

# FTEC 5520 (Week 2 - 3)

---

# Agenda -

## Application of Cryptographic Tools and Digital Currency

### Week 1 - 2

1. Payment, Currency, Money

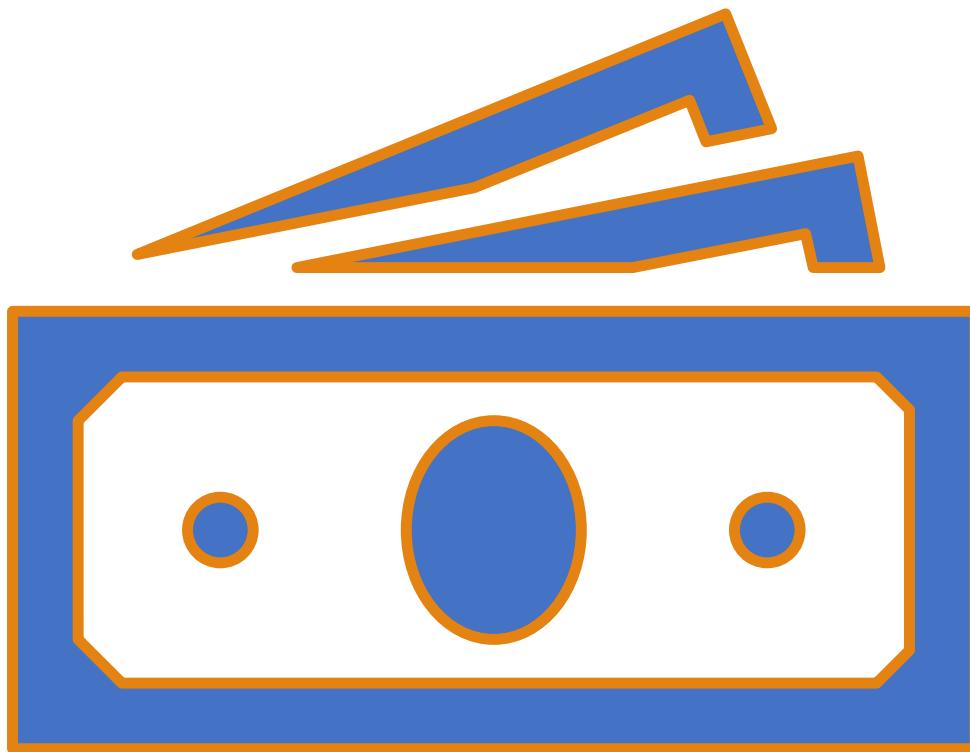
2. Role of Payment Systems

3. Digital Currency and Cryptocurrency

4. Trust, Anonymity (What is Privacy and  
Anonymity)

5. Cryptocurrencies in Hong Kong

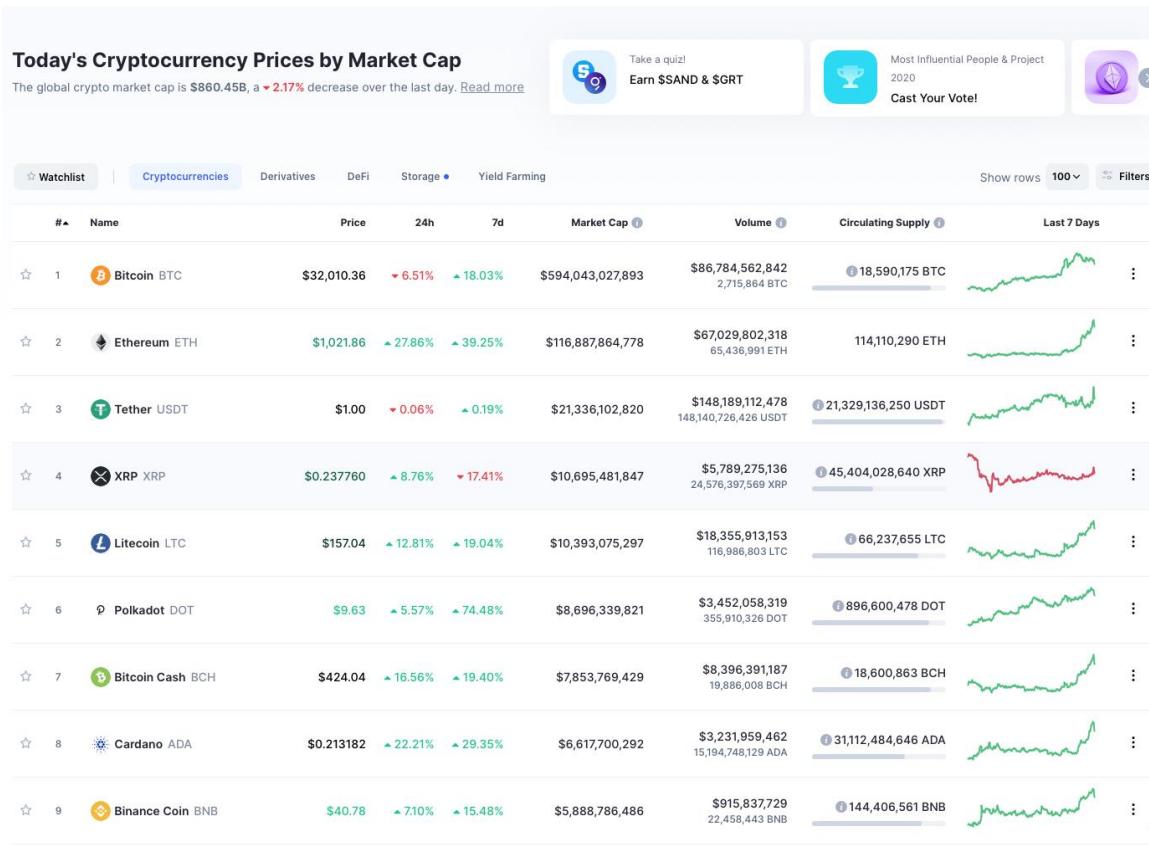
6. Latest update of Cryptocurrencies



Currency, Digital  
Currency, Virtual  
Currency  
CryptoCurrency

---

# Cryptocurrency (4 Jan 2021)



Bitcoin rose more than 290% from the previous year, and 43% last December alone, which made it its best month since May 2019.

The potential of this cryptocurrency has generated quick profits and the same expectations for the possibility of becoming a conventional payment method have obtained the demand of investors.

In 2020, the rise of Bitcoin is **driven by institutional investment**. Large hedge funds and publicly traded companies are driving this bull cycle and they don't present the same reputational drawbacks that retail investors do.

# Cryptocurrency (22 Jan 2022)

加密貨幣市場接連下跌 市值蒸發超過1萬億美元



Vildana Hajric

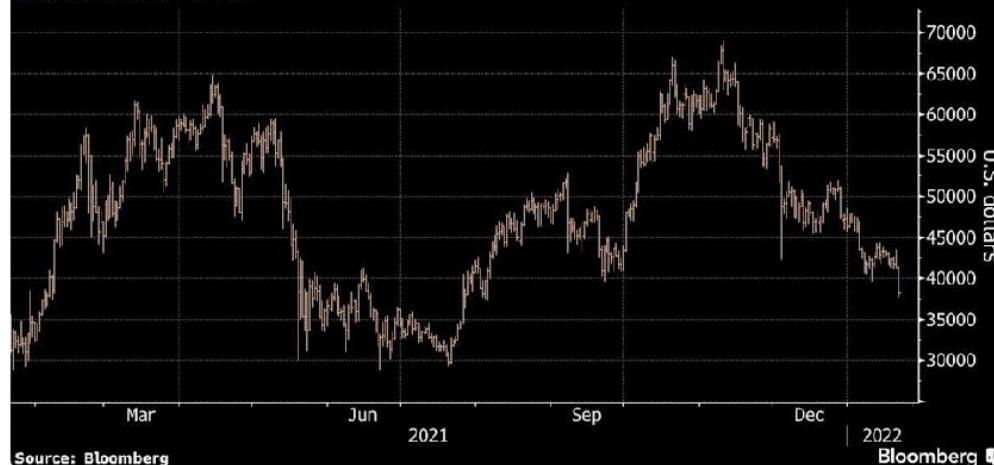
2022年1月22日 週六 下午2:04 · 2分鐘文章



## Red Notice

**Bitcoin plunge wipes out billions in a jiffy**

■ XBT-USD Cross Rate - Last Price



## Crypto meltdown erases \$1 trillion in value

*Bitcoin down 50% from November peak as risk-off sentiment batters cryptocurrencies*

PUBLISHED : 22 JAN 2022 AT 19:00

WRITER: BLOOMBERG NEWS



# Where and how can you use Cryptocurrencies

Treasury & Capital Markets

## Pricerite becomes first HK retail chain to accept cryptocurrencies as payment

Home furnishing chain will accept cryptocurrencies including Bitcoin, Ethereum and Litecoin, and will accept more in due course

30 Aug 2019 | The Asset

Hong Kong home-furnishing chain Pricerite has become the first local retail chain to accept cryptocurrencies as payment across all of its stores. The innovation “providing consumers with added payment convenience” is in partnership with Weever FinTech, the crypto brokerage of CASH Financial Services Group (CFSG), and QFPay, a major mobile payment technology.

Powered by Weever FinTech’s crypto-settlement service and QFPay’s payment technology, Pricerite is accepting Hong Kong dollar-equivalent payments in cryptocurrencies including Bitcoin (BTC), Ethereum (ETH) and Litecoin (LTC) – with more “high-ranked, high-liquidity” cryptocurrencies to be accepted in due course. In addition to offering crypto payment solutions, QFPay provides Pricerite with other e-wallet acceptance functions to satisfy the evolving needs of different customers.

Pricerite CEO James Leung says, “This partnership with Weever FinTech and QFPay breaks new ground in Hong Kong’s retail industry.”

### Bitcoin ATMs

The most convenient way to buy Bitcoin is an ATM. Usually you only need to show the ATM the QR code of your Bitcoin address, insert bank notes and confirm the exchange rate. The process takes less than 30 seconds, is anonymous but can cost up to 8% in fees. Prepare your wallet ahead of time, and bring exact change. ATMs generally accept only HKD bank notes, some insist on the first note being of HKD 500 denomination or above.

Bitcoin ATMs are located at:

#### Kowloon

**Prudential Hotel**, The Lobby, 222 Nathan Road, **Jordan**  
**Bitwork**, Unit 01-04, 7/F, FTLife Tower, No. 18 Sheung Yuet Road, **Kowloon Bay**  
**Pricerite**, MegaBox L5, 38 Wang Chiu Road, **Kowloon Bay**  
**Tencent WeStart**, 6/F, KOHO, 75 Hung To Road, **Kwun Tong**  
**FunTower**, 29/F, 35 Hung To Road, **Kwun Tong**  
**S Tattoo Studio**, 1/F, Reclamation Street 470F, **Mong Kok**  
**196 Portland Street**, G/F, 196 Portland Street, **Mong Kok**  
**Sin Tat Plaza**, S32, 2/F, 83 Argyle Street, **Mong Kok**  
**Sin Tat Plaza**, St5, 1/F, 83 Argyle Street, **Mong Kok**  
**President Commercial Centre**, Shop 322, 3/F, 608 Nathan Road, **Mong Kok**  
**Presidental Commercial Centre**, W Plaza, CHIC之堡, Shop 113, 602-608 , Nathan Road, **Mong Kok**  
**Sino Centre**, 19/F, 582-592 Nathan Road, **Mong Kok**  
**Ho King Commercial Centre**, Shop 30, 1/F, 2-6 Fa Yuen Street, **Mong Kok**  
**Bo Yan Building**, G/F, 1 Horse Shoe Lane, **Ngau Tau Kok**  
**Golden Luzon Agency**, G/F, 15 Tit Shu Street, **Tai Kok Tsui**  
**Metro Sham Shui 謩之都**, Shop 038, 3/F, Kam Wah Mansion, 226-242 Cheung Sha Wan Rd, **Sham Shui Po**  
**Metro Sham Shui 謩之都**, Shop 160, 2/F, Kam Wah Mansion, 226-242 Cheung Sha Wan Road, **Sham Shui Po**  
**Metro Sham Shui 謩之都**, Shop 25, 2/F, Kam Wah Mansion, 226-242 Cheung Sha Wan Road, **Sham Shui Po**  
**New Capital Computer Centre**, Shop 117, 85-95 Un Chau Street, **Sham Shui Po**  
**Little School**, Shop 206, 2/F, Mira Place, 132 Nathan Road, **Tsim Sha Tsui**  
**Color Rich**, 35A Kimberley Road, **Tsim Sha Tsui**  
**Solo Building**, Shop 1216, 12/F, 41-43 Carnarvon Road, **Tsim Sha Tsui**  
**Cke Mall**, Shop 290, 36 Chungking Mansions, **Tsim Sha Tsui**  
**Hotel Hart**, 4/F, 4 Hart Ave, **Tsim Sha Tsui**  
**Nathan Hotel**, 387 Nathan Road, Starbucks Coffee, **Yau Ma Tei**

#### Hong Kong

DATA: CANTON MONEY OR ABERDEEN STREET WEBSITE. IMAGE: C/S E BANK HONG KONG

# 【虛擬貨幣的新窗口】ETF 再挑戰美國發行

2020 年比特幣以及虛擬貨幣可算是特別的一年，幾年前首次代幣發行 (ICO) 的爆破，接踵而來的是去中心化金融 (Defi) 的興起，而上年美國上市公司微策略 (MicroStrategy) 大手買入比特幣，持倉量超越美國政府，投資總額超過 10 億，MicroStrategy 的股價亦一飛沖天。大勢所趨，虛擬貨幣以比特幣為首已經成為資產類別一部分，很多家庭基金以及機構投資者已經開始及計劃配置資產於虛擬貨幣上。但可惜的是，虛擬貨幣對於這些機構投資者而言，是一樣比較新的東西，要確立虛擬貨幣本身的擁有權，對於機構投資者已經是的一大難題，所以對著這些虛擬貨幣，好多機構投資者都是有心無力。退而求其次，這些投資者會選擇買如 MicroStrategy 這樣的概念公司或相關挖礦的公司。

市場上都有投資虛擬貨幣相關的衍生產品，例如是芝加哥商業交易所上市的比特幣期貨，但對於一般大眾投資者而言，期貨是小眾的活動，所以都是以專業投資者為主。一般大眾投資者選擇的是購買 Grayscale 的虛擬貨幣信託基金，道理就是你買信託基金的單位，而信託基金就代你買相對的虛擬貨幣。這些信託基金對大眾參與虛擬貨幣市場，是一個極大的幫助，只要你有證券戶口就可以作買賣，不需要開設虛擬貨幣戶口，不需要解決重新入金的問題。

但是信託基金最大的問題就是基金架構，因為監管問題美國證監會未有批准成立 ETF (指數基金)型的基金形式，今天 Grayscale 用的還是信託基金形式。ETF 形式是開放的，亦即是基金份額可以隨投資者多少而增加減少，相反信託基金形式是封閉的，今天投資者對虛擬貨幣投資需求上升，可惜信託基金形式的份額不可隨時增加，大眾搶基金份額，造成的結果就是基金價格高於基金下面持有的資產價格。

可笑的是今天機構投資者用盡不同方法增持虛擬貨幣，由於美國證監會未允許虛擬貨幣 ETF，大眾散戶投資者只可以通過信託基金形式這樣的一個低效工具去投資虛擬貨幣，而定價亦是明顯錯誤的，大眾散戶面臨錯價的風險，但富豪、對沖基金和私募基金等認可投資者擁有專業投資者的優勢。

美國前證監會主席 Jay Clayton 上個月離開證監會，而全球最大 ETF 公司 VanEck Associates Corp. 再次入表申請發行虛擬貨幣 ETF，新人事又是否會有新作風？這個是市場期待的，虛擬貨幣 ETF 的成立不只是代表一個產品的成立，而這將會是開放虛擬貨幣給予世界有證券戶口投資者的一個窗口。

# Currency or Traditional Currency

A currency (from Middle English: **curraunt**, "in circulation", from Latin: *currens*, -*entis*), in the most specific use of the word, **refers to money** in any form when in actual use or circulation as a medium of exchange, especially circulating banknotes and coins

Currencies can be classified into two monetary systems:

- fiat money and commodity money, depending on what guarantees the value (the economy at large vs. the government's physical metal reserves)

## Cash

- cash is current assets comprising currency or currency equivalents that can be accessed immediately or near-immediately



Fiat money is the physical money (coins and paper money)

# Types of Money (Another interpretation)

Fiduciary money (fiat money, legal tender)

- Issued by a central bank
- Has real discharging power (to discharge debts)
- Cannot be refused

Scriptural money (not legal tender)

- Not issued by a central bank
- E.g. bank accounts, traveler's cheques, gift certificates, Octopus
- Discharging power based on trust in issuer
- Can be refused

	Token	Notational	Hybrid
Fiduciary	<ul style="list-style-type: none"><li>• Cash</li><li>• Government bearer bond</li></ul>	<ul style="list-style-type: none"><li>• Account with central bank</li></ul>	<ul style="list-style-type: none"><li>• Government check</li></ul>
Scriptural	<ul style="list-style-type: none"><li>• Certified check</li><li>• Traveler's check</li></ul>	<ul style="list-style-type: none"><li>• Bank account</li><li>• Frequent flyer miles</li></ul>	<ul style="list-style-type: none"><li>• Personal check</li><li>• Gift certificate</li></ul>

# Monetary system

---

A monetary system is a system by which a government provides money in a country's economy.

Modern monetary systems usually consist of the national treasury, the mint, the central banks and commercial banks

## Commodity money system

- A commodity money system is a monetary system in which a commodity such as gold or seashells is made the unit of value and physically used as money.
- The money retains its value because of its physical properties.
- Media of exchange include gold, silver, copper, salt, peppercorns, tea, decorated belts, shells, alcohol, cigarettes, silk, candy, nails, cocoa beans, cowries and barley.



## Commodity-backed money (Representative Money)

- Many currencies have consisted of bank-issued notes which have no inherent physical value, but which may be exchanged for a precious metal, such as **gold standard (gold certificate)**
- The **silver standard (silver certificate)** was widespread after the fall of the Byzantine Empire, and lasted until 1935, when it was abandoned by China.

## Fiat money

- The alternative to a commodity money system is fiat money which is defined by a central bank and government law as legal tender even if it has no intrinsic value.
- Originally fiat money was paper currency or base metal coinage, but in modern economies it mainly exists as data such as bank balances and records of credit or debit card purchases, and the fraction that exists as notes and coins is relatively small

# Monetary system (Money Supply in the US)

---

M1 = coin and currency in circulation plus checking accounts

- Coin
- Currency
- Demand Deposits
- Travelers Cheques

M2 = M1 plus short-term liquid assets

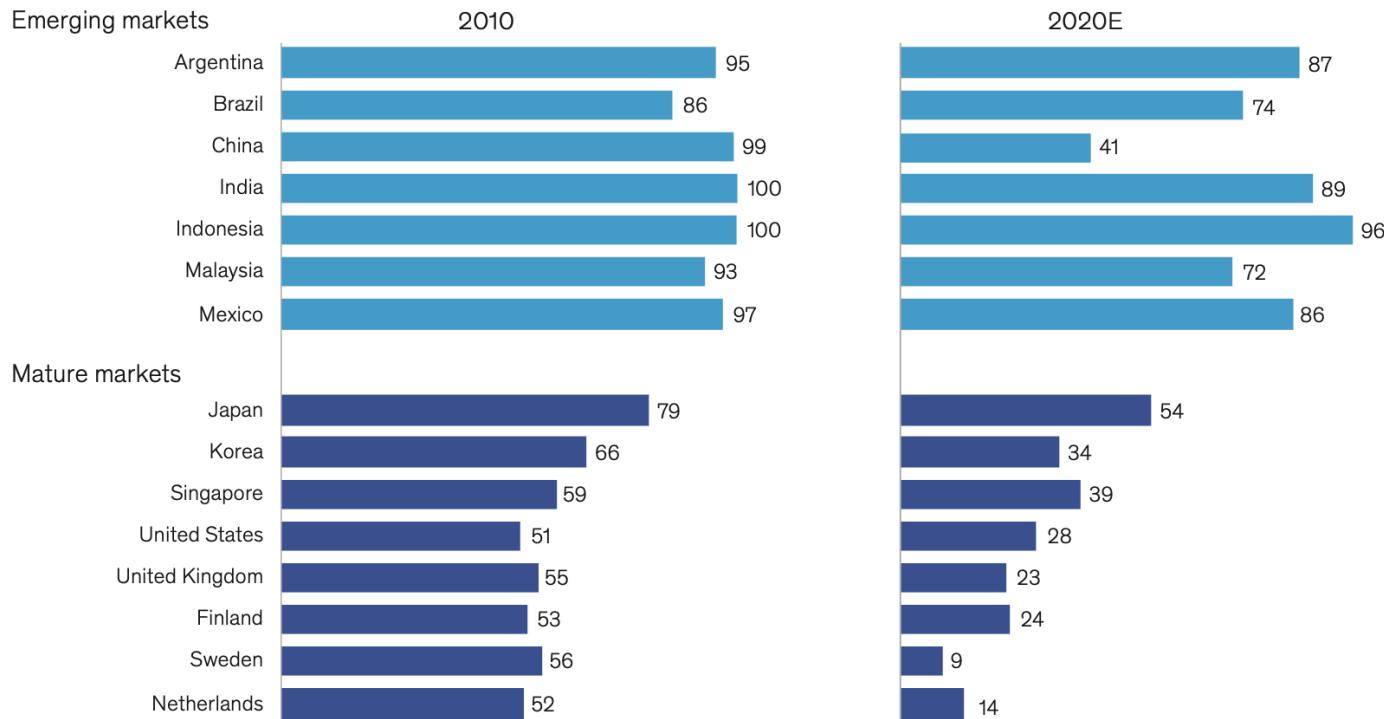
- Saving Deposits
- Time Deposits
- Certain CDs
- Money Market Deposit Accounts
- Money Market Mutual Funds
- + M1

# Currency vs Cryptocurrency

TRADITIONALS	CRYPTOCURRENCIES
Exchange of money to acquire something of value	Value is exchanged in the form of cryptocurrencies
They are physical	They are virtual
Its core is located in a specific country or group of countries	They are global
Central Banks and financial reserves control them	They are controlled by all users and blockchain technology
Become part of the economic system through bonds	Become part of the market directly
Great inflation and interest rate influence	Supply/Demand is the only influence
Issued by governments	Decentralized and depending on the cryptocurrencies organization
Value transfers are very slow and bureaucratized	Peer-to-peer payments are made instantaneously without intermediaries
Commission costs	Costs come from software maintenance
Not every person in the world has the power to have a bank account	They can be used by the whole society, including those parts of the population without access to financial resources

# Cash usage in post Covid-19

---



---

Source: McKinsey Global Payments Map

2020-mckinsey-global-payments-report-vf.pdf

## E-Krona – electronic form of money

---

Project in the spring of 2017 to examine the scope for the **Riksbank** to issue a central bank digital currency (CBDC), a so-called **e-krona**.

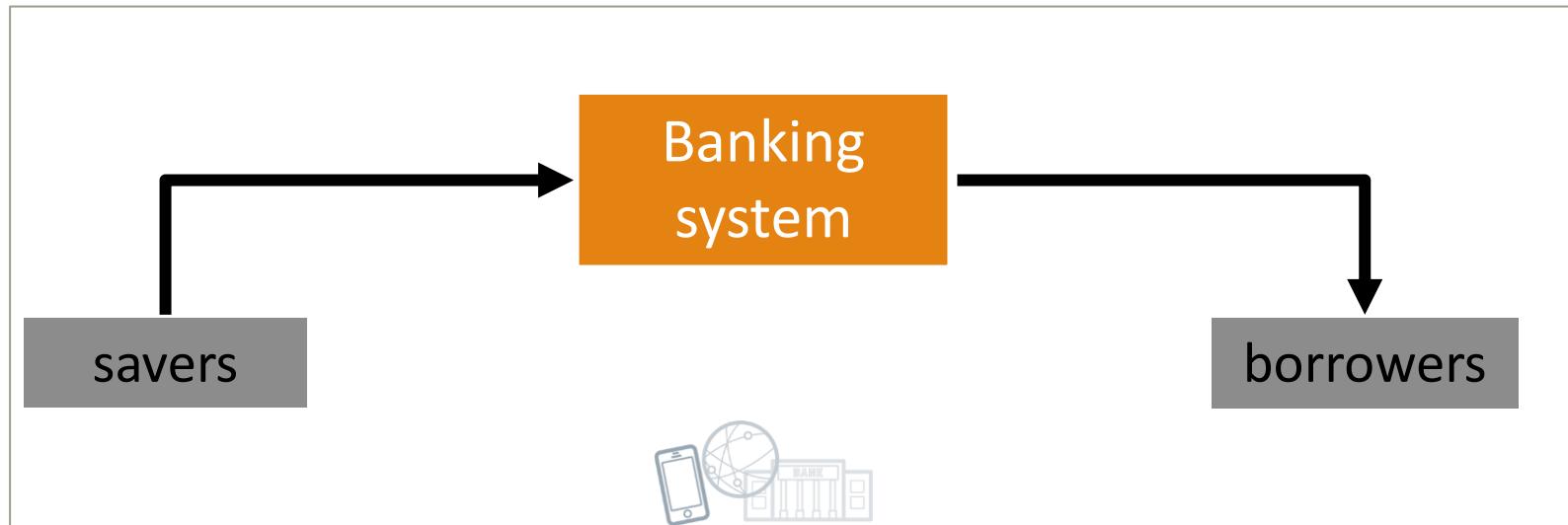
The Riksbank has therefore submitted a proposal to the Riksdag (the Swedish Parliament) that the need for an e-krona should be investigated by a group of experts in different areas, see: The Riksbank proposes a review of the concept of legal tender.

The Riksdag (the Swedish Parliament) agrees with the Riksbank that an inquiry is needed, read more on the Riksdag's website (in Swedish only).

# Economic role of banks

Banks perform the economic role of a financial intermediary.

Handle deposit



# Hong Kong Monetary Authority

---



**HKMA** formed in 1993 with merger of Exchange Fund and Commissioner of Banking to perform role of the central bank.

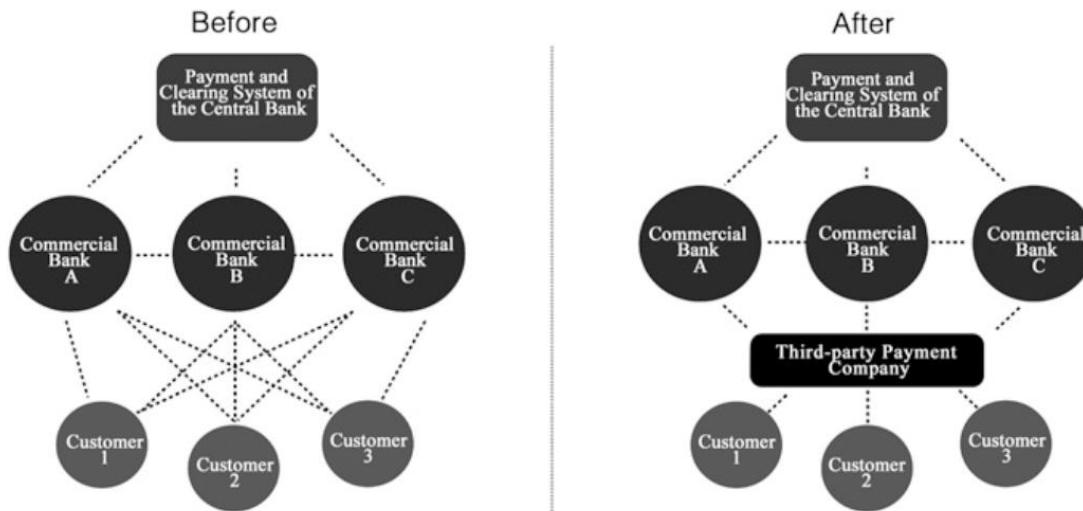
Prior to 1988, interbank settlement done on the books of HSBC

- These 10 out of 170 banks, in turn, settled with Hongkong Bank, which then settled with the HKMA in a one-to-one basis.
- Hongkong Bank acted as the clearing house under this system, settling payments across its books in a net basis on the day following the transactions.

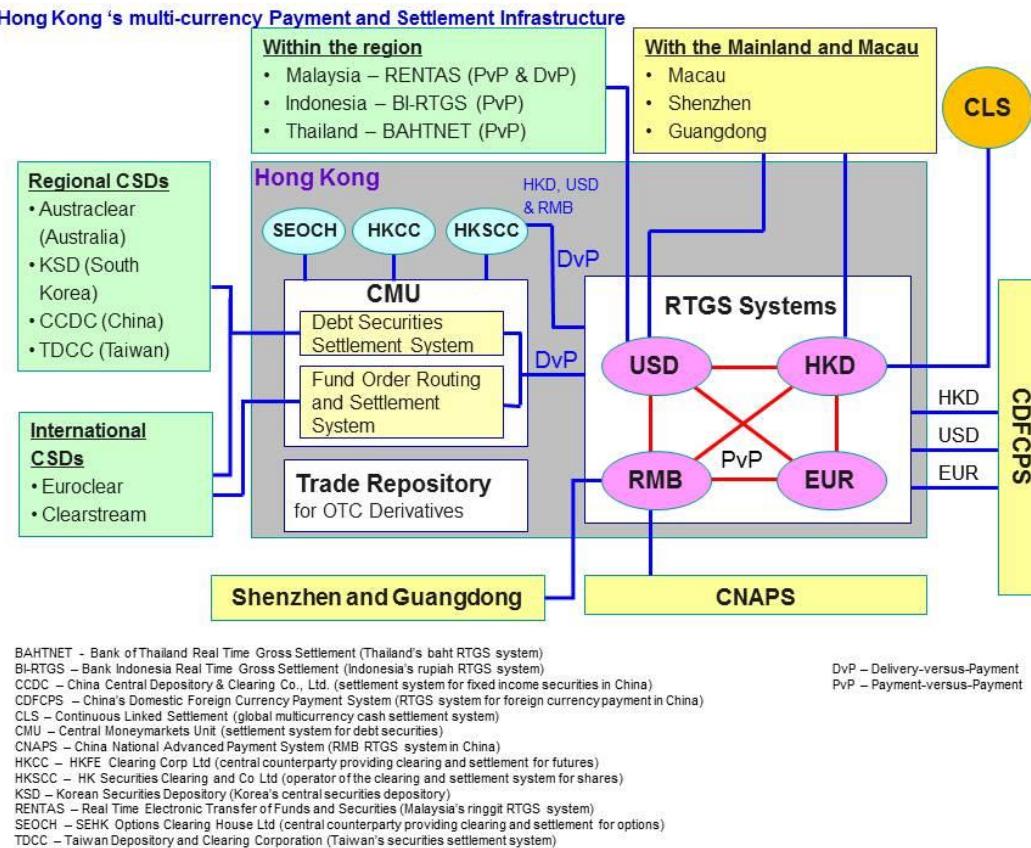
# Role of Payment Systems

A system for payment card transactions:

- Provide confidential transmission.
- Authenticate parties involved.
- Ensure integrity of payment instructions for goods and services order data.
- Ensure integrity of payment authorization provided by payment gateway.



# Overview of Hong Kong's multi-currency Payment and Settlement infrastructure





---

The Society for Worldwide Interbank Financial Telecommunication (SWIFT), legally S.W.I.F.T. SC, is a Belgian cooperative society providing services related to the execution of financial transactions and payments between banks worldwide.

The SWIFT messaging network is a component of the global payments system.

SWIFT acts as a carrier of the messages containing the payment instructions between financial institutions involved in a transaction.

SWIFT was founded in Brussels on 3 May 1973 under the leadership of its inaugural CEO, Carl Reuterskiöld (1973–1989), and was supported by 239 banks in 15 countries. The SWIFT secure messaging network is run from three data centers, located in the United States, the Netherlands, and Switzerland.

Alternatives to the SWIFT system include:

- CIPS – sponsored by China, for trade-related deals in the Chinese currency with Chinese clearing banks
- SFMS - sponsored by India
- SPFS – sponsored by Russia, mostly composed of Russian banks
- INSTEX – sponsored by the European Union, limited to non-USD transactions for trade with Iran, largely unused and ineffective

Swift data showed that the Chinese yuan accounted for 3.2 per cent of global payments in January, far below the US dollar, which accounted for 39.92 per cent of settlements, the euro on 36.56 per cent and the British pound at 6.3 per cent.

CIPS



---

The Cross-Border Interbank Payment System (CIPS) is a payment system which offers clearing and settlement services for its participants in cross-border RMB payments and trade. It is a significant financial market infrastructure in China. CIPS is sometimes referred to as the China Interbank Payment System.

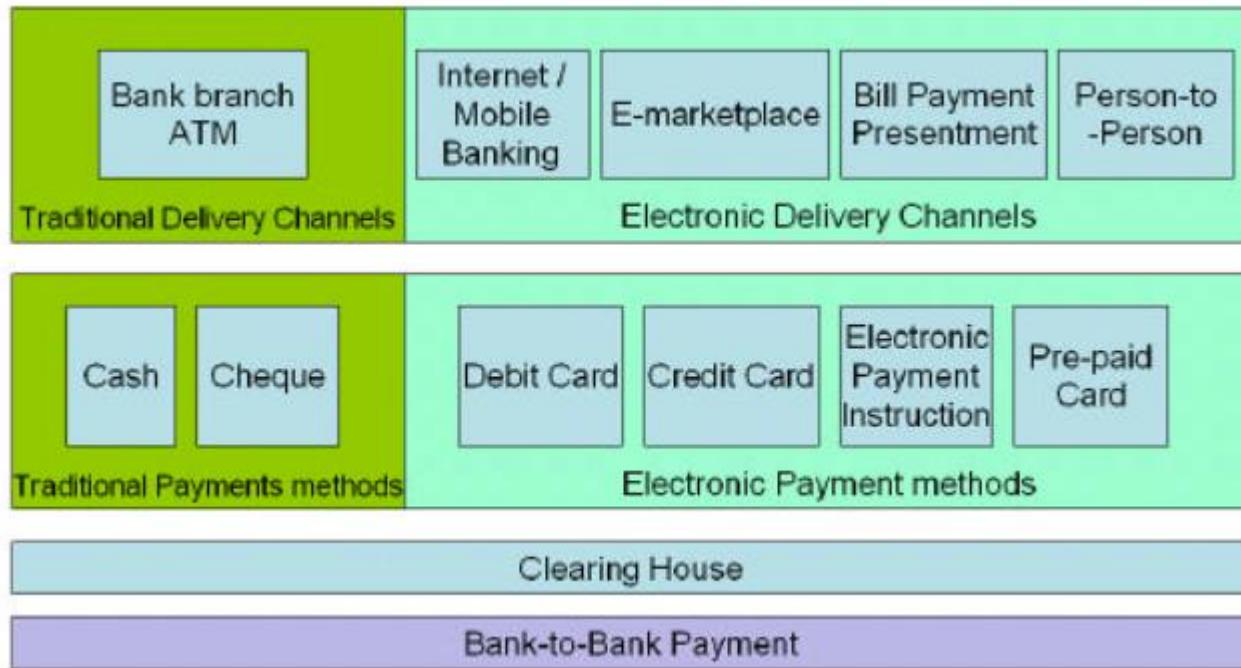
On 8 October 2015, the first batch of direct participants included 19 Chinese and foreign banks which were set up in mainland China, and 176 indirect participants which cover 6 continents and 47 countries and regions.

On 25 March 2016, CIPS signed an MoU with SWIFT with mutual understanding of deploying SWIFT as a secure, efficient and reliable communication channel for CIPS's connection with SWIFT's members, which would provide a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardised and reliable environment.

CIPS would **not facilitate funds transfer**; rather, it **sends payment orders**, which must be settled by correspondent accounts that the institutions have with each other.

CIPS uses the SWIFT industry standard for syntax in financial messages. Messages formatted to SWIFT standards can be read and processed by many well-known financial processing systems, whether or not the message traveled over the SWIFT network.

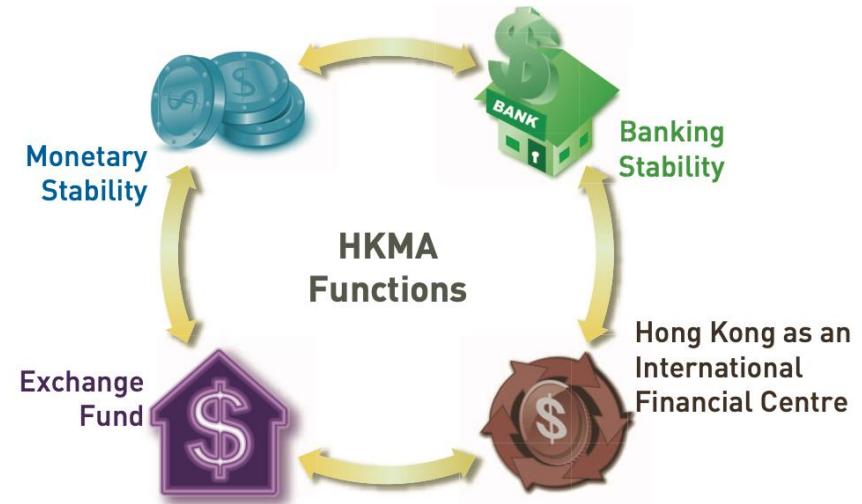
# A typical Payment System



# Central Banking Goals

## Functions of the Central Bank

- Provide reserves
- Issuance and circulation of legal tender notes and coins
- Regulate and supervise banking system
- Manage foreign exchange reserves
- Conduct Government Bond Auctions

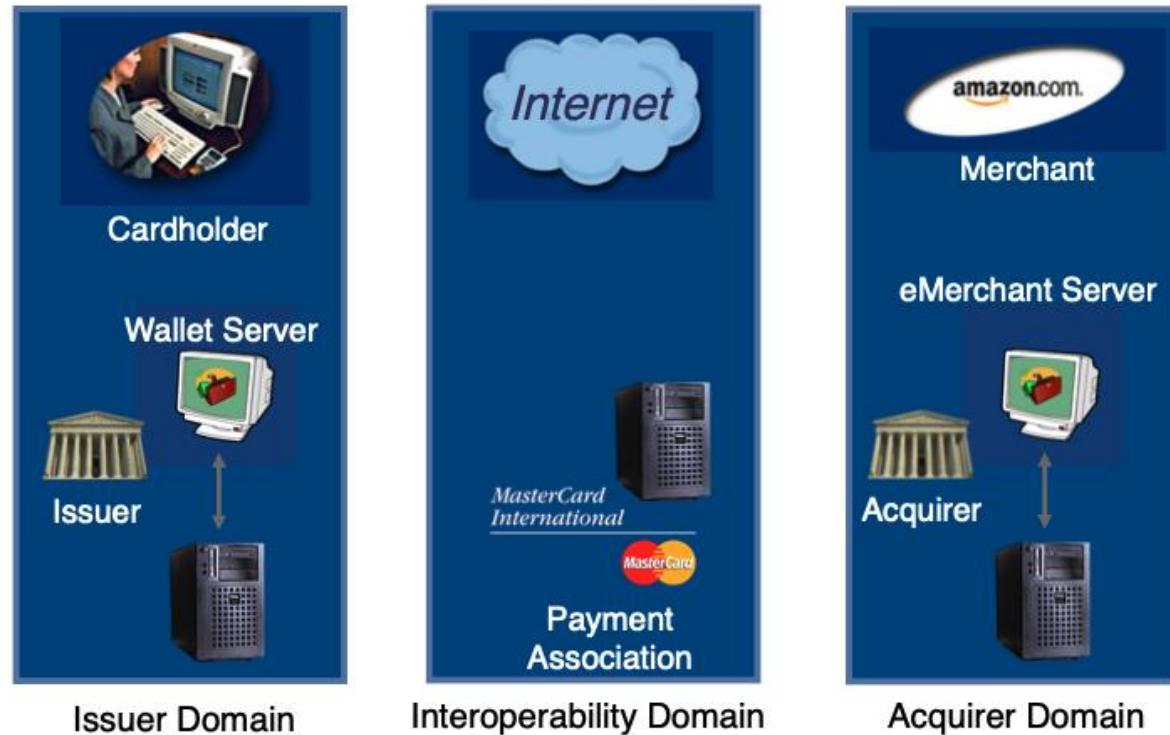


# 3-Domain (3-D) Secure for Credit Card payment

Authenticate user without a certificate

Challenge provided by Issuing Bank

- Such as One-Time-Password (OTP) from via a separate channel (e.g. SMS)

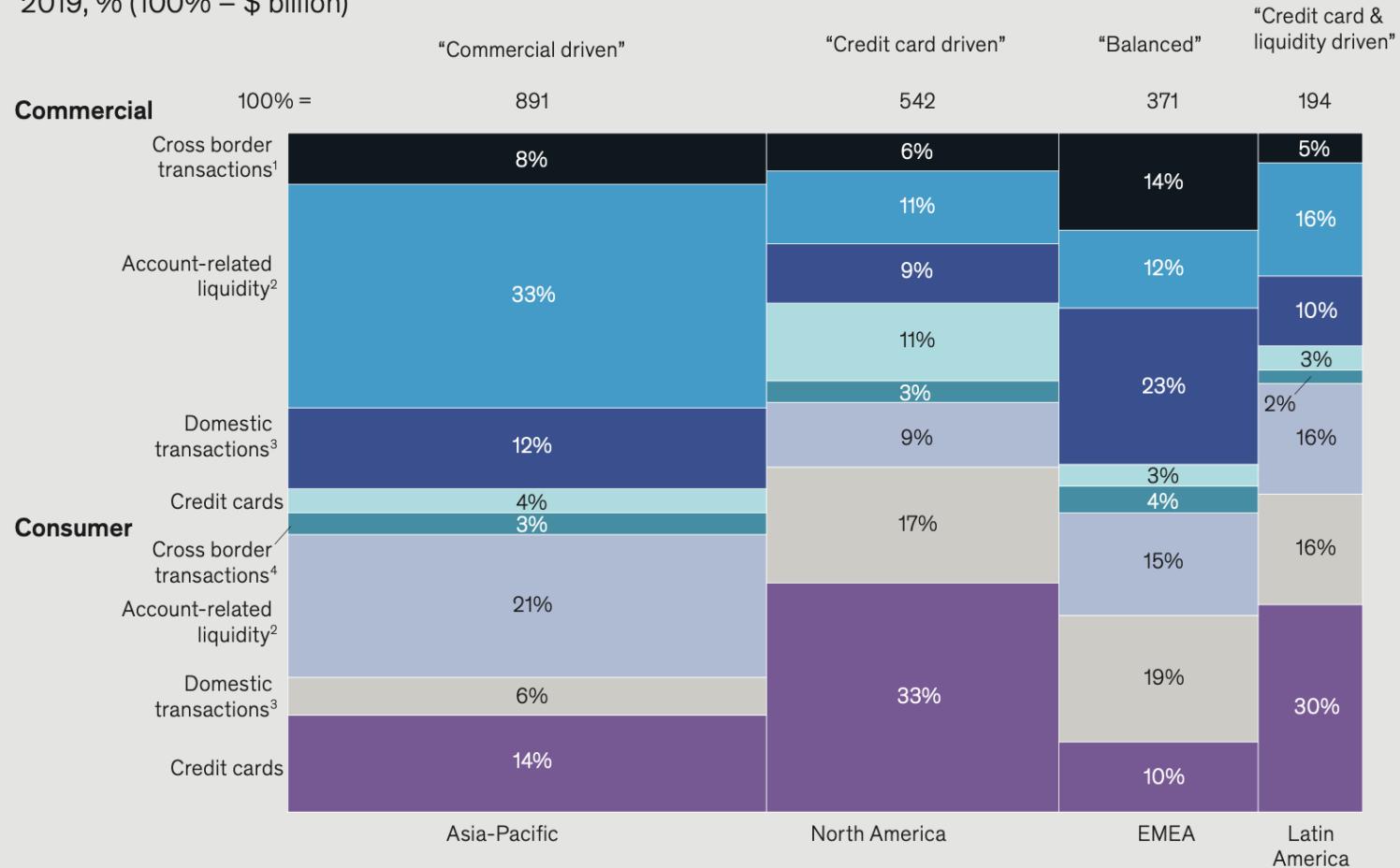


# Global Payments revenue pool (2019)

**Asia-Pacific continued to dominate the global payments revenue pool.**

## Payments revenue,

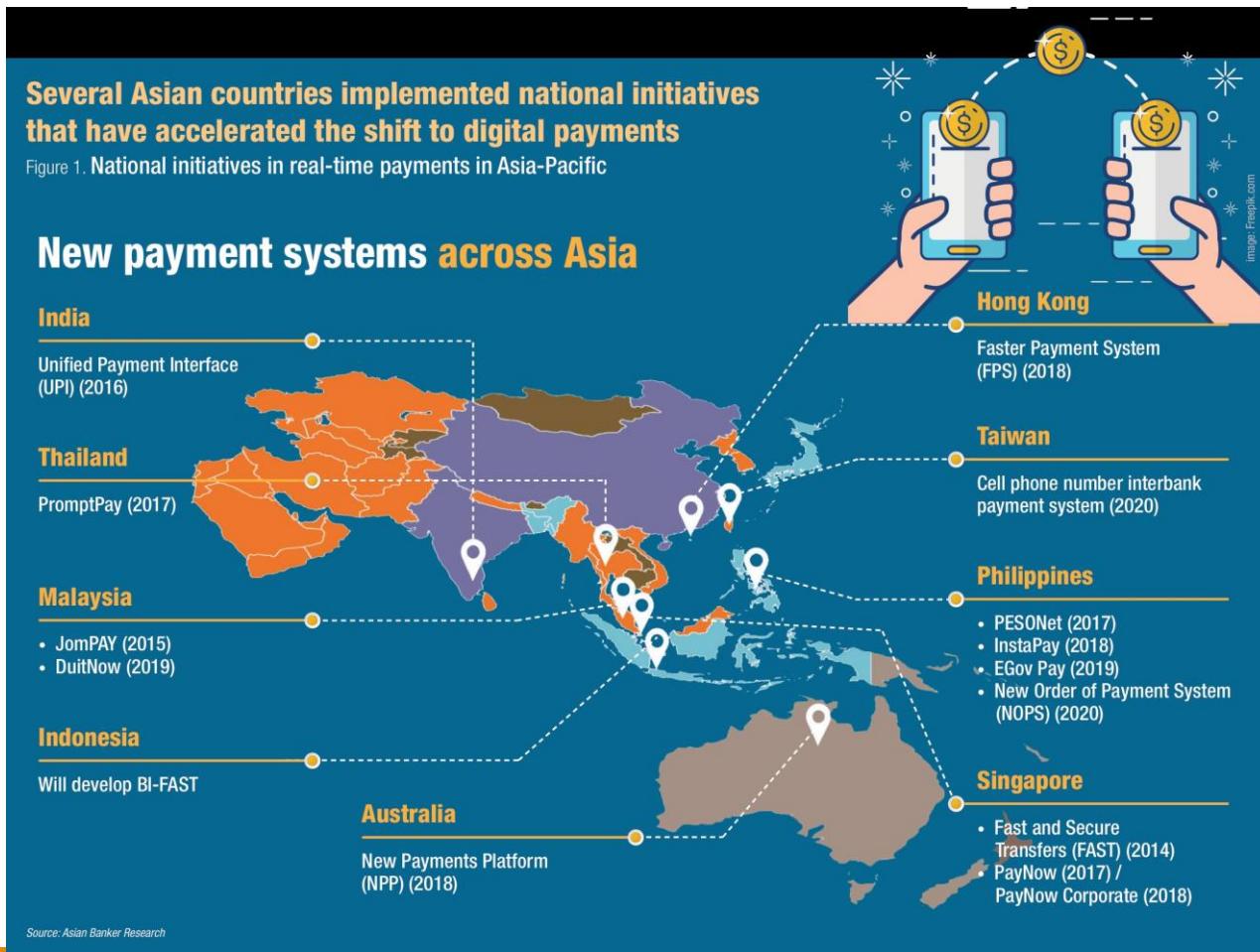
2019, % (100% = \$ billion)



# Digital Currency and Digital Payment System

---

# New Payment Systems Across Asia (2021)



# E-Payment

---



Octopus card



NFC Payment



E-Cheque



Peer-to-peer  
payment



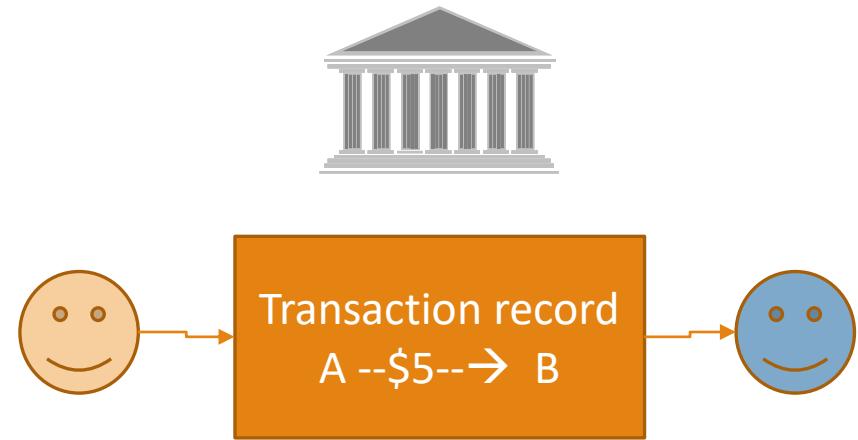
Bitcoin

# Virtual Bank and Payment Transaction

---

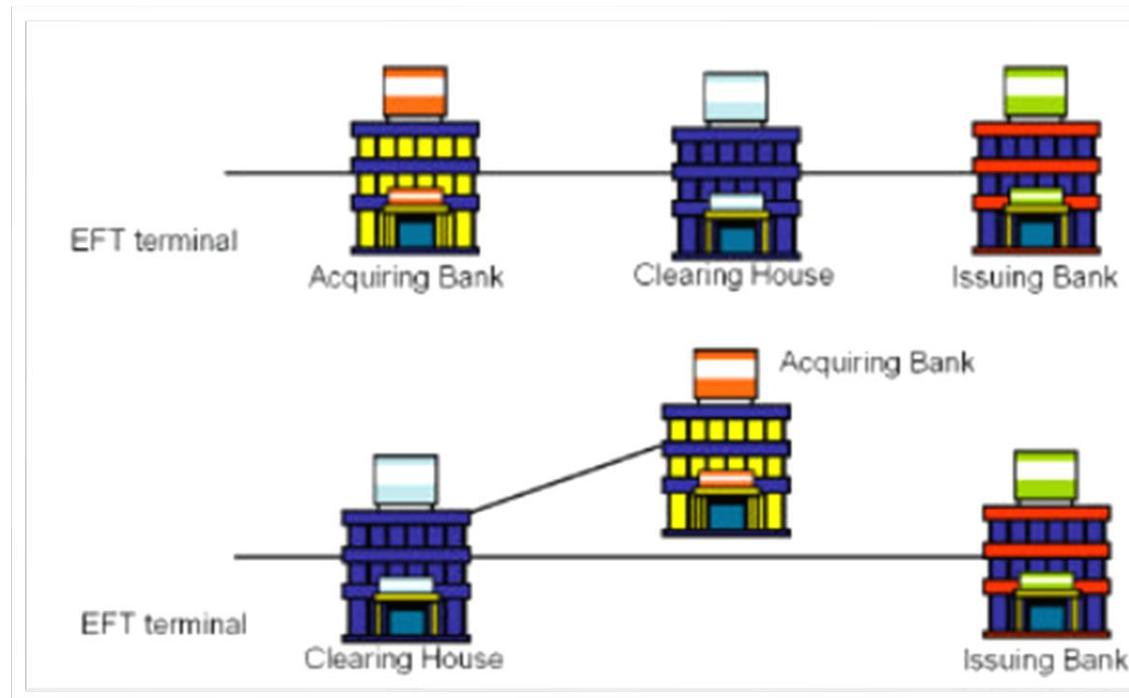
Provide banking and related services online without actual physical branch

- Pay bills online
- Check account details
- Secure loans
- Withdraw and deposit money
- Use of magnetic ink character recognition code
- Electronic fund transfer scheme
- RTGS
- ...

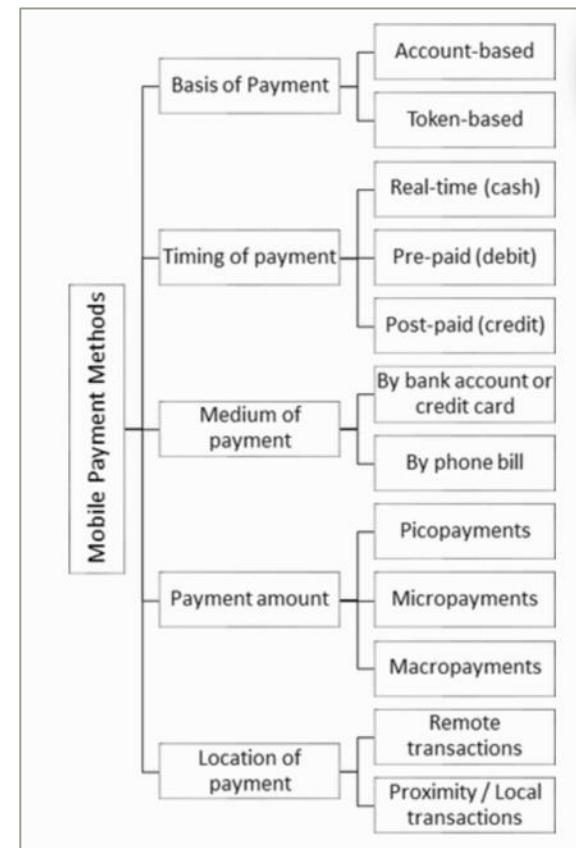
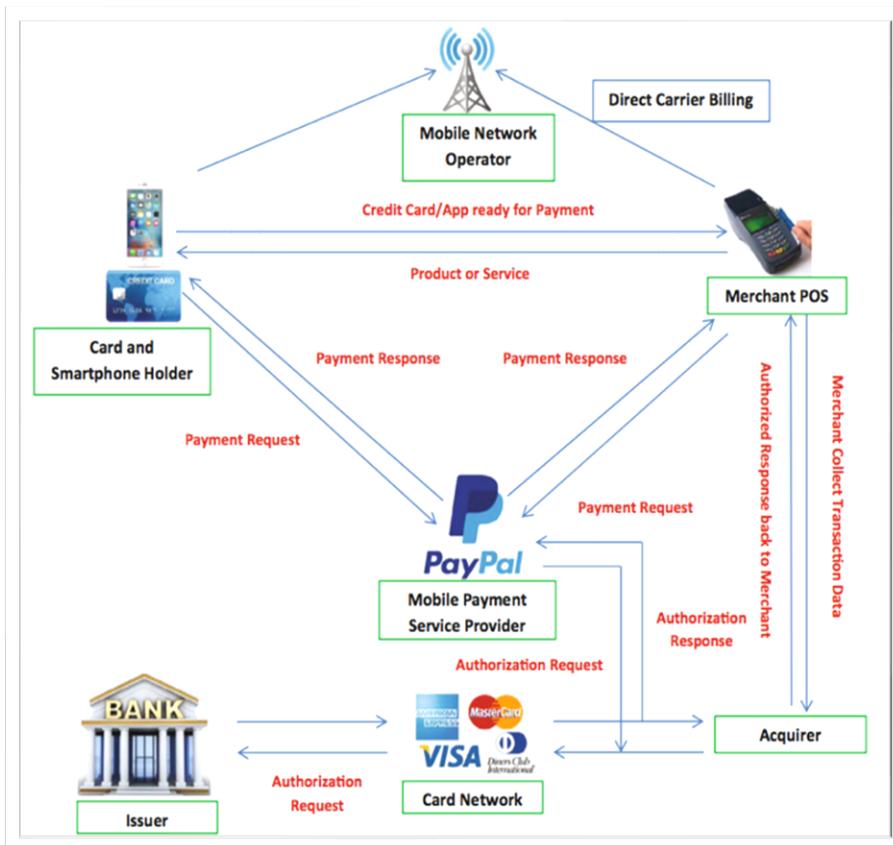


Accuracy, Integrity, Security, Privacy

# Electronic Funds Transfer (EFT)



# Mobile Payment Process



Types of Mobile Payment Methods

# Store Value Facilities

**港電子錢包開戰 百批5家獲牌**

TNG增五千零售點 港幣支付寶10月推



**首批5家獲發牌儲值支付工具營運商**

持牌人現時運作範疇	Alipay Financial Services (支付寶錢包)	TNG (Asia) (TNG 電子錢包)	八達通卡有限公司 (八達通卡、好易屏)	HKT Payment (Tap & Go 拍住賞)	財富數據 (WeChat Pay)
	線上支付	✓	✓	✓	✓
P2P轉帳	✗	✓	✓	✓	✗
實體卡	✗	✗	✓	✓	✗

**營運商反應**

未來策略	10月推出港幣支付寶，可用港元支付淘寶購物免手續費。	會增加1500個零售點，包括大型連鎖飲食店，支援TNG錢包。	未來會增加優惠及加強服務，好易屏賬戶將會分離。	短期內推出一系列新功能，進一步提升Tap & Go拍住賞的流動付款服務，讓全港市民透過WeChat
------	----------------------------	--------------------------------	-------------------------	---

**13家儲值支付工具(SVF)牌照持牌人**

SVF持牌人	現時運作範疇			
	線上支付	銷售點/流動支付	P2P轉帳	實體卡
1. 支付寶	✓			
2. 拍住賞	✓	✓	✓	✓
3. 微信錢包	✓	✓	✓	
4. TNG	✓		✓	
5. 八達通	✓	✓	✓	✓
6. 快易通有限公司	✓	✓	✓	
7. PayPal Hong Kong Limited	✓	✓		✓
8. Optal Asia Limited				
9. 三三金融服務有限公司				
10. UniCard Solution Limited				
11. 易票聯支付技術有限公司				
12. 通匯（香港）投資諮詢有限公司				
13. 僑達國際有限公司				

**以下為獲批出SVF牌照的預付卡**

- 3. Optal Asia Limited
- 9. 三三金融服務有限公司
- 10. UniCard Solution Limited
- 11. 易票聯支付技術有限公司
- 12. 通匯（香港）投資諮詢有限公司
- 13. 僑達國際有限公司

# Store Value Facilities



**香港流動支付大混戰**

涉及儲值功能  
要申請SVF牌

**手機綜合錢包**

TNG Tap&Go 支付寶 ALIPAY  
微信支付 OCTOPUS

部分功能：  
• 網上支付  
• 實體店支付  
• 個人對個人(P2P)轉帳  
• 配合實體卡使用

不需申請SVF牌

**手機轉帳**

JetPay 中國銀行 BANK OF CHINA HSBC  
HSBC

• 用戶可使用P2P過數  
• 不涉及現金儲存功能

**手機支付** Apple Pay

• 直接把信用卡資料加密後傳送至商戶  
• 不涉及現金儲存功能

# Faster Payment System at a glance



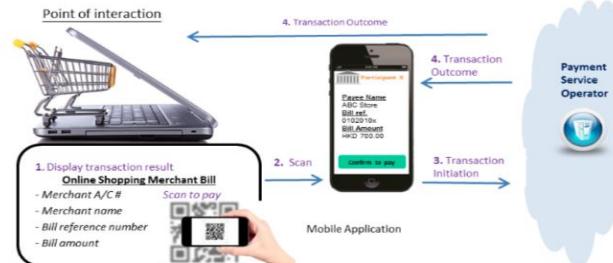
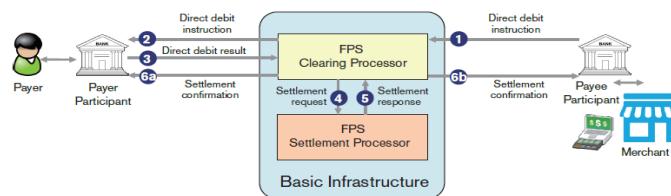
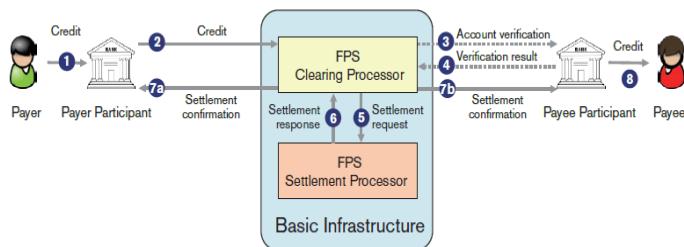
With **FPS**, consumers can now make or receive instant payments to or from individuals, merchants or businesses through a registered mobile phone number, an e-mail address or a QR code.

**FPS** is operated by the Hong Kong Interbank Clearing Limited.

Majority of retail banks and e-wallet operators have participated to provide instant payment service.

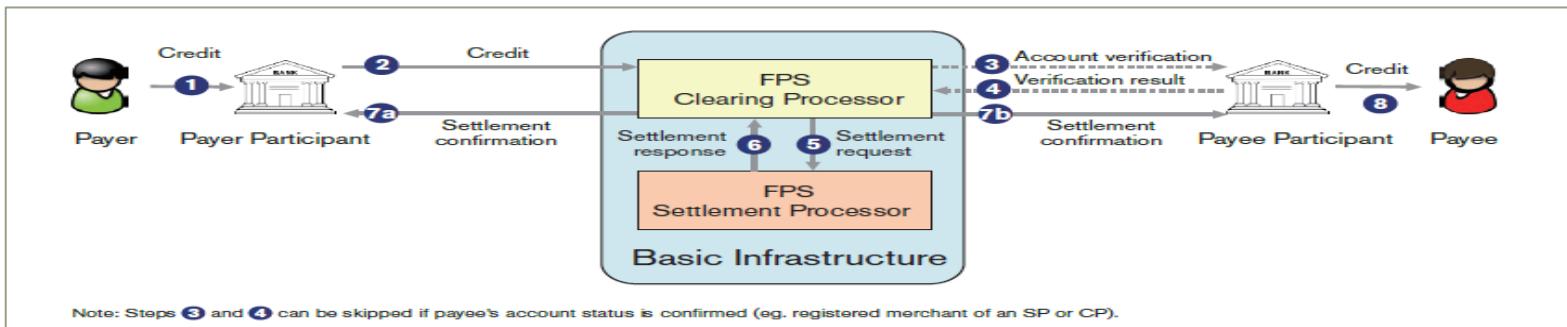
The public can use the **FPS** service through the online platforms/mobile apps of participating banks and e-wallet operators, e.g. register their mobile phone number or e-mail address with the **FPS** as an account proxy for receiving funds and carry out transfers and make payments.

# Faster Payment system

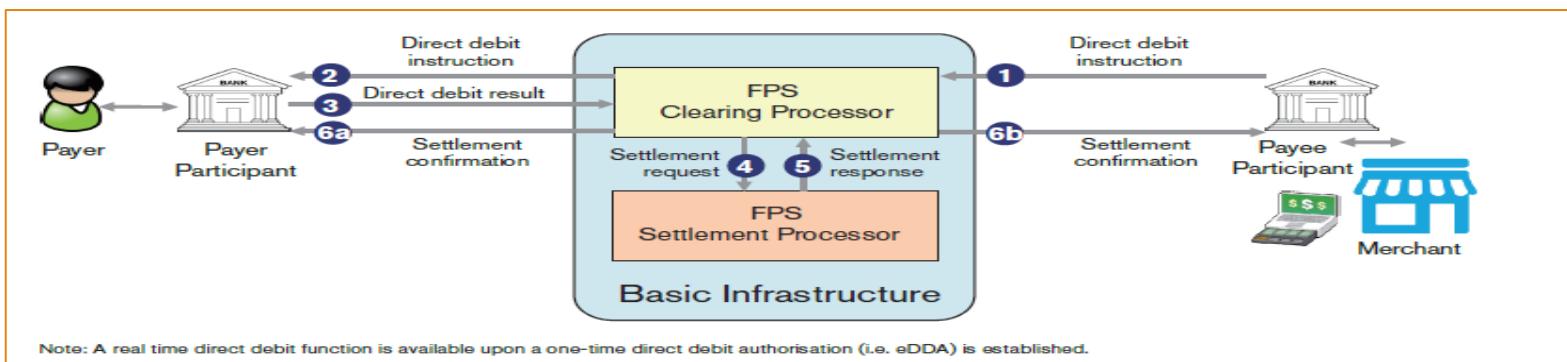


# Participants / Payments

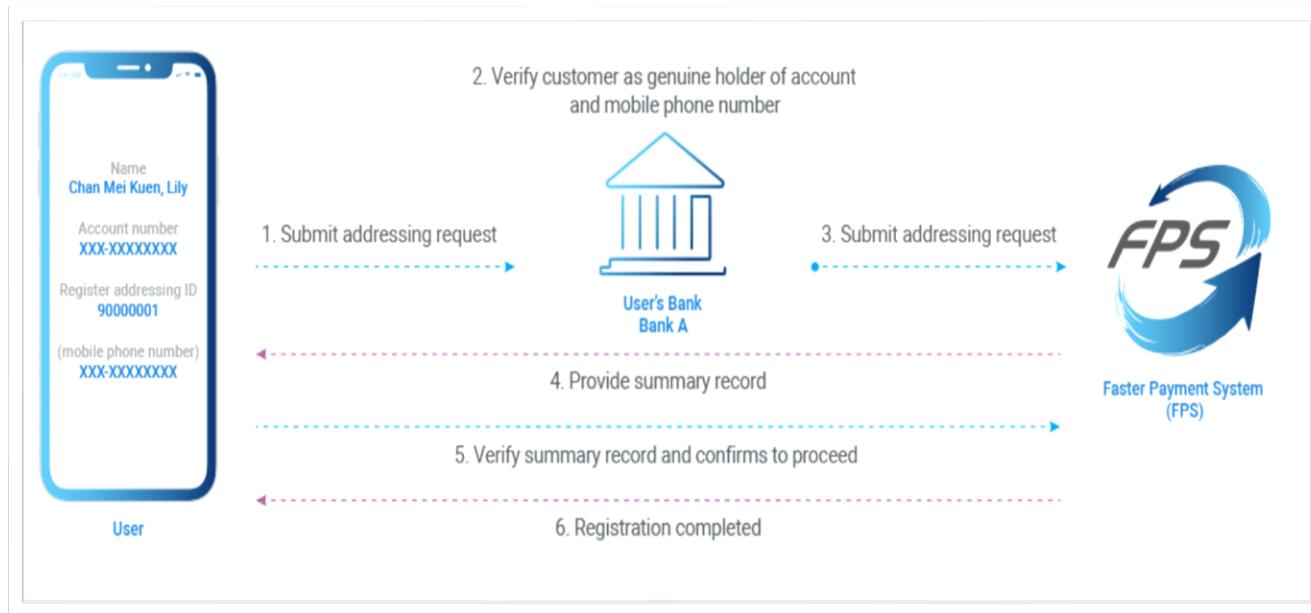
## Credit Transfer



## Direct Debit



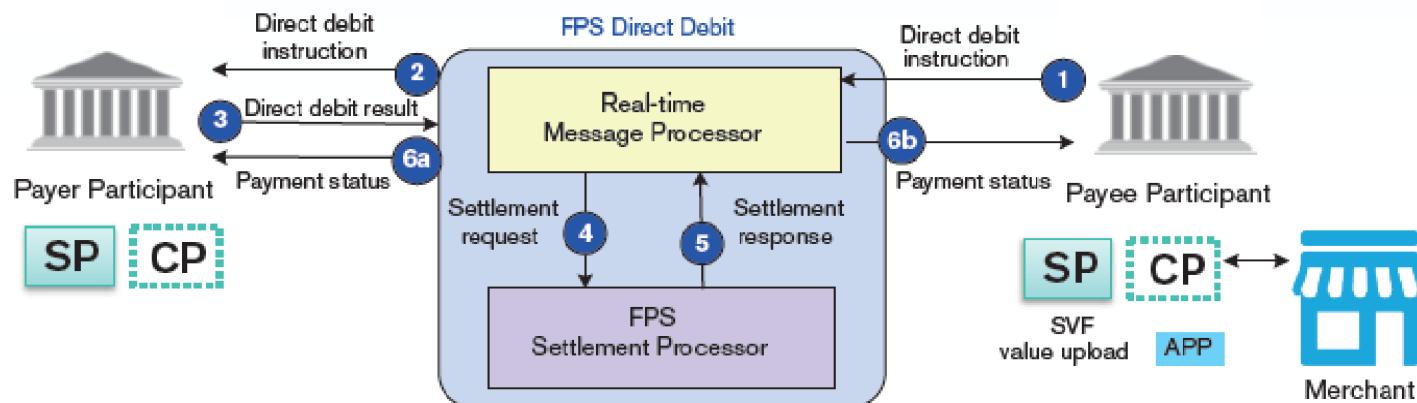
# FPS Registration Process (Addressing Service)



User allowed to register more than one account with the same mobile phone number, the user needs to select which account will be the default account for receiving FPS payment.

# Settlement mechanism / Liquidity arrangement / ISO Standard

The **FPS** adopts the **RTGS** mechanism under which each transaction is settled on a transaction-by-transaction basis. This differs from a deferred net settlement (DNS) mechanism where payments at customer level take place immediately, but the corresponding interbank payments are netted and settled separately at a later stage. The adoption of real-time settlement in the FPS effectively eliminates the credit risk exposure accumulated across different settlement participants.



# FPS Rules / HKMA Guideline (Security Requirement Highlight)

---

## Rules for Faster Payment System

### Section 6.8 Responsibility of Participants

6.8.1 the control of access to the FPS Console and the security of the Participant's terminal(s) connecting to HKICL  
....

6.8.2 the operation of all equipment and software relating to the access to the FPS Console and terminal(s) connecting to HKICL;

6.8.3 ensuring that:

(a) the access to and/or use of the FPS Console is in full compliance with these FPS Rules;

(b) all data transmitted from terminals owned by, or under its control, through which it gains access to the FPS Console

## TM-E-1 Risk Management of E-banking (considered FPS is part of E-Banking)

### 5. System and network security for Internet banking

5.1. Confidentiality and integrity of information

5.2. Internet infrastructure

5.3. Application system security

5.4. Threat monitoring and vulnerability assessment

Annex A: Items to be reported in independent assessment

# Variations of Fast Payment System

## QR-Cash (Standard Chartered Bank)

<https://www.sc.com/hk/bank-with-us/app-sc-mobile/qrcash/>

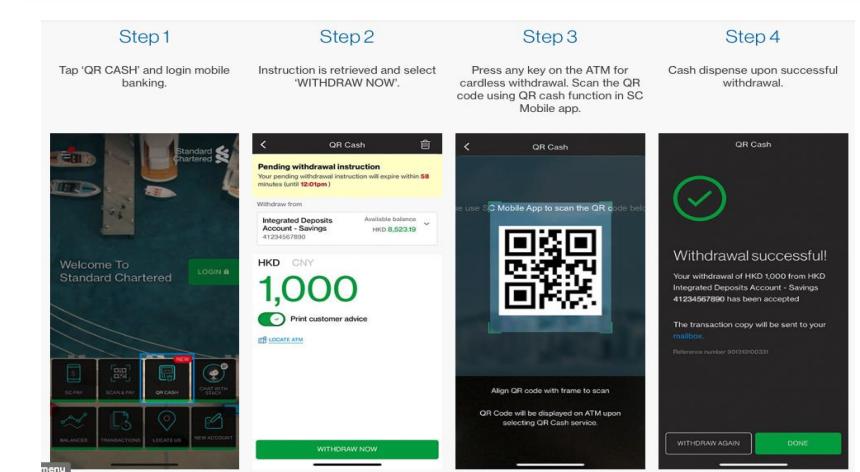
- Cash withdrawal with PIN and ATM card

## Threat

- QR code reply attack
- QR code and location translation attack

## Risk Control

- Daily cardless withdrawal limit is HKD10,000 or equivalent currency subject



# How to use e- Cheque

## Issue an e-Cheque via Business Internet Banking



Before you can create/issue an e-Cheque, you are required to register for the Bank-Cert (Corporate) service. This service essentially enables you to have a unique digital signature for issuing e-Cheques. You can refer to our Quick Reference Guide for details.

Please read Hongkong Post's [Certificate Subscriber Agreement](#) (including the [Certification Practice Statement](#) referred to therein) carefully before proceeding. You must check "I AGREE" below to acknowledge that you have read the agreement, that you understand it, and that you agree to it. If you do not accept the agreement, do not apply for or accept the issuance of a digital certificate.

I Agree.

By checking "I Agree", you acknowledge that you have read and understood the Certificate Subscriber Agreement and that you will comply with its terms. If you do not agree with the Certificate Subscriber Agreement please do not proceed.

### Notes:

1. Bank-Cert (Corporate) Service will be effective from the next business day\* after you have successfully registered the service.
2. e-Cheque issuance service will be enabled for all of the current account(s) of the Company which can be accessed via the online internet banking profile maintained by the Company with the Bank. Please note that e-Cheque issuance service is not available for any account to which cheque book services are not available or otherwise determined by the Bank from time to time.
3. The use of e-Cheque service shall at all times be governed by the General Terms and Conditions (For Personal Sole Account, Joint Account and Business Account Holders) or the Business Integrated Account Terms and Conditions (as applicable to your account(s)).

\*The reference to "business day" means a day, other than a Saturday, Sunday or public holiday, on which banks are open for general business in Hong Kong.

# eCheque Requirement

## e-Cheque Service

The e-Cheque Service makes your cheque payment easier and more convenient. e-Cheque retains all the basic features of paper cheques, plus more benefits:



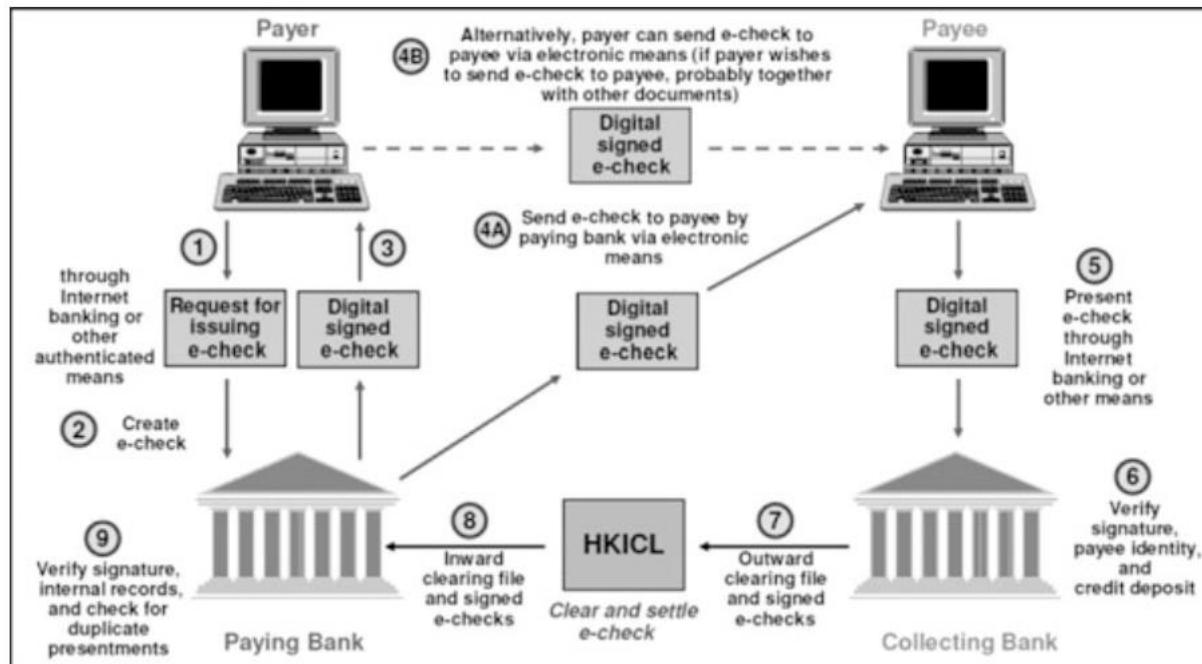
- **Issuance**  
e-Cheque can be issued anytime, anywhere at Personal e-Banking
- **Security**  
Each e-Cheque will carry your signature, which is digitally signed using the electronic certificate issued by the recognised certification authority
- **Delivery**  
You can simply send your e-Cheque to your payee electronically
- **Deposits**  
Your payee will just need to deposit e-Cheques online without visiting our branch

To start issuing e-Cheque, you need to have:

A current account under your name (sole or either-to-sign)	
An activated new Security Device	
Non-zero limit on non-registered third party transfer limit	
A mobile phone to receive SMS from the number registered in our record	

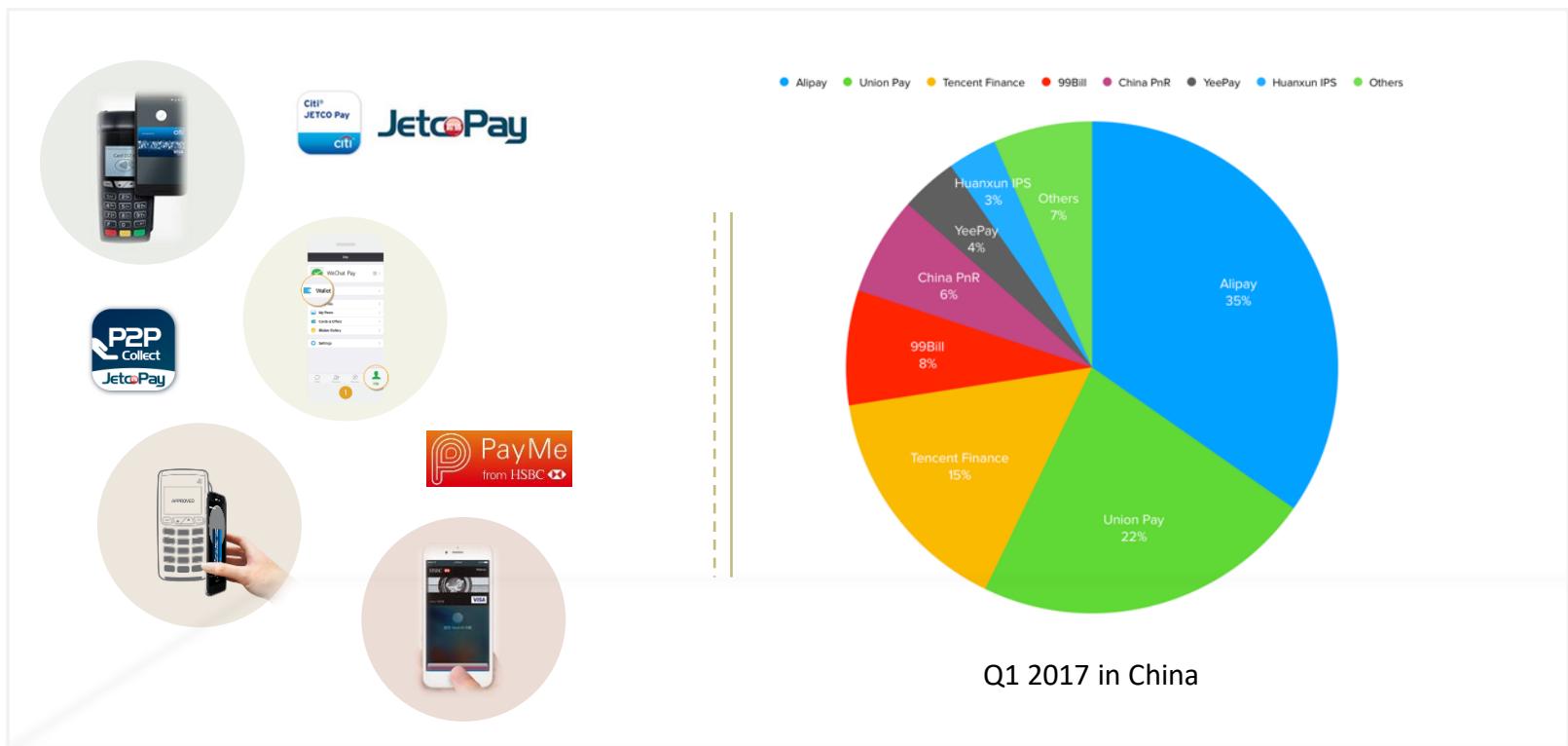
Please [read FAQs](#) on how to get yourself ready for issuing e-Cheque.

# E-Cheque via Internet

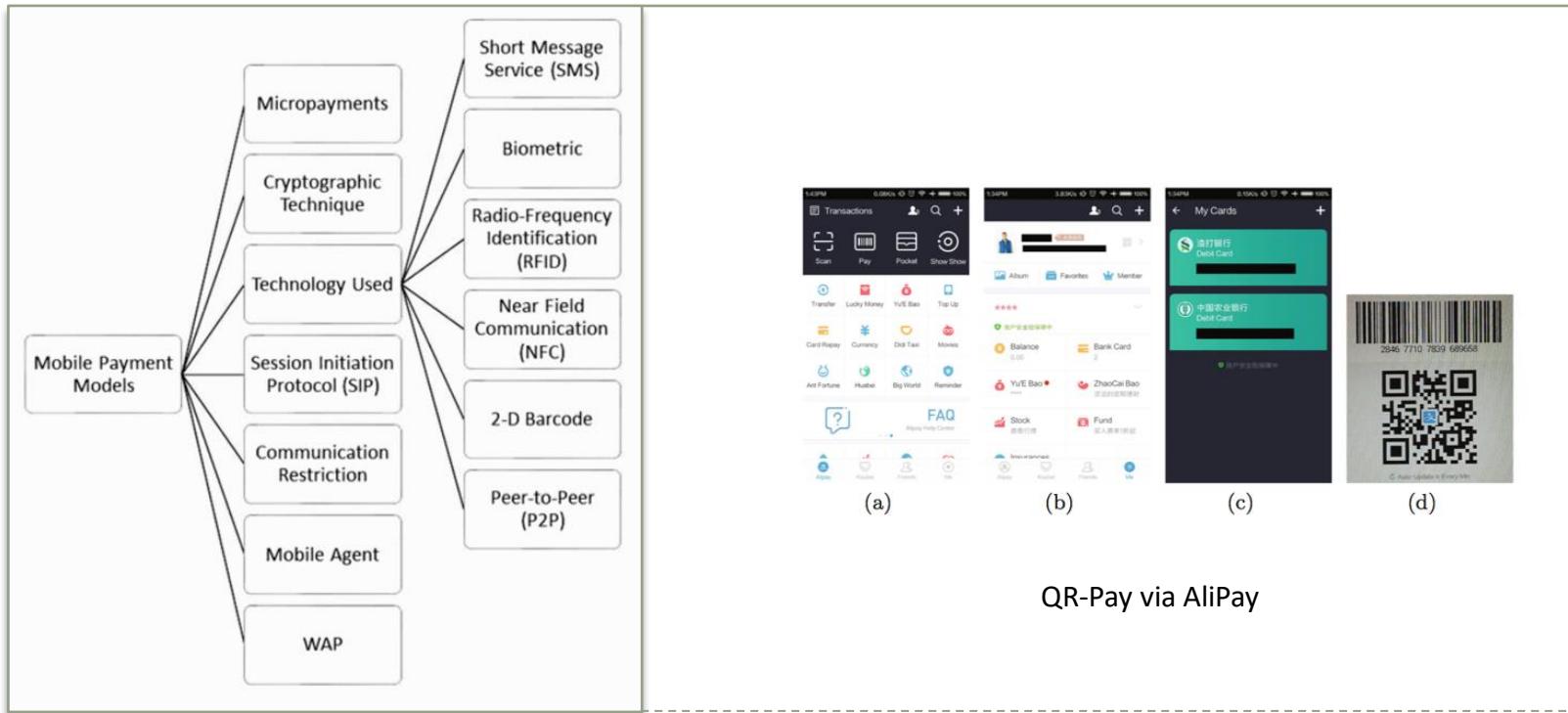


# Mobile and Online Payment

## Available Mobile Payment



# Mobile Payment Models



# QR-Payment (Alipay as example)

The users can check their balance and top-up money to the wallet by linking one or more debit/credit cards, or authorize Alipay wallet to direct deduct money from the debit/credit cards

To make a payment at the merchant, simply tap the “Pay” button to generate a one-time 1-D barcode and a 2-D QR Code, both of which are associated with an 18-digit number that is the identification number for this particular transaction

After merchant's EFTPOS scans the QR Code, the payment can be made instantly.

Alipay claims that once the QR code is scanned, the Alipay wallet will verify its source before carrying out payment instructions and sensitive user's information is stripped.



# Accounting System

---

## Single-Entry Accounting

- On the one hand, was a simple, easy to maintain the system as it was a one-sided accounting system
- But on the other, it was impossible to authenticate or examine its accountability
- Cannot determine who paid what, who owes how much, which debts are unpaid, etc

## Double-Entry Accounting

- Developed almost 600 years ago with the purpose of making the accounting system more comprehensive
- Instead of maintaining one ledger, the accountant keeps two;
  - one for incoming
  - one for outgoing.

## Triple-Entry Accounting

- Triple-Entry Accounting is somewhat misleading as there isn't any third entry; instead, a third component is added to the debit and credit system
- All transactions would be simultaneously posted in three places: with the two parties to the transaction and with an independent recording entity.
- All accounting entries are cryptographically sealed by a third entry and thus, it works as a deterrent towards manipulations and financial fraud.

# Digital Currency and Cryptocurrency

---

# Cash vs Digital Cash

## What is the nature of Cash

- Transaction without double spending
- Payment cannot be modified
- Distributed processing
- Non-repudiated transaction
- Limited/controlled quantity
- Anonymous, untraceable, unlinkable
- Acceptable by user
- Can be exchanged to smaller amounts

## Sample of Digital Cash

- NetCash
- NetCheque
- CyberCash
- CyberCoin
- CheckFree
- DigiCash
- Millicent
- MicroMint



# Digital Currency vs Cryptocurrency

---

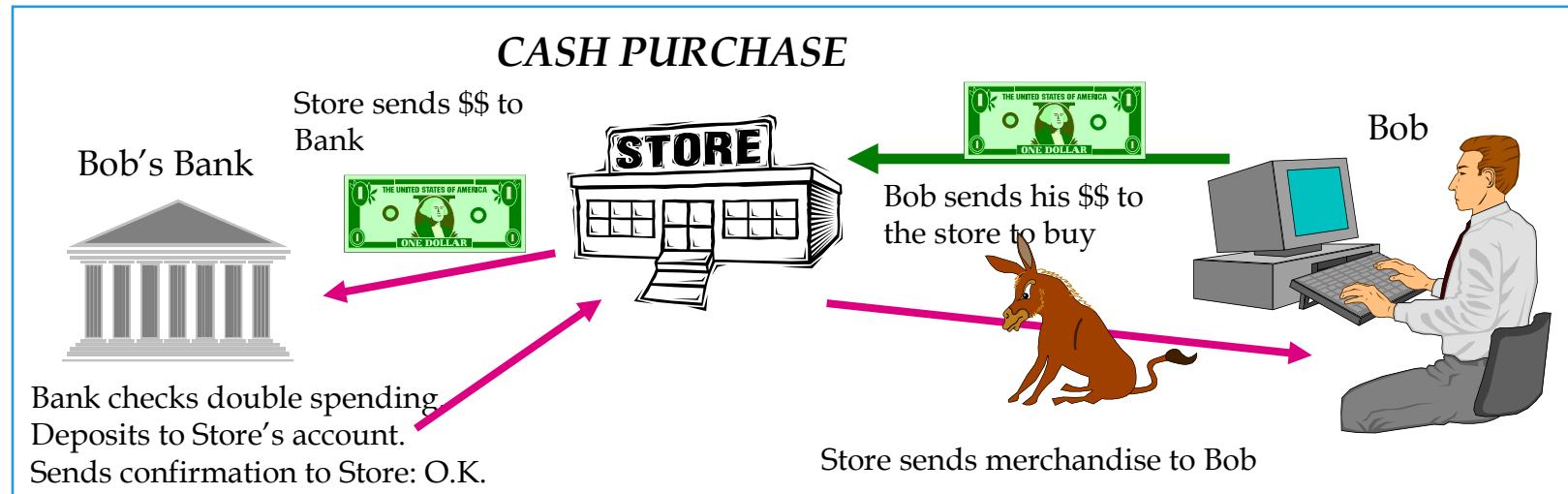
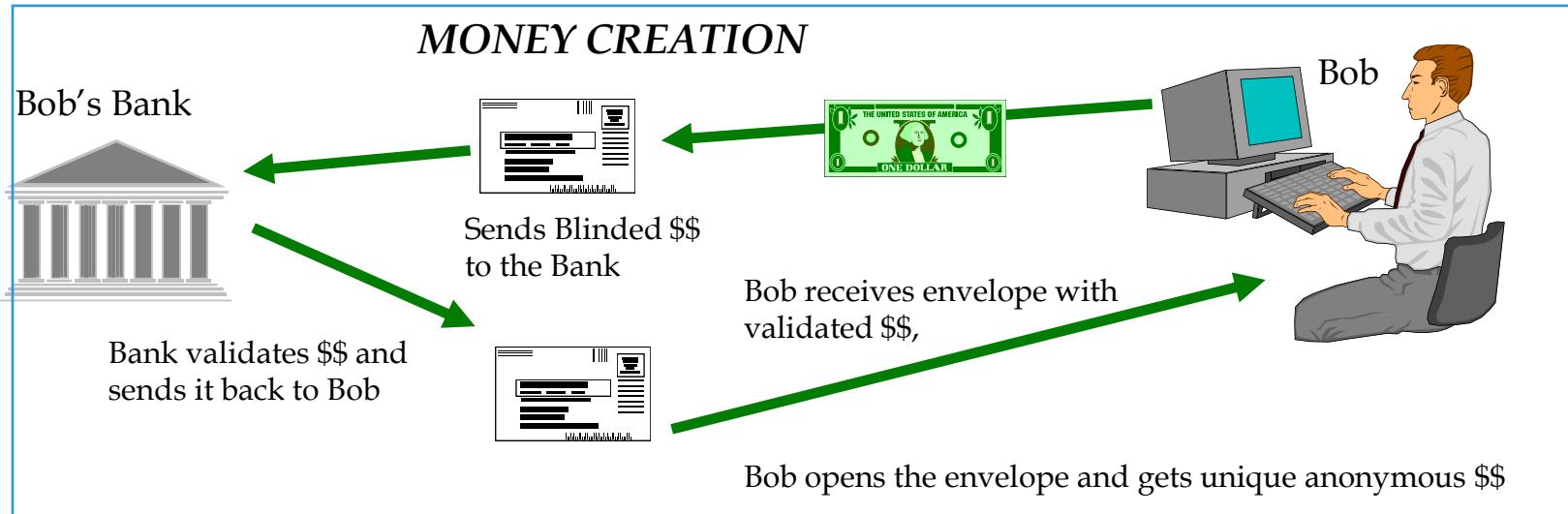
## Virtual currency – Digital Currency

- According to the European Central Bank's 2015 "Virtual currency schemes – a further analysis" report
- Virtual currency is a **digital representation of value, not issued by a central bank**, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money
- Digital currencies are **centralized**, meaning that transaction within the network is regulated in a centralized location, like a bank.
- Digital currencies are **another name for money** used to pay for specific goods or services on the Internet
- Can receive, transfer and/or exchange digital currency for another currency
- It may be and could be representing cashless society

## Cryptocurrency

- Cryptocurrencies are a specific variant of digital currencies.
- Cryptocurrencies are **algorithm powered currency used as tokens in select online communities** and backed by certain technologies, assets or projects.
- They are mostly used in **peer-to-peer payments** but are now increasingly used to pay for real-world goods and services.
- Cryptocurrency is considered secure, reliable and trustworthy as it is **based on cryptography**.
- Cryptocurrencies are **decentralized**, and the regulations inside the network are governed by the majority of the community.
- Cryptocurrencies are **transparent**. Anyone and everyone **is able to see any and all transactions** made and received by any user, as all revenue streams are placed in a public chain – the blockchain.

# Digital Currency – Digital Cash



# History of digital currency before Bitcoin

Date	Cryptocurrencies	Reference
1983	David Chaum's untraceable payments	Blind signatures for untraceable payments. In CRYPTO, 1982.
1990	David Chaum's DigiCash Blindly signed coins	Untraceable electronic cash. In CRYPTO, 1990.
1993	Netcash by MIT as coupons	
1994	Cybercash	<a href="https://en.wikipedia.org/wiki/CyberCash">https://en.wikipedia.org/wiki/CyberCash</a>
1994	Mondex as digital Wallet	<a href="https://en.wikipedia.org/wiki/Mondex">https://en.wikipedia.org/wiki/Mondex</a>
1995	NetBill	NetBill: An internet commerce system optimized for network-delivered services. IEEE Personal Communications, 2(4):34–39, 1995.
1997	Hashcash	<a href="http://www.hashcash.org/papers/announce.txt">http://www.hashcash.org/papers/announce.txt</a>
1997	Visa Cash as smart card e-cash	<a href="https://en.wikipedia.org/wiki/Visa_Cash">https://en.wikipedia.org/wiki/Visa_Cash</a>
1997	Micropayments	PayWord and MicroMint: Two simple micropayment schemes. In Security Protocols Workshop, 1997.
1998	Wei Dai's distributed e-cash – b-cash	<a href="http://www.weidai.com/bmoney.txt">http://www.weidai.com/bmoney.txt</a>
1998	Nick Szabo's bit gold	<a href="https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0">https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0</a>

# History of digital currency before Bitcoin

Date	Cryptocurrencies	Reference
1998	Lottcry	Publicly Verifiable Lotteries: Applications of Delaying Functions. In Financial Cryptography, 1998.
1999	Auditable anonymous e-cash	T. Sander and A. Ta-Shma. Auditable, anonymous electronic cash. In CRYPTO, 1999. T. Sander, A. Ta-Shma, and M. Yung. Blind, auditable membership proofs. In Financial Cryptography, 2001.
2003	Karma	Karma: A secure economic framework for peer-to-peer resource sharing. In Workshop on Economics of Peer-to-Peer Systems, 2003.
2004	Peppercoin	Peppercoin micropayments. In Financial Cryptography, 2004.

# Untraceable Payment

---



## Blind signature

- The bank can not trace which account the funds were withdrawn.
- How to handle bribery, extortion, black-market purchases, and other illicit payments?



## Extending the scheme

- note numbers created by payer
- bank signs the envelope
- bank still does not know who is paying who unless payer initiates a trace

# DigiCash

**DigiCash Inc.** was an electronic money corporation founded by David Chaum in 1989. DigiCash transactions were unique in that they were anonymous due to a number of cryptographic protocols developed by its founder.

**DigiCash** was a form of early electronic payment which required user software in order to withdraw notes from a bank and designate specific encrypted keys before it can be sent to a recipient. This advancement of public and private key cryptography allows electronic payments to become untraceable by the issuing bank, the government, or a third party.

## DigiCash

created and rolled out by David Chaum

**1982**

David Chaum Publishes "Blind Signatures for Untraceable Payments"

*Blind Signatures for Untraceable Payments*  
David Chaum - 1982

*First Bank to Launch Electronic Cash*  
DigiCash - 10/23/1995

*BUSINESS DIGEST*  
The New York Times - 10/23/1995

*Today, Shoppers on Internet Get Access to Electronic Cash*  
The New York Times - 10/23/1995



Later photo of the DigiCash team.

**1996**

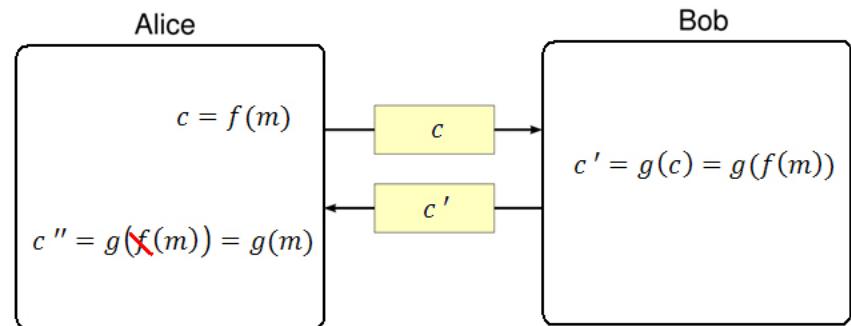
DigiCash Partners With EUNet For

# DigiCash

Security was ensured by public key digital signature schemes. The RSA blind signatures achieved unlinkability between withdrawal and spend transactions.

In cryptography a blind signature, as introduced by David Chaum, is a form of digital signature in which the content of a message is disguised (blinded) before it is signed.

DigiCash filed for Chapter 11 in November 1998. First Virtual Holdings had quit the business in August 1998, merging with Email Publishing and renaming itself MessageMedia in December. Awash in losses, CyberCash dropped its "CyberCoin" in the U.S. early this year.



## BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science  
University of California  
Santa Barbara, CA

### INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns.

On the one hand, knowledge by a third party of the payee, amount, and time of payment for every transaction made by an individual can reveal a great deal about the individual's whereabouts, associations and lifestyle. For example, consider

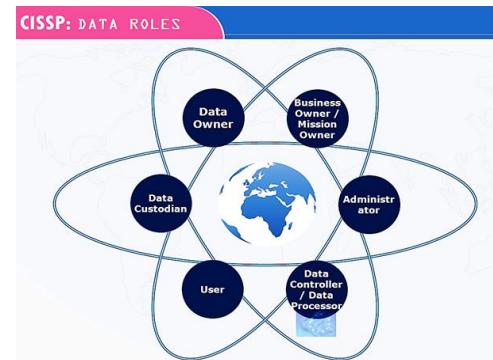
# Basic knowledge of Privacy in Currency

---

# Data Privacy Terms

Data ??	Descriptions
Data Subject	Individual who is the subject of personal data
Data Controller	Person who determines the purposes for which and the manner in which any personal data is, or is to be processed.
Data Processor	Any person who processes the data on behalf of the data controller.
Data Steward	Responsible for data content, context, and associated business rules. More focus on data quality
Data Custodian	Responsible for safe custody, transport, storage of the data and implementation of business rules.
Data Owner	holds legal rights and complete control over data elements. Possess the ability to define distribution and associated policies.

*"Freedom from unauthorized intrusion or observation"*  
- Merriam-Webster



(Data Controller and Data Processor are terms from Data Protection Law)

- Data controller <- Cloud Customer
- Data Processor <- CSP

# OECD privacy

---

- OECD - Organization for Economic Co-operation and Development is a forum for "countries committed to democracy and the market economy"
- Provide the most commonly used privacy framework, reflected in existing and emerging privacy and data protection laws, and serve as the basis for the creation of leading practice privacy programs and additional principles
-  8 core principles



# OECD privacy principles

---

## 1. Collection Limitation Principle

- There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject

## 2. Data Quality Principle

- Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date

## 3. Purpose Specification Principle

- The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose

## 4. Use Limitation Principle

- Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
  - a) with the consent of the data subject; or
  - b) by the authority of law

# OECD privacy principles (cont.)

---

## 5. Security Safeguards Principle

- Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data

## 6. Openness Principle

- There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller

## 7. Individual Participation

- An individual should have the right:
  - a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
  - b) to have communicated to him, data relating to him
    - i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him;
  - a) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
  - b) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended

## 8. Accountability Principle

- A data controller should be accountable for complying with measures which give effect to the principles stated above

# Trust, Anonymity and Privacy

---

Physical cash is an anonymous medium of exchange, so using it is a way to obtain bitcoin anonymously where no one except trading partners exchange identifying data.

## Cash Trade

- Cash-in-person trades are an old and popular method.
- Cash-by-mail works by having the buyer send physical cash through the mail
- Cash deposit is a method where the buyer deposits cash directly into the seller's bank account
- Cash dead drop is a rarely used method

# Trust, Anonymity and Privacy

Bitcoin has been used by many criminals in receiving their payment.

So is that bitcoin not traceable?

Is blockchain anonymous?

Anonymity and privacy = basic human needs.

## Here's how criminals use Bitcoin to launder dirty money

Tumbler services and unregulated exchanges are tools for cleaning cryptocurrency



**eToro**

This is why pros trade Bitcoin CFDs on eToro:  
Secured account with a reputable company

**Get Started**

60% of retail investor accounts lose money when trading CFDs with eToro. Consider whether you can afford to take the risk of losing your money. Highly volatile unregulated investment product. No EU investor protection. This is not investment advice.

Most popular



This blockchain-themed maths puzzle can earn you a share of \$100,000

<https://thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2/>

# How to maintain privacy

---



## Stay Anonymous

- No name, no identifier
- No IP address
- Minimal audit logging



## Don't use blockchain for sensitive transactions



## Enforce encryption

# Trust, Anonymity

Blockchain networks, because of encryption based on complex and robust cryptographic principles, can frequently be obfuscated quite effectively in a way that your transactions and data cannot be traced back to you.

It is indeed highly possible to make blockchain completely anonymous and private in nature, and this largely depends on what kind of cryptographic algorithm has been used for setting up a certain network.

For blockchain networks underlying privacy coins like Monero and DASH, anonymity is key. When you transact Monero actually uses a different **secret address** each time.

In certain other cases, blockchain can be pseudonymous rather than anonymous, which is the case with the Bitcoin blockchain.

## For Bitcoin

- Wallet address and transaction details are recorded in the blockchain
- Bitcoin transaction is linked to bitcoin address only.
- It is pseudonymous instead of anonymous cause intelligent tracker can link the address with all the transactions

## Privacy Coins Compared

	Balance Visibility	Sender Privacy	Cryptographic Privacy
Zcash	Only Transaction Addresses	✓	✓
Monero	X	✓	✓
Dash	✓	✓	X
PIVX	Normal Tokens	✓	✓
Bitcoin Private	Only Transaction Addresses	✓	✓
Ethereum	✓	X	X
Bitcoin	✓	X	X

# Privacy Levels

Privacy level content	Descriptions
Privacy among the participants of the network	Guaranteeing anonymity to whom are participating the network through cryptographic mechanisms triggered on-chain
Data privacy	Guaranteeing privacy on transactions, smart contracts and other data encrypting them on-chain or off-chain
Contract privacy	Guaranteeing privacy regarding the terms of the contract through a range proofs

# Necessary Nature of CryptoCurrencies

What is the nature of Cash

- Transaction without double spending
- Payment cannot be modified
- Distributed processing
- Non-repudiated transaction
- Limited/controlled quantity
- Anonymous, untraceable, unlinkable
- Acceptable by user
- Can be exchanged to smaller amounts

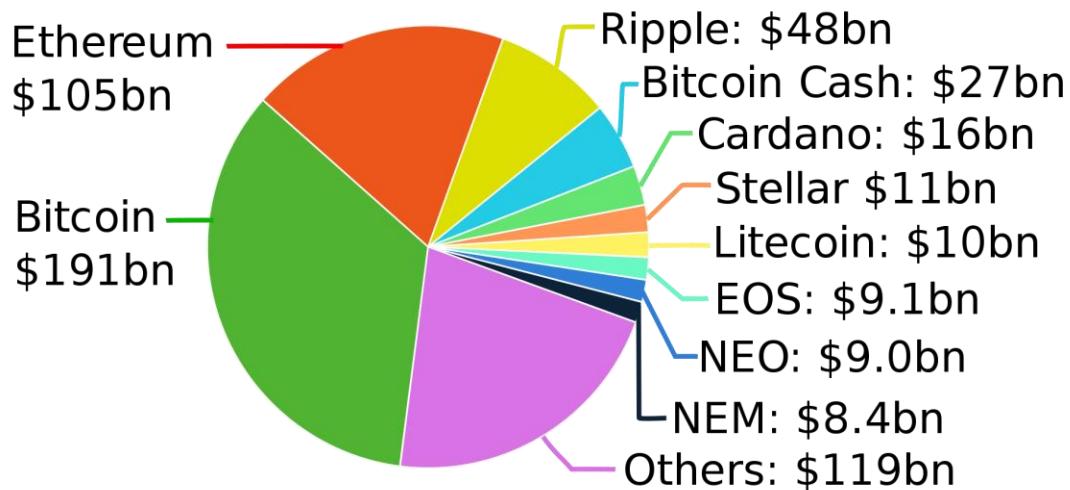
What's wrong in the development direction?

Why not accepted?

What's the alternative?

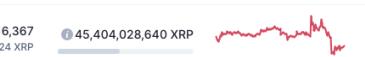


# Current status of CryptoCurrencies



By 19 Aug 2018

# Cryptocurrency Prices by Market Cap (25 Dec 2020 vs 24 Feb 2021)

#	Name	Price	24h	7d	Market Cap	Volume	Circulating Supply	Last 7 Days
1	Bitcoin BTC	\$24,111.37	▲ 3.10%	▲ 6.40%	\$447,512,958,787	\$42,248,584,002 1,754,165 BTC	18,580,781 BTC	
2	Ethereum ETH	\$619.80	▲ 3.93%	▼ 3.44%	\$70,536,350,752	\$14,387,026,733 23,247,715 ETH	113,978,308 ETH	
3	Tether USDT	\$0.998717	▼ 0.08%	▼ 0.03%	\$20,671,628,831	\$67,777,326,377 67,818,435,147	20,684,166,934 USDT	
4	XRP XRP	\$0.357171	▲ 26.84%	▼ 37.67%	\$16,088,175,443	\$15,731, 44,396,031	18,636,862 BTC	
5	Litecoin LTC	\$119.75	▲ 10.62%	▲ 12.61%	\$7,887,794,136	\$9,833 82,49	114,796,830 ETH	
6	Bitcoin Cash BCH	\$314.44	▲ 8.07%	▲ 0.96%	\$5,834,492,433	\$5,104, 16,274	154,532,785 BNB	
7	Cardano ADA	\$0.159268	▲ 6.79%	▼ 2.76%	\$4,937,088,504	\$1,204 7,592,656	34,761,096,222 USDT	
								
								
								
								

<https://coinmarketcap.com>

# Securing Commercial Transactions

---

## Encryption

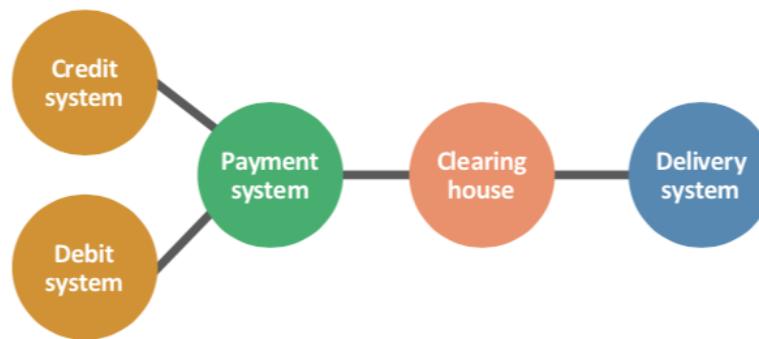
## Digital Signatures

### Blind Signatures for untraceable payment

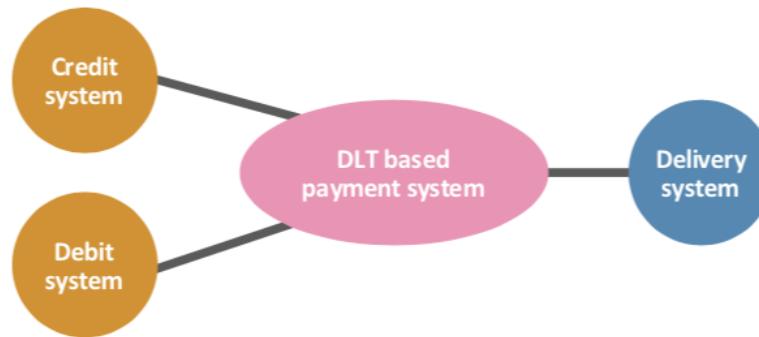
- carbon-paper-lined envelopes
- carbon image of signature from outside an envelope appear inside the envelope
- a blindly signed slip (by the bank) inside the envelope can be used for your subsequent purchases in a shop (of course you have to pay in order for the bank to sign the slip)
- The shop verify the signature and get money from the bank

# Legal Payment vs hybrid DLT

---



a) A simplified block diagram of a legacy payment system



b) A simplified block diagram of a hybrid DLT and legacy payment system

# Status of CryptoCurrencies in Hong Kong

---

Date	Descriptions
09 Jan 2014	Secretary for Financial Services and the Treasury says that there are high risks in exchanging, trading, and holding bitcoin; there are no physical currency guarantees; and its value is highly speculative. Also suggested that Hong Kong was monitoring the virtual currency market and was particularly concerned about money laundering. (Ref: <a href="https://www.fstb.gov.hk/en/docs/pr20140108_e.pdf">https://www.fstb.gov.hk/en/docs/pr20140108_e.pdf</a> )
11 Feb 2015	The Hong Kong Monetary Authority issued a statement warning the public about the risks involved in virtual currency trading after a bitcoin exchange allegedly stole its clients' funds. The statement also stated that Bitcoin is a virtual "commodity" and not legal tender. (Ref: <a href="https://www.hkma.gov.hk/eng/key-information/press-releases/2015/20150211-3.shtml">https://www.hkma.gov.hk/eng/key-information/press-releases/2015/20150211-3.shtml</a> )
25 Mar 2016	A senior Hong Kong official indicated, in response to a question submitted during a meeting of the Legislative Council of Hong Kong, that the government does not see a need for legislation that would regulate or ban bitcoin activities. The statement indicated that bitcoins are not a legal tender, and their value is not backed by any physical items, issuers or the real economy. (Ref: <a href="https://www.info.gov.hk/gia/general/201503/25/P201503250463.htm">https://www.info.gov.hk/gia/general/201503/25/P201503250463.htm</a> )

# Status of CryptoCurrencies in Hong Kong

Date	Descriptions
11 Nov 2016	The Hong Kong Monetary Authority (HKMA), ,in partnership with the Hong Kong Applied Science and Technology Research Institute (ASTRI). published a white paper on distributed ledger tech. The paper presents blockchain as a tool that “carries enormous potential” depending on the kind of application but highlights that from the regulatory perspective, risks remain (Ref: <a href="https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf">https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf</a> )
19 Mar 2018	Hong Kong's Securities and Futures Commission (SFC) has ordered the shutdown of an ICO by Black Cell Technology and directed the return of funds to investors who have purchased the tokens. The SFC was prompted to halt the operations over concerns that Black Cell had engaged in potentially unauthorized promotion of the ICO and unlicensed regulated activities (Ref: <a href="https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR29">https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR29</a> )

# Cryptocurrency

---

## The Definition of Cryptocurrency

- Cryptocurrency is an **independent digital currency**
- Independent will be achieved through decentralization of Issuing, Transaction, Storage of the Cryptocurrency
- Cryptocurrency coin is a cryptographic token, but it's never the other way around, meaning that not all cryptographic tokens are cryptocurrencies.

## According to Dr. Pavel Kravchenko

- Cryptocurrency related Digital Assets can be categorized as:
  - Non-auditable digital currency
  - Cryptographic tokens
    - Auditable digital currency
  - Cryptocurrency



# Digital Dollar Exploration Gets Backing From Treasury Secretary Yellen (22 Feb 2021)



Full steam ahead for the digital dollar — but no go for bitcoin as (widespread) transaction mechanism?

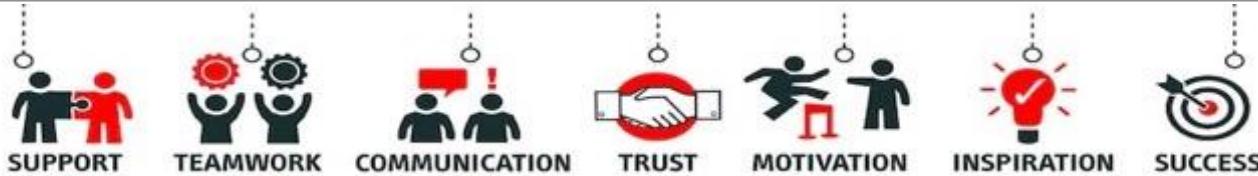
U.S. Treasury Secretary Janet Yellen said at a virtual conference held Monday (Feb. 22) by the New York Times that central banks should examine creating and issuing sovereign digital currencies.

As quoted in the Times, Yellen said that a digital dollar, overseen by the Federal Reserve, tied to the blockchain, could result in “faster, safer and cheaper payments,” according to the discussion, as quoted by the newspaper.

But in terms of the actual creation, issuance and distribution of digital dollars, Yellen posed what might be seen as existential questions. “What would be the impact on the banking system? Would it cause a huge movement of deposits out of banks and into the Fed? Would the Fed deal with retail customers or try to do this at a wholesale level? Are there financial stability concerns? How would we manage money laundering and illicit finance issues? There’s a lot of things to consider here, but it’s worth looking at.”

Those considerations stand in stark contrast to the likes of bitcoin, where Yellen seemingly downplayed the potential of that banner crypto, saying, “I don’t think that bitcoin is widely used as a transaction mechanism. It’s an extremely inefficient way of conducting transactions and the amount of energy that’s consumed in processing those transactions is staggering.”

## Closer cross-border collaboration



The HKMA will strengthen its efforts to collaborate with several authorities in other jurisdictions in the development of Fintech.



### Hong Kong Trade Finance Platform (HKTFP)

Latest initiatives being pursued include

- Cooperation with the Office of Financial Development Service of the Shenzhen Municipal Government
- Development of a Distributed Ledger Technology (DLT) platform to digitalize banks' trade finance processes in Hong Kong, with potential connectivity with Singapore's trade platform.

# Joint statement on the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project (23 Feb 2021)

 News and Media Smart Consumers Data, Publications and Research Regulatory Resources Key Functions About Us

**Press Releases**

23 Feb 2021 **Joint statement on the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project**

The Hong Kong Monetary Authority (HKMA), together with the Bank of Thailand (BOT), the Central Bank of the United Arab Emirates (CBUAE) and the Digital Currency Institute of the People's Bank of China (PBC DCI), today announced the joining of the CBUAE and the PBC DCI to the second phase of Project Inthanon-LionRock<sup>1</sup>, a central bank digital currency project for cross-border payments initiated by the HKMA and the BOT. This joint effort is strongly supported by the Bank for International Settlements Innovation Hub Centre in Hong Kong and the project has been renamed as "m-CBDC Bridge".

Building on the experience learnt from Project Inthanon-LionRock, the m-CBDC Bridge project will further explore the capabilities of distributed ledger technology (DLT), through developing a proof-of-concept (PoC) prototype, to facilitate real-time cross-border foreign exchange payment-versus-payment transactions in a multi-jurisdictional context and on a 24/7 basis. The m-CBDC Bridge project will also explore business use cases in a cross-border context using both domestic and foreign currencies.

Following the joining of the CBUAE and the PBC DCI, the m-CBDC Bridge project will further foster a conducive environment for more central banks in Asia as well as other regions to jointly study the potential of DLT in enhancing the financial infrastructure for cross-border payments. Eventually, the outcome is expected to alleviate the pain points in cross-border fund transfers, such as inefficiencies, high cost and complex regulatory compliance. Most importantly, the participating central banks will take into account the results of the PoC work to evaluate the feasibility of the m-CBDC Bridge project for cross-border fund transfers, international trade settlement and capital market transactions.

**Hong Kong Monetary Authority**  
Bank of Thailand  
Central Bank of the United Arab Emirates  
Digital Currency Institute of the People's Bank of China  
23 February 2021

**LATEST PRESS RELEASES**

23 Feb 2021 Fraudulent website related to Union Bancaire Privée, UBP SA

23 Feb 2021 Fintech Co-operation between the Hong Kong Monetary Authority and the Central Bank of the United Arab Emirates

23 Feb 2021 Joint statement on the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project

23 Feb 2021 Exchange Fund Bills Tender Results

22 Feb 2021 Fraudulent website related to Citibank (Hong Kong) Limited

 [View All](#)

# Closer cross-border collaboration

## Guangdong-Hong Kong-Macao Greater Bay Area Collaboration



**Fintech Award**

- HKMA/Office of Financial Development Service of Shenzhen (OFDS)
- Recognize and reward outstanding Fintech products and solutions

**Soft-landing Scheme**

- HKMA/OFDS/Cyberport
- Feasibility of establishing cross-border soft-landing facilities in Shenzhen

**Talent Development Programme**

- Renowned high-tech companies in Shenzhen
- Summer intern positions for Hong Kong students

# Crypto currencies

<https://www.thechinfamily.hk/web/en/financial-products/fintech/ico-bitcoin/basic-concept-bitcoin.html>

...Bitcoin and other “cryptocurrencies” are considered to be “virtual commodities” and are not legal tenders....

**What is “Cryptocurrency”? What is Bitcoin?**

**Bitcoin is a virtual commodity and is not a currency. The market generally calls bitcoin and alikes as “cryptocurrencies” or ‘virtual currencies’.**

**Bitcoin Born in 2009**

Bitcoin was the first “cryptocurrency” that was introduced in 2009, and since then, thousands of alternative “cryptocurrencies” have emerged such as Ether, Ripple and Litecoin etc.

You can imagine bitcoin as a series of complicated and encrypted passwords which can be transferred electronically.

Bitcoin can be used as a means to “pay”/exchange for goods or services with merchants who accept them.

Bitcoin is operated under blockchain technology to verify and record transactions.

Though it is called bitcoin, it does not physically exist. There is no actual physical bitcoin.

Bitcoin is not backed by any bank, government, not supported by its issuers or tied to any tangible assets.

# P2P Lending & CrowdFunding

---

## PEER-TO-PEER LENDING

Practice of lending money to individuals or businesses through online services that match lenders with borrowers.

- operate online
- run with lower overhead
- provide the service more cheaply than traditional financial institutions
- The interest rates can be set by lenders who compete for the lowest rate on the reverse auction model or fixed by the intermediary company
- Extending crowdsourcing to unfamiliar lenders and borrowers opens up new opportunities

E.g.: WeLab, Best Leng, EasyLend, Finance One

## CROWDFUNDING

Practice of funding a project or venture by raising small amounts of money from a large number of people, typically via the Internet.

Crowdfunding is a form of crowdsourcing and alternative finance



# Decentralized Finance (DeFi)

---

Decentralized finance (DeFi) is an emerging financial technology based on **secure distributed ledgers** similar to those used by cryptocurrencies.

The system removes the control banks and institutions have on money, financial products, and financial services.

A distributed database is accessible across various locations; it collects and aggregates data from all users and uses a **consensus mechanism** to verify it.

DeFi uses a layered architecture and highly composable building blocks

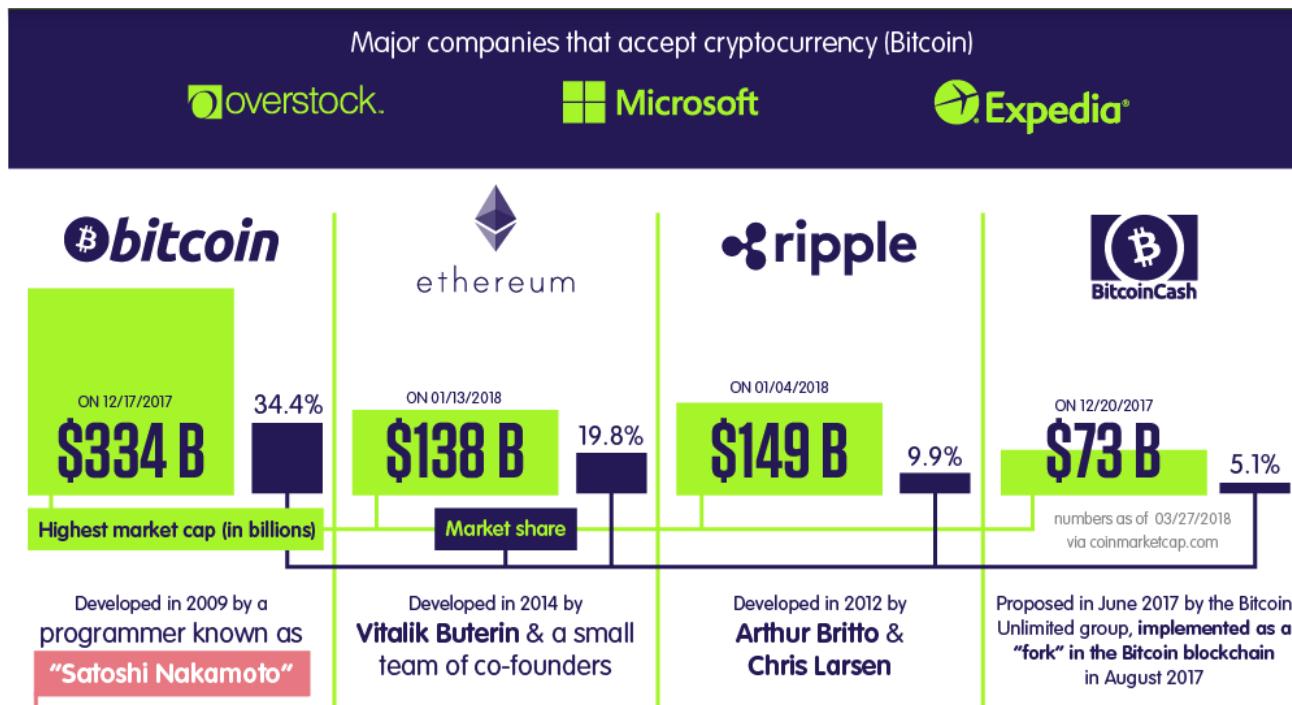
## Benefit of DeFi

- eliminates the fees that banks and other financial companies charge
- hold money in a secure digital wallet
- Can perform transaction without need of approval
- can transfer funds in seconds and minutes

# Application of Blockchain Technology to Cryptocurrencies alternative coins

---

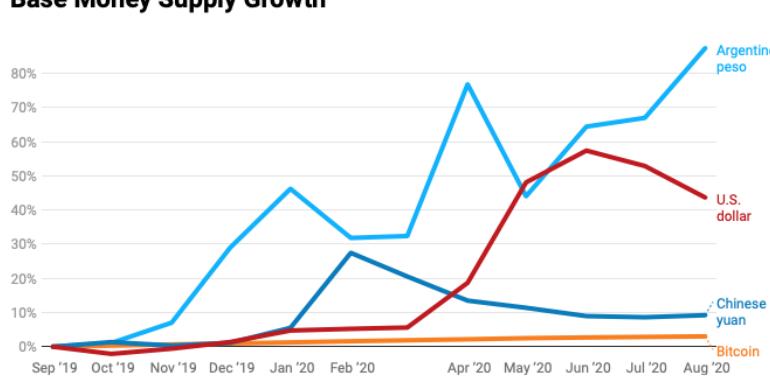
# About Cryptocurrency



From Definitive Guide to CryptoCurrencies

# Base Money Supply Growth

**Base Money Supply Growth**



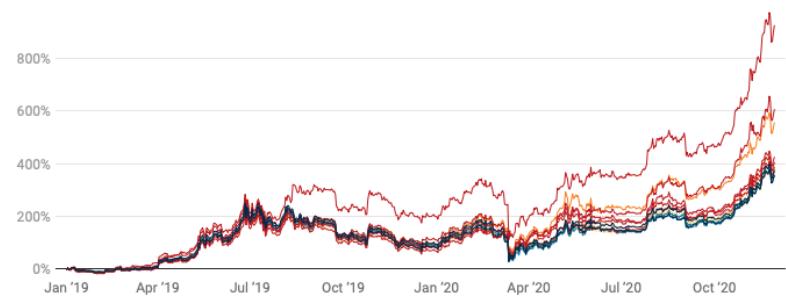
Percent growth in M0 money supply from Sept. 30, 2019 - Aug. 31, 2020

Source: Trading Economics • [Get the data](#) • Created with Datawrapper

[Nov 17, 2020] Bitcoin is nearing its prior all-time high (ATH), set in December 2017. It's entirely plausible that we could regain the heady \$20,000 level within the next few weeks or months.

**BTC vs. G20 Currencies**

Legend: EUR, ARS, AUD, BRL, CAD, CNY, INR, IDR, JPY, KRW, MXN, RUB, ZAR, TRY, GBP, USD

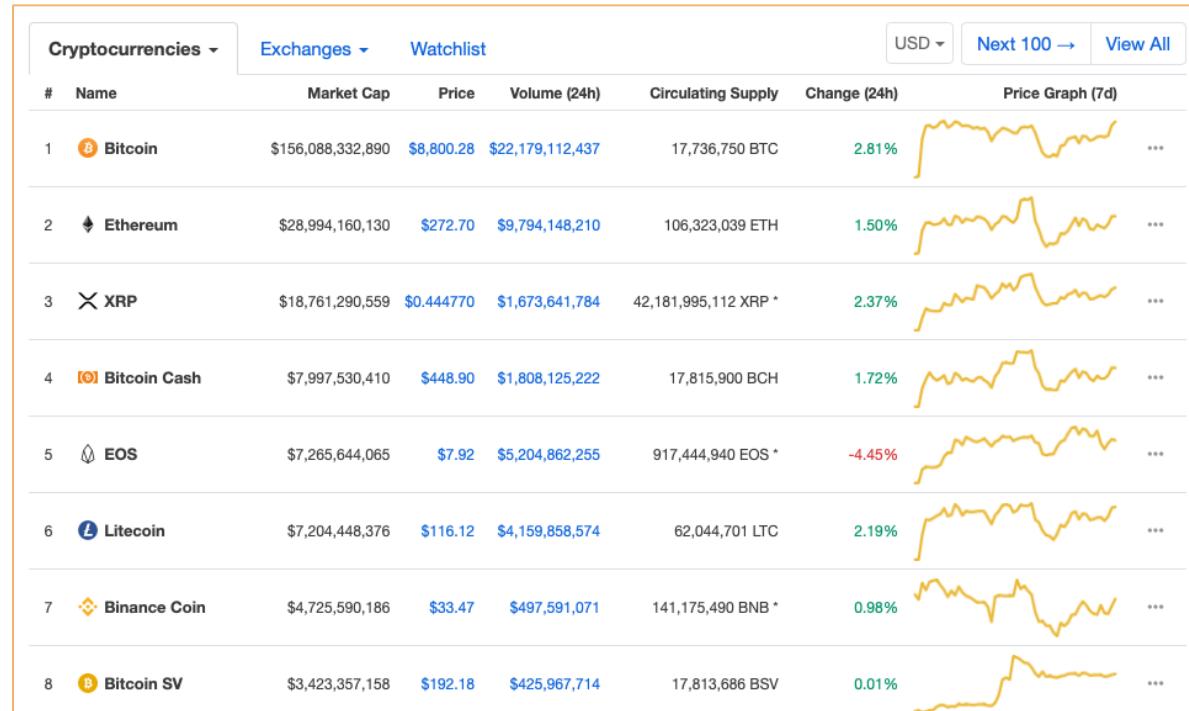


BTC exchange rate percent increase from January 1st, 2019 to November 29th, 2020

Source: Google Finance • [Get the data](#) • Created with Datawrapper

# Cryptographic Exchanges

- There are more than 2,216 cryptocurrencies in circulation by 2019
- A combined market cap of over \$278 billion (\$289 billion in 2018), according to CoinMarketCap data



<https://coinmarketcap.com>

# Birth of Altcoins

---



Within a couple years of launching, it had become clear that Bitcoin was the first fully decentralized cryptocurrency to gain significant adoption, but there were some aspects with which people were not fully satisfied.

**Namecoin** was the first significant fork away from Bitcoin. Interestingly, it was less about creating a new currency and more about utilizing the immutable nature of the blockchain, a use case we'll address more in the next chapter.



**Litecoin** was released through 2011, aimed to improve upon Bitcoin in two ways. For one, Litecoin's block times were 2.5 minutes, four times faster than Bitcoin's, which would be important for merchants needing faster confirmation of consumer's payments.

Litecoin used a different hash function in the proof-of-work process—also known as a block hashing algorithm

# Diem (Libra)

---



In 2019, Facebook established Libra, a declaration of independence from government money, but while retaining centralized management, in order to create a rent-seeking mechanism that adds to the wealth of the network stakeholders.

Libra, backed by Facebook, its army of subordinate tech companies and 2.4 billion users, hopes to generate its own monetary system, while capturing the network value for itself.

Diem (Formerly known as Libra) is a **permissioned blockchain private digital currency** proposed by the American social media company Facebook.

The Libra blockchain is not decentralised the way the Bitcoin is. With the Bitcoin blockchain, anyone can theoretically run a node, even if that's expensive

The currency and network do not yet exist, and only rudimentary experimental code has been released

# Diem (Terminated) on 28 Jan 2022

---



---

Facebook 曾經推動過一個加密貨幣計劃，希望藉着開發新的加密貨幣系統，可以促進跨境交易以及成為新的電子貨幣模式，不過後來由於各國監管當局一直不給予支持，最近終於宣佈終止計劃。

名為 Libra 的加密貨幣開發計劃最初在 2019 年由 Facebook（現改名 Meta）公佈，當時他們希望建立一個新的加密貨幣系統，由 Facebook 主導同時擁有一定的獨立性，消息公佈時，有知名機構包括 PayPal、eBay、Mastercard、Stripe、Visa 等等參與，不過後來多國監管機構一直反應負面，令計劃遲遲未獲許可。

在多個合作夥伴紛紛退出之後，Facebook 在 2020 年 12 月將其改名 Diem，並且表示其獨立性提升，Facebook 的影響力會更低。不過最近 Diem 終於宣佈解散，其資產將會以約 2 億美元售予 Silvergate。他們表示，與監管機構商討後結果顯示計劃無法推進。

來源：[WSJ](#)

unwire.hk Mewe 專頁：<https://mewe.com/p/unwirehk>

<https://unwire.hk/2022/02/01/facebook-cryptocurrency-venture-to-wind-down-sell-assets/fun-tech/>  
<https://techmonitor.ai/technology/emerging-technology/facebook-diem-stablecoin-cryptocurrency>

# Central Bank Digital Currency Questions

---

Should Central Banks Currently Issue Digital Reserves to Commercial banks

Should Commercial Banks Provide Digital Currency (Deposits) to Public

How to handle Private Sector is Experimenting with Stable Value Tokens

Should Direct Access to Digital Reserves be Expanded?

Should promote competition in banking system

How to address payment system ‘pain points’?

How to manage the degree of anonymity?

How to handle transfer mechanism?

# China's Digital Currency Electronic Payment (DCEP)

---

Sep 2020, A payment system created by the Chinese state and known as Digital Currency Electronic Payment (DCEP).

Like Bitcoin, DCEP utilises a blockchain technology, a type of digitised ledger used to verify transactions.

Blockchain acts as a universal record of every transaction ever made on that network, and users collaborate to verify new transactions when they occur.

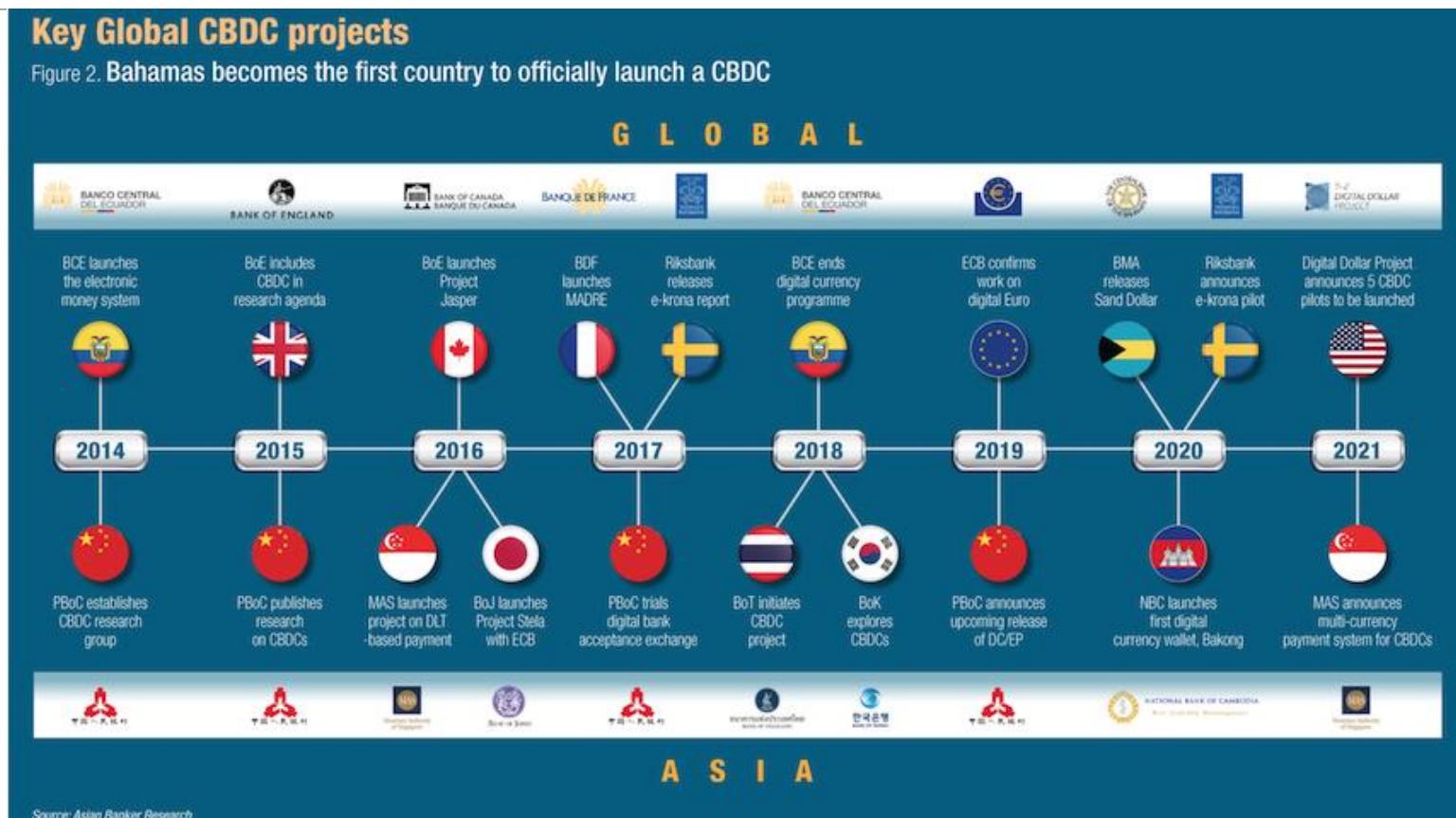
The DCEP is backed by yuan deposits held by China's central bank and has been under development for slightly more than five years.

DCEP differs from existing cryptocurrencies because it is legal tender, centralized, and not anonymous. Promoting a concept it calls “controllable anonymity”

# Global CBDC

## Key Global CBDC projects

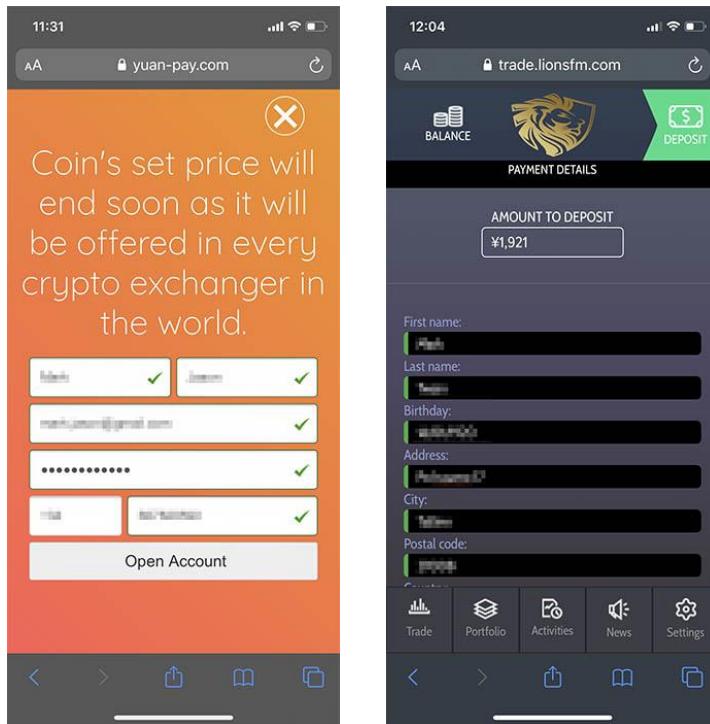
Figure 2. Bahamas becomes the first country to officially launch a CBDC



<https://www.theasianbanker.com/updates-and-articles/central-bank-digital-currency-disruption-has-arrived>

# China Officially Backs a CryptoCurrency (Feb 2021)

China, in an unprecedented move, just announced that they are officially adopting a certain cryptocurrency as China's official coin!



## CHINA ANNOUNCED OFFICIAL CRYPTOCURRENCY SALES OPEN IN

It's finally happened. A major worldwide government has just bestowed a huge vote of confidence and legitimacy onto the world of cryptocurrencies. China, in an unprecedented move, just announced that they are officially adopting a certain cryptocurrency as China's official coin!

The government of China just informed us that they have chosen a preferred firm for the purchase and marketing of their new coin - [YuanPay Group](#). The sales of China's coin officially started February 12 of 2021 and currently these coins can be bought only from [YuanPay Group](#).

In fact, China deputy minister of finance, Liu Kun, informed us that their new official coin starting price is just ¥0.12 cents!

1 Chinese Yuan equals 0.12 Euro

# China's top regulators ban crypto trading and mining, sending bitcoin tumbling (Sep 2021)

---

SHANGHAI/LONDON, Sept 24 (Reuters) - China's most powerful regulators on Friday intensified a crackdown on cryptocurrencies with a blanket ban on all crypto transactions and mining, hitting bitcoin and other major coins and pressuring crypto and blockchain-related stocks.

Ten agencies, including the central bank, financial, securities and foreign exchange regulators, vowed to work together to root out "illegal" cryptocurrency activity, the first time the Beijing-based regulators have joined forces to explicitly ban all cryptocurrency-related activity.

The People's Bank of China (PBOC) said cryptocurrencies must not circulate and that overseas exchanges are barred from providing services to China-based investors. It also barred financial institutions, payment companies and internet firms from facilitating cryptocurrency trading nationally.

In September 2019, China accounted for 75% of the world's Bitcoin energy use. By April 2021, that had fallen to 46%.

# China's CBDC Has Been Used for \$9.7B of Transactions (Nov 2021)

China's central bank digital currency (CBDC) has been used to conduct 62 billion yuan (\$9.7 billion) of transactions as of the end of October.

A People's Bank of China (PBOC) official said Wednesday that 140 million people had opened wallets for the digital yuan, or "eCNY," according to a report by Reuters.

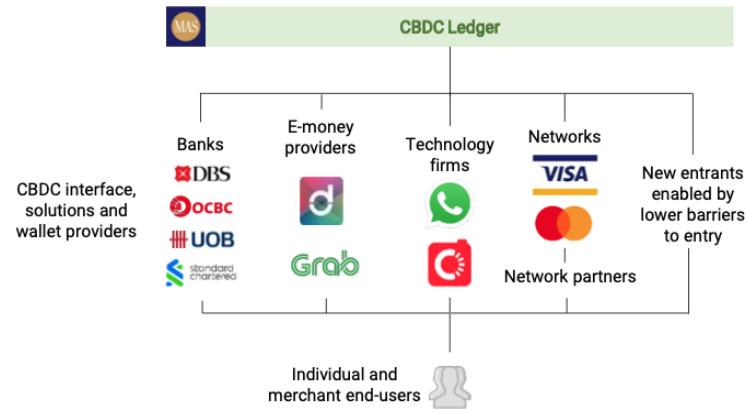
CNBC said "But the PBOC's digital yuan comes with a number of problems that make it less attractive in Western countries. Critics say it's too centralized and could be used to boost government surveillance. That's because, unlike cash, people's digital transactions can be tracked online."



# Singapore MAS – A Retail Central Bank Digital Currency (Nov 2021)

The Monetary Authority of Singapore (MAS) announced (30 August 2021) the 15 finalists for the global competition to develop retail Central Bank Digital Currency (CBDC) solutions (Global CBDC Challenge)

The Challenge was held in partnership with the International Monetary Fund, World Bank, Asian Development Bank, United Nations Capital Development Fund, United Nations High Commission for Refugees, United Nations Development Programme, and the Organisation for Economic Co-operation and Development



Represented by	Participating Organisations	Solution Name
ConsenSys	ConsenSys and Visa	CBDCgo - digital currency, seamless acceptance
Criteo	Criteo SA, Secretarium Ltd. and Intel® Corporation	The Atomic CBDC Solution
Giesecke+Devrient advance52 GmbH	Giesecke+Devrient advance52 GmbH	G+D Filia

<https://www.mas.gov.sg/news/media-releases/2021/mas-announces-winners-of-the-global-cbdc-challenge>

# Singapore MAS – A Retail Central Bank Digital Currency (Nov 2021)

Solution Name	Represented by	Participating Organisations	Solution Description
CBDCgo - digital currency, seamless acceptance	ConsenSys	ConsenSys and Visa	ConsenSys and Visa are partnering to build a Visa Retail CBDC Payment module supported by the ConsenSys Blockchain Infrastructure to demonstrate the concept of how a retail CBDC solution can cater for widespread and frictionless use. (without needing to change their payment or acceptance network)
The Atomic CBDC Solution	Criteo	Criteo SA, Secretarium Ltd. and Intel® Corporation	Using Secretarium's Secure-enclave <b>Distributed Ledger Technology</b> (SDLT) leveraging Intel SGX Chip for the secure enclaves, the solution aims to provide a <b>high-performance DLT</b> that is suited for <b>highly secretive financial transactions</b> , ultra large scale CBDCs. Compared to traditional DLT, SDLT allows for <b>transactions to be committed and encrypted in memory on chain or in ledger</b> .
G+D Filia	Giesecke+Devrient advance52 GmbH	Giesecke+Devrient advance52 GmbH	G+D Filia solution is a <b>token-based digital currency resembling cash</b> , enhanced with smart features and without the friction of physical money. It has been designed from the very beginning to allow for consecutive offline payments. Filia works <b>both on smartphones and hardware wallets</b> , can provide full privacy at the payment layer and supports programmable use cases. To achieve that, a different approach from the standard DLT platforms were taken. They do not record account balances or transaction metadata on a blockchain, but only the <b>validity of a particular token together with its denomination</b> .

<https://www.mas.gov.sg/news/media-releases/2021/mas-announces-winners-of-the-global-cbdc-challenge>

# E-HKD consultation paper (Dec 2021)

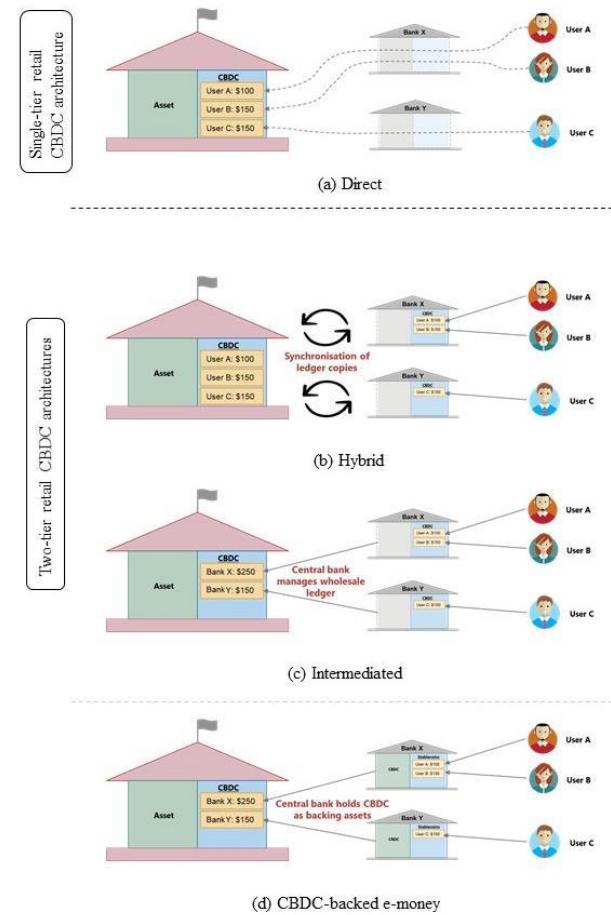
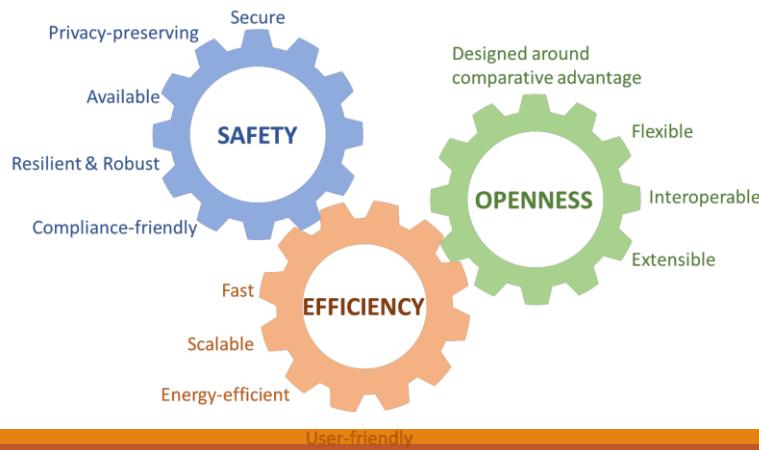
## Different architectural design

- Direct (1-tier) rCBDC model
- 2-tier rCBDC model

## Key design concern

- Over-issuance prevention
- Privacy-preserving transaction
- Flexible architecture

## Design Principles for 2-tier distribution infrastructure for rCBDC



# Cross-border CBDC developments (2021)



<https://www.theasianbanker.com/updates-and-articles/central-bank-digital-currency-disruption-has-arrived>