者と受取者のアカウントアドレスを指定している
Concealment of Amount	×	提供額・受取額を直接指定している

4.DAG系暗号資産の匿名性：Hedera Hashgraph

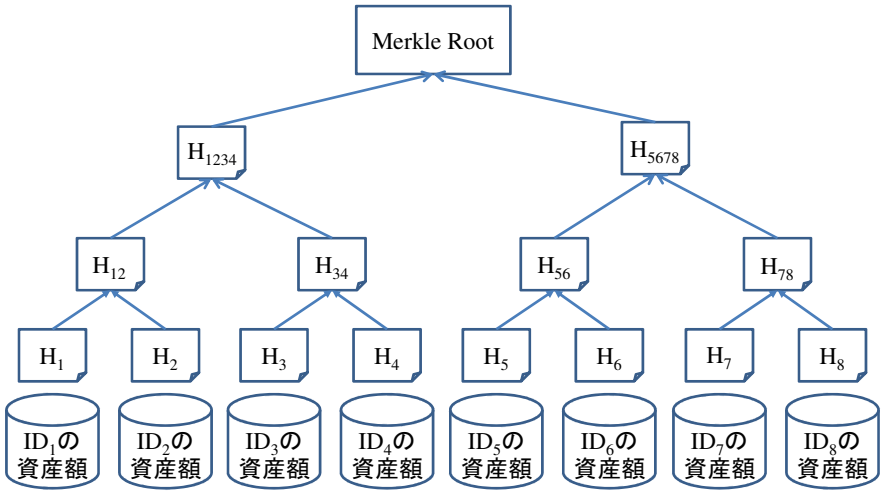
Hedera HashgraphのDAGチェーンの例



Hedera Hashgraphトランザクション

トランザクション		
転送$_1$	アカウントID$_1$	転送資産額$_1$
転送$_2$	アカウントID$_2$	転送資産額$_2$
署名	提供アカウントによる トランザクションへの署名	

各時点のState例
（各アカウントIDが保有する資産額を格納）



4.DAG系暗号資産の匿名性：Hedera Hashgraph

Hedera HashgraphのDAGチェーンの匿名性評価

要件名称	評価	評価の根拠
Pseudonymity of UII	○	個々のアカウントに対応する鍵ペアは乱数により生成され、アカウントIDはシステムが自動的に付与し、使用される
Unlinkability of UIIs	△	必要に応じ新たなアカウントを生成し、鍵ペア、アカウントIDを使用することができるが、一般には資産を合算し管理するアカウントの数はトランザクションの数よりかなり少ないことが想定され、同じアドレスが使用される可能性が高い
Untraceability of assets/users between Transactions	×	暗号資産は個々のトランザクションで管理されるわけではなく、利用者のアカウントに合算され管理される。提供に使用する場合、そのアカウントIDを直接指定している
Untraceability of assets/users within Transaction	×	提供者と受取者のアカウントIDを指定している
Concealment of Amount	×	提供額・受取額を直接指定している

5. まとめ

DAG系暗号資産の匿名性の比較

要件名称	IOTA	Obyte	Nano	Hedera	Bitcoin
Pseudonymity of User Identification Information(UII)（利用者識別情報の仮名性）	○	○	○	○	○
Unlinkability of UIIs（利用者識別情報間の非連結性）	○	○	△	△	○
Untraceability of assets/users between Transactions（トランザクション間の利用者/暗号資産の非追跡性）	×	×	×	×	×
Untraceability of assets/users within Transaction（トランザクション内の利用者/暗号資産の非追跡性）	×	×	×	×	×
Concealment of Amount（移転資産額の秘匿）	×	×	×	×	×

ビットコインをはじめとする一般のブロックチェーン系暗号資産に比べ，
タングル型の場合は同程度の匿名性，ラティス型の場合は匿名性は低い、という結果

（参考）DAG系匿名暗号資産DERO

①Moneroと同様の匿名化

CryptoNote Protocol（リング署名、ペダーセンコミットメント等）

②推定される匿名性

Pseudonymity of UII ➔ ○

Unlinkability of UIIs ➔ ○

Untraceability of assets/users between Transactions ➔ △

Untraceability of assets/users within Transaction ➔ △

Concealment of Asset amount ➔ ○

（ブロック/トランザクションの具体的なデータ構造は未公開？）

DAG系暗号資産で高い匿名性を主張している暗号資産（DERO以外）

Cardano（ADA）、Aidos Kuneen、Tangram（Sneak）、COTI等

終

ご清聴、ありがとうございました。