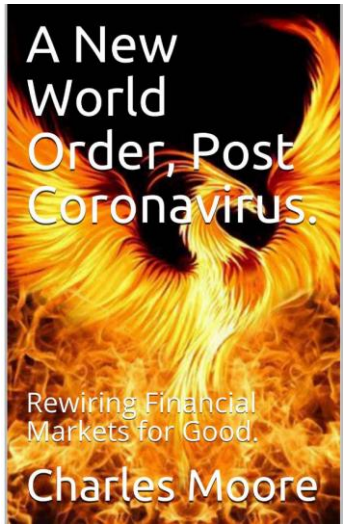
Innovative implementation of Central Bank Digital Currency (CBDC), actually, Cash and World Currency Unit (WCU)

Brief explanation of the proposed solution:

CBDC, WBU and Proof-of-Concept use cases

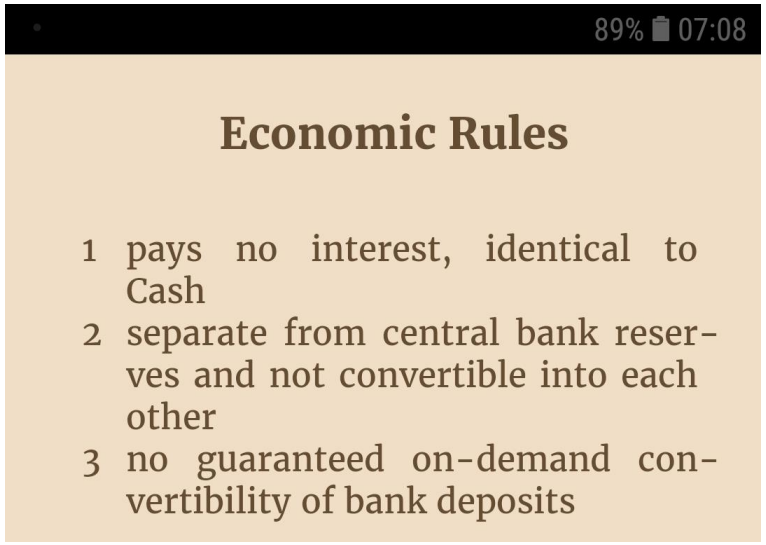
The main source is the book
"A New World Order, Post Coronavirus. Rewiring Financial Markets for Good."



Agenda

- Executive summary
- Architecture of the CBDC solution
  - legality, security, triple accounting, witnesses, cost, performance
- CBDC use cases
- Architecture of WCU to support cross-border payments
- CBDC + WCU use cases
- Deployment at Central Bank
  - Value-Added Reseller (VAR) role

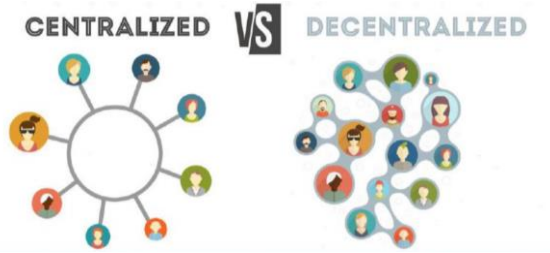
Executive summary



- Central Bank Digital Cash (CBDC)
  is digital bearer asset and legal tender
- Person-to-person value transfer with triple-entry accounting
- BIS model 1 unconditional transfer with legal finality in ~ 100ms
- Security of cryptographic keys with Hardware Security Module (HSM)
- Legal codification of assets, binds the technology to the legal framework
- Free retail, RTGS and cross-border (with WCU) payments
- Innovative FinTech architecture: legality, resilience, performance

Architecture of the CBDC solution Legality (1)

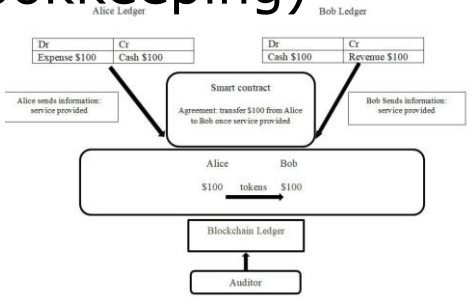
- Central Bank Digital Cash (CBDC) is **digital bearer financial asset as legal tender**
- Decentralised transfer of value between people (person-to-person)
  - Global Secure Identity provides the transaction end points
  - A person (human) can have any number of secure identities
  - Each Secure Identity has one and only one **Private Block Chain Ledger**



- Global **Inter-Ledger Protocol** (ILP)
  - People rather than devices terminate all ILP transfers of value
  - Patented in the year 2000 and publicly available since the year 2010

Architecture of the CBDC solution Legality (2)

- **Trust Points**
  - Each transaction is founded upon **triple-entry accounting** (bookkeeping)
  - The third leg (for each Secure Identity) is a mutual **trust point**(s) or **witness**(es) of the transacting parties
  - This forms the **Public Block Chain Ledgers**
  - These can be traditional entities like banks, exchanges, or marketplaces (local communities) etc.
  - Determined solely by the people involved in the transaction
  - See as also "Triple Entry Accounting.pdf"



Source: https://www.researchgate.net/publication/336645713
"Triple-entry accounting with blockchain: How far have we come?"

Architecture of the CBDC solution Legality (3)

- All transactions are Person-to-Person value transfers
  - Payment Vs Payment (PVP) of digital bearer cash
  - Asset Vs Asset (AVA) of digital bearer assets
  - Asset Vs Payment (AVP or DVP) as a dual flow of PVP and AVA
- Free market exchange of assets via atomic swap **Decentralised Asset Exchange** (DAX) on top of Inter-Ledger Protocol (ILP)
  - Supports PVP, AVA, or AVP flows with on-market matching between supply and demand
  - **BIS model 1 unconditional transfer with legal finality in ~ 100ms**
  - Trust Points co-ordinate flows of value between People

Architecture of the CBDC solution “Security by design” by architecture

- The Hardware Security Modules (HSMs) used with all Private Block Chain Ledger chains are FIPS 140-2 overall level 2 and selected level 3 certified hardware products
- The Level 3 certified capabilities critical to the Block Chain Ledgers:
  - Cryptographic Module Specification: Level 3
  - Roles, Services, and Authentication: Level 3
  - Physical Security: Level 3
- Chosen architectural decisions provide unprecedented levels of legality, security, resilience and performance

Architecture of the CBDC solution
Cost and performance

Friction free global decentralised financial market with BIS model 1 unconditional transfer with legal finality in ~ 100ms

System	*Transactions*	*Latency*	*Pay Sate*	*Model 1*	*Transaction Fee*
Block Chain Ledger	Infinite	100 ms	Settle	Y /D	Zero
Mastercard	40,000 tps	130 ms	Auth (2 days)	N /C	1.55% - 2.6%
PayPal	193 tps	2.5 seconds	Auth (3 days)	N /C	2.9% plus $0.30 USD
Visa	1,700 tps	5 seconds	Auth (2 days)	N /C	1.43% - 2.4%
RBA Fast Payments	1000 tps	15 seconds	Settle	N /C	~$30 AUD
Ethereum	20 tps	15 seconds	Settle (1 Min)	N /D	~$3-$300 USD
Bitcoin	7 tps	10 minutes	Settle (1 Hr)	N /D	~$2-$75 AUD
Auth = Authorisation Only,					
Settle = Settlement (including any clearing)					
Model 1 = Bank International Settlements defined Model 1 gross, atomic settlement.					
D=Decentralised, C= Centralised (double spend prevention)					

This table is based on publicly available data obtained end of 2017 – beginning 2018.

Zero Counterparty and **Zero** capital risk, within any global value transfer between any two parties to the transitions. (TPS means Transaction Per Second)

CBDC solution use cases

1. CBDC life cycle
2. CBDC flow in retail (person-to-person)
3. CBDC flow in RTGS (bank-2-bank, etc.).
4. Two-level structure possibility
5. Three-level structure possibility
6. Universal access
7. Resilience

CBDC solution use cases
1. CBDC life cycle

- Create at a commercial bank (from cash to CBDC)
  - Scan the national banknotes
  - Send these national banknotes to the Central Bank to be destroyed
  - Mint (issue) CBDC
  - Destruct the national banknotes
- Create at the Central Bank
  - Mint (issue) CBDC

CBDC solution use cases
2. CBDC flow in retail

Watch an example
https://vimeo.com/161428106

CBDC – Central Bank Digital Cash (not Currency)
DAX – Decentralised Asset Exchange
HSM – Hardware Secure Module
SIN – Secure Identifier

Digital witness (e.g. a marketplace) via **Public** Block Chain Ledger

Debit	Credit	SIN	Debit	Credit	SIN
5	0	Bob	0	5	Alice

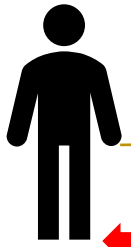
Debit	Credit	SIN
5	0	Bob

Alice **Private** Block Chain Ledger

Inter-Ledger Protocol
between three
Block Chain Ledgers

Debit	Credit	SIN
0	5	Alice

Bob **Private** Block Chain Ledger



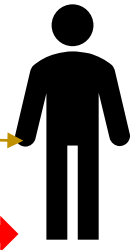
CBDC

Cloud HSM

Secure channel

Cloud HSM

CBDC



Alice (Payer)

DAX

Bob (Payee)

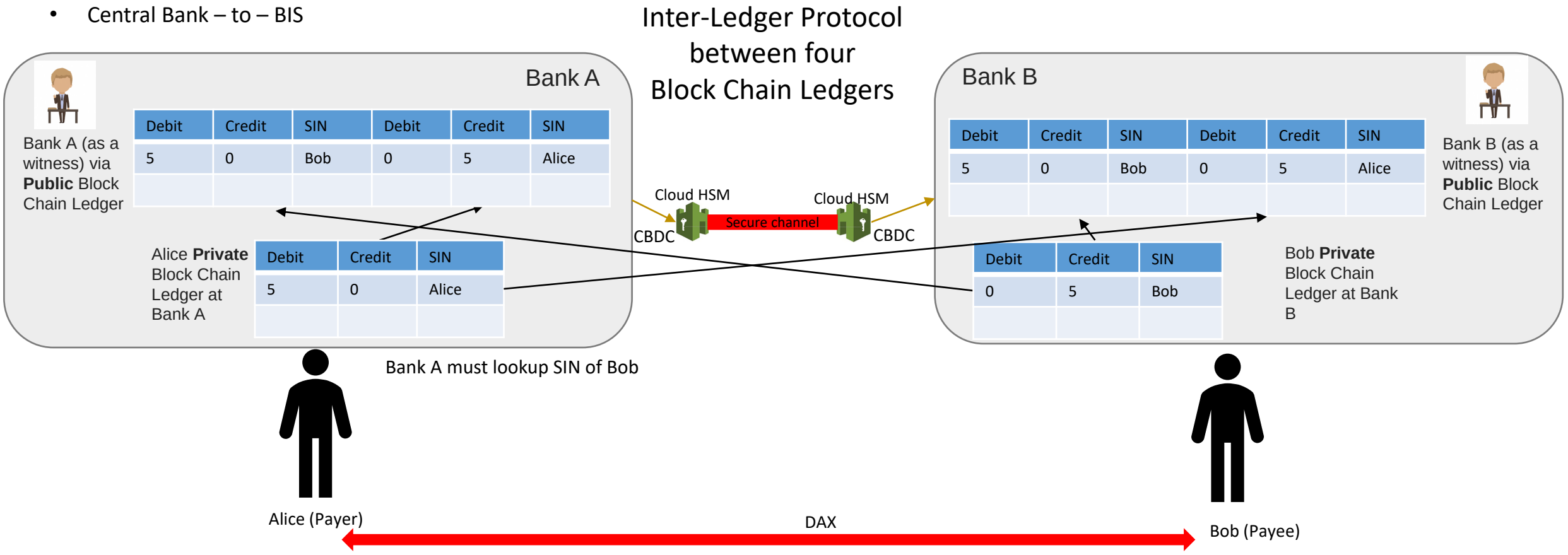
Some CBDC moves from one HSM to another HSM

CBDC solution use cases
3. CBDC flow in RTGS

RTGS may occur in several configurations

- Bank – to – Bank
- Central Bank – to – Central Bank
- BIS – to – Central Bank
- Central Bank – to – BIS

CBDC – Central Bank Digital Cash (not Currency)
DAX – Decentralised Asset Exchange
HSM – Hardware Secure Module
SIN – Secure Identifier



CBDC solution use cases
4. Two-level structure possibility

- This is the case for involving commercial banks
  - The Central Bank mints CBDC
  - The Central Bank transfers CBDC to commercial banks
  - Those commercial banks provide CBDC to clients

CBDC solution use cases
5. Three-level structure possibility

- This is case for non-sovereign currency like Euro
  - The European central bank mints CBCD
  - Such CBDC are transferred to the country central bank, e.g. the Deutsche Bundesbank
  - The country central bank transfers CBDC to commercial banks
  - Those commercial banks provide CBDC to clients

CBDC solution use cases
6. Universal access

- The CBDC must be inclusive & accessible to everyone including those without a smartphone (as formulated by Bank of Japan in https://www.boj.or.jp/research/brp/psr/data/psrb200702.pdf)
- There is a potential option (to be further analysed) – this is Japan national travel card SUICA which is accepted as cash for transportation services and in some shops

CBDC solution use cases
7. Resilience

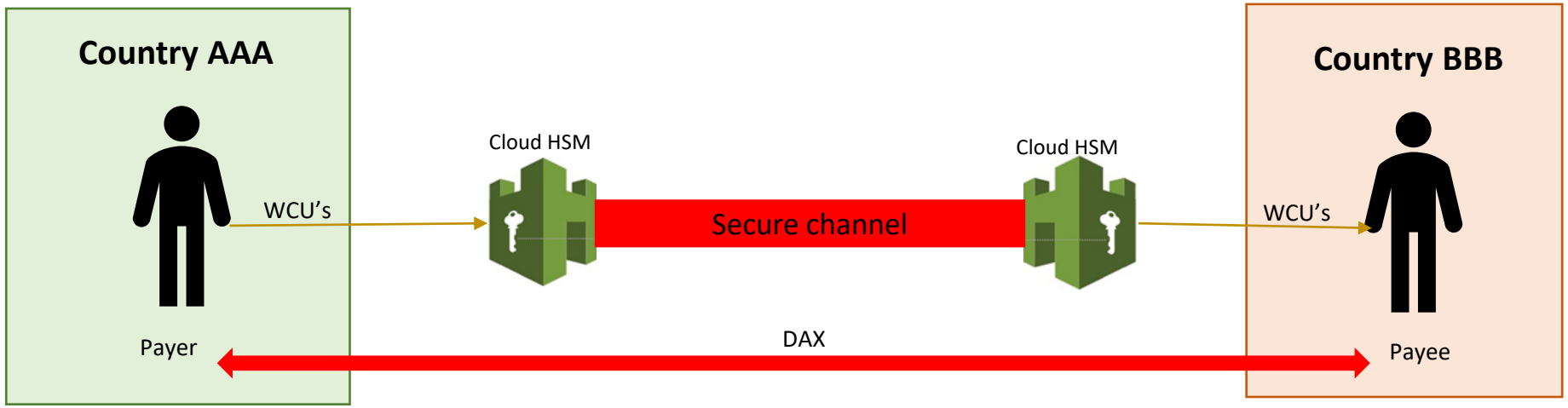
- CBDC solutions must maintain CBDC capacity for offline transactions or transfers. A CBDC with more robust offline capabilities could be useful as payment method during power & internet outages. (as formulated by Bank of Japan in https://www.boj.or.jp/research/brp/psr/data/psrb200702.pdf)
- This offline functionality is covered by PAYANY feature of the ILP
- Potentially, prepaid cards (like SUICA) can be used

A vision for FMI for frictionless (quick, free and with legal finality) cross-border payments

BIS – Bank of International Settlements
FMI – Financial Market Infrastructure
WCU – World Currency Unit
CBDC – Central Bank Digital Cash (not Currency)
DAX – Decentralised Asset Exchange
HSM – Hardware Secure Module

Basics of solution architecture

1. BIS govern, manage and operate FMI
2. Central Banks buy/sell WCU's on the WCU market
3. People buy/sell WCU's from/to their Central Bank via CBDC



Architecture of the CBDC + WCU solution Key elements of WCU (1)

- World Currency Unit (WCU) is the **universal medium of exchange** and **unit of account** for all central bank to central bank digital cash cross-border payments
- WCU is a digital bear asset with worldwide legal tender status
- **WCU is for money velocity not to store of value**
  - The WCU is based upon the dematerialisation of the majority of the world supply of **400-troy-ounce Gold Delivery gold bar**
  - The WCU bit is 1/1000 of 1 ounce of dematerialised 400-ounce gold bar
  - The solution provides a fully transparent payment infrastructure, which is supported via the universal World Currency Unit

Architecture of the CBDC + WCU solution Key elements of WCU (2)

- All currency pairs between Fiat Sovereign Currencies and the World Currency Unit are **priced** via a Decentralised Asset Exchange.
- The matching of supply vs demand for fiat digital cash, represents the proportional global equity claim by each nation state.
- The WCU balance held within the World Currency Units represents the net sovereign state economic production value.
- The instantaneous free market pricing of each WCUXXX currency pair, via a fixed supply of World Currency Units, allows each nation state digital cash to normalize its currency to the world economy.
- The right of all sovereign nations to control their own fiat currency within their nations borders is restored.
- The Bank of International Settlements as the banker to Central Banks provides central banks access to the World Currency Unit Supply.

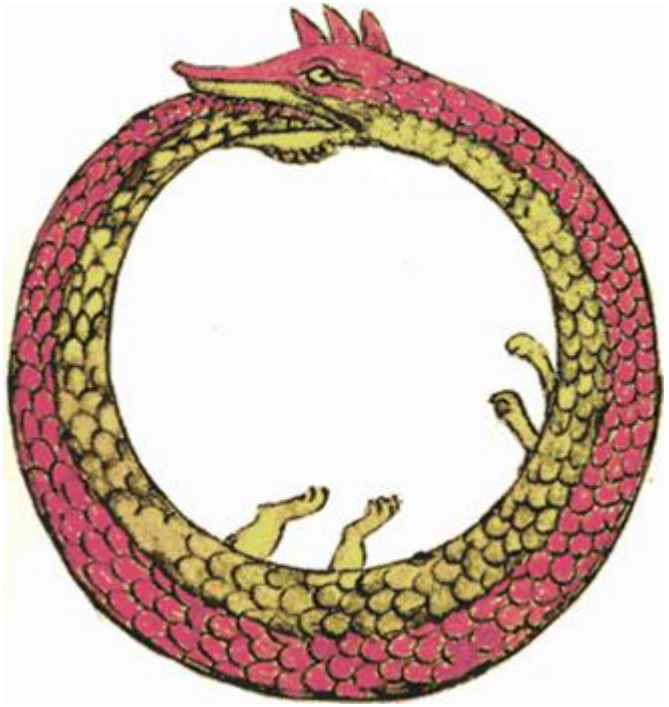
Architecture of the CBDC + WCU solution WCU security innovation - Circular Block Chain Ledger

The entire world currency unit supply is implemented within a proprietary set of circular block chain ledgers. The circular block chain ledgers were modelled on, the **ouroboros** which eats its tail to sustain its life, in an eternal cycle of renewal forming an unbreakable infinite loop. The physical construction of the circular block chain ledgers implements the ouroboros model.

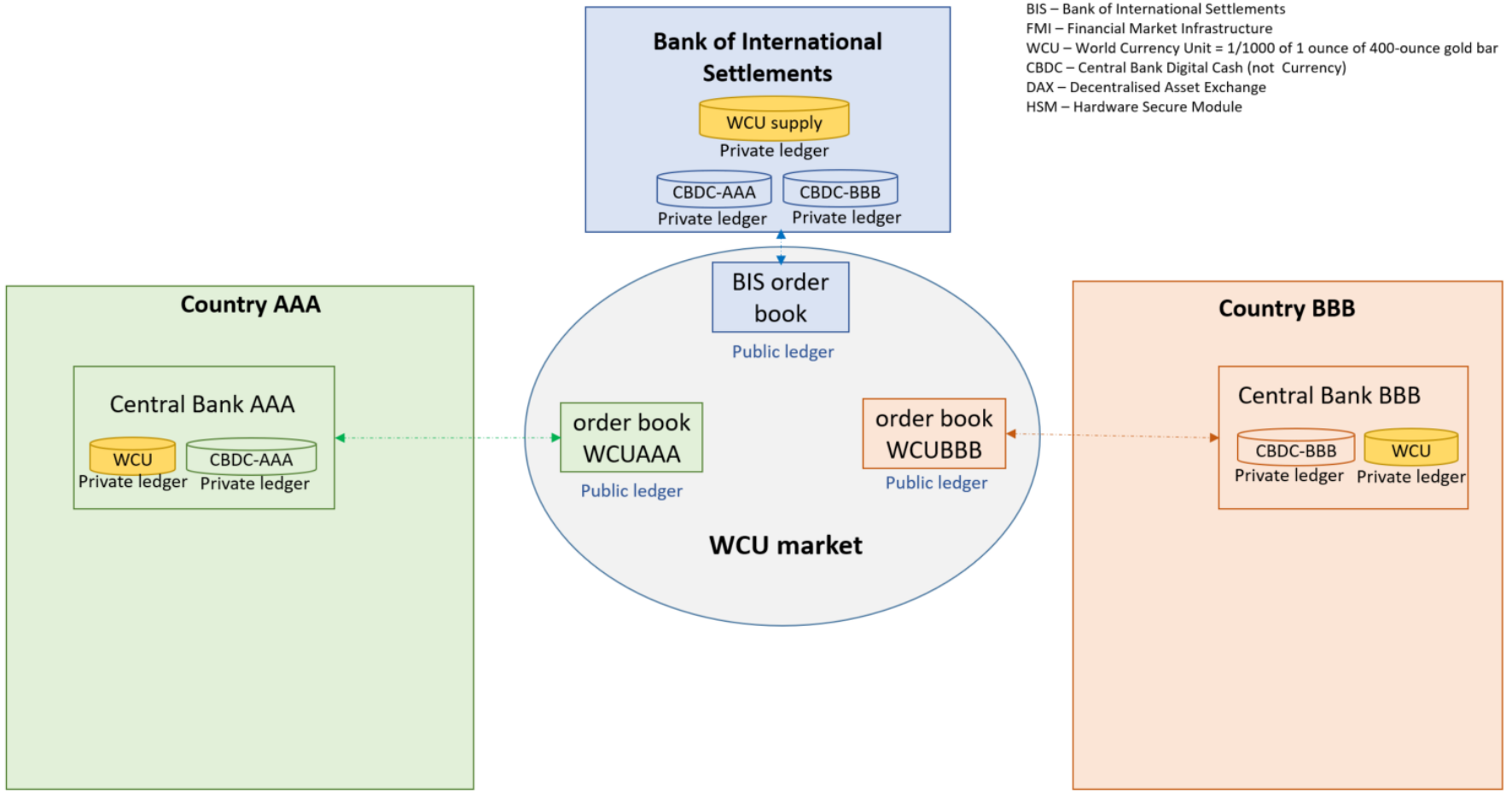
The evolutionary programing algorithms executed continuously until a majority consensus on the circular blockchain was established, at this point the final round of execution was baselined.

The World Currency Units are codified on HSM protected digital bearer keys, hence as the supply is progressively dispersed throughout the world's population, each of the World Currency Unit circular block chain ledger key pairs will be progressively destroyed until, at the point of full distribution there shall not exist a single HSM key. At this point, the HSMs can be detached from the World Currency Unit supply and the system becomes immutable. The World Currency Unit supply is the first currency which cannot be inflated or destroyed.

The net result is an immutable World currency unit supply to eternity.



Architecture of the CBDC + WCU solution Financial Market Infrastructure



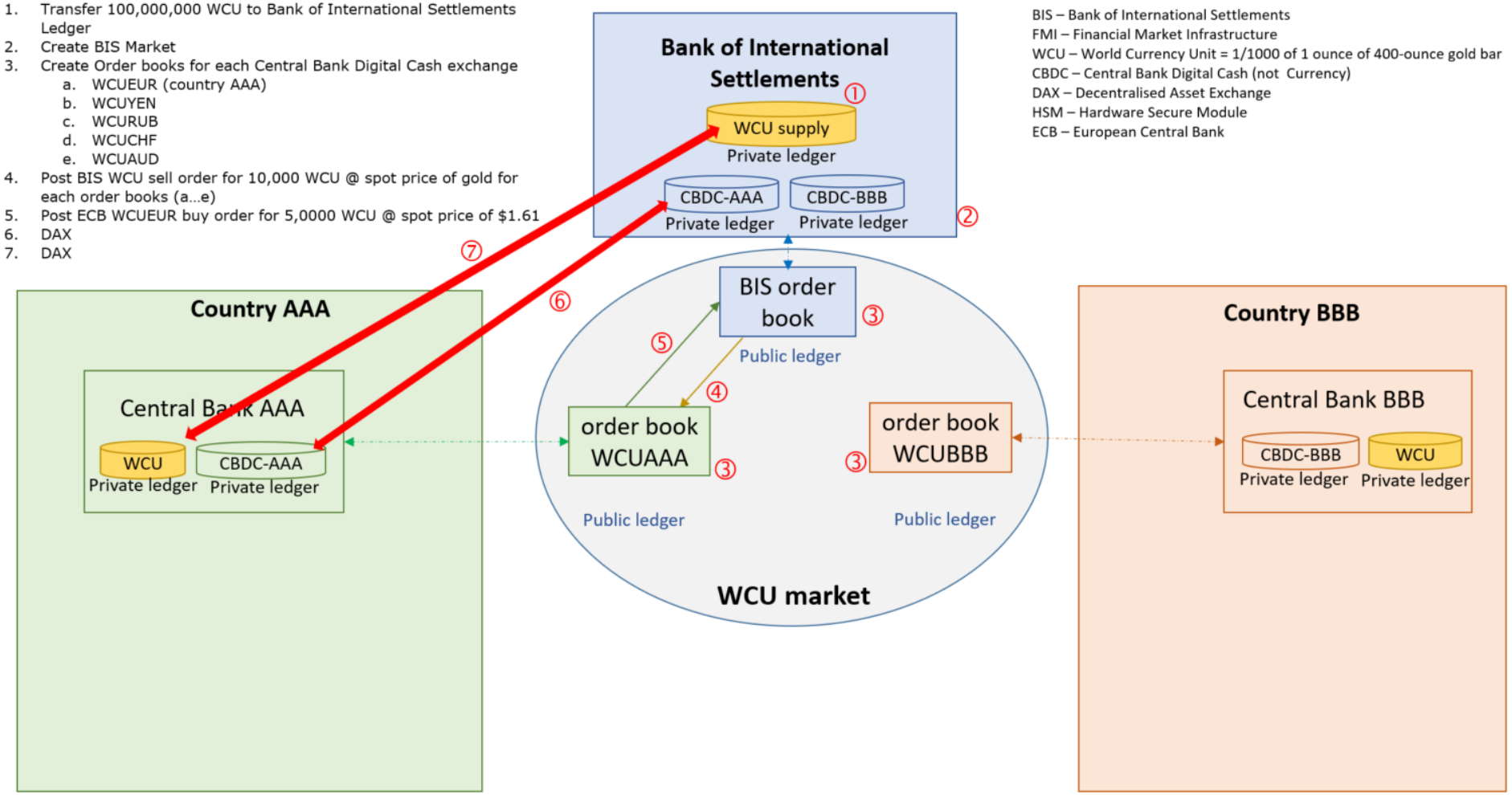
CBDC + WCU use cases

7. WCU boot
8. WCU life cycle
9. Flow of cross-border payment

CBDC + WCU use cases
7. WCU boot

BOOT WCU free market (including BIS WCU sell order)

1. Transfer 100,000,000 WCU to Bank of International Settlements Ledger
2. Create BIS Market
3. Create Order books for each Central Bank Digital Cash exchange
   a. WCUEUR (country AAA)
   b. WCUYEN
   c. WCURUB
   d. WCUCHF
   e. WCUAUD
4. Post BIS WCU sell order for 10,000 WCU @ spot price of gold for each order books (a…e)
5. Post ECB WCUEUR buy order for 5,0000 WCU @ spot price of $1.61
6. DAX
7. DAX



BIS – Bank of International Settlements
FMI – Financial Market Infrastructure
WCU – World Currency Unit = 1/1000 of 1 ounce of 400-ounce gold bar
CBDC – Central Bank Digital Cash (not Currency)
DAX – Decentralised Asset Exchange
HSM – Hardware Secure Module
ECB – European Central Bank

Please read the book starting from position 2971 for more detail

See also "The WCU Supply.pdf"

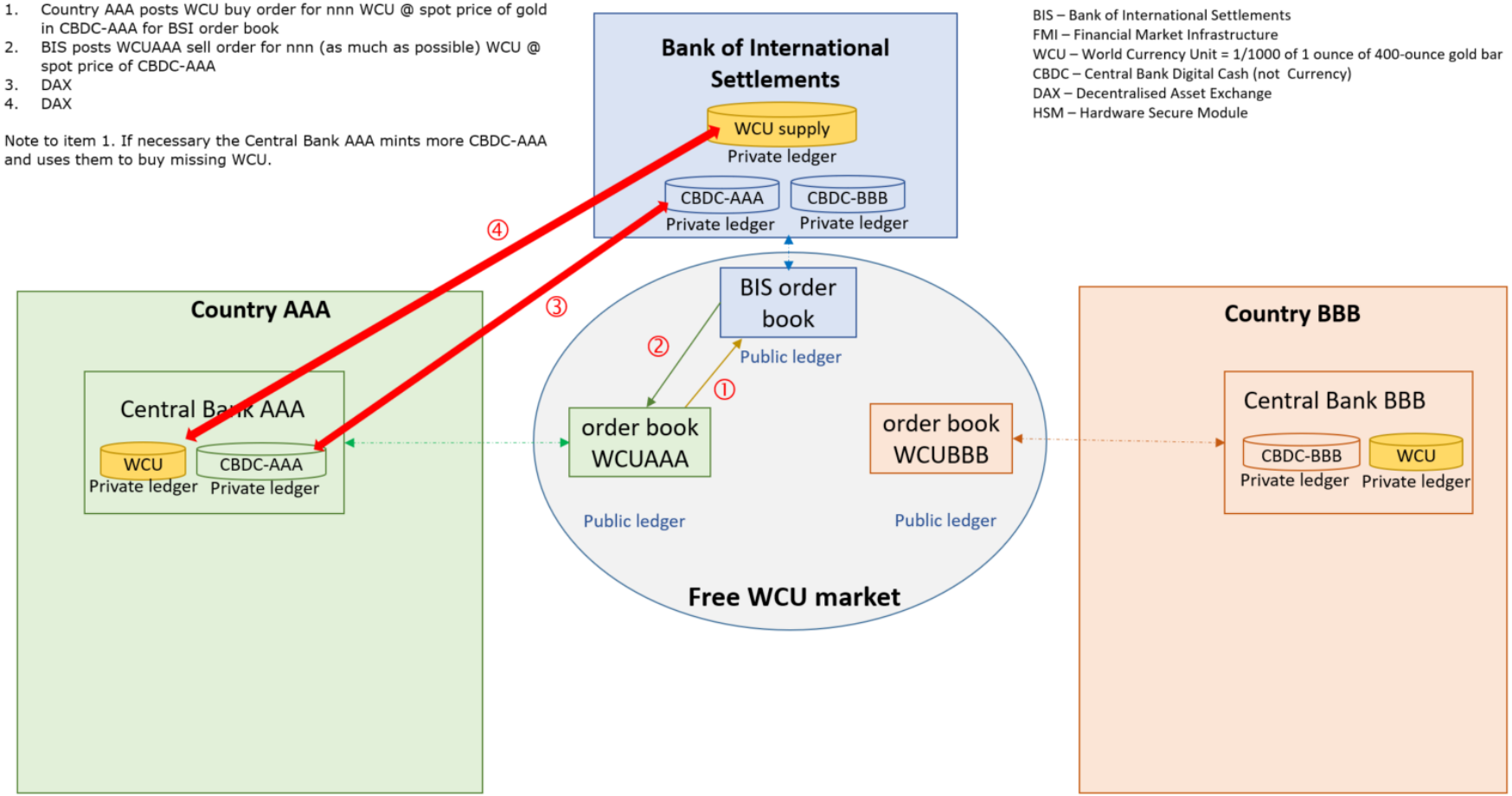
CBDC + WCU use cases
8. WCU life cycle (1)

Country AAA buy order for WCU

1. Country AAA posts WCU buy order for nnn WCU @ spot price of gold in CBDC-AAA for BSI order book
2. BIS posts WCUAAA sell order for nnn (as much as possible) WCU @ spot price of CBDC-AAA
3. DAX
4. DAX

Note to item 1. If necessary the Central Bank AAA mints more CBDC-AAA and uses them to buy missing WCU.

BIS – Bank of International Settlements
FMI – Financial Market Infrastructure
WCU – World Currency Unit = 1/1000 of 1 ounce of 400-ounce gold bar
CBDC – Central Bank Digital Cash (not Currency)
DAX – Decentralised Asset Exchange
HSM – Hardware Secure Module



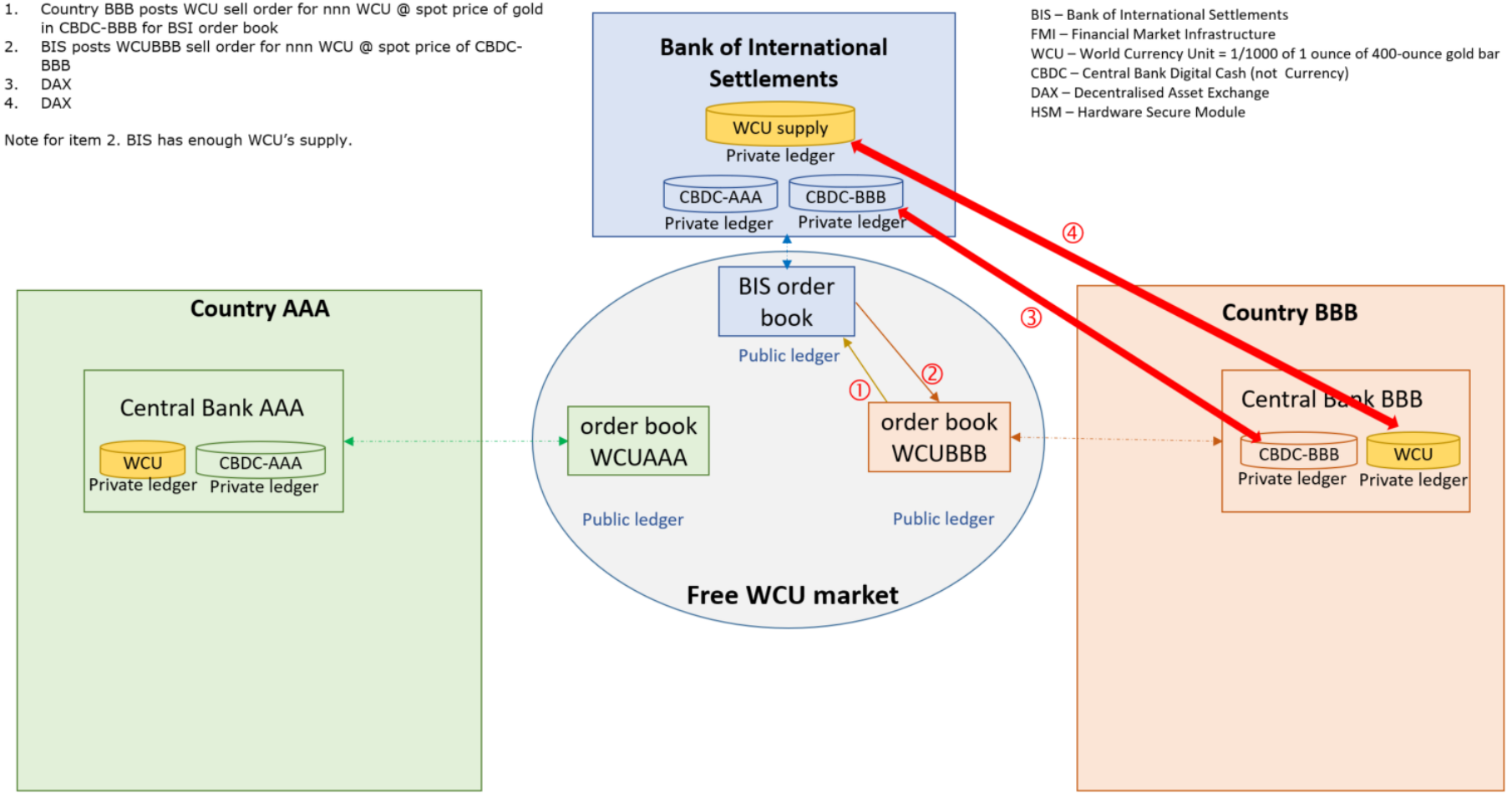
CBDC + WCU use cases
8. WCU life cycle (2)

Country BBB sell order for WCU

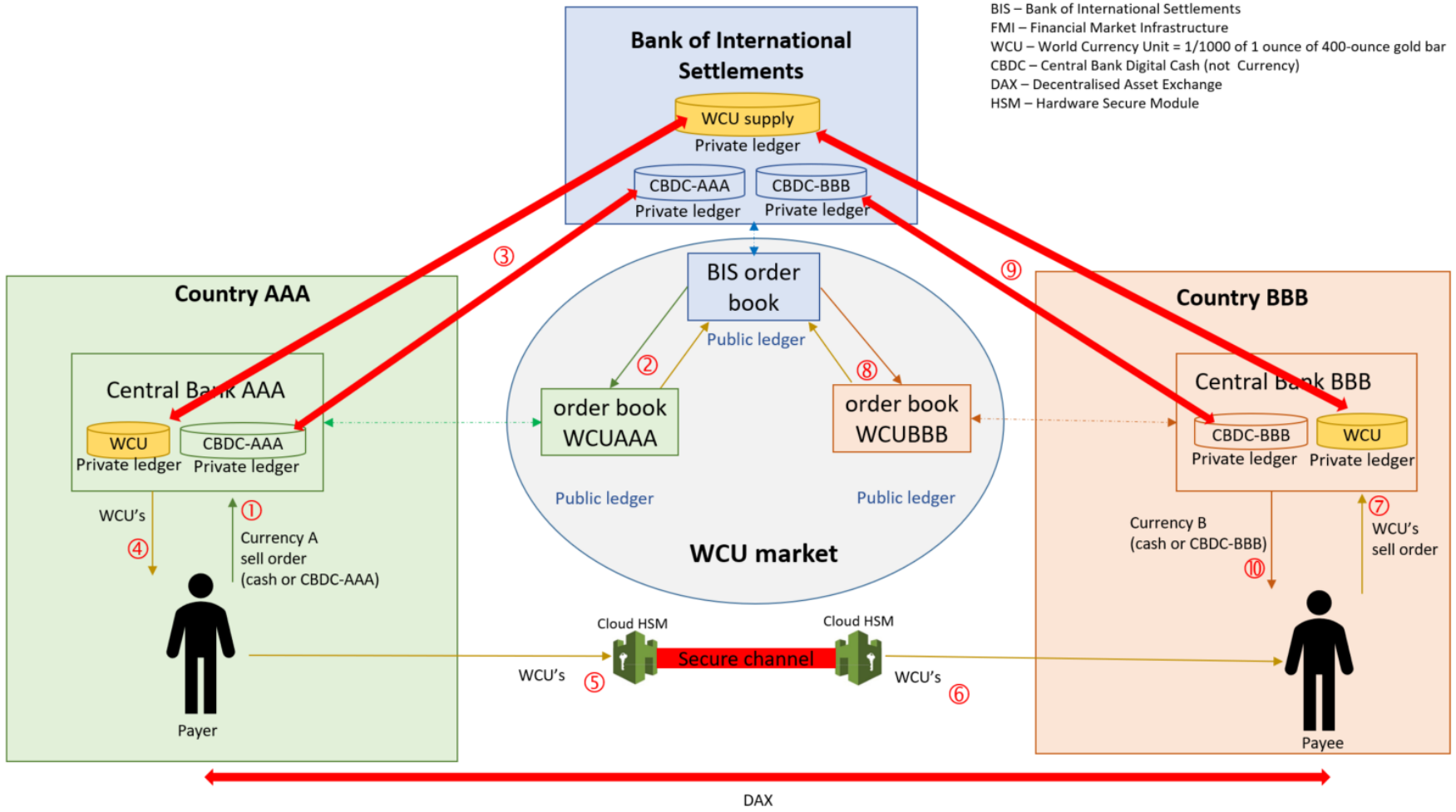
1. Country BBB posts WCU sell order for nnn WCU @ spot price of gold in CBDC-BBB for BSI order book
2. BIS posts WCUBBB sell order for nnn WCU @ spot price of CBDC-BBB
3. DAX
4. DAX

Note for item 2. BIS has enough WCU's supply.

BIS – Bank of International Settlements
FMI – Financial Market Infrastructure
WCU – World Currency Unit = 1/1000 of 1 ounce of 400-ounce gold bar
CBDC – Central Bank Digital Cash (not Currency)
DAX – Decentralised Asset Exchange
HSM – Hardware Secure Module



CBDC + WCU use cases
9. Flow of cross-border payment



- This model supports the existing cash, direct People-to-People payments without the intermediation of any central bank (once the local fiat currency, including as CBDC, is converted by the central bank into World Currency Units). At the same time each nation state has full control over its sovereign currency and provides the guaranteed liquidity within its fiat currency. Participants within this model do not face credit risks associated with claims on the central bank currency, because the central bank is not subject to default within its sovereign currency.

VAR role for CBDC at Central Bank

- Solution provider
  - Technology and software – yearly license
  - Installation owned and controlled by the Central Bank
  - A secure boot source code and example code with SOPs are supplied. These can be integrated into the banking SOPs and CONOPS via VAR team
- National Value Added Reseller (VAR) team
  - Success fee
  - Owning any end user applications or developments including mobile app with API for CBDC solution (including off-line transaction implementation)
  - 1st and 2nd line support

VAR role for WCU

- Solution provider
  - Technology and software – one-off license purchase, 15 % annual maintenance
- National Value Added Reseller (VAR) team
  - Success fee
  - Local consulting + IP
  - 1st and 2nd line support

Supporting documents

- https://samarin.biz/pubs/CBDC-Interoperability.pdf
- https://samarin.biz/pubs/CBDC-Legal-Finality.pdf
- https://samarin.biz/pubs/CBDC-Privacy.pdf
- https://samarin.biz/pubs/CBDC-Resilience.pdf
- https://samarin.biz/pubs/CBDC-Universal-Access.pdf
- https://samarin.biz/pubs/CBDC-Security.pdf
- https://samarin.biz/pubs/CBDC-Legality.pdf
- https://samarin.biz/pubs/CBDC-Financial-Inclusion.pdf

Question?

- alexandre.samarine@gmail.com
- +41 76 573 40 61