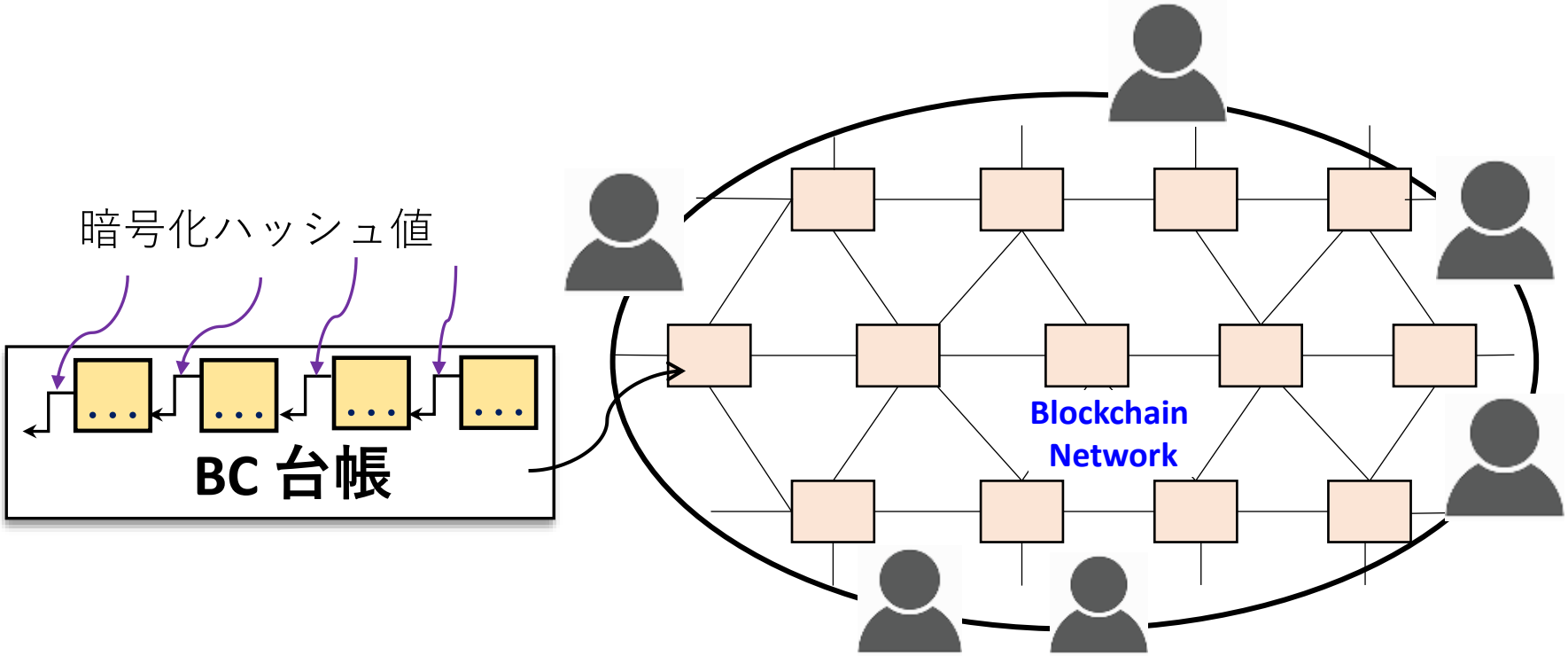
高効率な産業のためのブロックチェーン ハードウェア・ソフトウェアシステム

奈良先端科学技術大学院大学　情報科学領域
コンピュティング・アーキテクチャ研究室研究科

助教　トラン ティ ホン

2021年10月15日

ブロックチェーン（BC）とは？



- 分散型 (Decentralized)
- 不変性 (Immutable)
- 透明性 (Transparent)

BCはSDGs、New Normal、Society 5.0の開発に重要な技術である

内容

新技術説明会
New Technology Presentation Meetings!

- ブロックチェーンハードウェアアクセラレータ（**BCA**）
  - ✓汎用用
  - ✓ブロックチェーンネットワークマイニング用

- ブロックチェーンソフトウェア
  - ✓Vac-chain: COVID-19ワクチンの管理・トレーサビリティシステムの開発

BCAとは？

新技術説明会
New Technology Presentation Meetings!

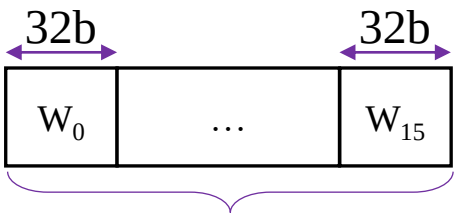
BCAは、ブロックチェーンネットワークを保護するため暗号化ハッシュ値(SHA-2, SHA-3など)を求めるハードウェア回路。BCAは、以下のアプリケーションに適用する：

- 分散型ブロックチェーンネットワークの保護
- IoTネットワークに対するデータ整合性とプライバシの保護
- デジタル署名
- ハッシュベースのメッセージ認証コード（HMAC)
- など。。。

SHA-256

13 × 48 operators

48 loops



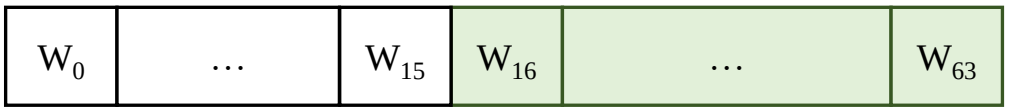
512-b input data

ME process

$$W_j = \sigma_1(W_{j-2}) + W_{j-7} + \sigma_0(W_{j-15}) + W_{j-16}$$

$$\sigma_0(x) = S^7(x) \oplus S^{18}(x) \oplus R^3(x)$$

$$\sigma_1(x) = S^{17}(x) \oplus S^{19}(x) \oplus R^{10}(x)$$



MC process

256-bit hash

26 × 64 operators

64 loops

$$Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$$

$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

$$\Sigma_0(x) = S^2(x) \oplus S^{13}(x) \oplus S^{22}(x)$$

$$\Sigma_1(x) = S^6(x) \oplus S^{11}(x) \oplus S^{25}(x)$$

$$T_1 = h + \Sigma_1(e) + Ch(e,f,g) + K_j + W_j$$

$$T_2 = \Sigma_0(a) + Maj(a,b,c)$$

$$h \leftarrow g;\ g \leftarrow f;\ f \leftarrow e;\ e \leftarrow d + T_1$$

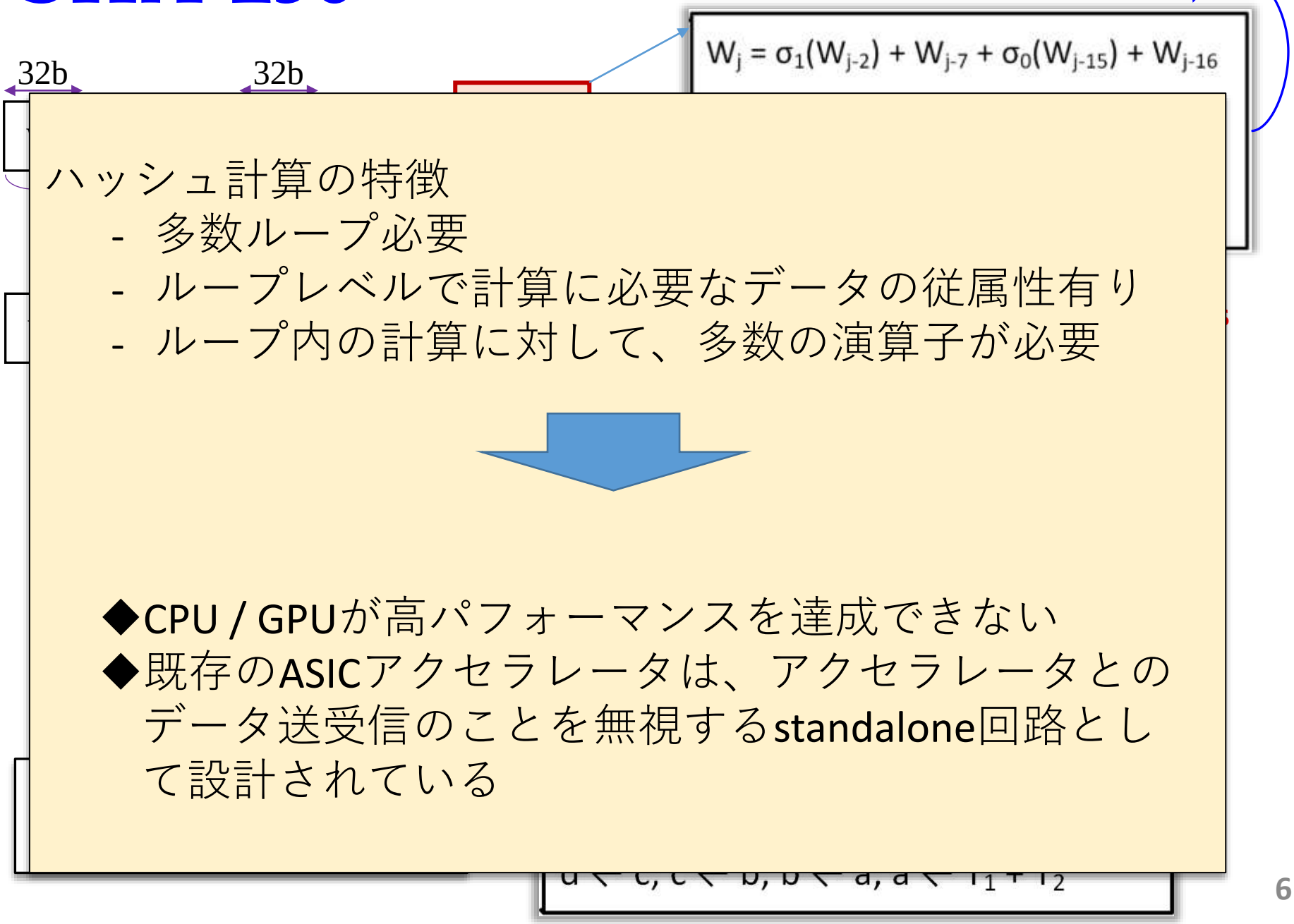
$$d \leftarrow c;\ c \leftarrow b;\ b \leftarrow a;\ a \leftarrow T_1 + T_2$$

>2000 operators for calculating 1 hash value

SHA-256

13×48 operators

48 loops



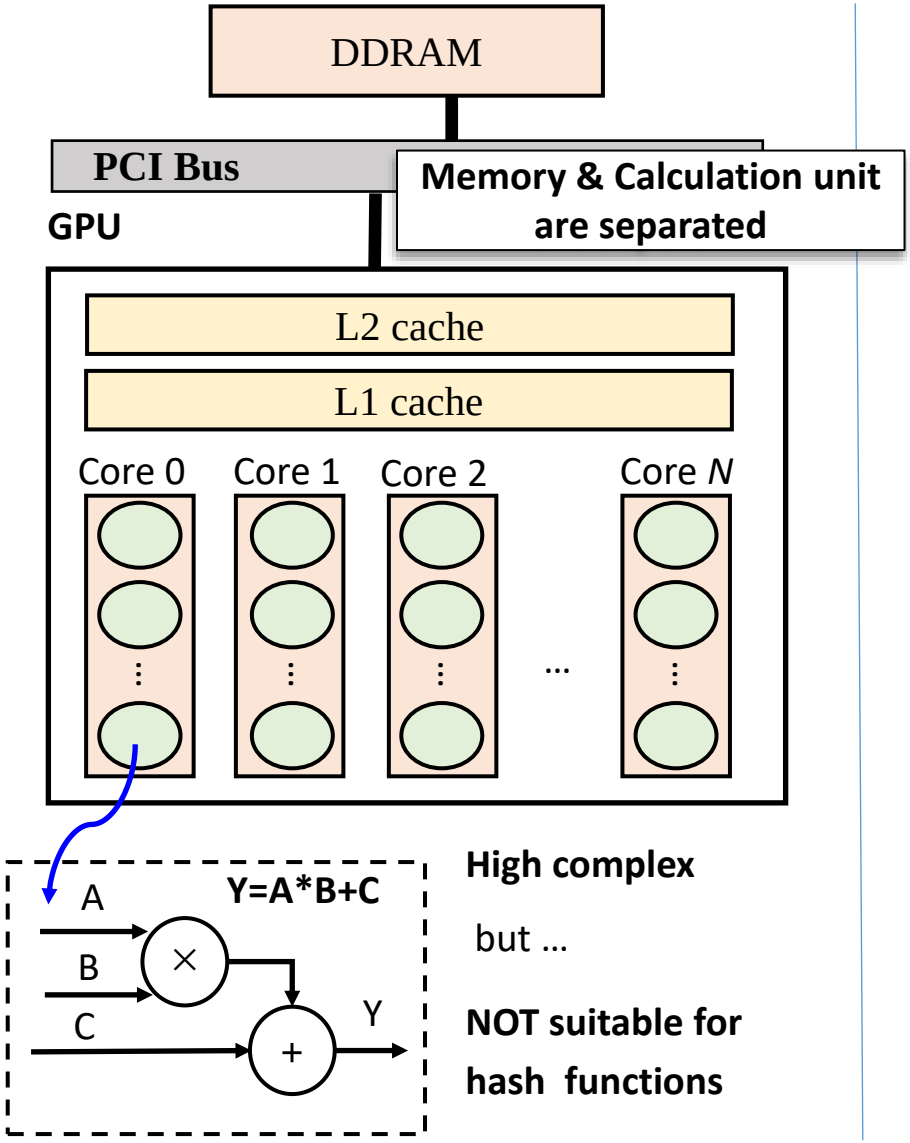
ハッシュ計算の特徴

- 多数ループ必要
- ループレベルで計算に必要なデータの従属性有り
- ループ内の計算に対して、多数の演算子が必要

◆CPU / GPUが高パフォーマンスを達成できない

◆既存のASICアクセラレータは、アクセラレータとのデータ送受信のことを無視するstandalone回路として設計されている

従来技術とその問題点

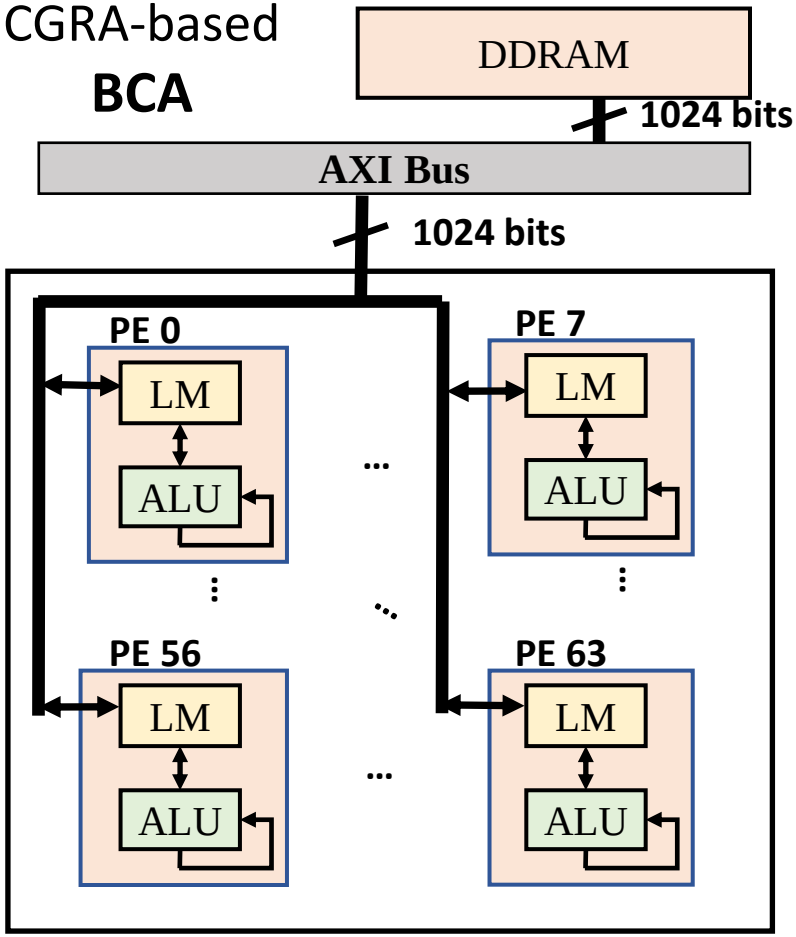


High complex

but …

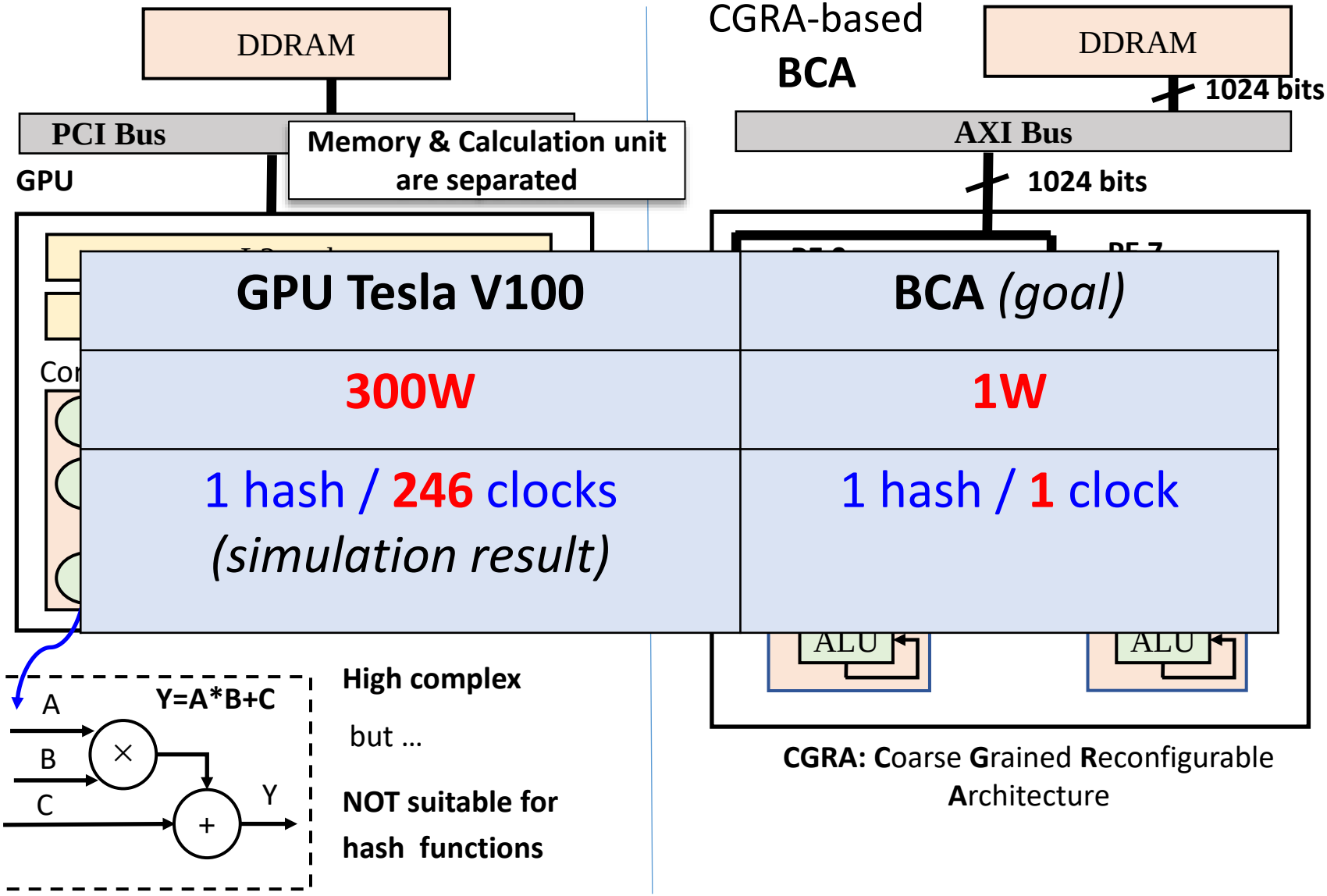
NOT suitable for hash functions

CGRA-based **BCA**

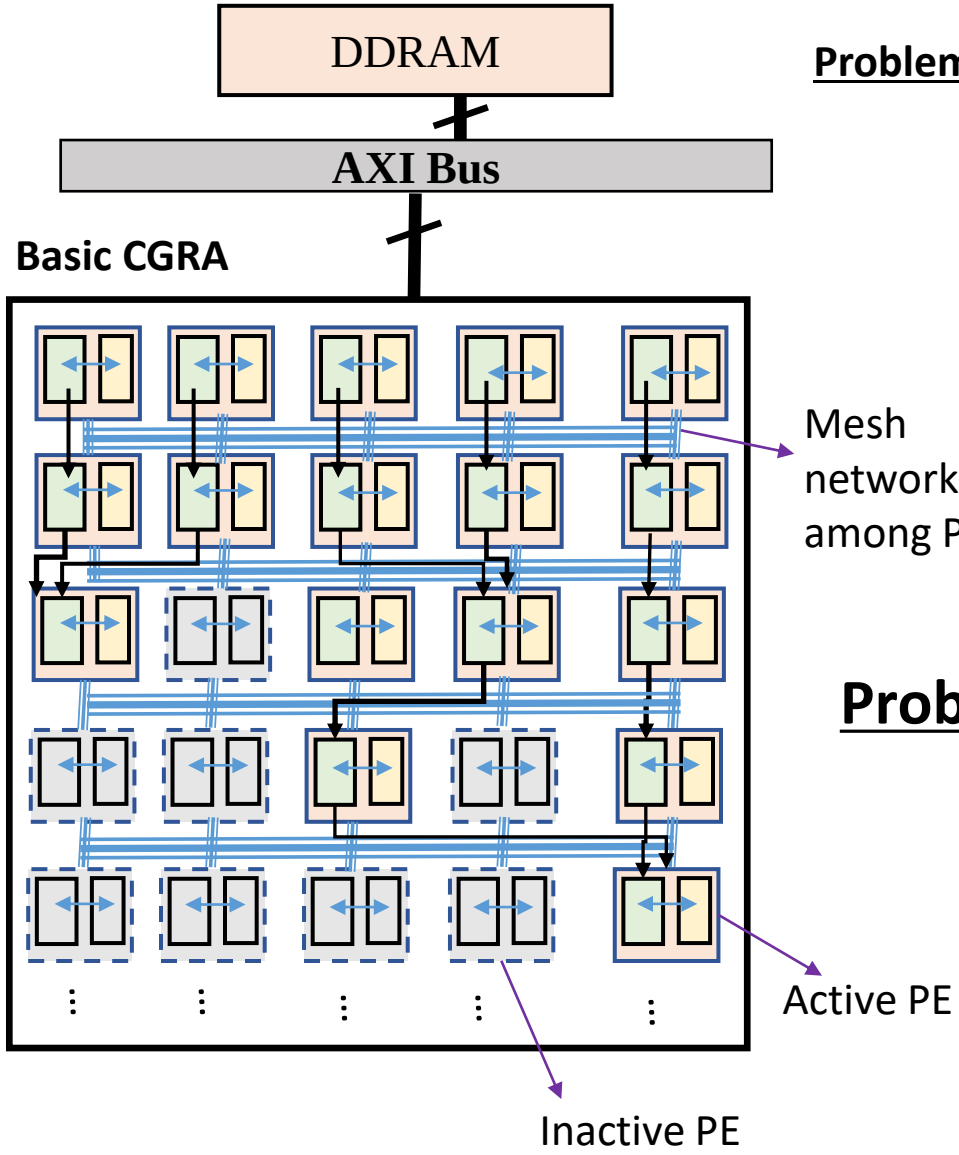


CGRA: **C**oarse **G**rained **R**econfigurable **A**rchitecture

従来技術とその問題点


DDRAM
PCI Bus
GPU
Memory & Calculation unit are separated
CGRA-based
BCA
DDRAM
1024 bits
AXI Bus
1024 bits
ALU
ALU
GPU Tesla V100
BCA (goal)
300W
1W
1 hash / 246 clocks
(simulation result)
1 hash / 1 clock
A
B
C
Y=A*B+C
Y
High complex
but …
NOT suitable for
hash functions
CGRA: Coarse Grained Reconfigurable Architecture

従来技術とその問題点



Problem 1: Multiple PEs / hash loop

Low speed, low efficiency

Problem 2: Mesh network among PEs

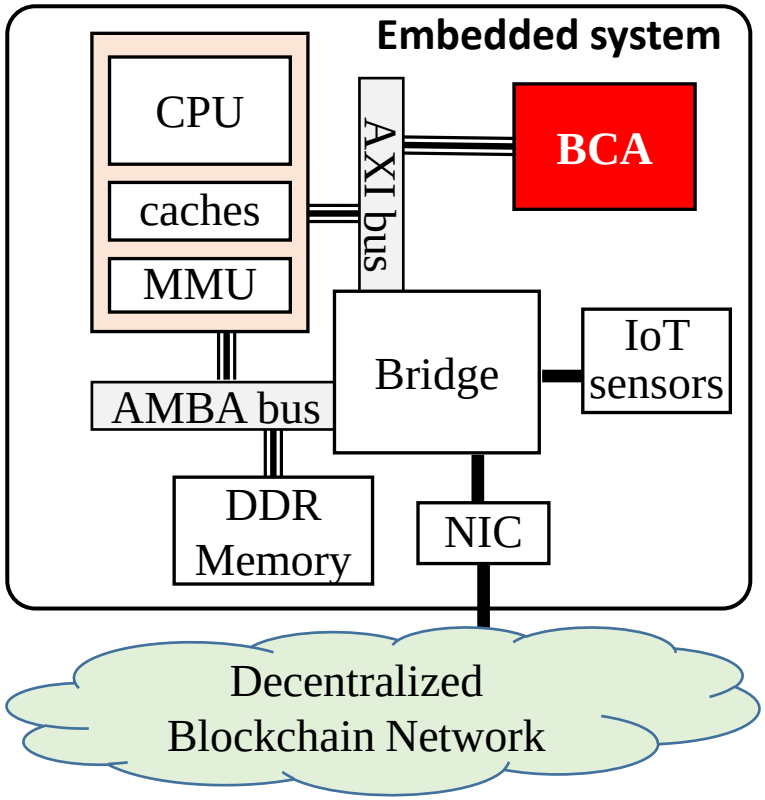
Large area &
High power consumption

BCA：目標と特徴

新技術説明会
New Technology Presentation Meetings!

目標：

- 高処理速度
- 低消費電力
- データ送受信の問題の解決



特徴：

- Pipelined ALU
- Multiple Local Memory
- Double Processing Elements
- Cascaded BCAs

内容説明

新技術説明会
New Technology Presentation Meeting

BCA Arch 1:
汎用用 SHA-256の計算機

アプリケーション：

- IoTネットワークに対するデータ整合性とプライバシの保護
- デジタル署名
- ハッシュベースのメッセージ認証コード（HMAC)

特徴：

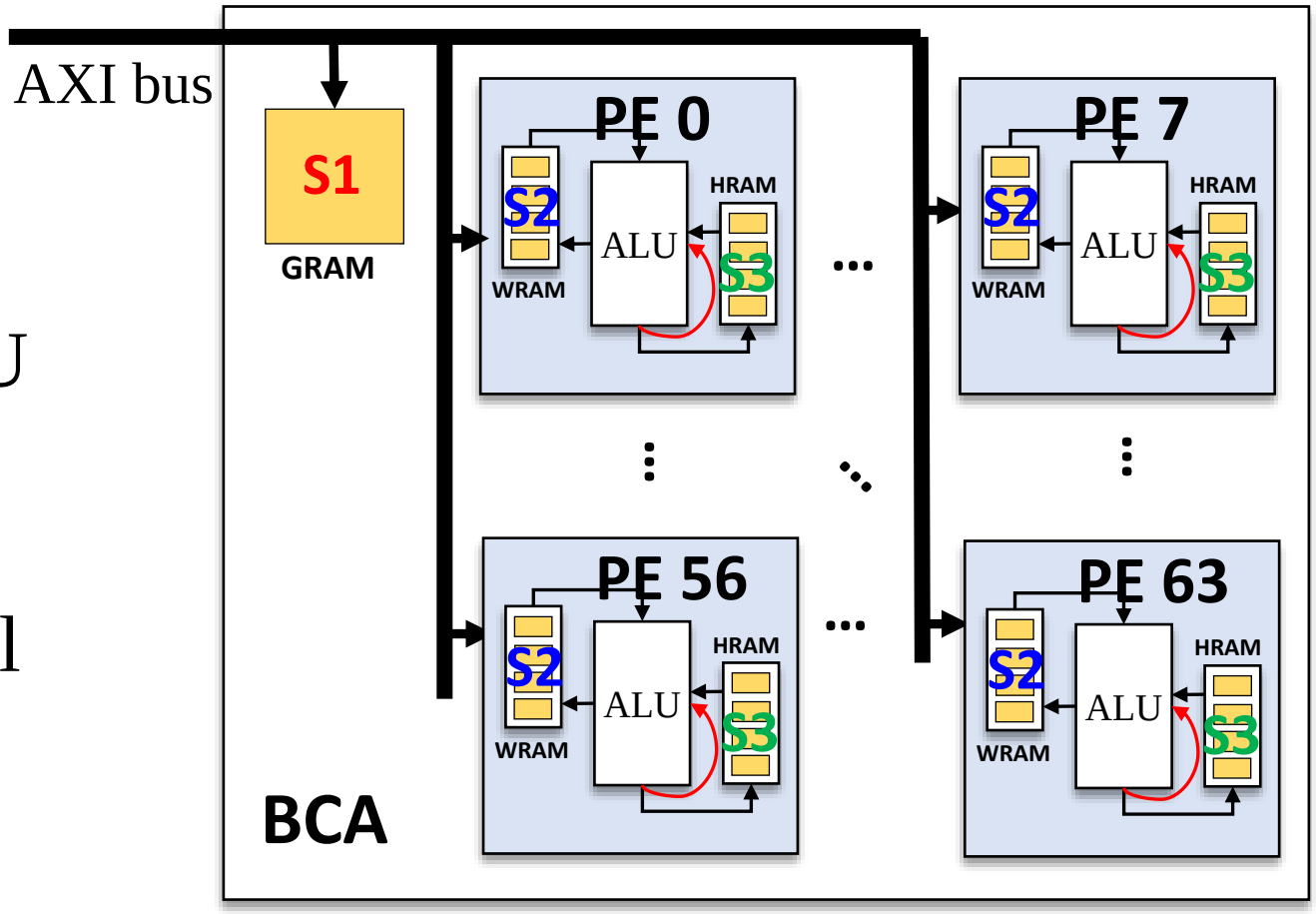
- BCAは、相互に**関連なし**ハッシュ関数を計算します
- 低処理速度で結構ですが、超低消費電力が必要です。

BCA Arch-1の概要アーキテクチャ

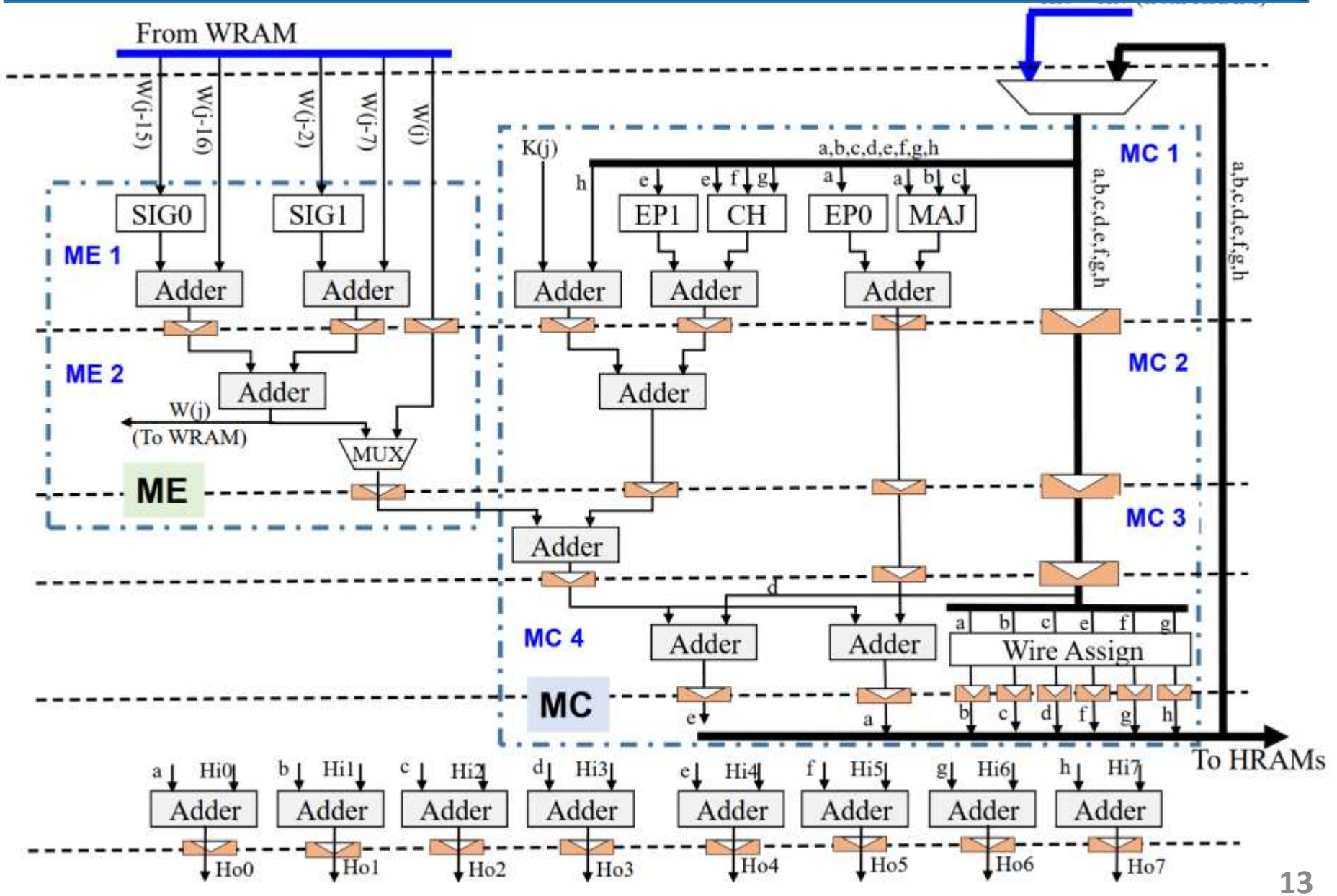
◆**Point 1:**
Pipelined ALU

◆**Point 2:**

Multiple Local Memory (Multimem)



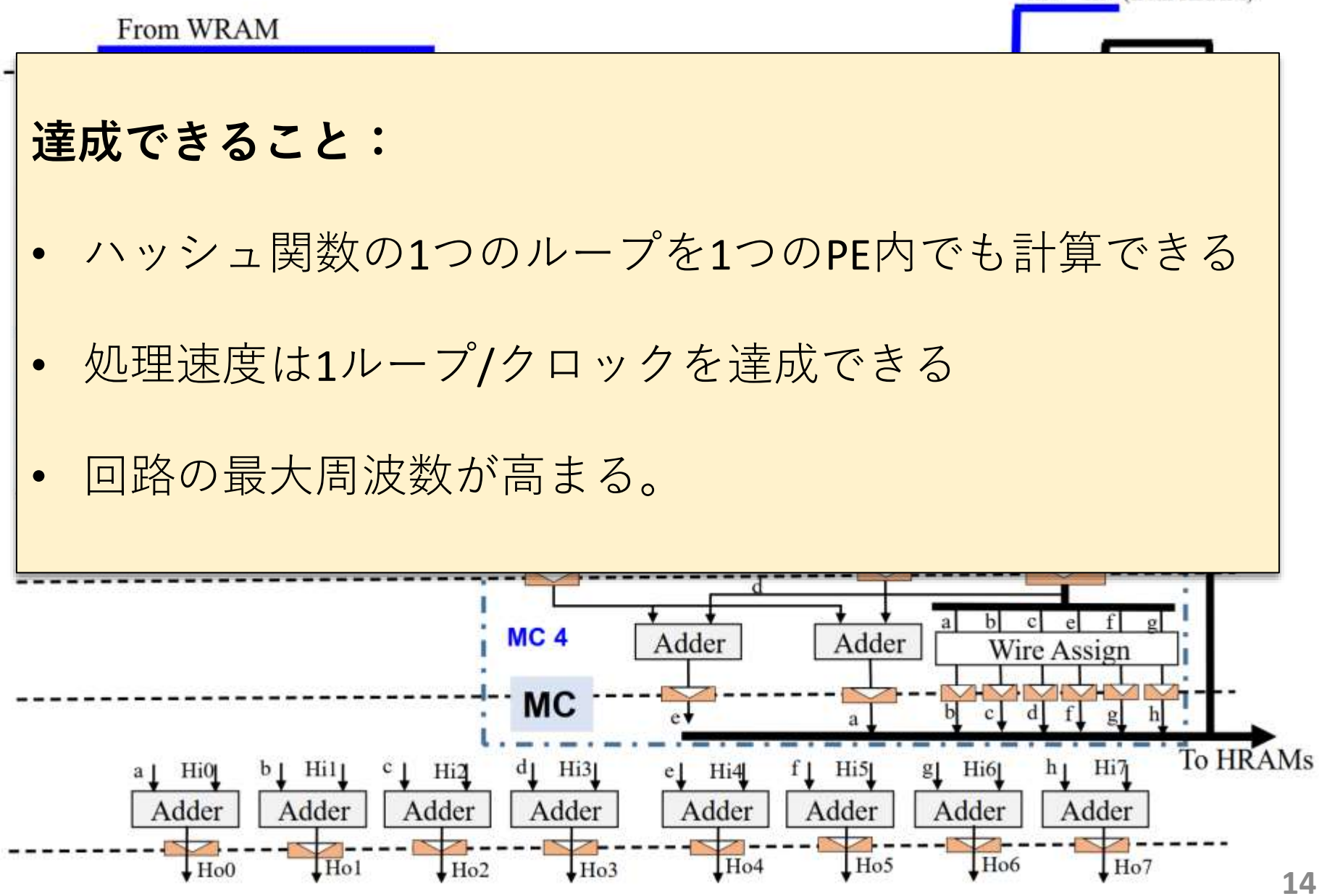
Point 1: Pipelined ALU



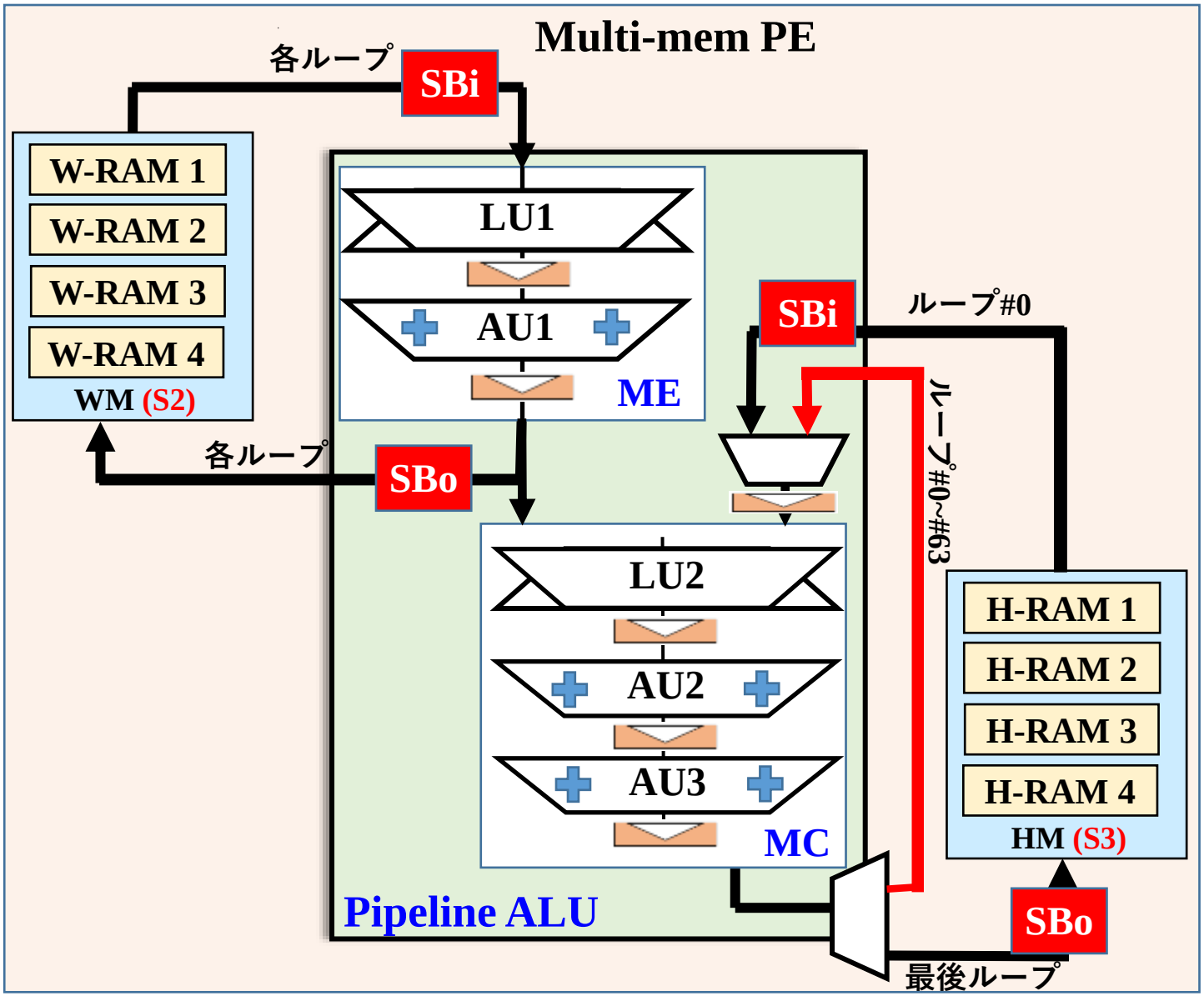
Point 1: Pipelined ALU

達成できること：

- ハッシュ関数の1つのループを1つのPE内でも計算できる
- 処理速度は1ループ/クロックを達成できる
- 回路の最大周波数が高まる。



Point 2: Multimem



Point 2: Multimem

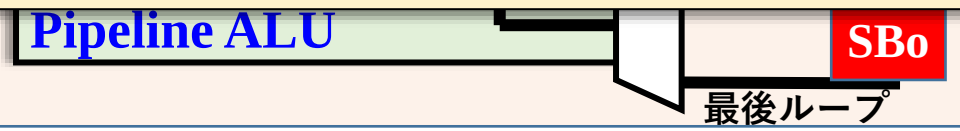
新技術説明会
New Technology Presentation Meetings!

達成できること：

◆ ALUには、クロックごとに15ワードのデータが必要であり、ローカルメモリがALUに十分なデータを効率的に提供する方法が必要。

提案されたMultimem（W-RAM、H-RAM）は、次のことを実現できる:

- 外部データアクセスを回避するのにALUに十分なデータを提供する
- ALUが100％の効率を達成できるようにする



16

内容説明

新技術説明会
New Technology Presentation Meetings!

BCA Arch 2:
ブロックチェーンネットワークマイニング用 Double SHA-256の計算機

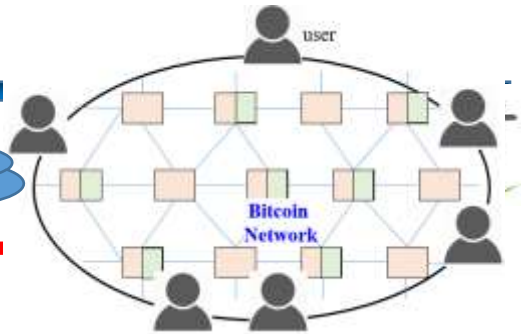
アプリケーション：

- Blockchain network mining

特徴：

- BCAは、Nonce値を変更することにより、ハッシュ関数を複数回計算する
- 高処理速度

BCAの応用 – Blockchain Mining



Mining pool
(transactions)

Merkle tree
hash

SHA-256

+1

Ver.	Prev. hash	Merkle Root	Time	Target	Nonce

Double
SHA-256

BCA

No

< target?

Yes

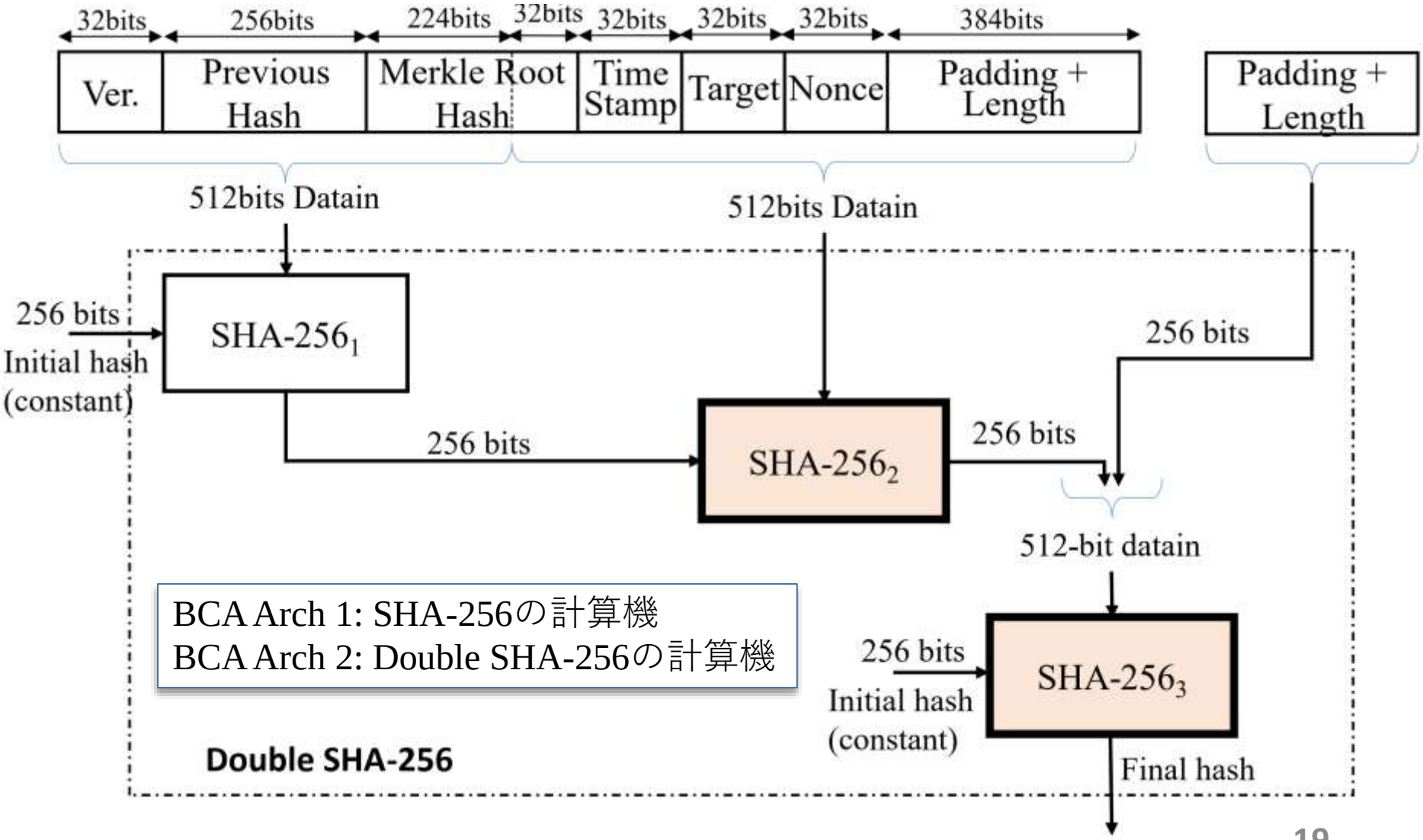
Header	Current block hash	Transaction raw data

Broadcast

Average 10^{20} repeat per block!

High speed low power Double SHA-256 circuit is required!

BCAの応用 – **Blockchain Mining**

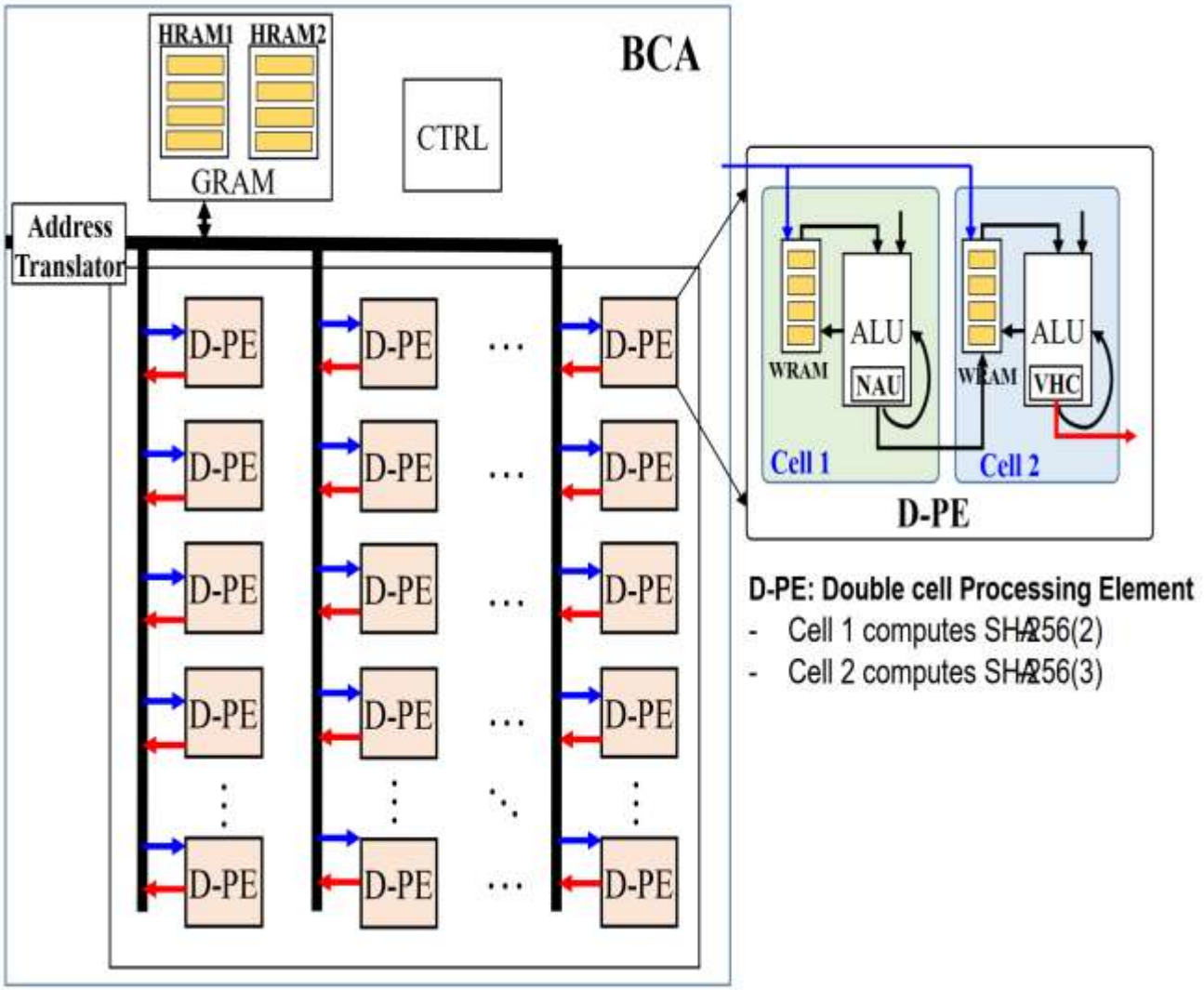


BCA Arch-2の概要アーキテクチャ

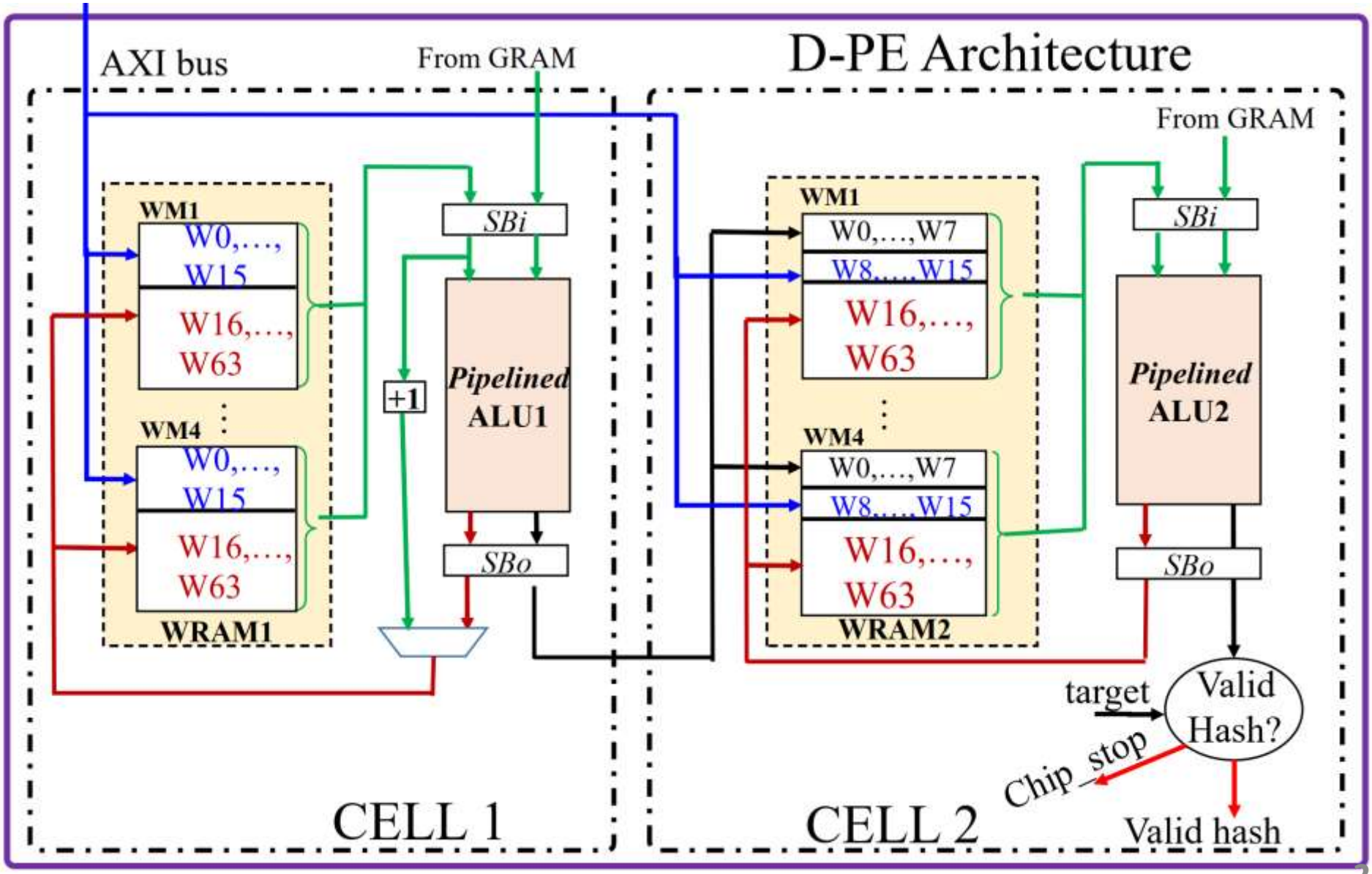
新技術説明会
New Technology Presentation Meetings!

◆**Point 3:**
Double-PE Architecture

◆**Point 4:**
Cascaded BCAs



Point 3: Double PE Architecture



Point 3: Double PE Architecture

新技術説明会
New Technology Presentation Meetings

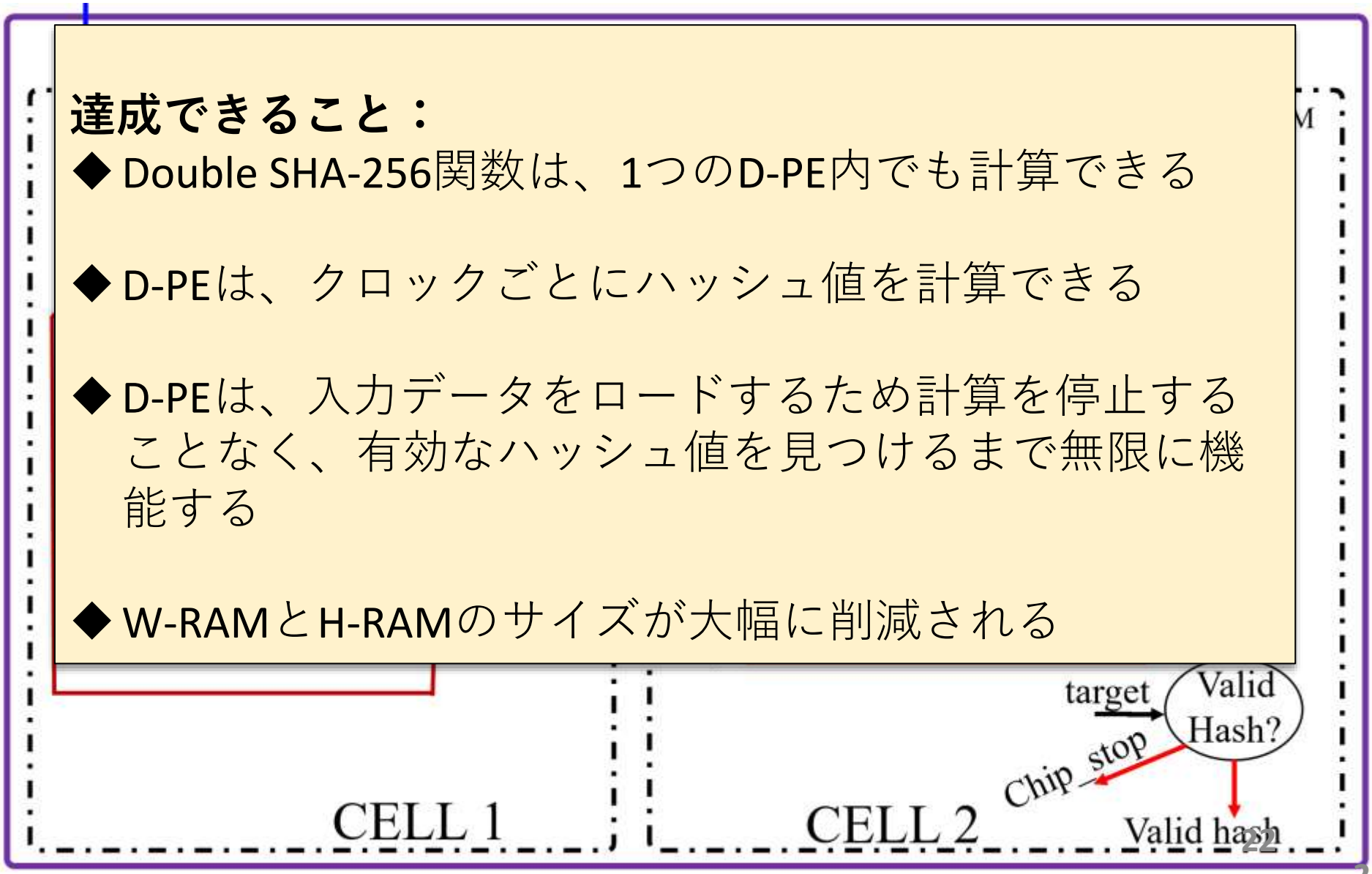
達成できること：

◆ Double SHA-256関数は、1つのD-PE内でも計算できる

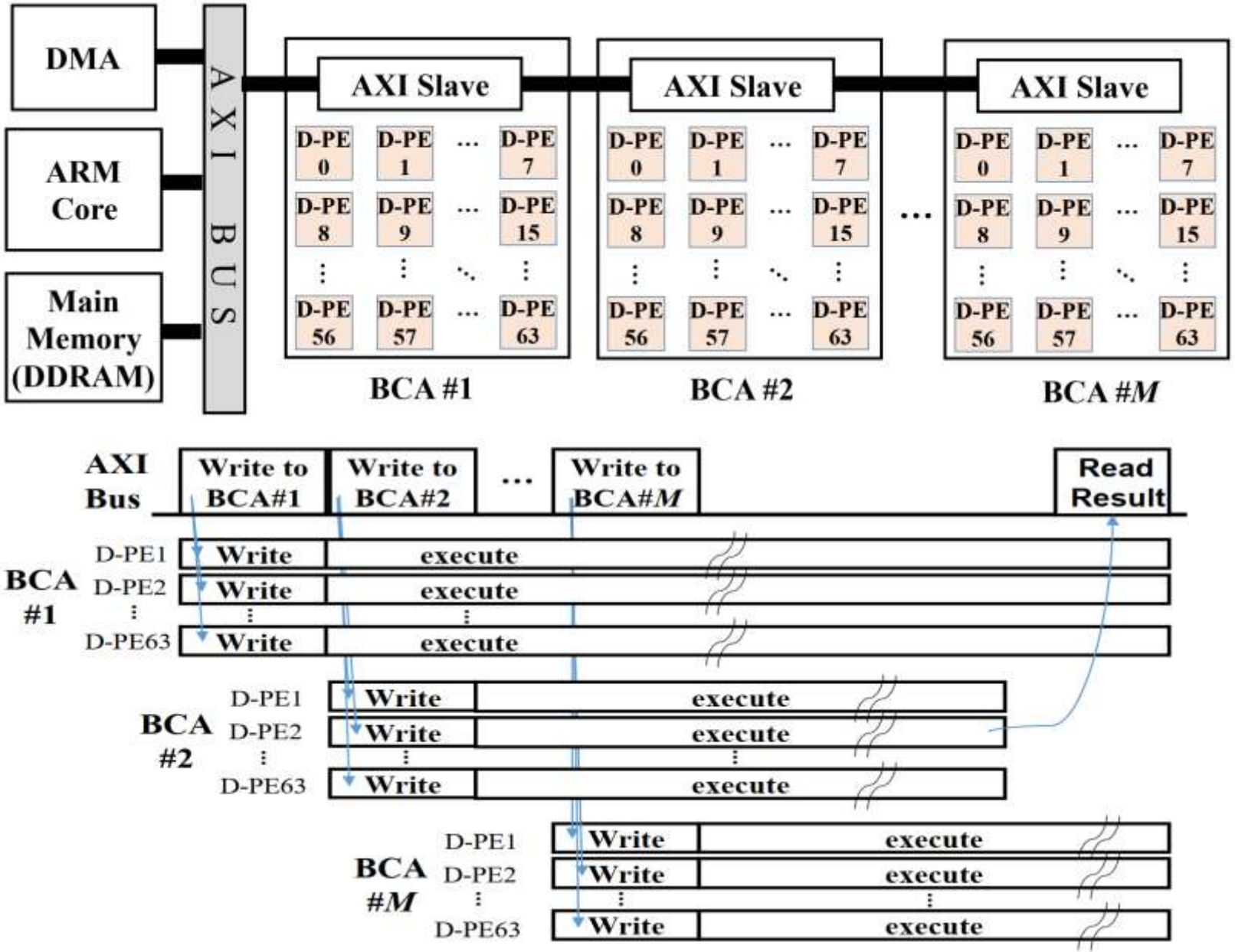
◆ D-PEは、クロックごとにハッシュ値を計算できる

◆ D-PEは、入力データをロードするため計算を停止することなく、有効なハッシュ値を見つけるまで無限に機能する

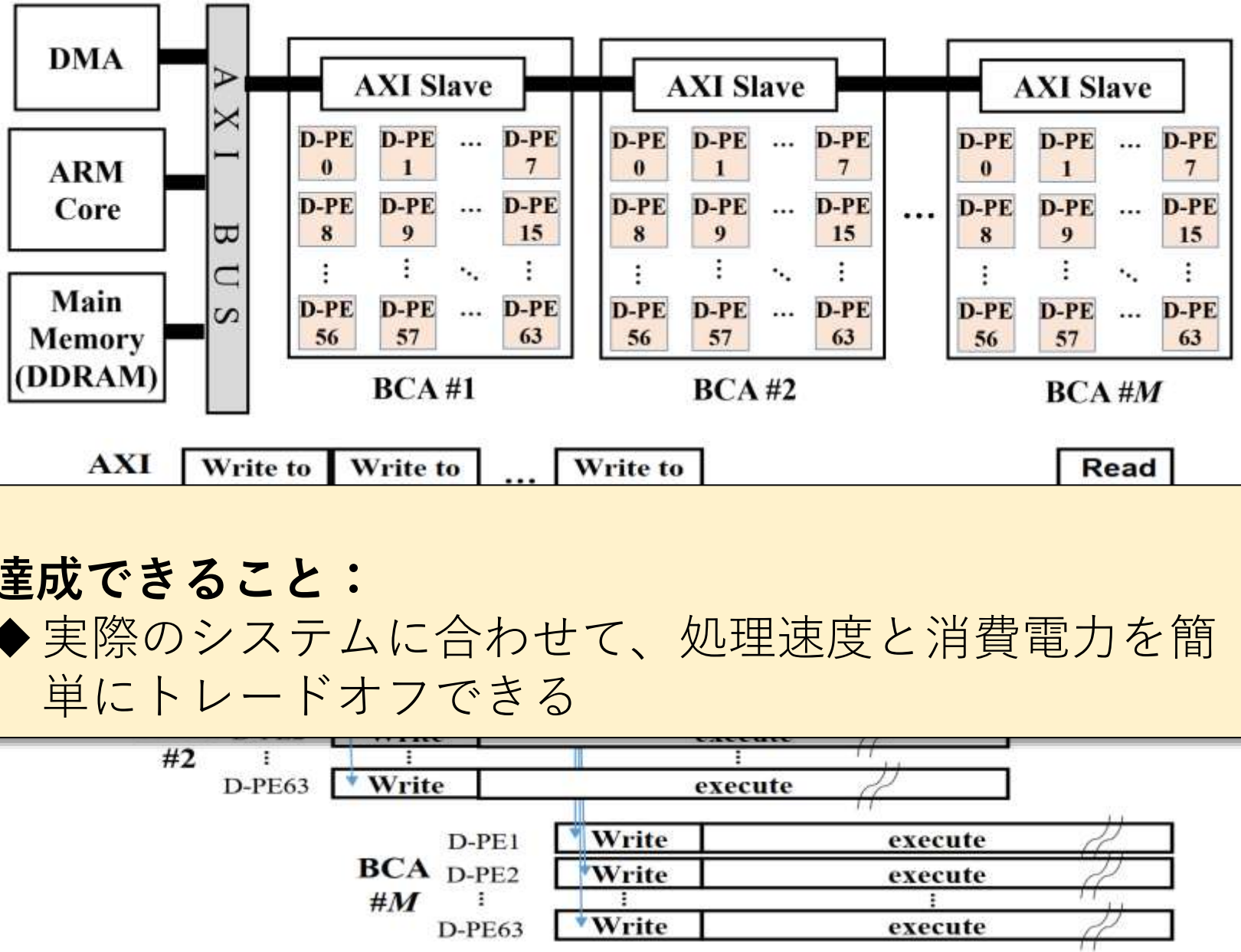
◆ W-RAMとH-RAMのサイズが大幅に削減される



Point 4: Cascaded BCA chips



Point 4: Cascaded BCA chips



達成できること：

◆実際のシステムに合わせて、処理速度と消費電力を簡単にトレードオフできる

実験の結果

新技術説明会
New Technology Presentation Meetings!

Platform		Tech.	Power (W) Measured	Exec. Time (second)	Throughput (Mhps)	Power Eff. (Mhps/W)	Area Eff. (Mhps/mm^2)
CPU Intel i9-10940X		ASIC 14 nm	164	394.77	11	0.67	-
GPU GTX 1080 Ti, 11 GB		ASIC 16 nm	188	23.26	185	0.98	0.393
GPU RTX 3070, 8 GB		ASIC 8 nm	197	20.78	207	1.05	0.528
GPU RTX 3090, 24 GB		ASIC 8 nm	346	10.45	411	1.19	0.654
GPU Tesla V100, 16 GB		ASIC 12 nm	163	13.04	329	2.02	0.404
Prop. BCA	FPGA ALVEO U280	FPGA 16 nm	**8.38**	11.95	360	**43**	-
	Layout Chip	ASIC 65 nm	**0.53**	-	90	**170** 1,381**	**3.6** 238*

* : Normalized area efficiency = Area Eff. × $(65\ nm/8\ nm)^2$
** : Normalized power efficiency = Power Eff. × $(65\ nm/8\ nm)$

CPU: **64 times**
GPU RTX 3090: **36 times**

内容

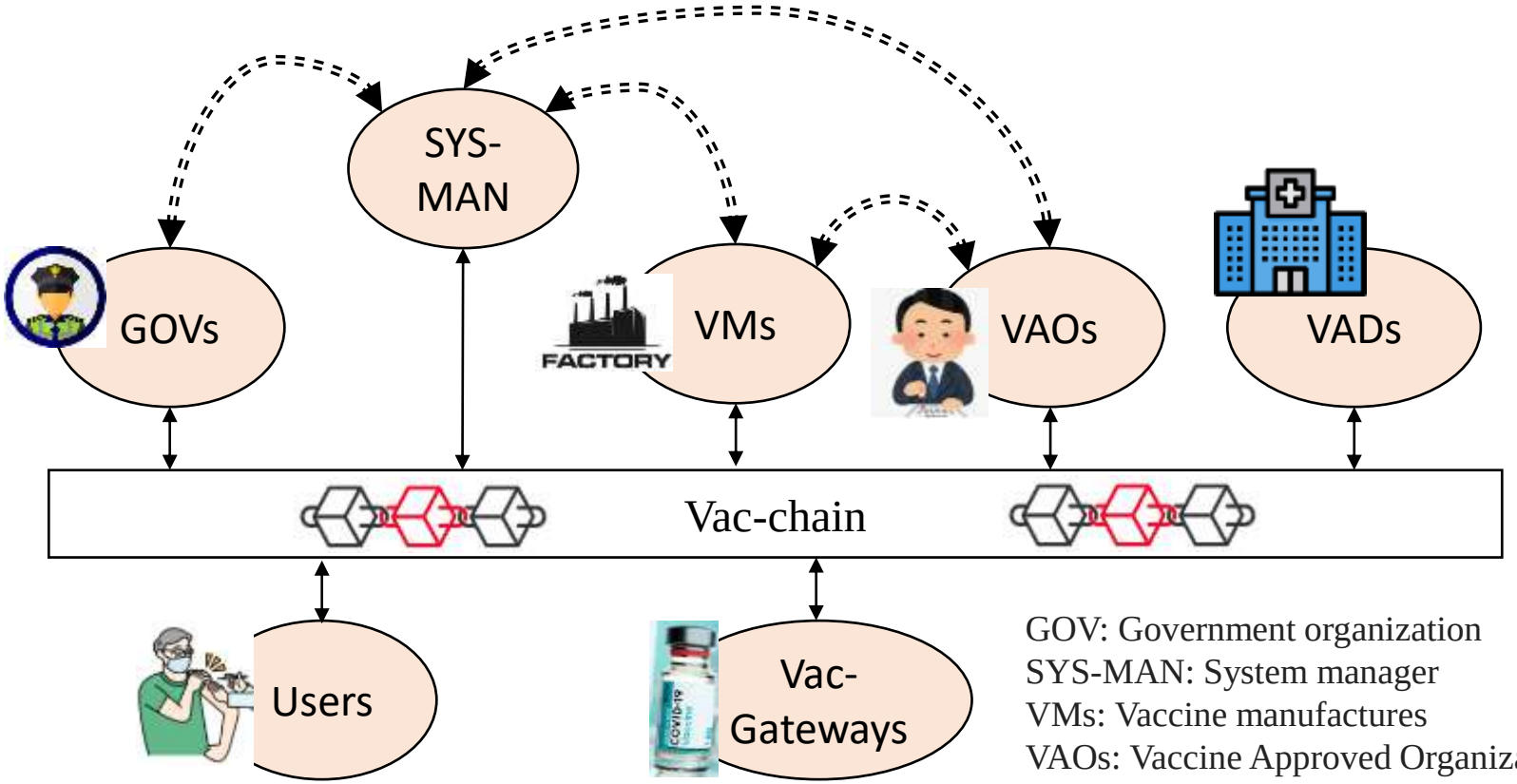
- ブロックチェーンハードウェアアクセラレータ(BCA）
  - ✓汎用用
  - ✓ブロックチェーンネットワークマイニング用

- **ブロックチェーンソフトウェア**
  - ✓Vac-chain: COVID-19ワクチンの管理・トレーサビリティシステムの開発

Vac-chainシステムの概要

Vac-chainの解決できる問題：

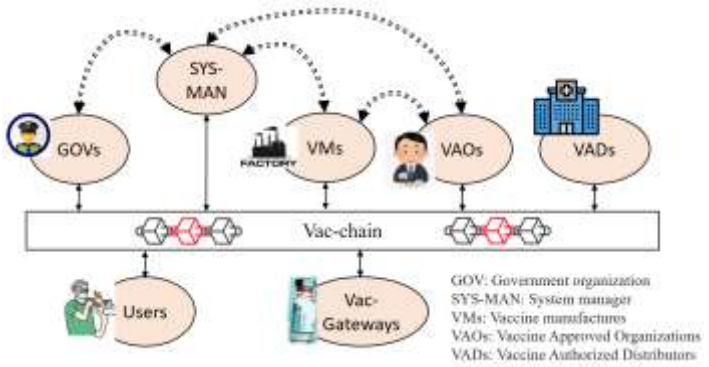
- 偽ワクチンの流通
- ワクチンの重篤な副作用の原因を調査するための情報不足
- ワクチンパスポート



GOV: Government organization
SYS-MAN: System manager
VMs: Vaccine manufactures
VAOs: Vaccine Approved Organizations
VADs: Vaccine Authorized Distributors

Vac-chainの重要な技術

偽ワクチン・品物に対策とは？



従来方法：

- 高価で特別なQRコードラベルを作成する必要がある
- 低い経済効率
- 偽物を完全に回避できない

提案方法：

偽のワクチンは、3つのセキュリティ手順を介してチェーンから排除される。

- **SYS-MAN**の警備員
- QRコードの大量の違法コピーを回避するための**CGCP方法**
- QRコードの単一の違法コピーを回避するための**GPP方法**

CGCP: Genuine Code Generator & Protector

GPP: Genuine Product Protector

まとめ

- ブロックチェーンハードウェアアクセラレータ（BCA)
  - ✓汎用用
  - ✓ブロックチェーンネットワークマイニング用
  - → **FPGAに乗せたBCAの電力効率はGPUの電力効率より36倍優れている**
- ブロックチェーンソフトウェア
  - ✓Vac-chain: COVID-19ワクチンの管理・トレーサビリティシステムの開発
  - →**経済的で高効率な偽物排除対策**

実用化に向けた課題

新技術説明会
New Technology Presentation Meetings!

ロ現在、完成したこと:

- ✓Arch-1 とArch-2の回路設計とFPGAボードでのパフォーマンス評価。
- ✓Xilinx Alveo U280とZCU102などFPGAボードで載せたArch-2はOffline Bitcoin miningの実装を完了。

ロしかし、以下の点が未解決です：

- ✓BCAのArch-2を使用してLive Bitcoin Miningの実装。
- ✓Arch-1は、FPGAボードのバスシステムの制限により、データ転送にボトルネックが残っている。

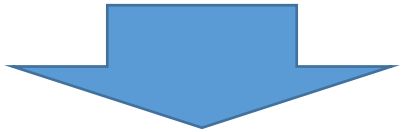
実用化に向けた課題

ロ今後の実施予定：

- ✓小型化（USBタイプにチップ化する）BCAを既存FPGAボード・PCに接続して、高速マイニングを実現する。
- ✓小型化（カードタイプにチップ化する）BCAをraspberry piボードに接続して、IoTシステムのデータ整合性とプライバシを保護する。

企業への期待

- ライセンス
- 共同研究



✓ 提案したBCAアーキテクチャを各アプリケーションに適用できるように

✓ Vac-chainまたは製品の偽造防止管理システムの開発と社会に適用できるように

本技術に関する知的財産権

新技術説明会
New Technology Presentation Meeting

- 発明の名称　：処理要素、その制御方法および制御プログラム、並びに処理装置
- 出願番号　：特願2021- 9164
- 出願人　：奈良先端科学技術大学院大学
- 発明者　：トラン テイ ホン、中島　康彦

お問い合わせ先

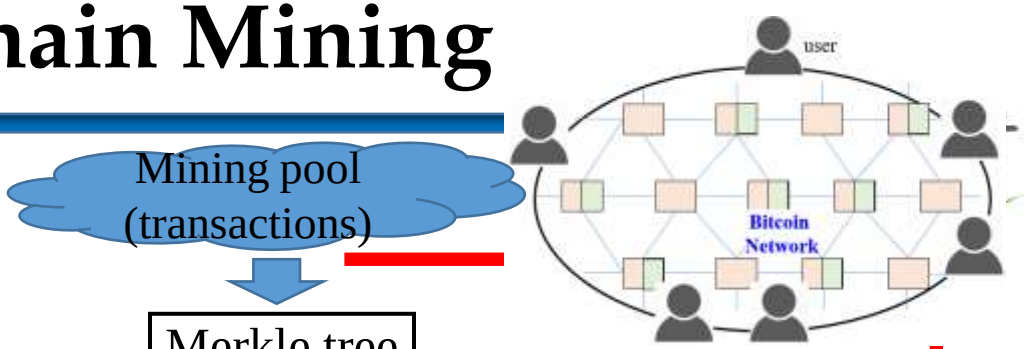
奈良先端科学技術大学院大学
産官学連携推進部門

ＴＥＬ　０７４３－７２－　５１９０
ＦＡＸ　０７４３－７２－　５１９４
e-mail　ip-3f@ip.naist.jp

APPENDIX

BCAの応用 – Blockchain Mining

BCAはSHA-256など暗号化ハッシュ値を求めるハードウェア回路である



Mining pool (transactions)

Merkle tree hash

SHA-256

+1

Ver.	Prev. hash	Merkle Root	Time	Target	Nonce

Double SHA-256

BCA

No

< target?

Yes

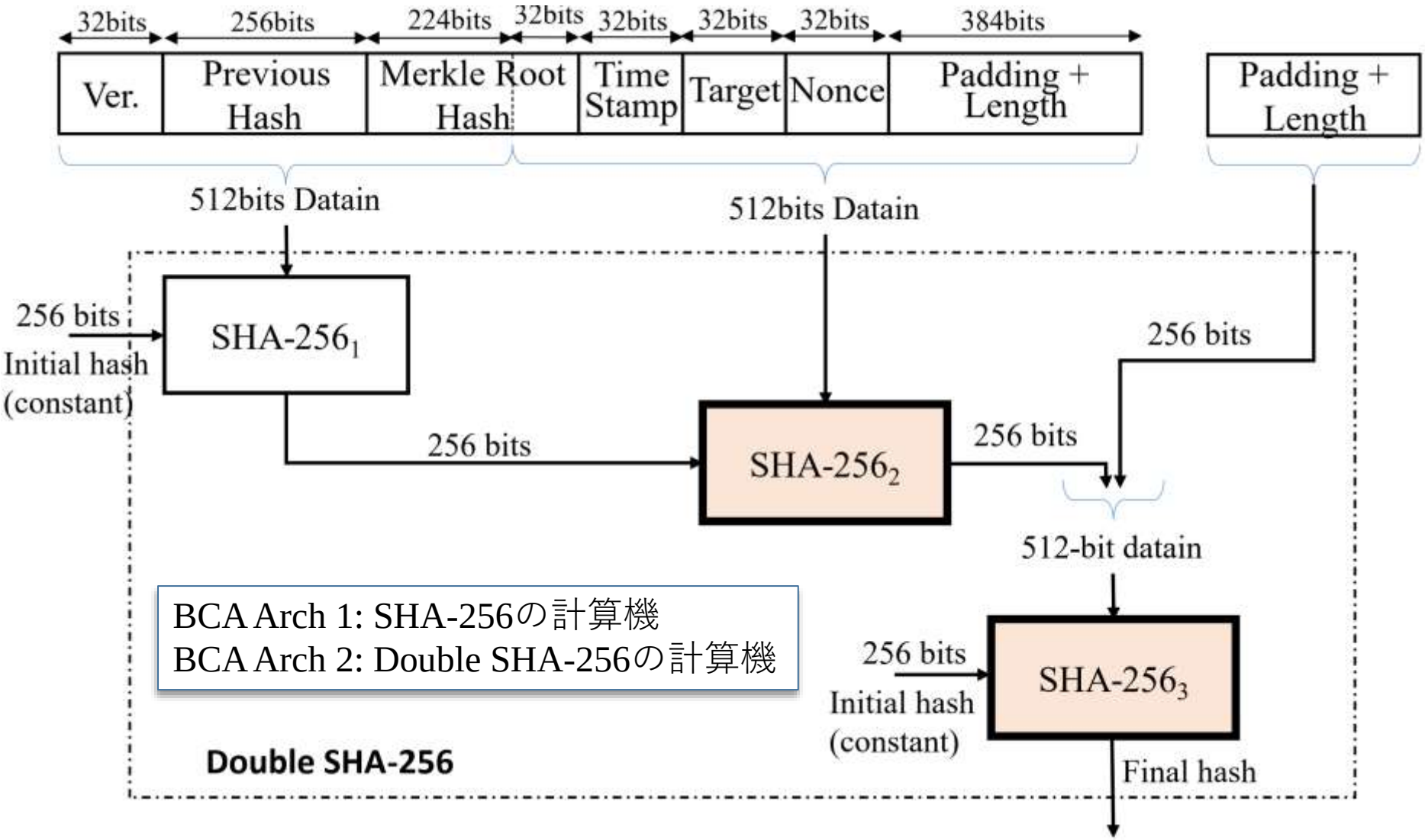
Header	Current block hash	Transaction raw data

Broadcast

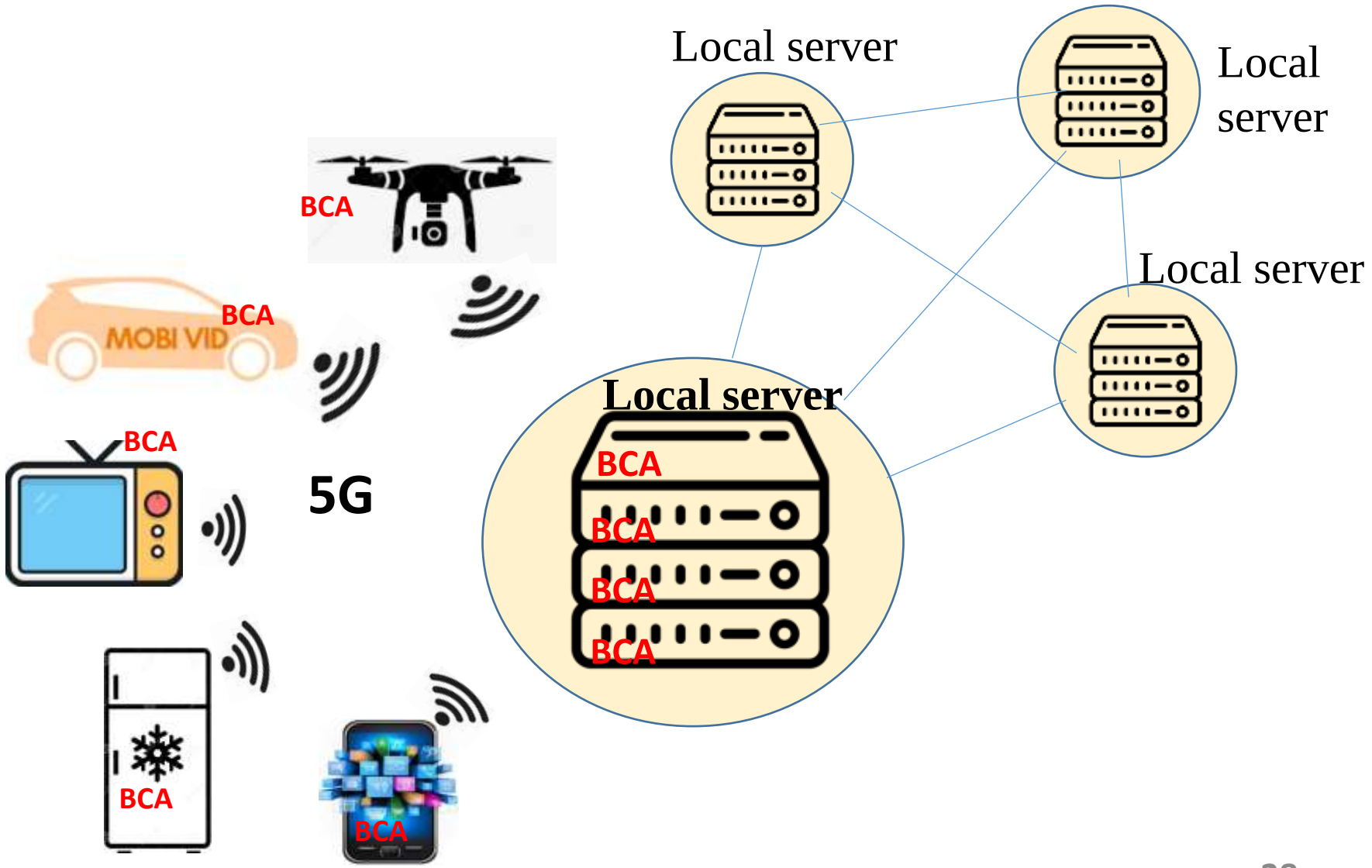
Average 10^{20} repeat per block!

High speed low power SHA-256 circuit is required!

BCAの応用 – **Blockchain Mining**



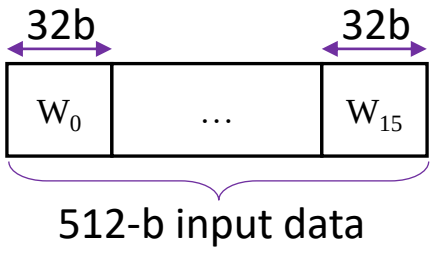
なぜ超低消費電力・高速BCAは必要？

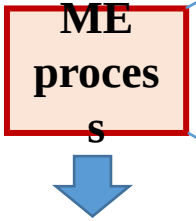


従来技術とその問題点

13 × 48 operators

48 loops





$$W_j = \sigma_1(W_{j-2}) + W_{j-7} + \sigma_0(W_{j-15}) + W_{j-16}$$

$$\sigma_0(x) = S^7(x) \oplus S^{18}(x) \oplus R^3(x)$$

$$\sigma_1(x) = S^{17}(x) \oplus S^{19}(x) \oplus R^{10}(x)$$

ハッシュ計算の特徴

- 多数ループ必要
- ループレベルで計算に必要なデータの従属性有り
- ループ内の計算に対して、多数演算子要り(>2000)
- ループ内のデータの従属性有り

$$T_2 = \Sigma_0(a) + Maj(a,b,c)$$

$$h \leftarrow g;\ g \leftarrow f;\ f \leftarrow e;\ e \leftarrow d + T_1$$

$$d \leftarrow c;\ c \leftarrow b;\ b \leftarrow a;\ a \leftarrow T_1 + T_2$$