數位貨幣的隱私強化技術與挑戰

左瑞麟

國立政治大學

資訊科學系 教授

研發處 副研發長

高教深耕辦公室 副執行長

人工智慧與數位教育中心 籌備主任

為何需要數位貨幣支付

- 傳統現金的缺點
  - 高額攜帶不便
  - 計算麻煩
  - 無法全球流通
  - 被偽造時不容易辨認出來
  - 不支援電子商務交易
- 後疫情時代來臨！！

Zero Touch Economy

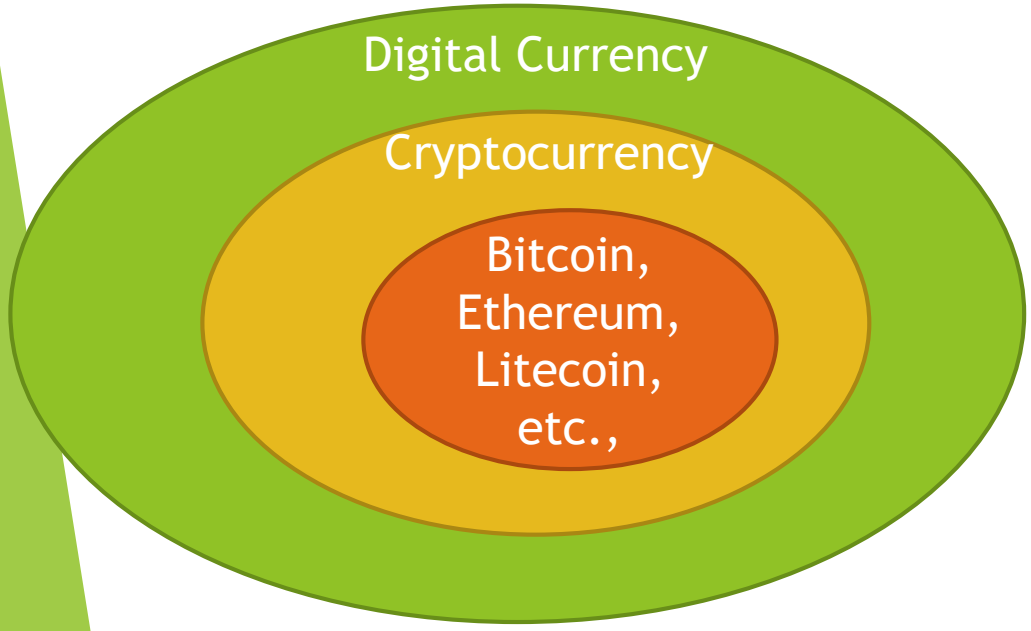
- 後疫情時代催生產業新格局
- 電子商務興起
- 數位交易為主流支付方式

數位貨幣(Digital Currency)

- 定義：將傳統的實體貨幣轉為無形的虛擬化電子貨幣，以代替真實的貨幣進行交易或轉帳
- 可以是法定貨幣或非法定貨幣
- 安全性與隱私保護特性需至少相等甚至高於於現行之實體貨幣
- Ex: 加密貨幣(cryptocurrency)
  - 比特幣，以太幣，門羅幣，穩定幣，etc.,

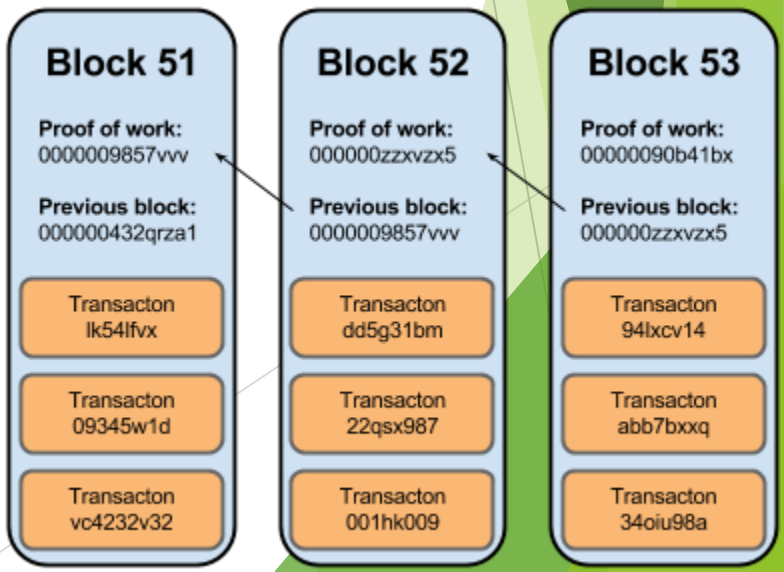
加密貨幣(Cryptocurrency)

- 加密貨幣 = 比特幣，以太幣等區塊鏈貨幣？
- 定義：泛指基於密碼技術構造的數位貨幣



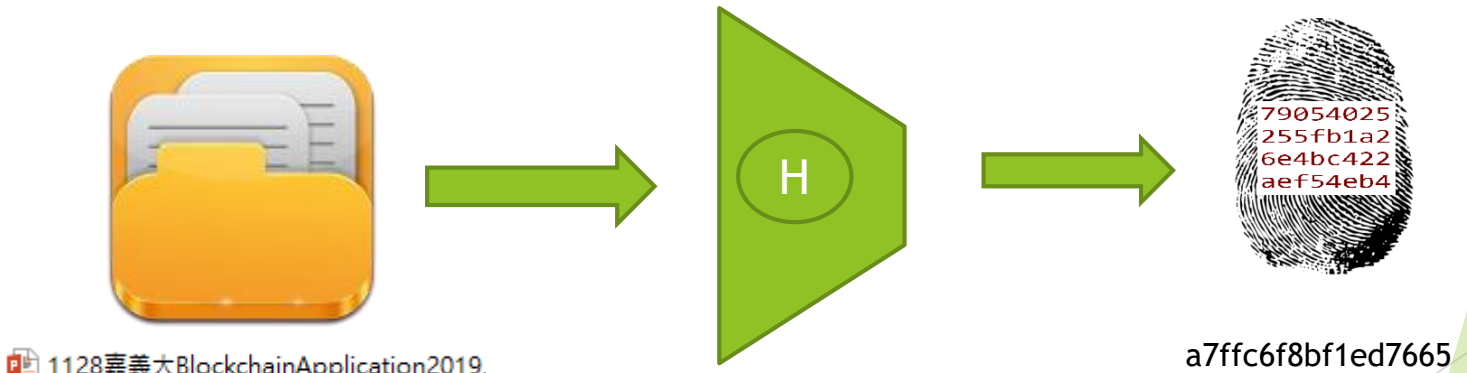
Cryptographic Primitives

- Cryptosystems used in bitcoin
  - Hash functions
    - SHA3, SHA256
  - Digital signature
    - ECDSA



Hash Functions

- An efficient function mapping binary strings of arbitrary length into binary strings of fixed length
- The output is called hash value



MD5, SHA Family

Comparison of SHA functions

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Rounds	Operations	Security (bits)
MD5 (as reference)		128	128 (4 × 32)	512	Unlimited[3]	64	And, Xor, Rot, Add (mod 2^{32}), Or	<64 (collisions found)
SHA-1		160		512	$2^{64} - 1$	80	And, Xor, Rot, Add (mod 2^{32}), Or	<80 (theoretical attack[4])
SHA-2	*SHA-224*	224	256 (8 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112
	SHA-256	256						128
	SHA-384	384	512 (8 × 64)	1024	$2^{128} - 1$	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192
	SHA-512	512						256
	SHA-512/224	224						112
	SHA-512/256	256						128
SHA-3	*SHA3-224*	224	1600 (5 × 5 × 64)	1152	Unlimited[5]	24[6]	And, Xor, Rot, Not	112
	SHA3-256	256		1088				128
	SHA3-384	384		832				192
	SHA3-512	512		576				256
	SHAKE128	*d* (arbitrary)		1344				min(*d*/2, 128)
	SHAKE256	*d* (arbitrary)		1088				min(*d*/2, 256)

Bitcoin

Ethereum

Digital Signatures

- A **digital signature** is a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender

General Model

A signature scheme consists of three (or more) related operations

- *Key pair generation* produces:
  - a public/private key pair
- *Signature operation* produces:
  - a signature for a message with a private key
- *Verification operation*:
  - checks a signature with a public key

Digital Signature Algorithm (DSA)

Global Public-Key Components

p prime number where $2^{L-1} < p < 2^L$ for $512 \le L \le 1024$ and L a multiple of 64; i.e., bit length of between 512 and 1024 bits in increments of 64 bits

q prime divisor of $(p - 1)$, where $2^{159} < q < 2^{160}$; i.e., bit length of 160 bits

g $= h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < (p - 1)$ such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudorandom integer with $0 < x < q$

User's Public Key

$y = g^x \bmod p$

User's Per-Message Secret Number

k = random or pseudorandom integer with $0 < k < q$

Signing

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1} (H(M) + xr)] \bmod q$

Signature = (r, s)

Verifying

$w = (s')^{-1} \bmod q$

$u_1 = [H(M')w] \bmod q$

$u_2 = (r')w \bmod q$

$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$

TEST: $v = r'$

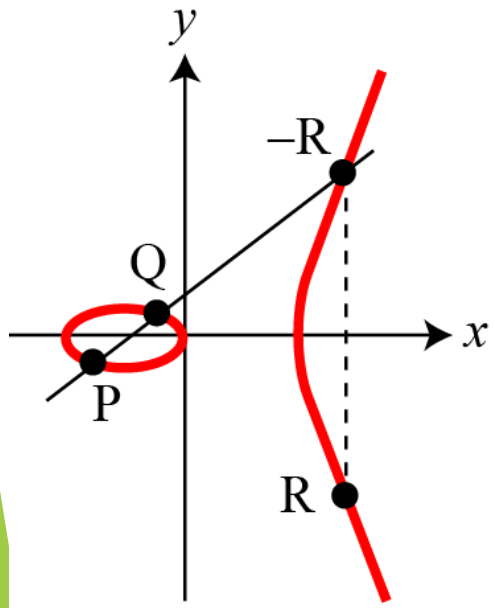
M = message to be signed

$H(M)$ = hash of M using SHA-1

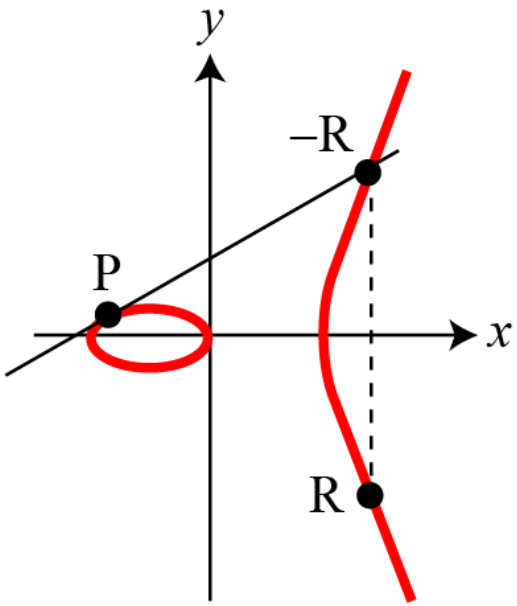
M', r', s' = received versions of M, r, s

EC over Real Numbers

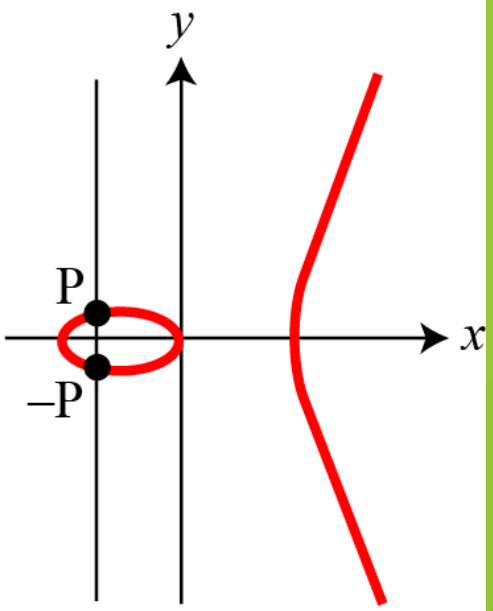
Three adding cases in an elliptic curve



a. (R = P + Q)



b. (R = P + P)



c. (O = P + (– P))

Elliptic Curve DSA

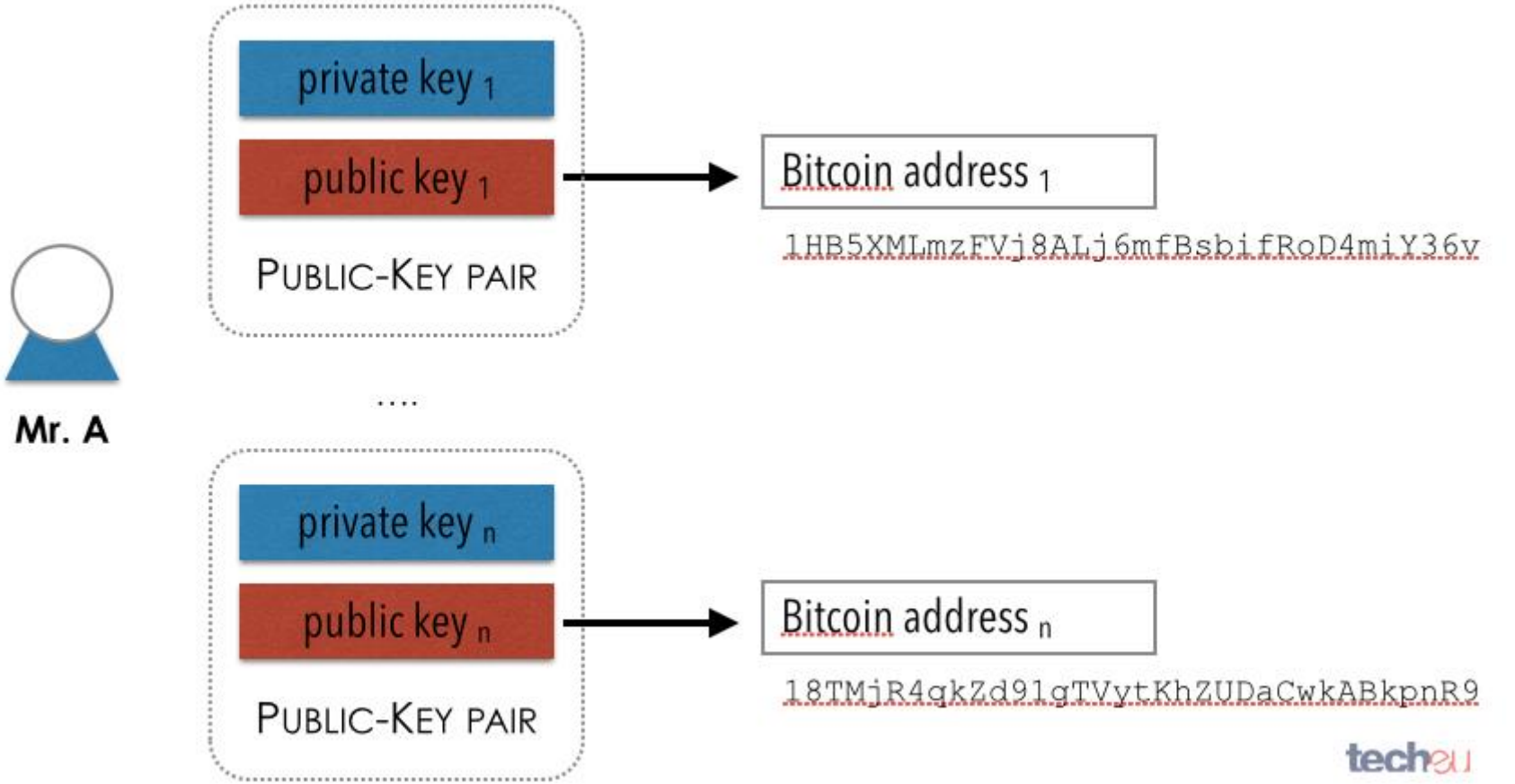
- Digital signature algorithm based on elliptic curve

Elliptic-Curve Digital Signature Algorithm (ECDSA)

NIST Guidelines for Public Key Sizes for AES			
ECC key size (bits)	RSA key size (bits)	Key size ratio	AES key size (bits)
163	1,024	1:6	
256	3,072	1:12	128
384	7,680	1:20	192
512	15,360	1:30	256

Supplied by NIST to ANSIX9F1

Bitcoin Address



Privacy-preserving Issue

- 區塊鏈（加密貨幣）所使用之密碼技術為雜湊函數(hash function)與數位簽章(digital signature)
- 無加解密技術，無法保障機密性

- 許多密碼學相關技術，可套用在區塊鏈應用上，增強隱私保護功能
  - Homomorphic encryption （同態加密）
  - ZK-Proof (零知識證明)
  - Ring signature (環簽章)
  - Designated verifier signature （指定驗證者簽章）
  - etc.

Homomorphic Encryption

Homomorphic Encryption

Homomorphism

$E_k(x) \oplus E_k(y) = E_k(x \otimes y)$

multiplicative homomorphism

$E_k(x) \oplus E_k(y) = E_k(x \times y)$

$E_k(3) \oplus E_k(6) = E_k(18)$

additive homomorphism

$E_k(x) \oplus E_k(y) = E_k(x + y)$

$E_k(3) \oplus E_k(6) = E_k(9)$

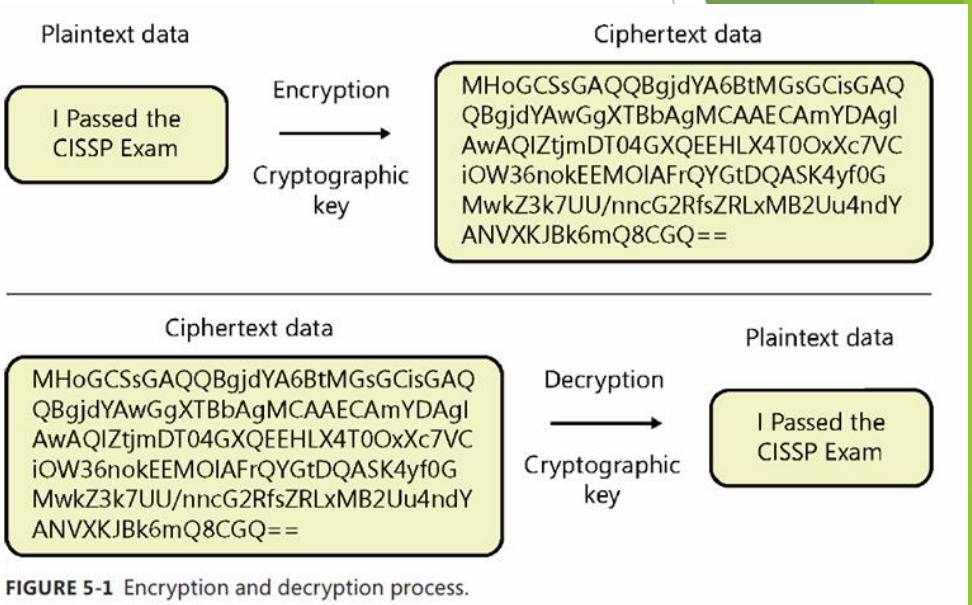


FIGURE 5-1 Encryption and decryption process.

⊕:Operation 1

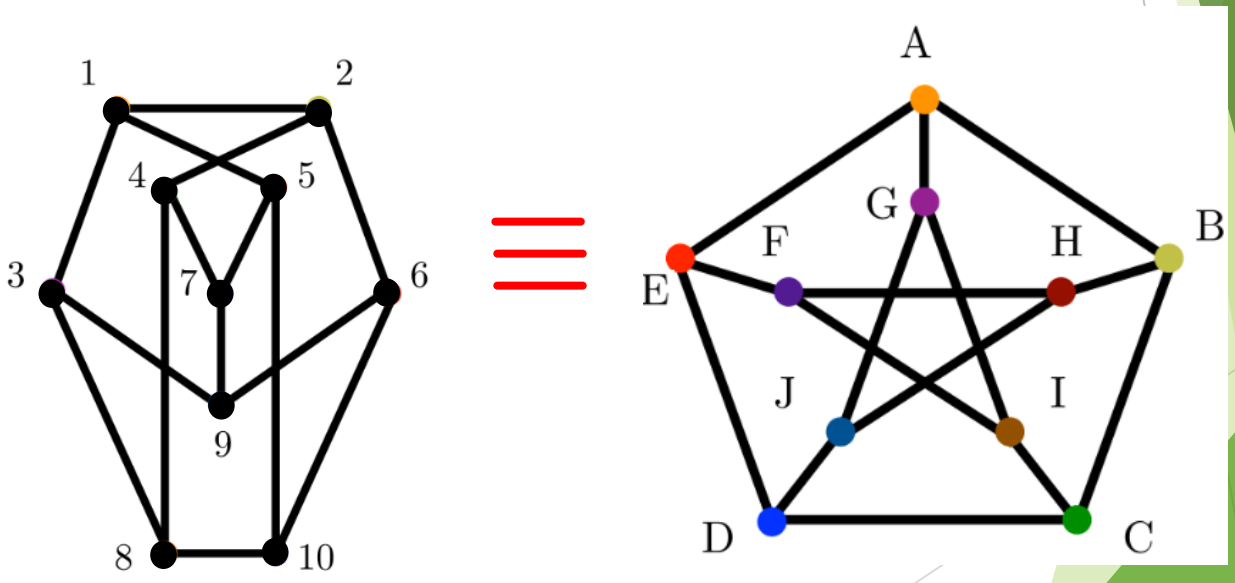
⊗:Operation 2

Zero Knowledge Proof (零知識證明)

- Zero Knowledge Proof (ZK-Proof)
- 1985年Goldwasser, Micali and Rackoff所提出
  - Turing Award 2012
- 概念
  - 在不洩漏某個特定資訊的情況下，也能證明自己確實知道此特定資訊

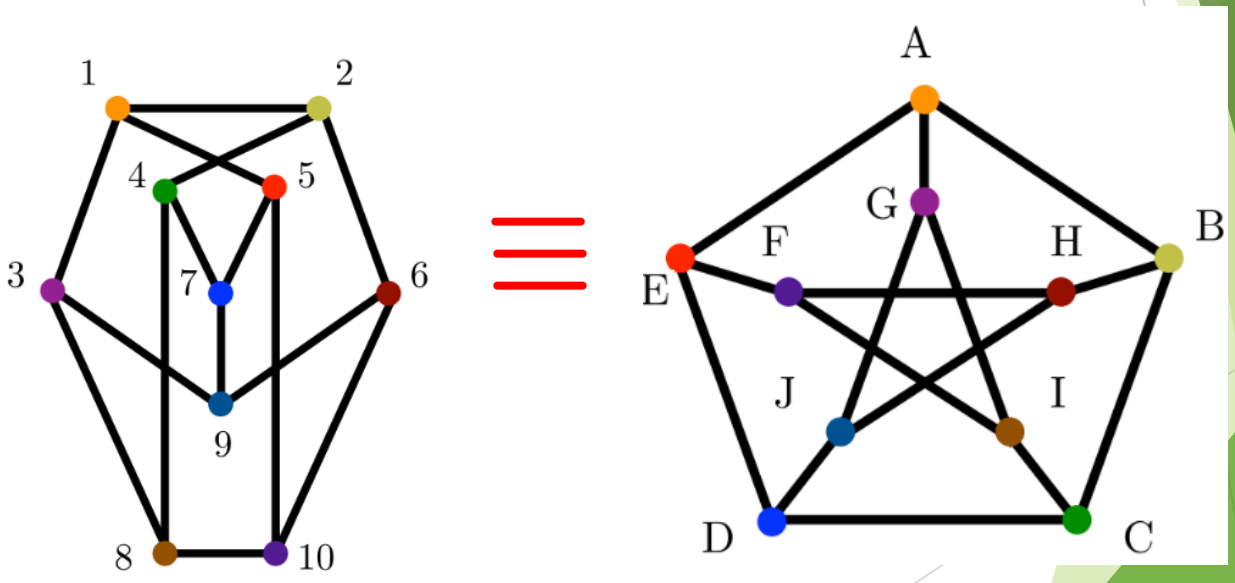
Example

- Ex:
  - Graph isomorphism
    - Two graphs G1 G2 are isomorphic

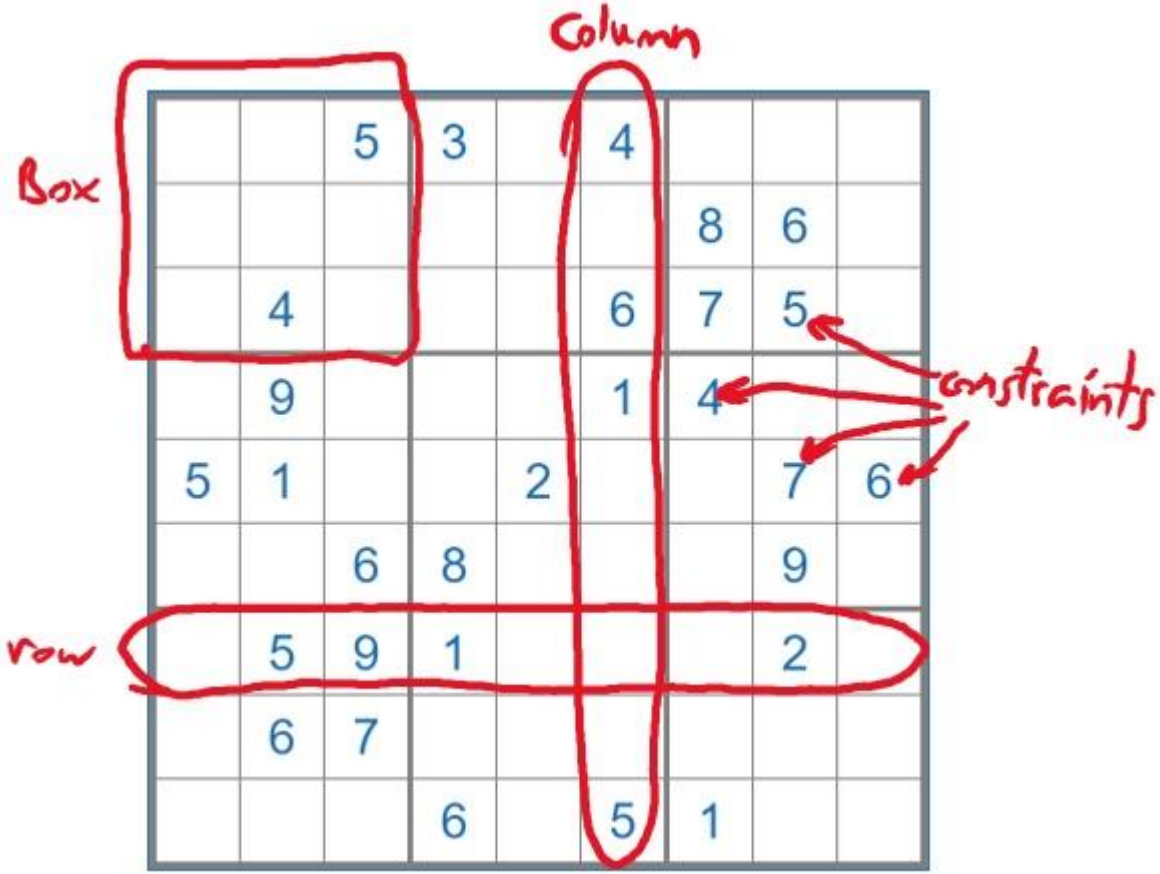


Example

- Ex:
  - Graph isomorphism
    - Two graphs G1 G2 are isomorphic



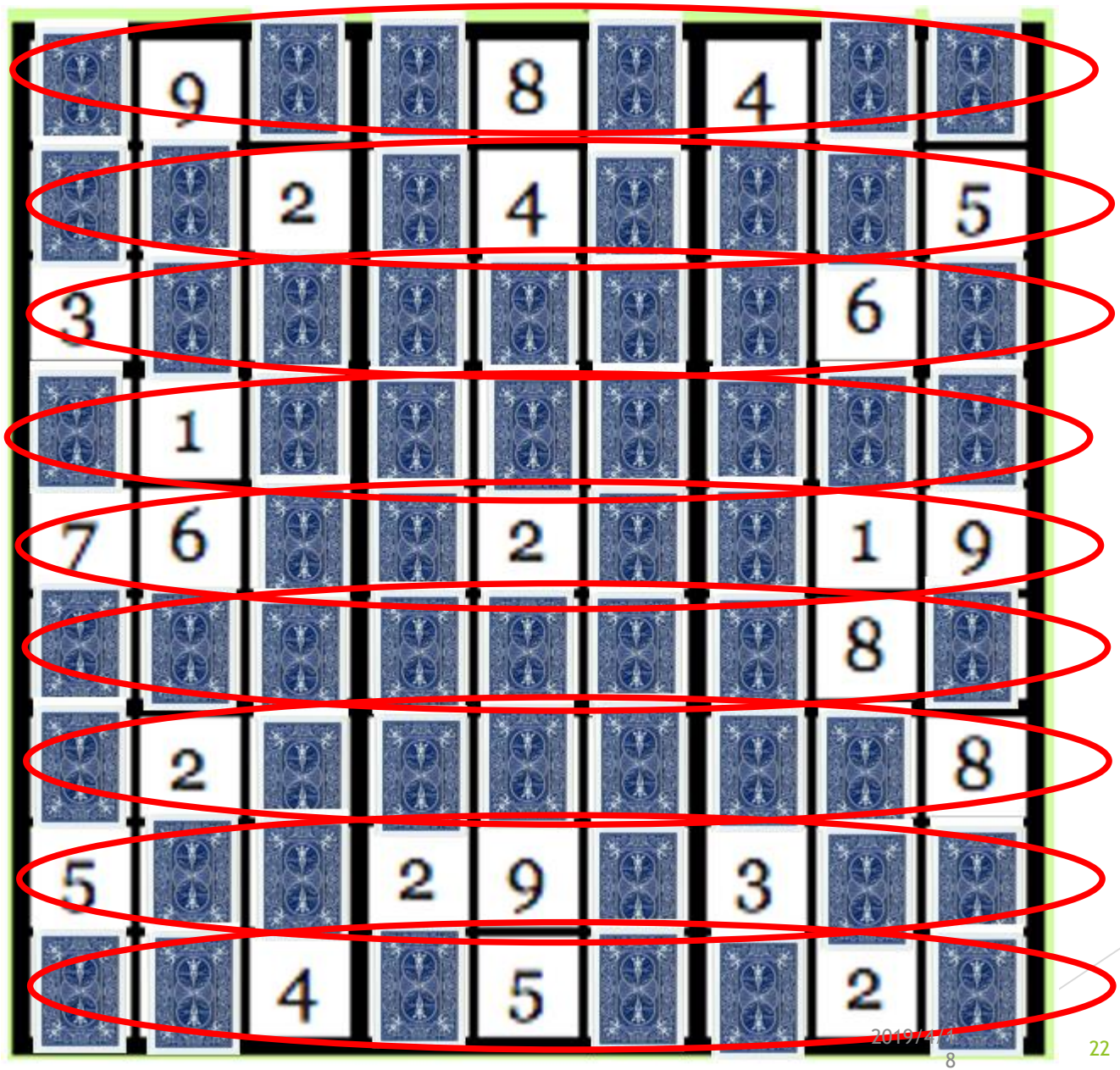
ZK Proof by Sudoku

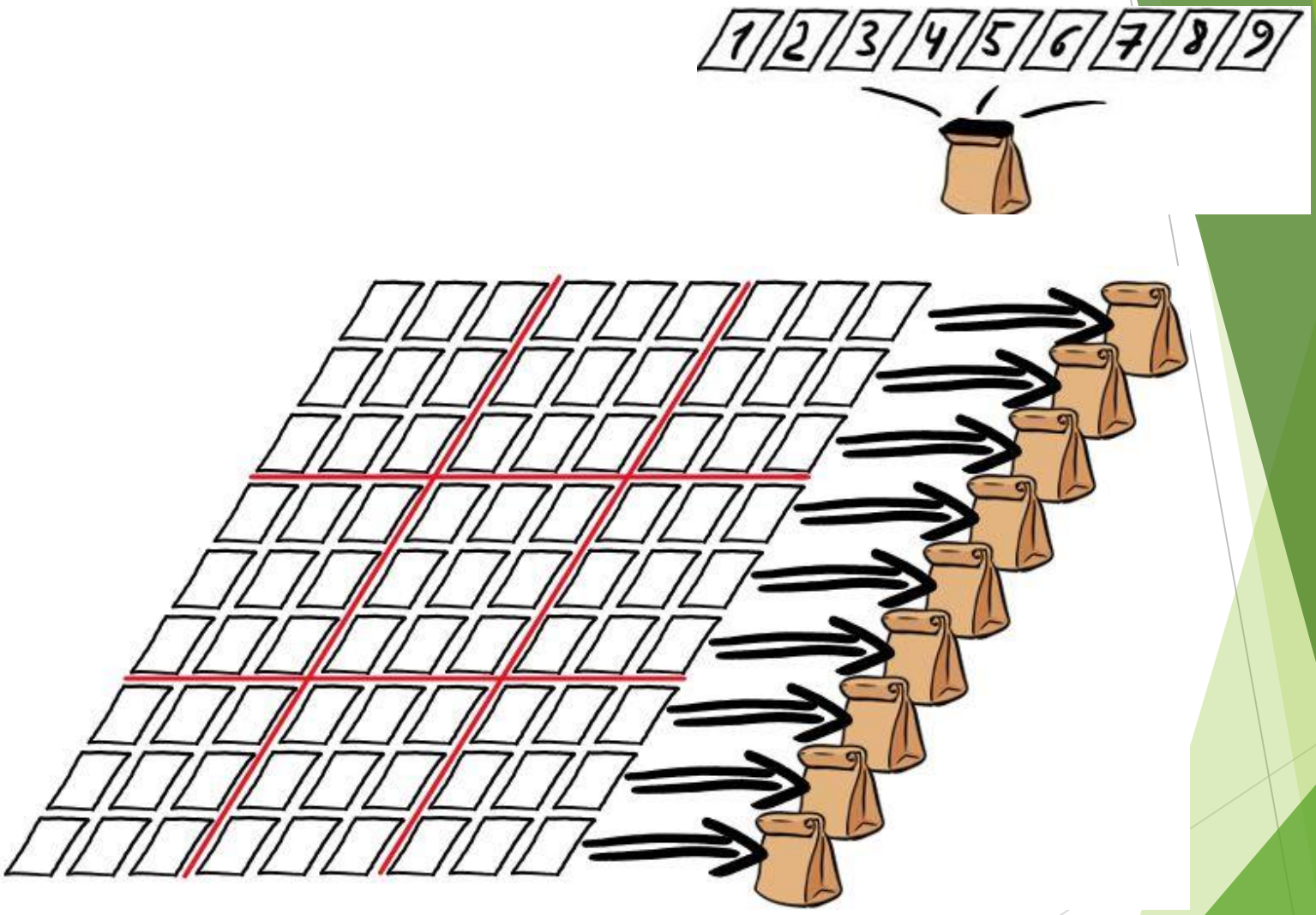


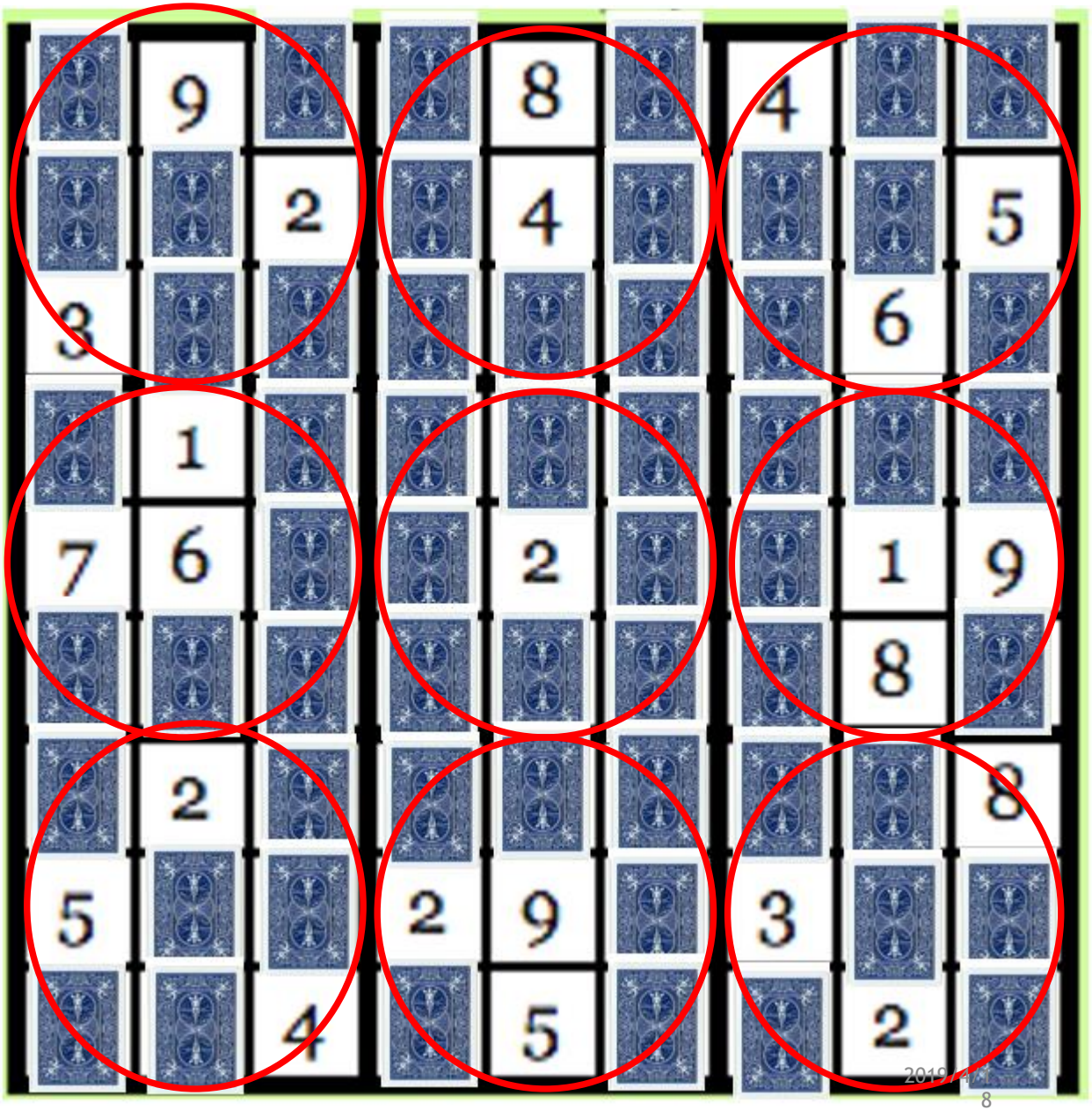
數獨

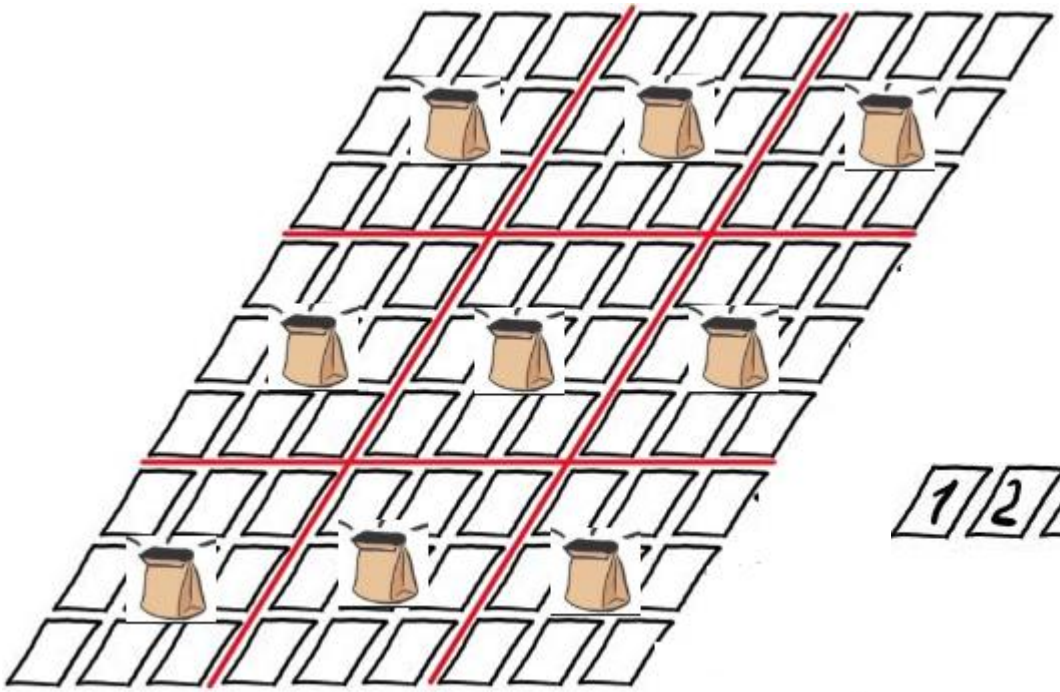
	9			8		4		
		2		4	1			5
3							6	
	1							
7	6			2			1	9
							8	
	2							8
5			2	9		3		
		4		5			2	

1	9	7	6	8	5	4	3	2
6	8	2	3	4	1	7	9	5
3	4	5	9	7	2	8	6	1
4	1	8	5	6	9	2	7	3
7	6	3	8	2	4	5	1	9
2	5	9	7	1	3	6	8	4
9	2	6	4	3	7	1	5	8
5	7	1	2	9	8	3	4	6
8	3	4	1	5	6	9	2	7

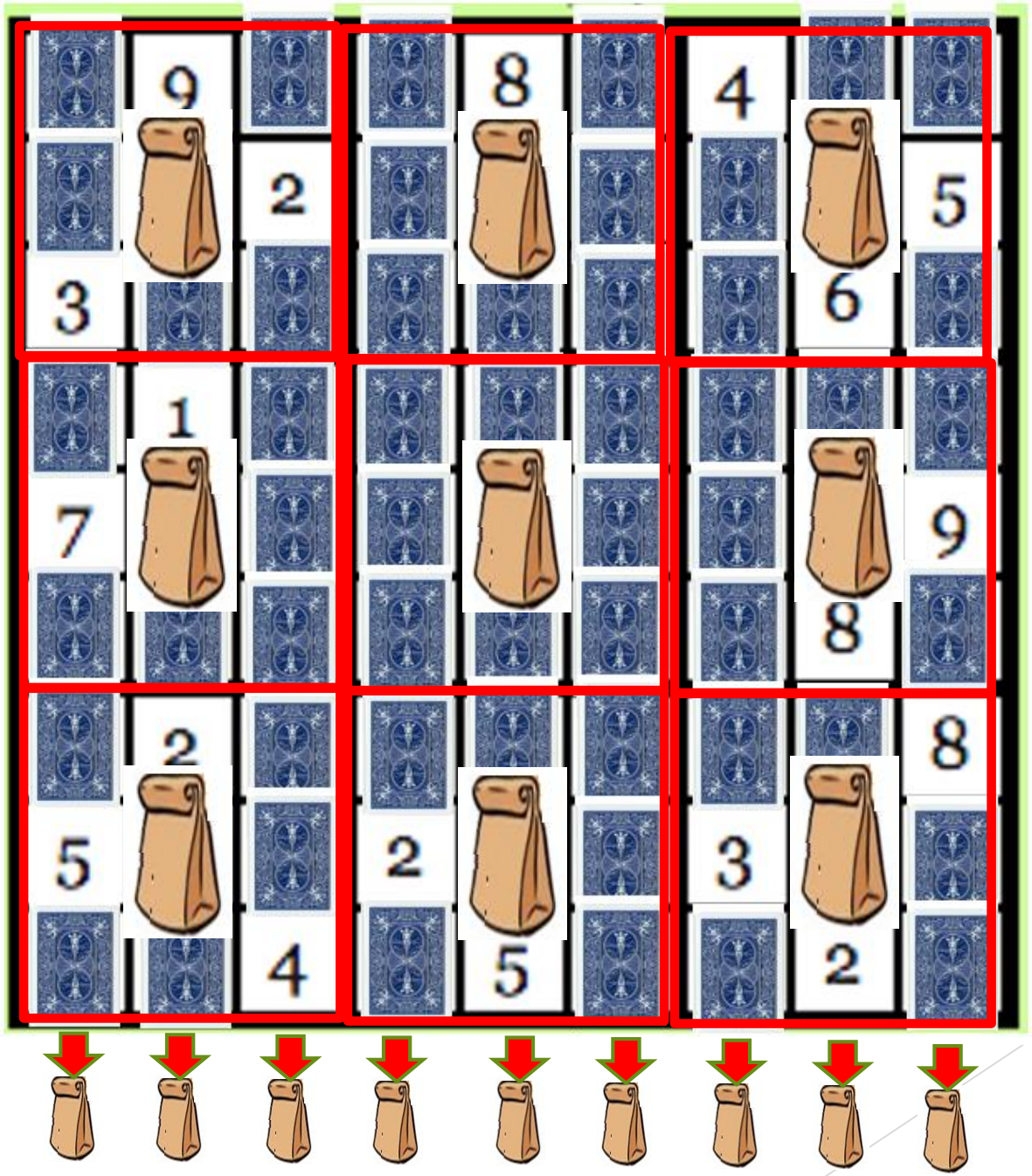

9 8 4
2 4 5
3 6
1
7 6 2 1 9
8
2 8
5 2 9 3
4 5 2


1 2 3 4 5 6 7 8 9


9
2
3
8
4
4
5
6
1
7
6
2
1
9
8
2
8
5
2
9
3
4
5
2




1 2 3 4 5 6 7 8 9


9
2
3
8
4
5
6
1
7
9
8
2
5
4
2
2
5
3
8
2

Zero Knowledge Range Proof

- Zero-Knowledge Range Proofs (ZKRP)允許在不洩漏一個祕密數字的情況下，證明其數介於某範圍內
- Ex : 7 是否介於 5 到 10 之間
- 區塊鏈上之應用:
  - 投票系統: 判斷投票者之年齡
  - 數位貨幣: 判斷消費者可用金額是否小於或等於錢包內總金額

Core Idea

- 數字 m 在某個範圍內$\{a, a+1, \ldots, b\}$時 ，(m-a+1)(b-m+1) 必為正數

Example : $a = 5, b = 10$

- $m = 4 \quad (m - a + 1) = (4 - 5 + 1) = 0$
- $m = 12 \quad (b - m + 1) = (10 - 12 + 1) = -1$
- $m = 7 \quad (m - a + 1)(b - m + 1) = (7 - 5 + 1)(10 - 7 + 1) = 12 > 0$

Core Idea

- 為了不洩漏m值，利用$\omega^2(m-a+1)(b-m+1)$ 代替$(m-a+1)(b-m+1)$，ω為一亂數。
- $\omega^2(m-a+1)(b-m+1)$ 為正數，$(m-a+1)(b-m+1)$ 必為正數
- 為了證明$\omega^2(m-a+1)(b-m+1)$為正數，$M+R=\omega^2(m-a+1)(b-m+1)$
- 目標: 證明M和R皆為正數，且不洩漏M, R之值

零知識範圍證明

Pover

- $c = g^m h^r \ mod\ N$
- $c_1 = c / g^{a-1} \ mod\ N$
- $c_2 = g^{b+1} / c \ mod\ N$
- $c' = c_1^{b-m+1} h^{r'} \ mod\ N$
- $EL_1 = EL(b-m+1, -r, r' | g, h, c_1, h | c_2, c')$
- $c'' = c'^{\omega 2} h^{r''} mod\ N$
- $SQR_1 = SQR(\omega, r'' | c', h | c'')$
- $M + R = \omega^2 (m-a+1)(b-m+1)$, 其中 $M = \alpha^2$
- $r_1 + z = \omega^2((b-m+1)r+r')+r''$
- $c'_1 = g^M h^{r1} \ mod\ N$
- $c'_2 = h^z \ mod\ N$
- $SQR_2 = SQR(\alpha, r_1 | g, h | c_1')$

公布

$c, c_1, c_2, c', c'', c_1', c_2', R, EL_1 SQR_1 SQR_2$

零知識範圍證明

Verifier

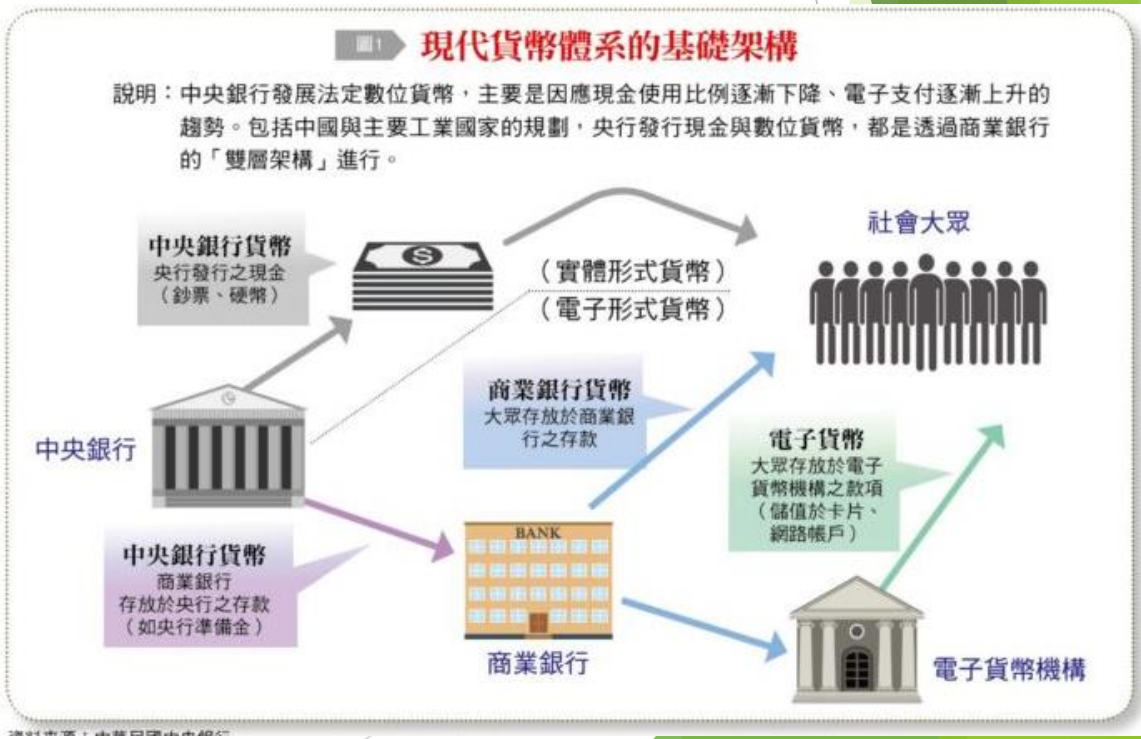
計算	$c_1 = c/g^{a-1}$
計算	$c_2 = g^{b+1}/c$
驗證	EL(b-m+1, -r, r'|g, h, c1, h|c_2, c')
驗證	SQR(ω, r‘’| c‘, h| c’‘)
驗證	$c'' = c'_1 c'_2 g^R \ mod\ N$
驗證	SQR(α, r1|g, h|c_1‘)其中($c'_1 = g^M h^{r1}$)
驗證	R > 0

Disadvantages of Blockchain-based Cryptocurrencies

- 非法定貨幣
- 市場波動大
- 交易無法追蹤
  - 無法監管
  - 淪犯罪及洗錢的工具

Central Bank Digital Currency (CBDC)

- 未來數位貨幣的主流
- 中央銀行發行
  - 可信賴
  - 法定貨幣（受司法管轄）
- 安全需求與特性
  - 隱私，匿名性 (可控匿名)
  - 普匯金融
  - 不可偽造
  - 不可重複使用
  - 不可追蹤（但可受監管）
  - 使用便利
  - 支援離線交易
  - etc



CBDC發展

- 中國數位人民幣計畫(2014)
  - 結合了中國央行，四大國有銀行，以及三大公營電信企業共同合作，是一種基於區塊鏈技術的加密貨幣體系，預計用來替代人民幣並與紙幣的屬性與功能完全一樣。未來任何中國機構和個人均不能拒絕接收DCEP。
- 韓國CBDC先導型計劃（2019）
  - 對CBDC的設計，技術，法規等各項要求進行完整與詳細的評估，以便在面臨世界各國的CBDC威脅時，能儘速做出應對。
- 日本數位日圓計畫(2020)
  - 針對數位日圓的設計之外，也研擬推動數位日圓相關的法案，提高未來日圓在新興市場的影響力。
- 台灣
  - 目前以推動批發行數位貨幣的可行性研究為主
  - 短期並無發行通用型數位貨幣之規劃。

Banknote A e

Central Bank

Commercial Bank

Commercial Bank

Customer

Merchant

CBDC Arch

Possible Problems:
1. Double spending
2. Traceable

Central Bank

Commercial Bank

Commercial Bank

Customer

Merchant

Blind signatures

- Proposed by David Chaum in 1982
  - Based on RSA signatures
- Allows a signer to sign a signature without knowing the message he/she signed
- The resulting signature can be publicly verified
- Untracability: the signer cannot link the message with the blind signature he/she did in the blinded signing phase

CBDC Arch

Check database

Central Bank

Commercial Bank

- Double spending prevention
- Untracability

Commercial Bank

Customer

Merchant

RSA Signature

	Choose large primes p, q and compute $n = p \cdot q$ Choose e such that $\gcd(e, \varphi(n)) = 1$, where $\varphi(\cdot)$ is Euler's totient function
Private	d such that $e \cdot d = 1 \bmod \varphi(n)$
Public	n, e
	$\varphi(n)$:(p-1)(q-1)
Signing Algorithm (message *M*)	
$\sigma \leftarrow m^d \bmod n$	*m=H(M)*
Output σ as the signature of *M*	
Verification Algorithm	

if *H(M)* = $\sigma^e \bmod n$ **then**
return `True`
else
return `False`	

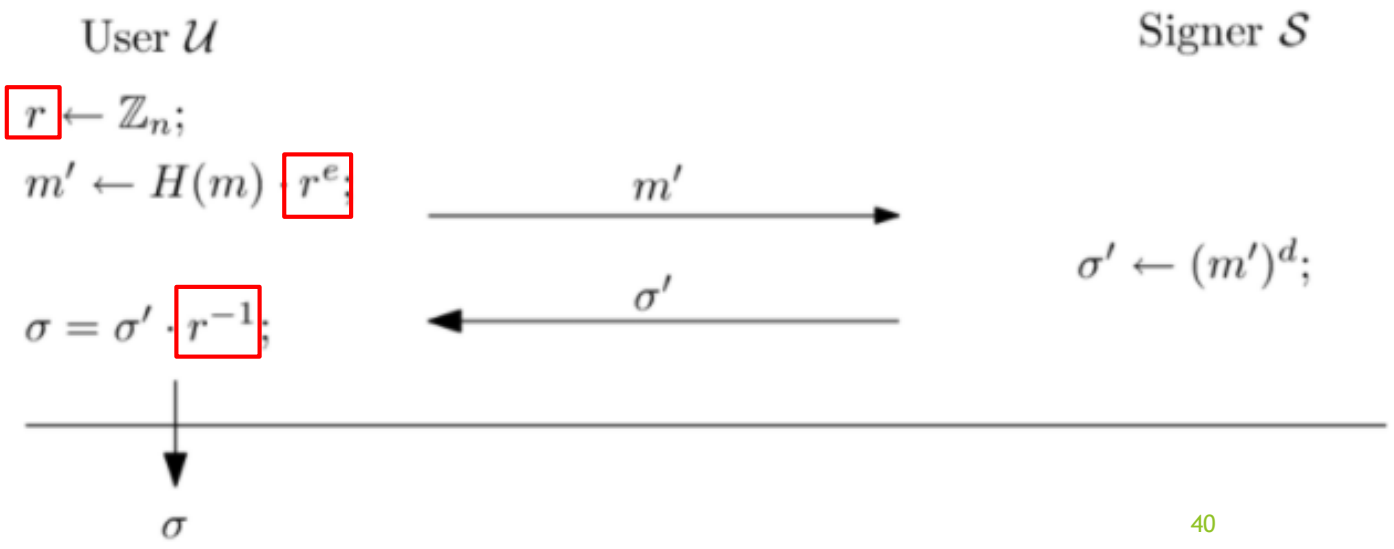
D. Chaum's Blind Signature (Based on RSA)

Common input: Public key $PK \stackrel{\text{def}}{=} (e, n)$, hash function $H : \mathcal{M} \to \mathbb{Z}_n$

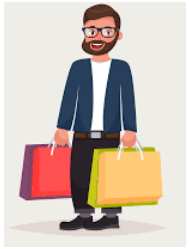
Signer's input: Secret key d

User's input: Message m

User's output: RSA signature σ on m



Ecash based on Blind signatures



Customer(user)

Open account

Withdraw (Blind Signature)

Commercial Bank

Central Bank(signer)

Check database

Confirmation (double-spending?)

Deposit the coin

User the coin with signature

Seller(verifier)

Verify

瑞士國家銀行數位貨幣計畫

How to issue a central bank digital currency

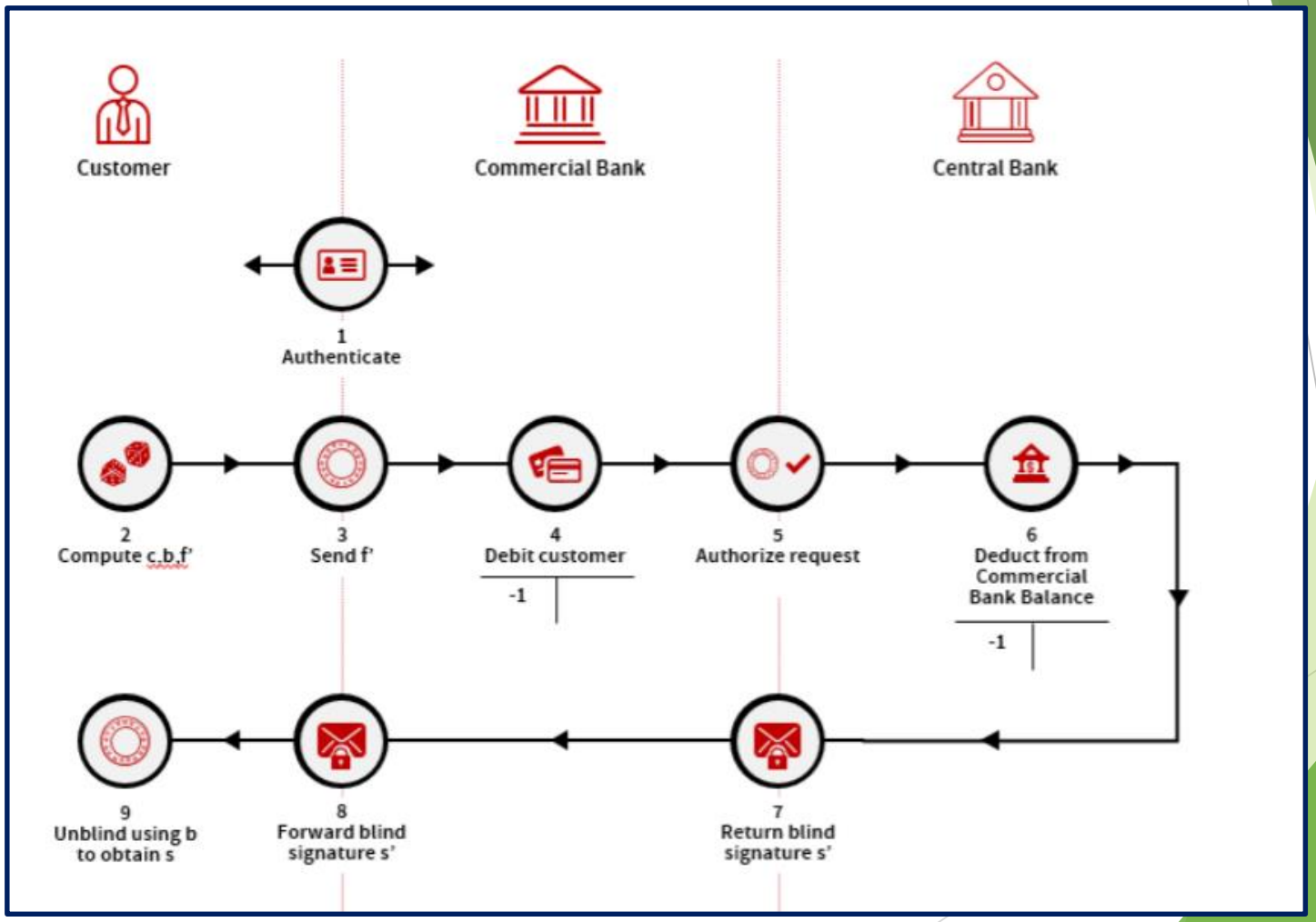
David Chaum, Christian Grothoff, Thomas Moser

SNB Working Papers
3/2021

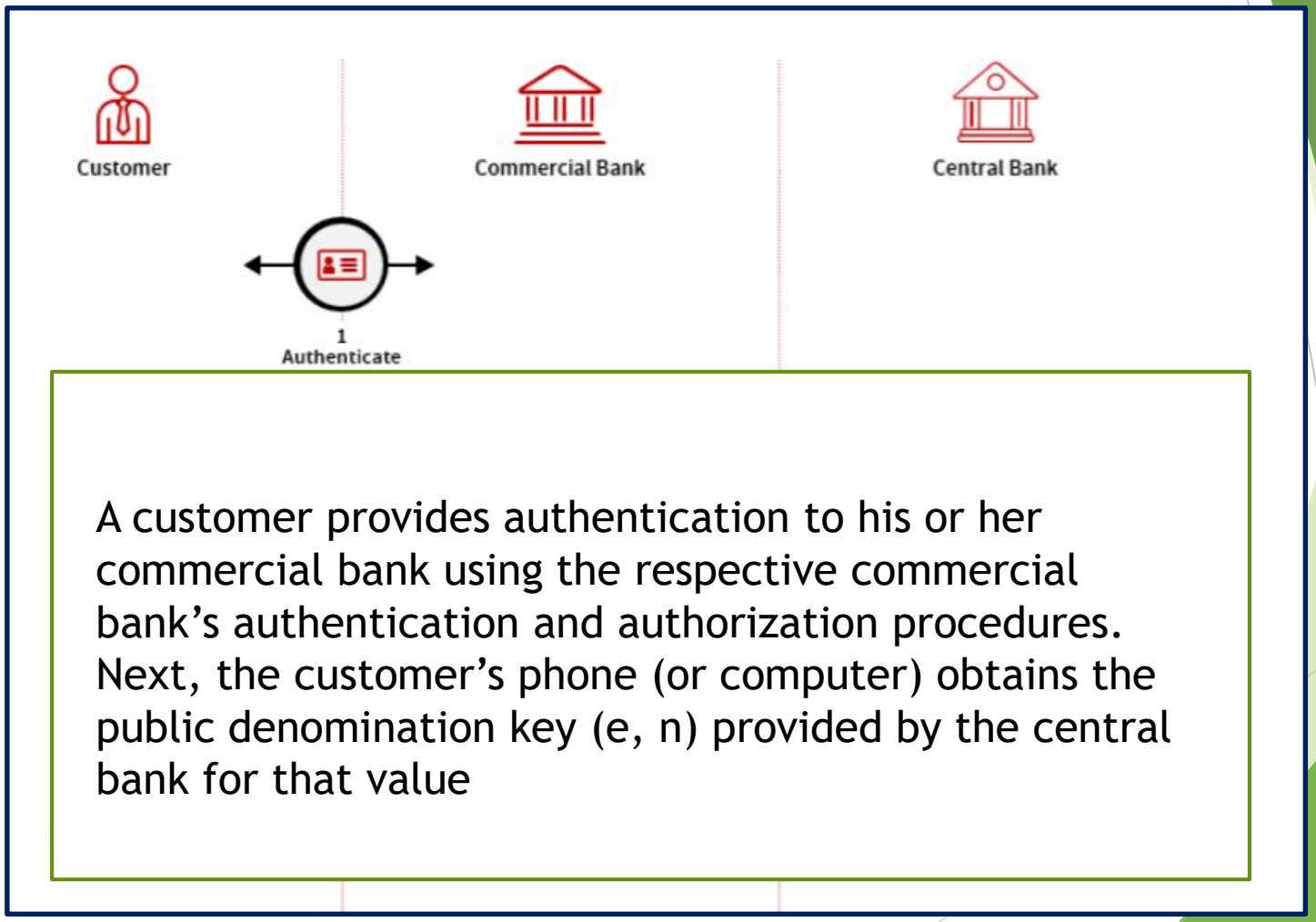
https://taler.net/papers/cbdc2021en.pdf

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

CBDC Withdraw

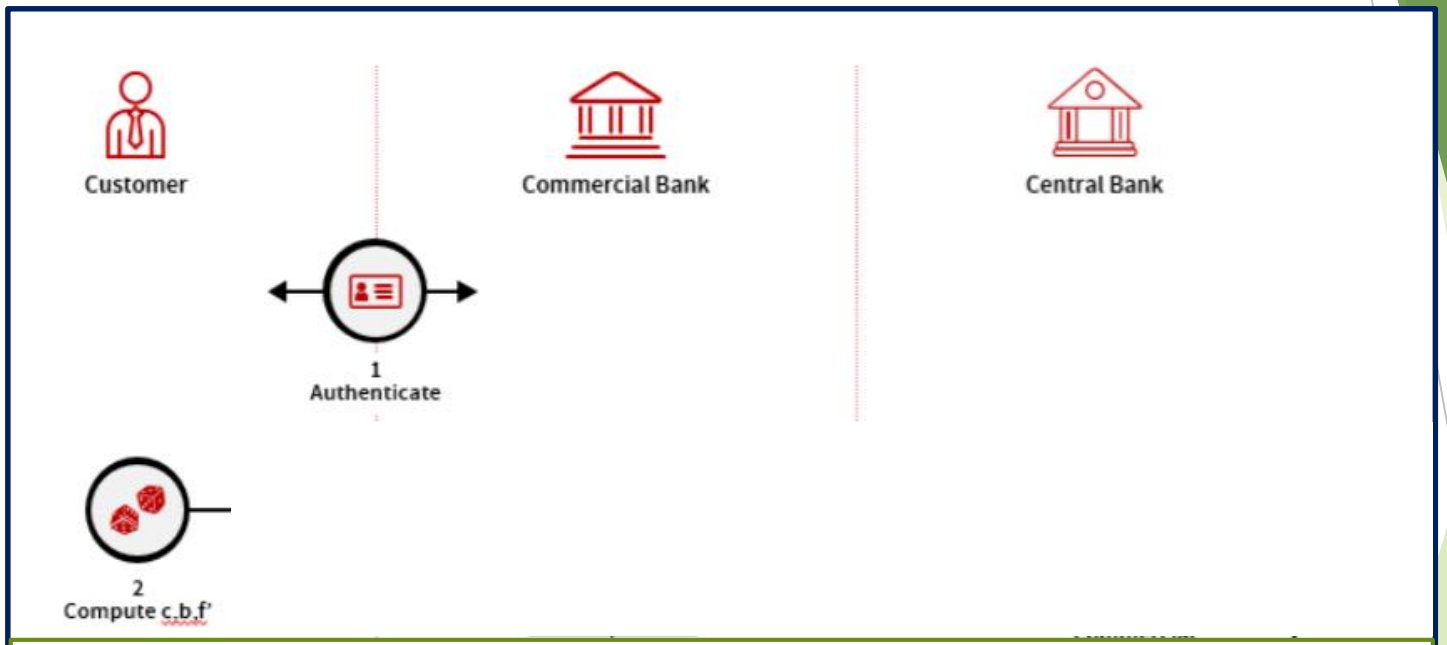


CBDC Withdraw-(1)



A customer provides authentication to his or her commercial bank using the respective commercial bank's authentication and authorization procedures. Next, the customer's phone (or computer) obtains the public denomination key (e, n) provided by the central bank for that value

CBDC Withdraw-(2)

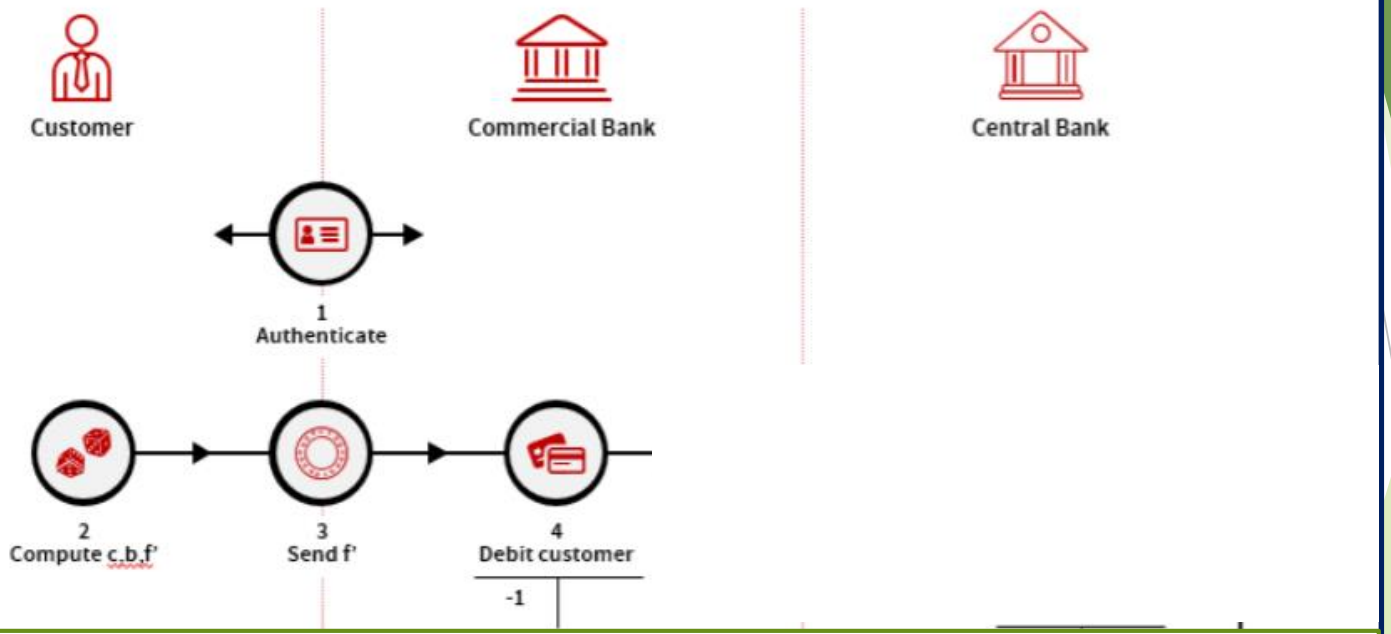


it then computes a key pair (c, C) for a coin, and chooses a blinding factor b. The coin's public key C is then hashed $f \leftarrow H(C)$ and blinded to $f' \leftarrow b^e f \bmod n$

CBDC Withdraw-(3)

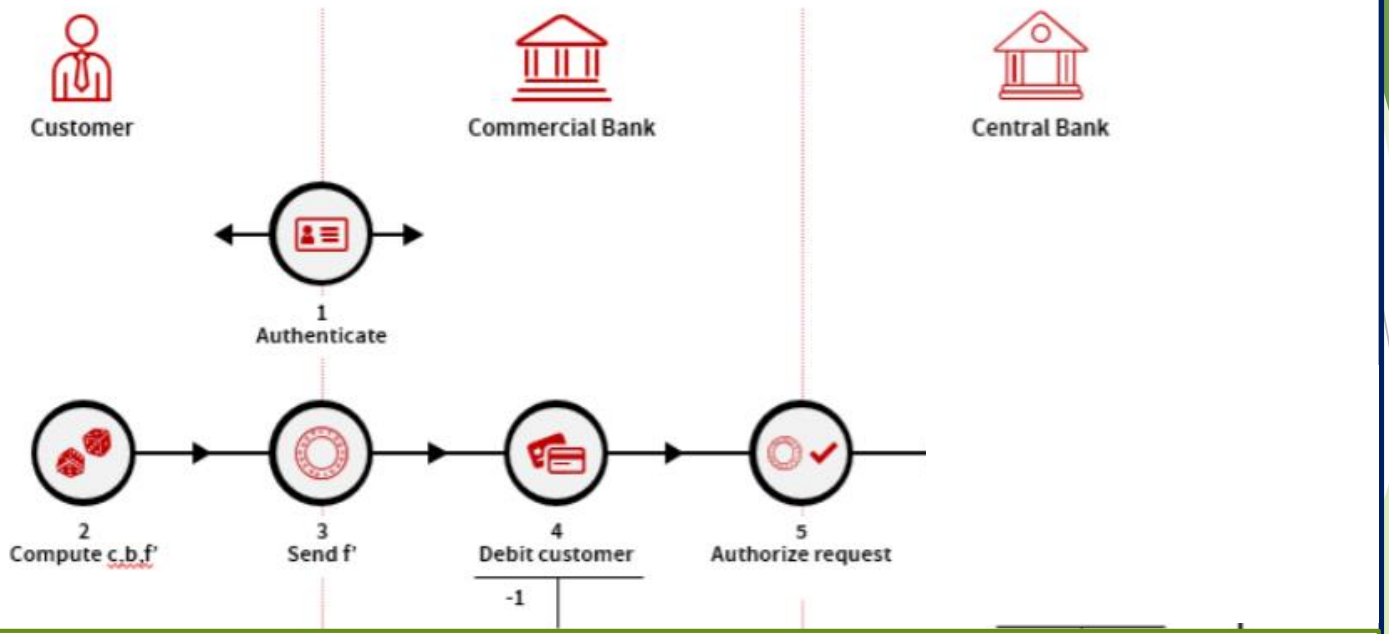
the customer's phone sends *f'* together with an authorization to withdraw the coin and debit the customer's account to the commercial bank via an established secure channel.

CBDC Withdraw-(4)



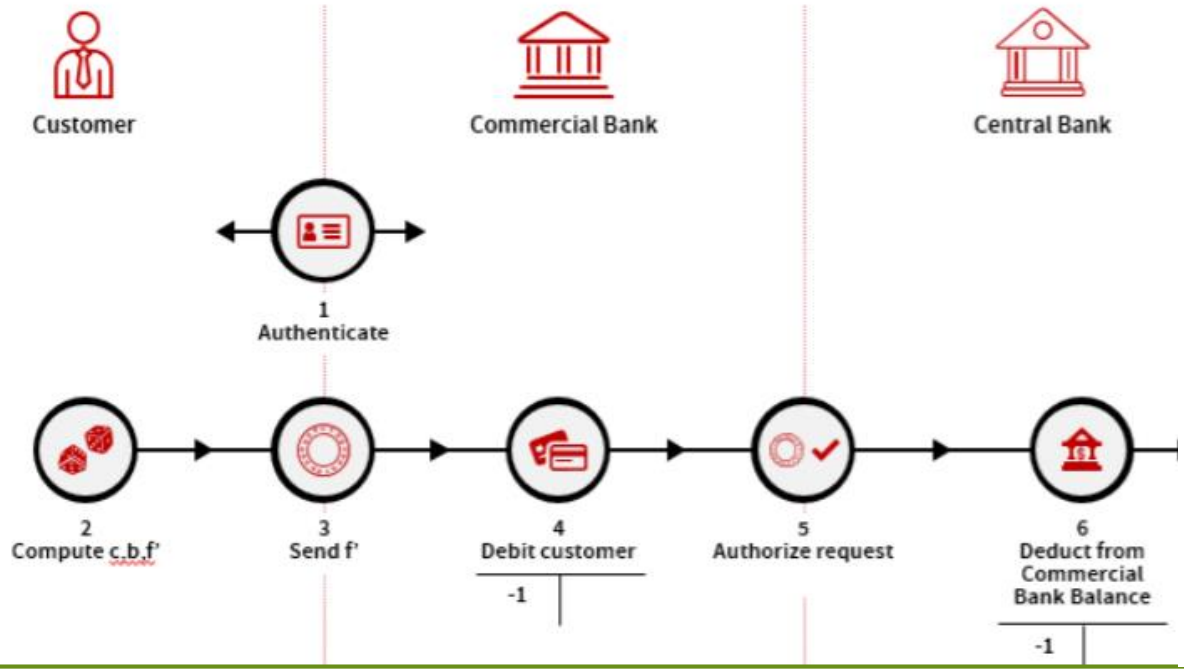
The commercial bank then debits the amount from the customer's deposit account.

CBDC Withdraw-(5)



The commercial bank digitally authorizes the request with its own bank branch digital signature and forwards the request and the blinded coin to the central bank for signing

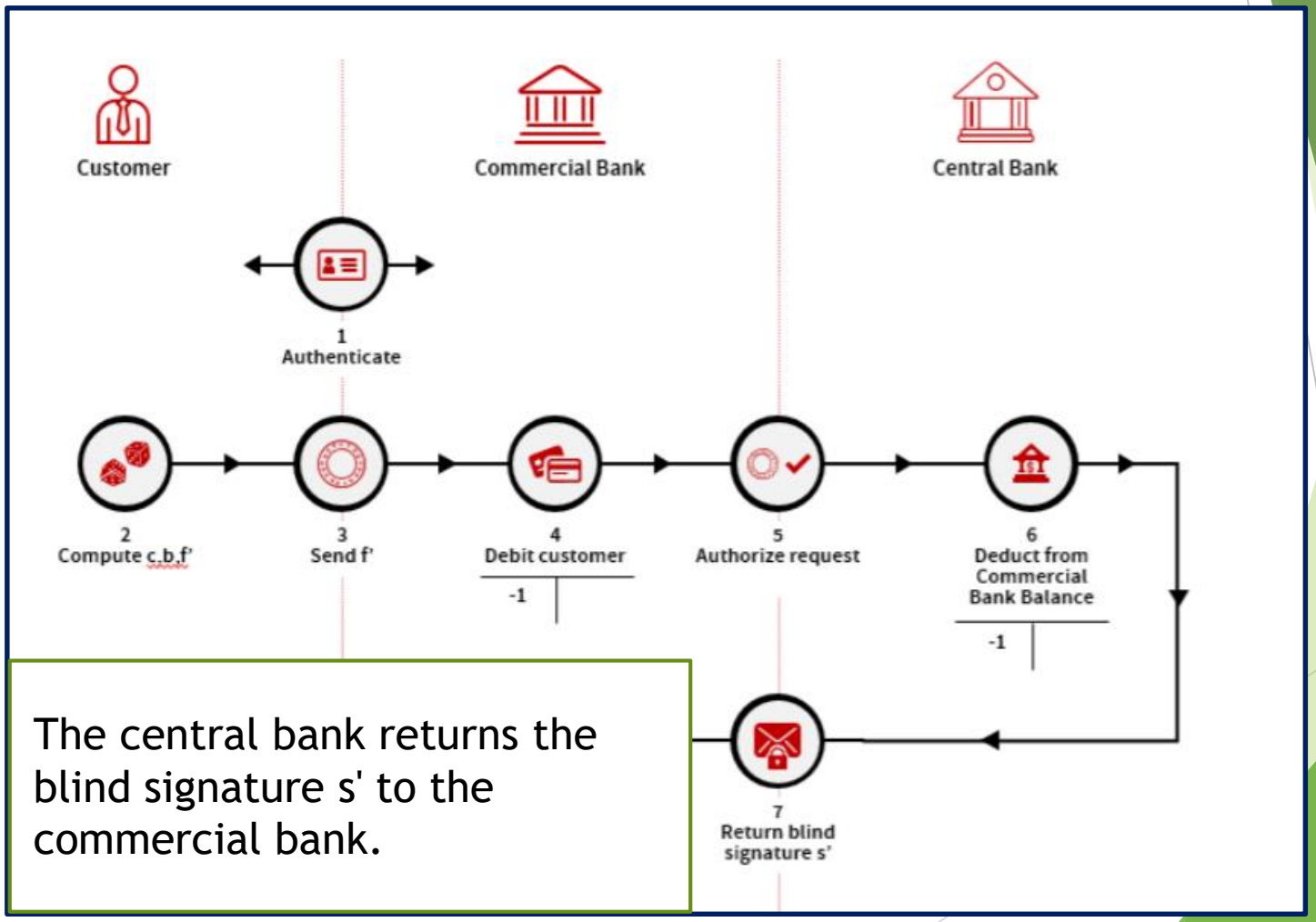
CBDC Withdraw-(6)



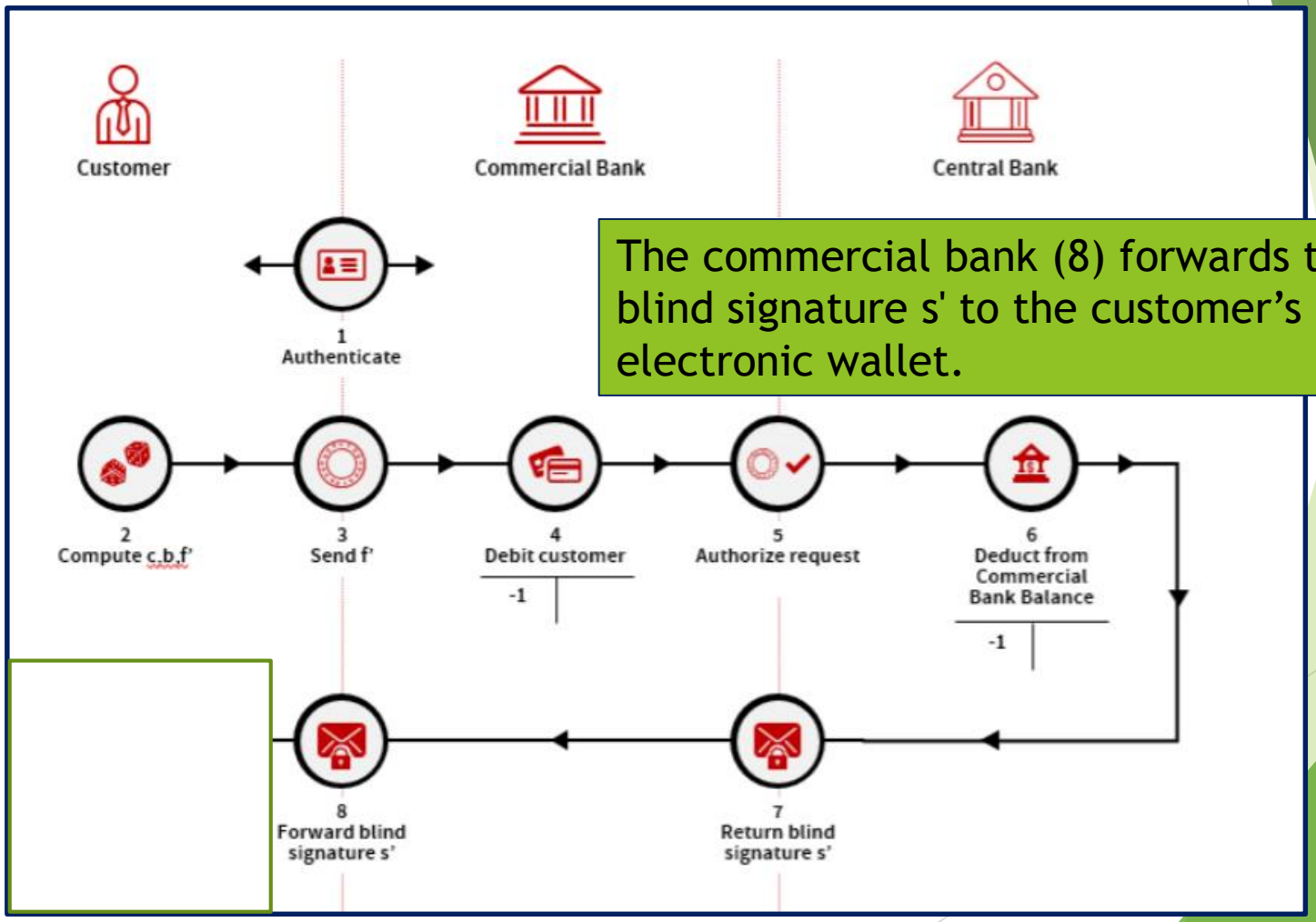
The central bank deducts the value of the coin from the commercial bank's central bank account, blindly signs the coin with the central bank's private key for the respective value *f'*.

$$s' = f'^{d} \bmod n = (b^{e}H(C))^{d} \bmod n = bH(C)^{d} \bmod n$$

CBDC Withdraw-(7)

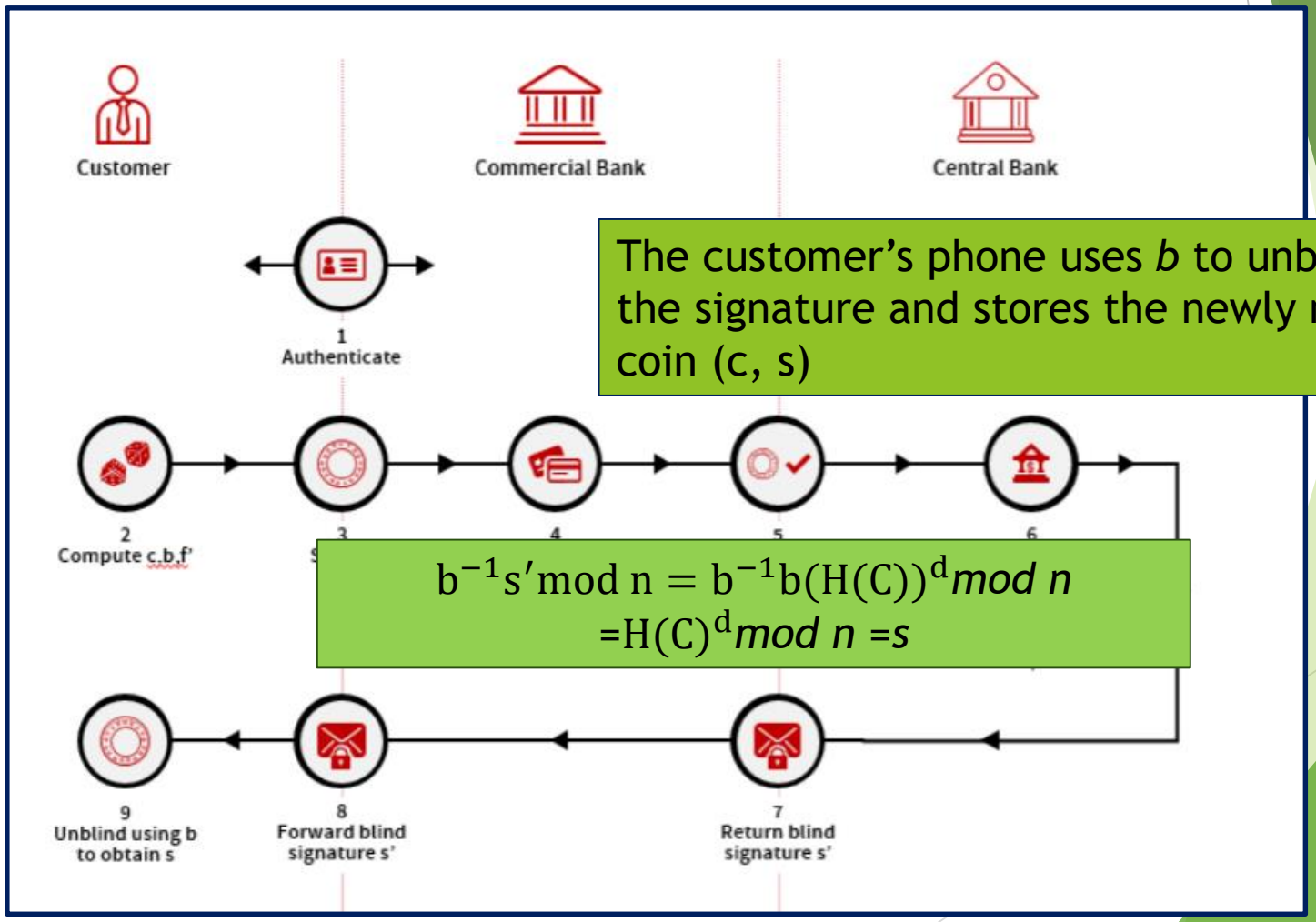


CBDC Withdraw-(8)

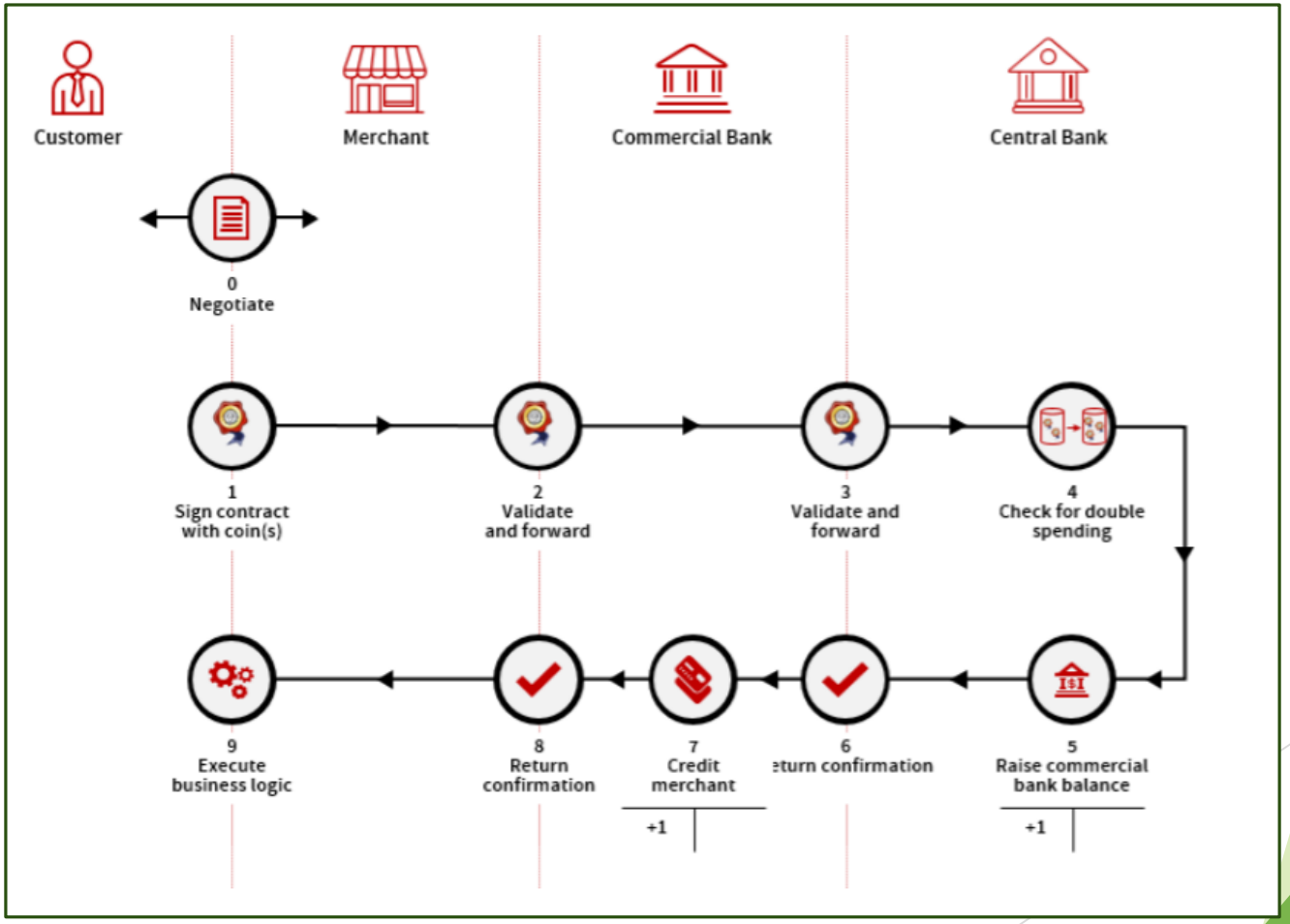


The commercial bank (8) forwards the blind signature s' to the customer's electronic wallet.

CBDC Withdraw-(9)



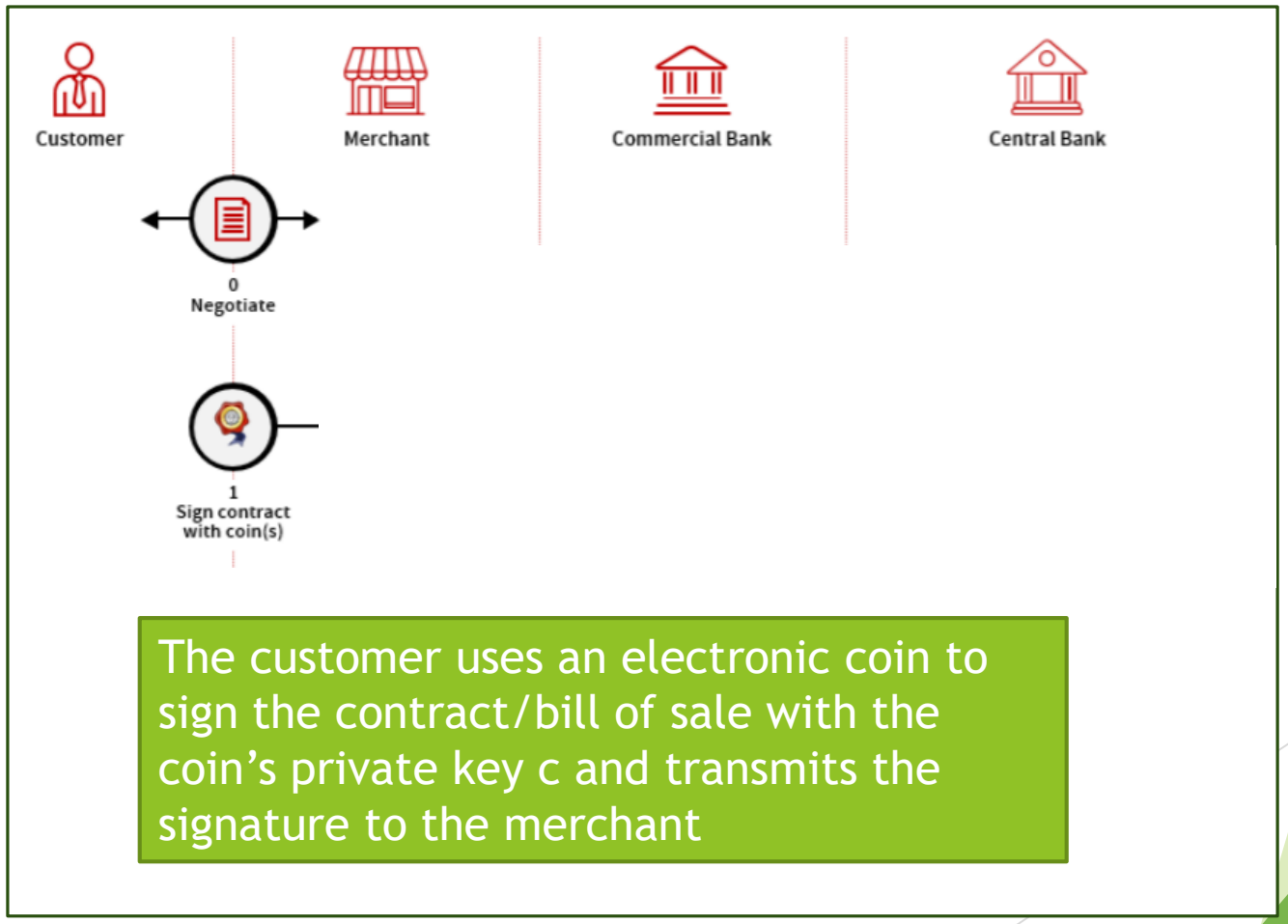
Spending and Depositing CBDC



Spending and Depositing CBDC –(0)

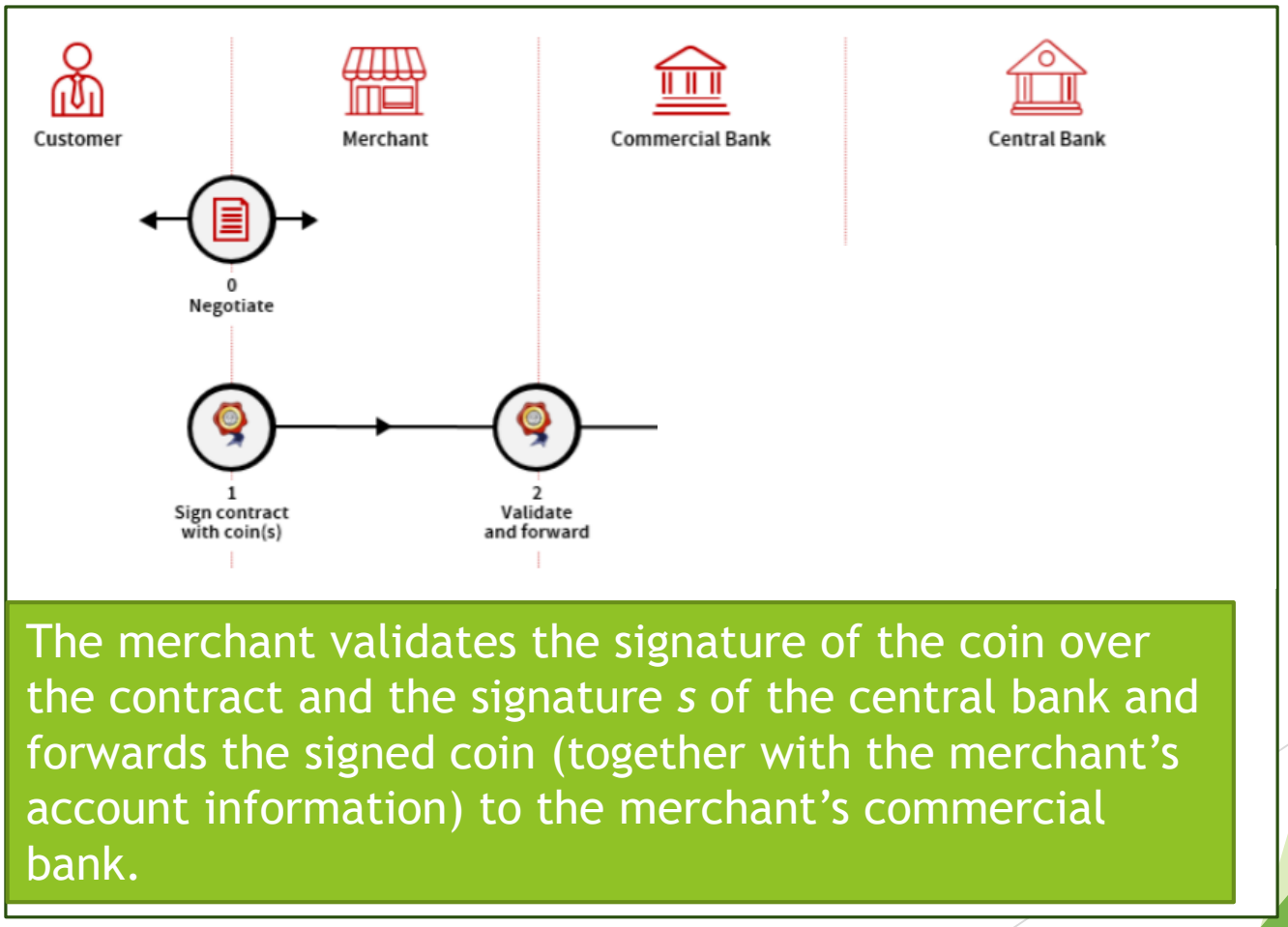
A customer and a merchant negotiate a business contract

Spending and Depositing CBDC –(1)



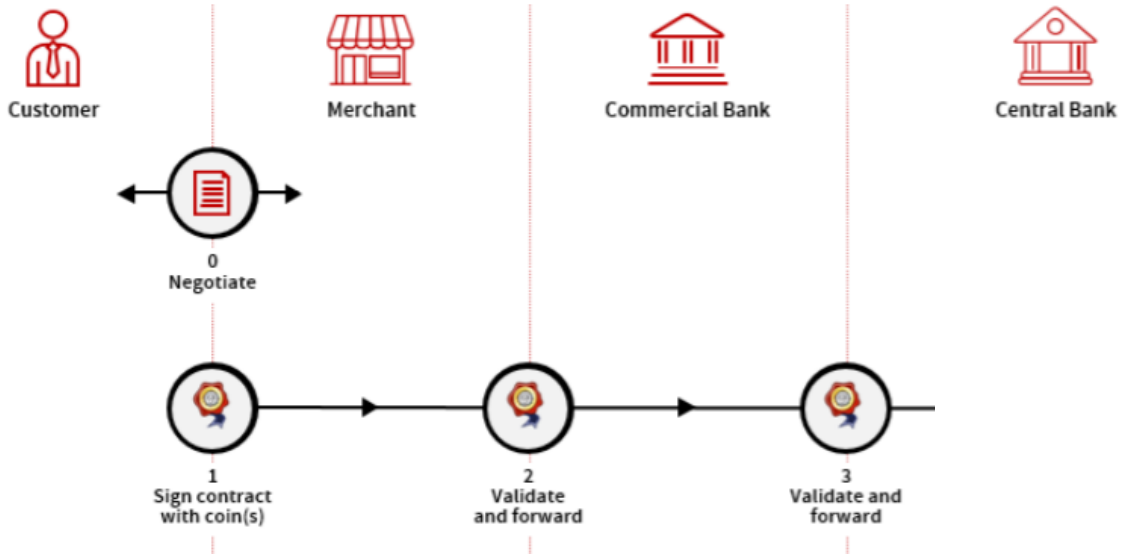
The customer uses an electronic coin to sign the contract/bill of sale with the coin's private key c and transmits the signature to the merchant

Spending and Depositing CBDC –(2)



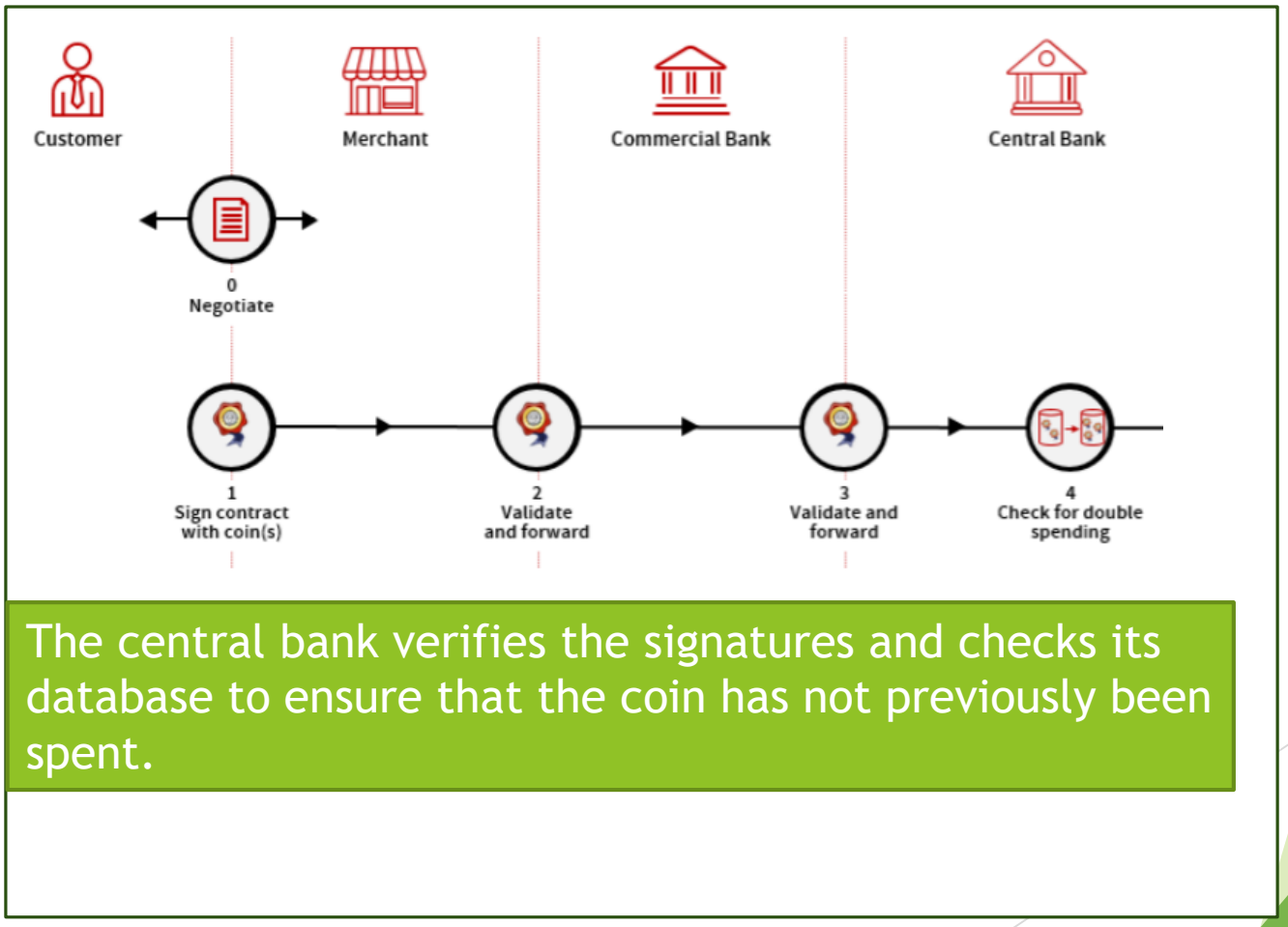
The merchant validates the signature of the coin over the contract and the signature *s* of the central bank and forwards the signed coin (together with the merchant's account information) to the merchant's commercial bank.

Spending and Depositing CBDC –(3)



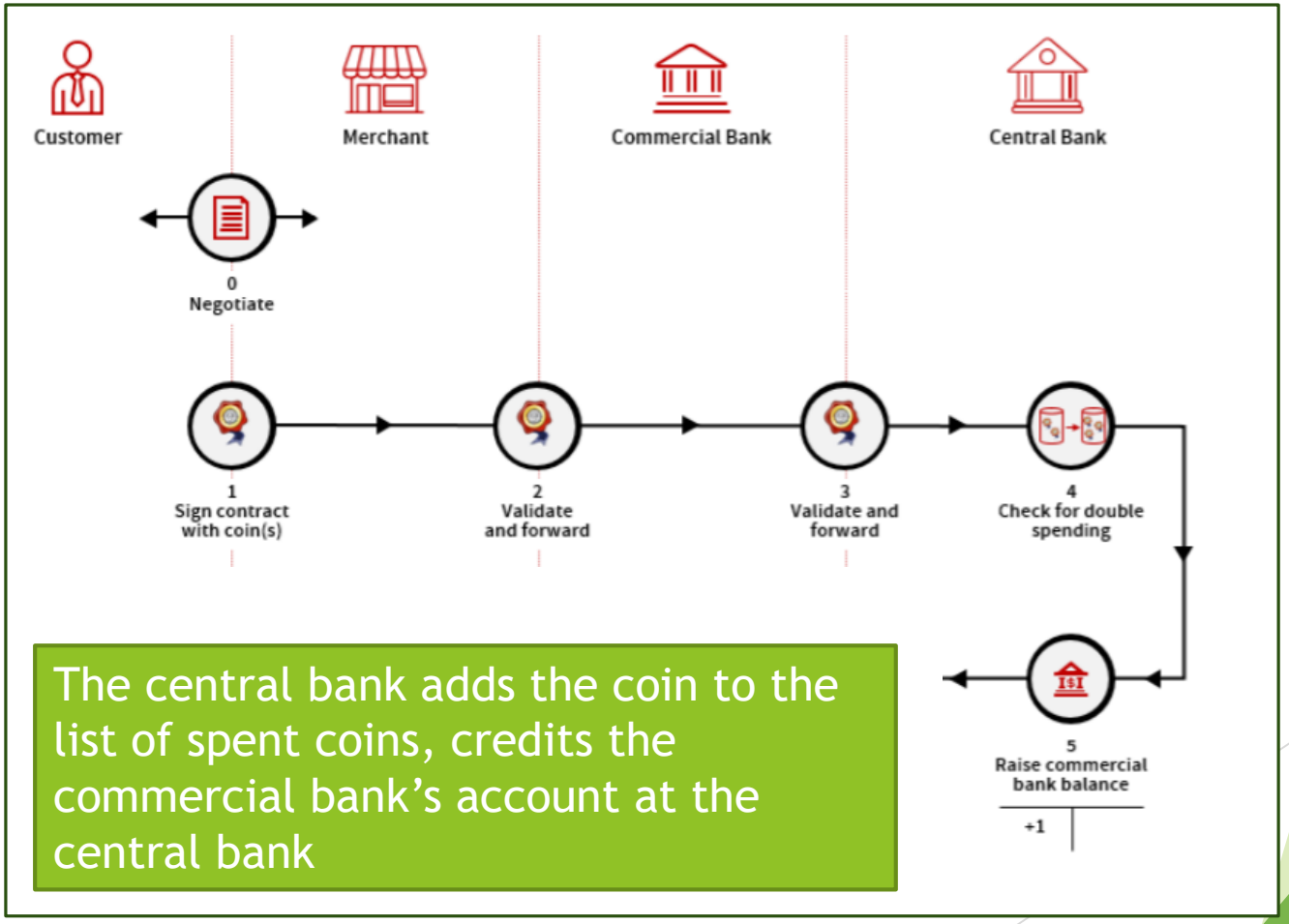
The merchant's commercial bank confirms that the merchant is one of its customers and forwards the signed coin to the central bank.

Spending and Depositing CBDC –(4)



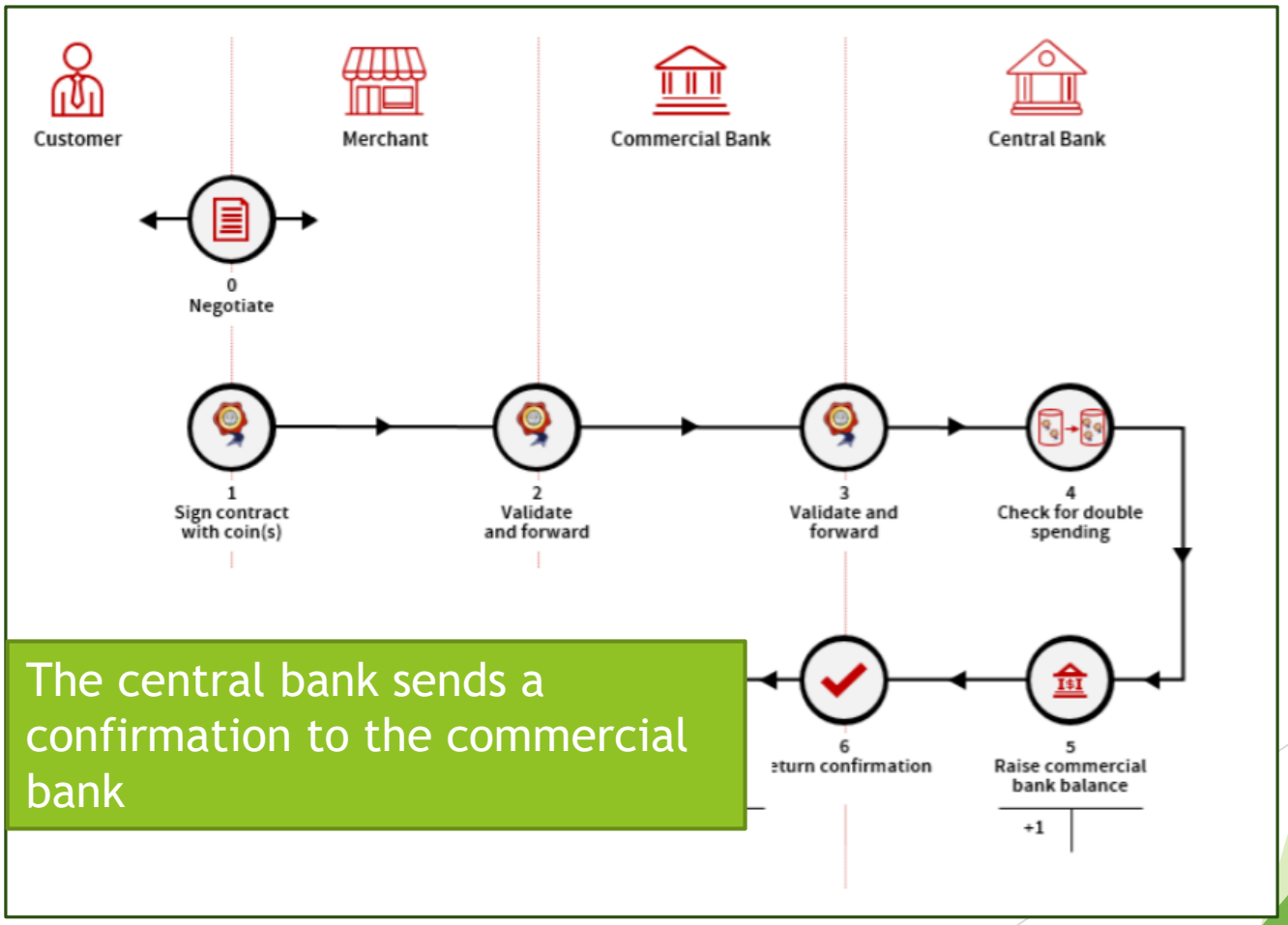
The central bank verifies the signatures and checks its database to ensure that the coin has not previously been spent.

Spending and Depositing CBDC –(5)



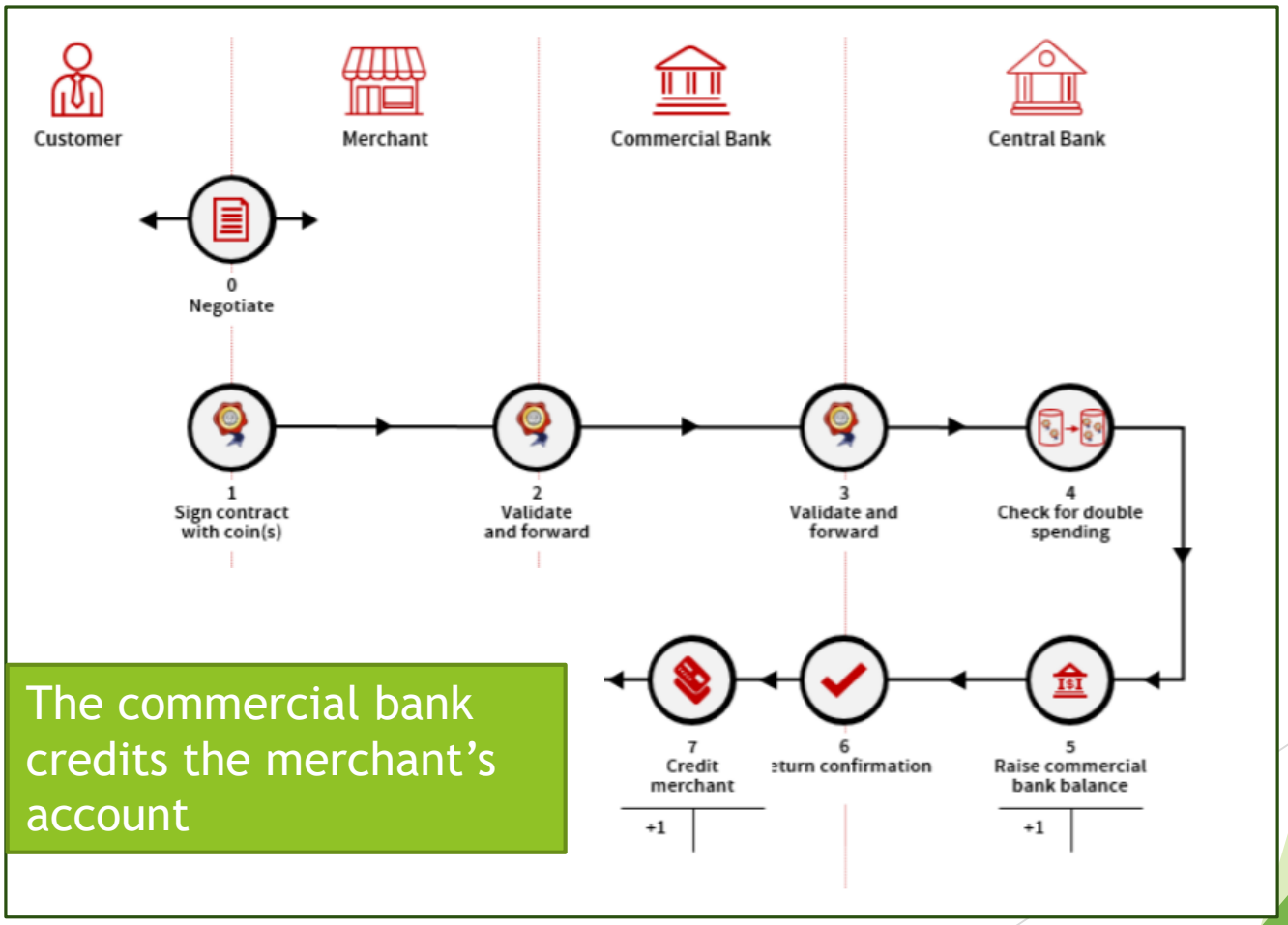
The central bank adds the coin to the list of spent coins, credits the commercial bank's account at the central bank

Spending and Depositing CBDC –(6)



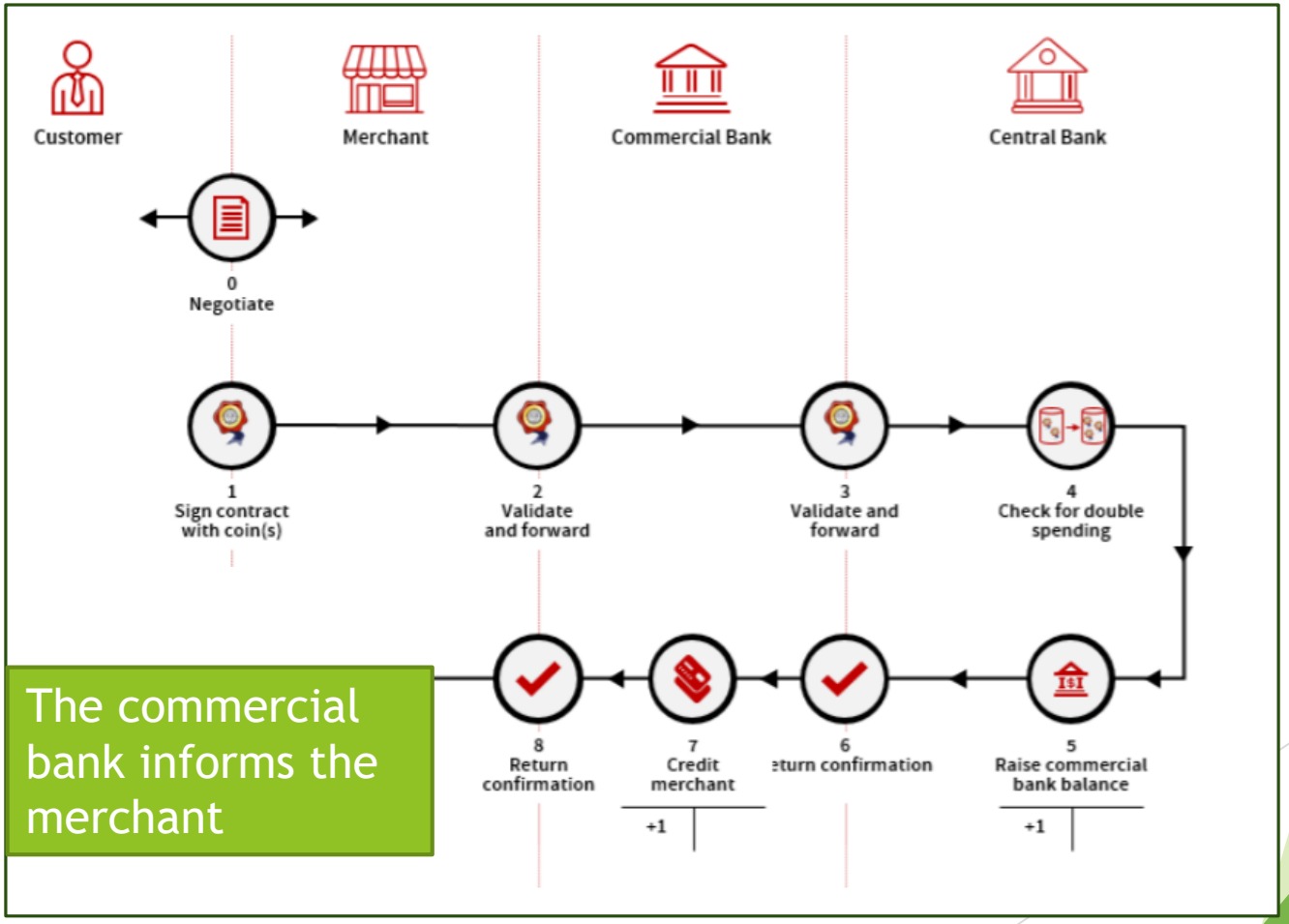
The central bank sends a confirmation to the commercial bank

Spending and Depositing CBDC –(7)

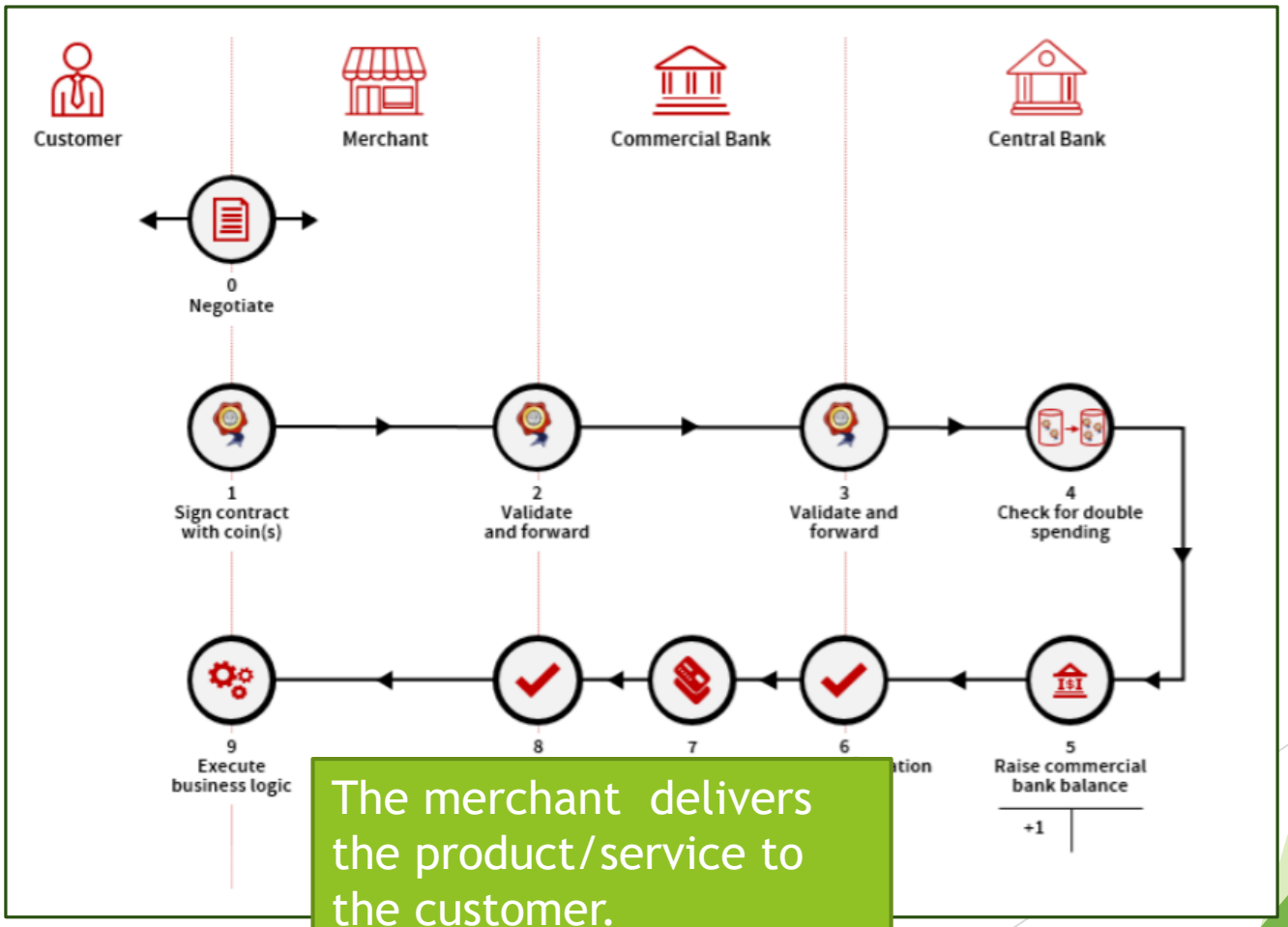


The commercial bank credits the merchant's account

Spending and Depositing CBDC –(8)

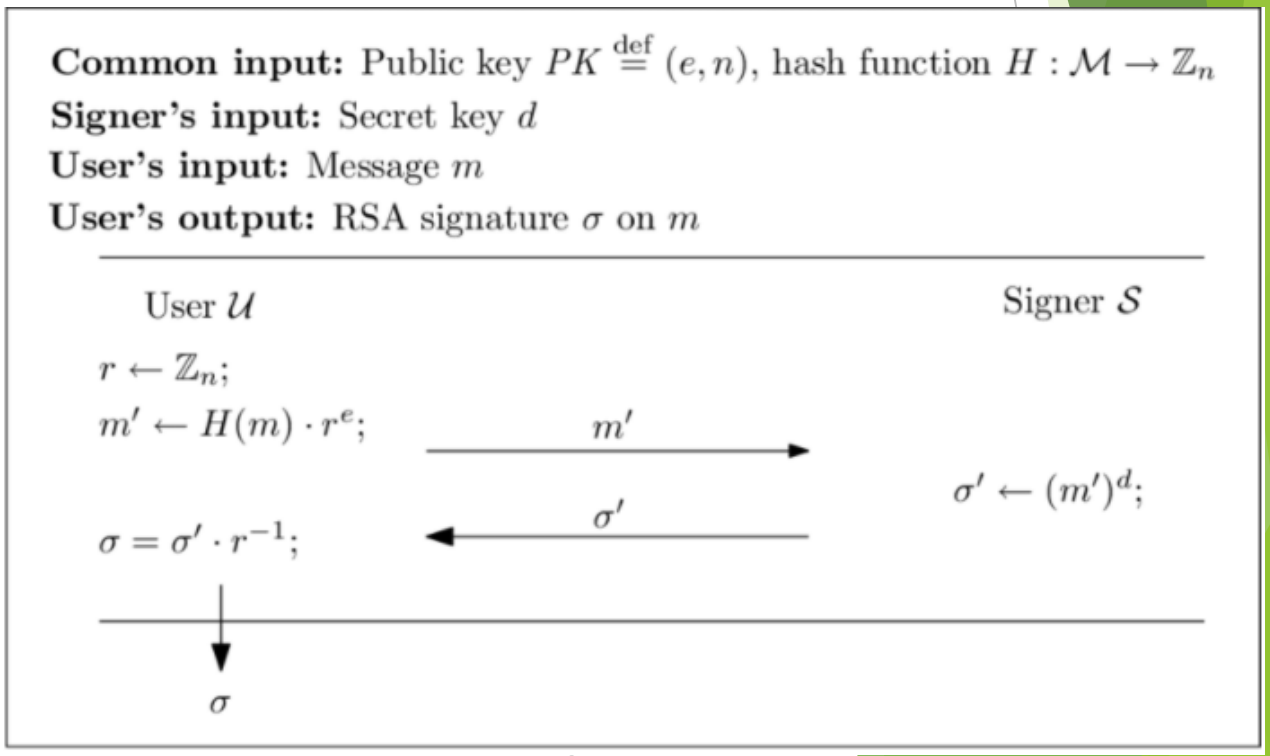


Spending and Depositing CBDC –(9)



How to Express the Denominations

- Using different key pairs
  - (pk1,sk1) for 1 NTD
  - (pk2,sk2) for 5 NTD
  - (pk3,sk3) for 10 NTD



How to Express the Denominations

(pk1,sk1) for 1 NTD
Alice

(pk2,sk2) for 5 NTD
Bob

(pk3,sk3) for 10 NTD
Eve

Current Disadvantages of SNB's CBDC

- Different key pairs required for different denominations
- No support for off-line transactions
- Inefficient exchange protocol
- Inefficient verification for large amount of digi cash
- Monitoring impossible

新世代央行數位貨幣
之關鍵技術研發與支付系統設計(1/2)

科技部資安前瞻計畫

MOST 110-2218-E-004 -001 -MBK

CBDC計畫研究動機

中央銀行
數位貨幣

CBDC計畫：主要成員

國立政治大學

左瑞麟 教授

資訊科學系

總計畫/子計畫一主持人

日本筑波大學博士

研究領域

-密碼學
-資訊安全
網路安全
-區塊鏈與隱私強化技術

陳　恭 教授

資訊管理學系

總計畫共同主持人

美國耶魯大學博士

研究領域

-程式語言設計
-區塊鏈智能合約分析
-社群媒體資料分析
-社群大數據

曾一凡 助理教授

資訊科學系

子計畫一共同主持人

國立中山大學博士

研究領域：

-密碼學
-資訊安全
-多接受者加密
-匿名性

國立嘉義大學

王智弘 教授

資訊工程系

子計畫二主持人

國立成功大學博士

研究領域:

-網路安全
-密碼技術
-入侵偵測與防禦

元智大學

陳昱圻副教授

資訊工程系

子計畫三主持人

國立中興大學博士

研究領域

-資訊安全
-密碼學
-保有隱私計算(與機器學習)
-區塊鏈技術與應用

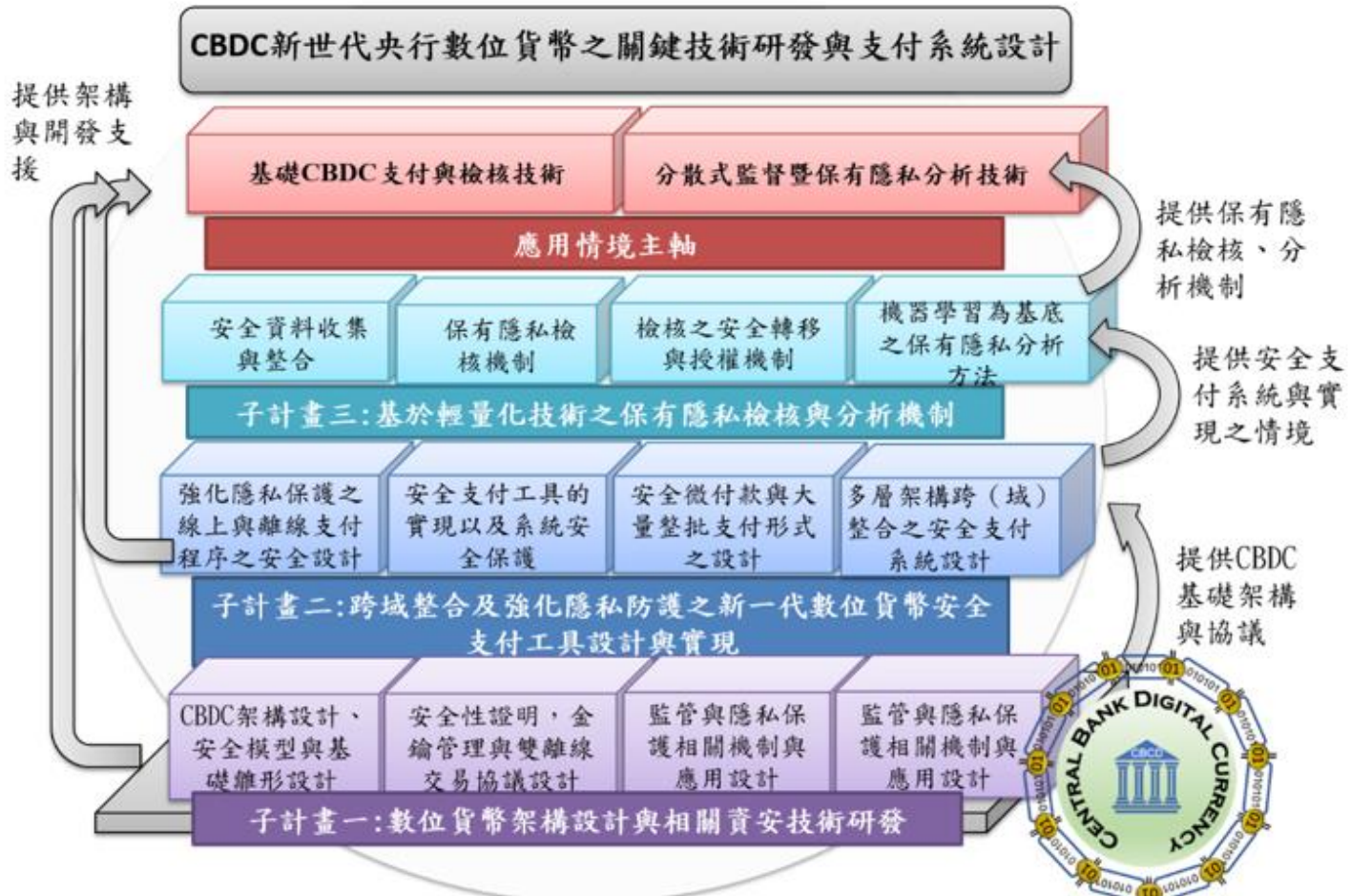
CBDC計畫簡介

總計畫：新世代央行數位貨幣之關鍵技術研發與支付系統設計

子計畫一	數位貨幣架構設計與相關資安技術研發
子計畫二	跨域整合及強化隱私防護之新一代數位貨幣安全支付工具設計與實現
子計畫三	基於輕量化技術之保有隱私檢測與分析機制

Our Project

- 新世代央行數位貨幣之關鍵技術研發與支付系統設計(1/2)
  110-2218-E-004 -001 -MBK



Current Disadvantages of SNB's CBDC

- Different key pairs required for different denominations
- No support for off-line transactions
- Inefficient exchange protocol
- Inefficient verification for large amount of digi cash
- Monitoring impossible

Our Solution – Partially Blind Signature

- Introduced by Abe in 2003
- An extension of blind signature schemes
  - allow a signer to explicitly include necessary information (denominations, expire date, etc.) in the resulting signatures under some agreement with the receiver
- Support one public key for different denominations

- *Hongxun Huang, Zi-Yuan Liu, Raylin Tso:* ***Partially Blind ECDSA Scheme and Its Application to Bitcoin.*** *DSC 2021: 1-8*

How to Express the Denominations

(pk1,sk1) for 1 NTD
Alice

(pk2,sk2) for 5 NTD
Bob

(pk3,sk3) for 10 NTD
Eve

How to Express the Denominations

(pk_{Alice}, sk_{Alice})

Partially blinded

Partially Blind ECDSA Signature

Partially Blind ECDSA

Signer

Denomination=10

User

$k_1, \alpha_1 \xleftarrow{\$} Z_q^*$

$K_1 = k_1 G$

$Z = H_1(10)$

K_1, A →

H_1 maps a string to elliptic curve point

$A = \alpha_1 Z$

Partially Blind ECDSA Signature

Partially Blind ECDSA

Signer

Denomination=10

User

$$k_2, \alpha_2 \xleftarrow{\$} Z_q^*, r_1, r_2 \xleftarrow{\$} Z_{N^2}^*$$

$$K = k_2 K_1 = (K_x, K_y)$$

$$t = K_x \bmod q$$

$$Z = H_1(10)$$

$$B = \alpha_2 Z$$

$$I = A + B = (\alpha_1 + \alpha_2)Z$$

$$C_1 = g^{H(m||I)} {r_1}^N \bmod N^2$$

$$C_2 = g^{t+\alpha_2} {r_2}^N \bmod N^2$$

C_1,C_2 with zero-knowledge proofs

Partially Blind ECDSA Signature

Partially Blind ECDSA

Signer

Denomination=10

User

C, α_1 →

$$s = {k_2}^{-1} Dec(C, (p, k)) \; mod \; q$$

$$R = \alpha_1 + \alpha_2 \; mod \; q$$

Signature $\sigma = (t, s, R)$

Partially Blind ECDSA Signature

Partially Blind ECDSA

User

Denomination=10

Verifier

$$I = RH_1(10)$$

H_1 maps a string to elliptic curve point

$$u = s^{-1}H(m||I) mod q$$

$$v = s^{-1}(t + R) mod q$$

$$(K_x', K_y') = uG + vQ$$

$$t' = K_x' \ mod \ q$$

Check whether $t' = t$.

$$m, 10, \sigma = (t, s, R) \longrightarrow$$

Current Disadvantages of SNB's CBDC

- Different key pairs required for different denominations
  - Our solution: Partially blind ECDSA signatures
- No support for off-line transactions
  - Our solution: Digi wallet supporting off-line transactions (embedded SE，TEE etc.)
- Inefficient exchange protocol
  - Our solution: under construction
- Inefficient verification for large amount of digi cash
  - Aggregate signature / batch verification
- Monitoring impossible
  - Our solution: secret sharing, DVS, etc.

Quantum secured CBDC

Conclusion

- 後疫情時代，零接觸經濟已是趨勢
- 數位貨幣發展成為主流
- 各國對央行數位貨幣之重視
- 介紹數位貨幣之發展與相關技術
- 隱私保護為數位貨幣發展的主要議題
- 對應之密碼技術漸受重視，以用來解決上述議題