

# **The World of Emerging Payment Systems**

## **A Brief Introduction**

**Joseph M. Vincent**

**Director of Regulatory & Legal Affairs**

**Washington State Department of Financial Institutions**

**Presentation to Financial Management Advisory Council**

**March 26, 2015**

# Disclaimer

**The contents of this PowerPoint presentation and the oral remarks made incident thereto reflect the personal views of Joseph M. Vincent and do not necessarily reflect either the positions or policy of the Washington State Department of Financial Institutions (“DFI”) or of Joseph M. Vincent, acting in his official capacity for DFI.**

The World of Emerging Payment Systems

# ESSENTIALS OF ANY PAYMENT SYSTEM

# The Most Important Factor in Any Payment System

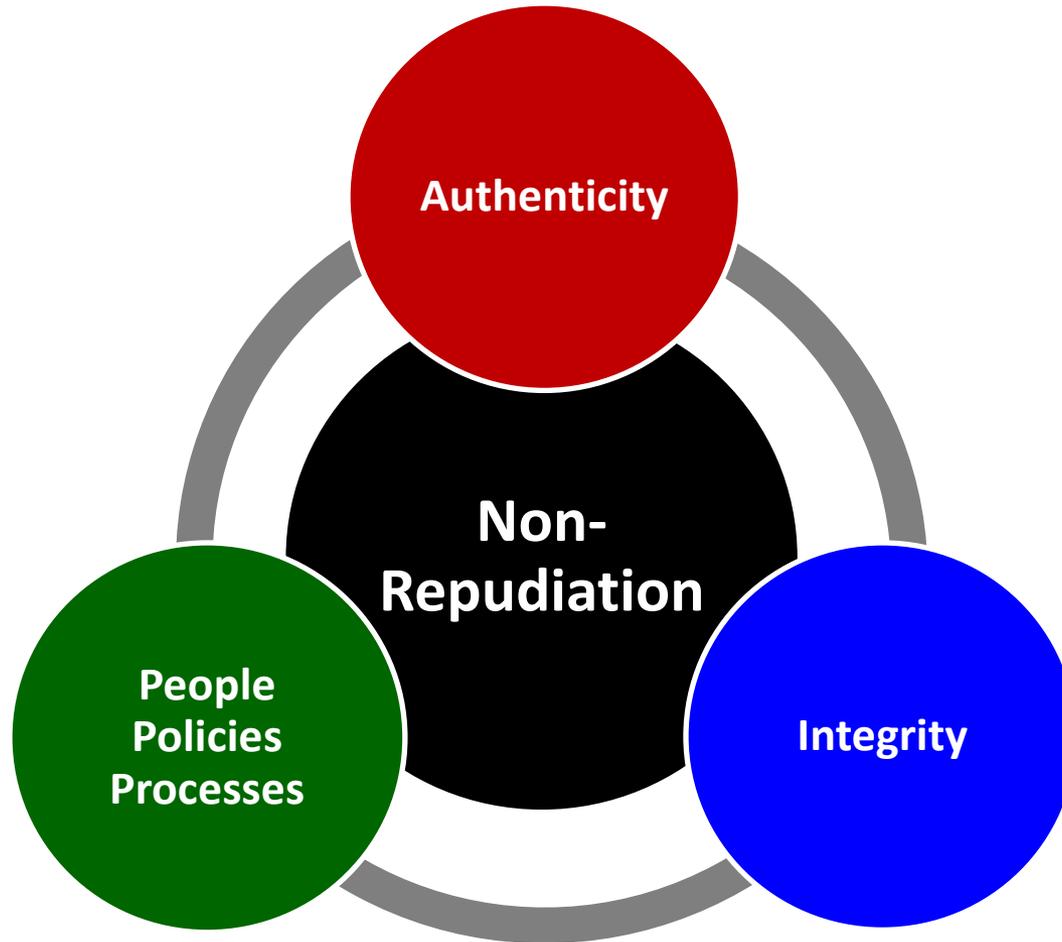


# Non-Repudiation

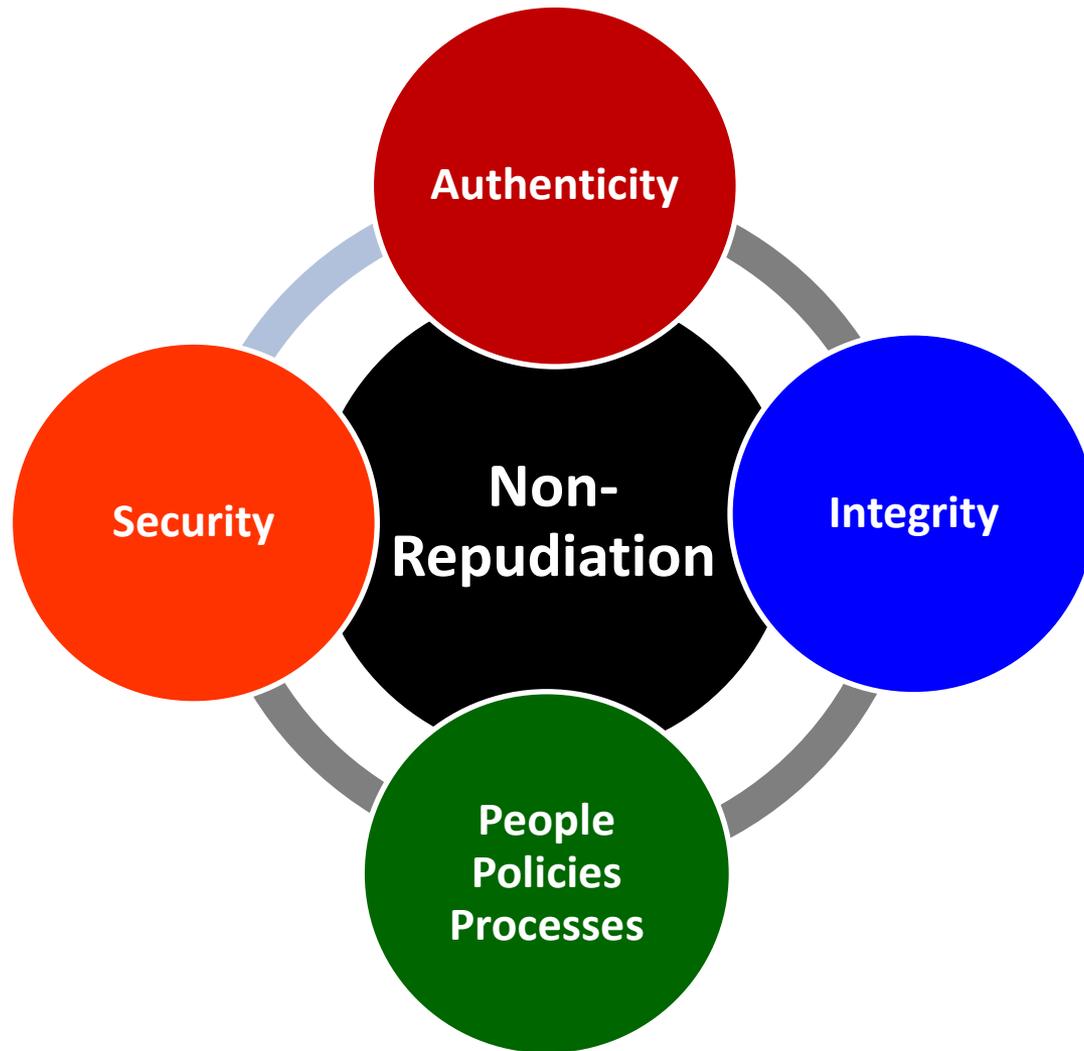


The maker of a communication will not be able to successfully challenge the *external* validity of the communication.

# Non-Repudiation



# Non-Repudiation *in the Digital Age*



The World of Emerging Payment Systems

# **SHORT HISTORY OF LEGACY PAYMENT SYSTEMS**

# Barter Exchange

**Barter** is a system of exchange by which goods or services are directly exchanged for other goods or services without using a medium of exchange, such as money.



"I need your service."

"...and I need YOUR service!"



# Immediate Use of Medium of Exchange



An immediate use of a **medium of exchange** is where one party hands the other money or its equivalent in exchange for the goods or service.

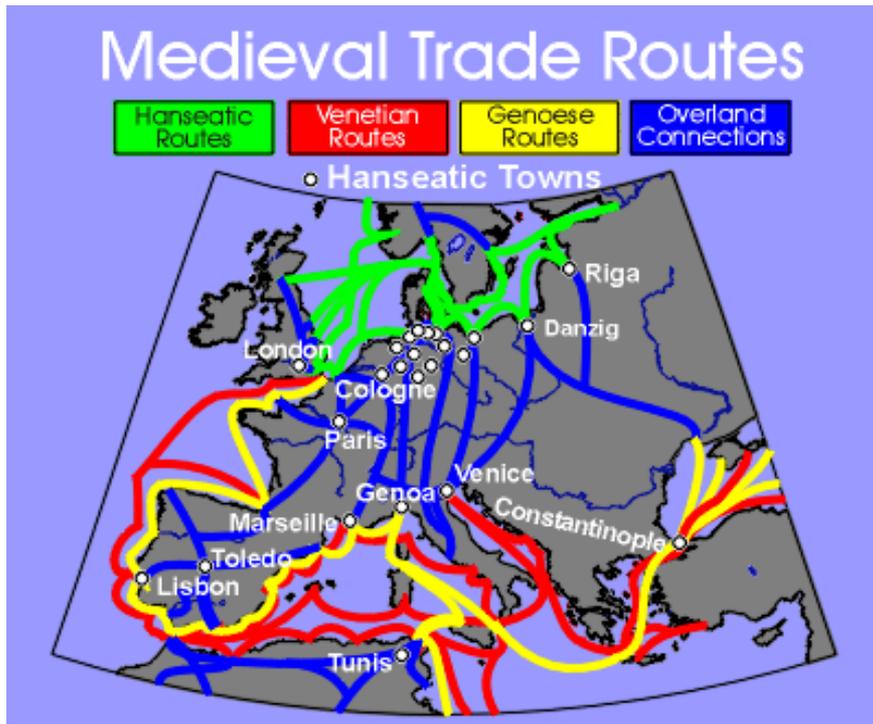


# Long-Distance Exchange

- Eventually people started using a medium of exchange to buy goods from a **long distance**, sending the money by highway and having the goods shipped back by highway.
- In either direction, there was the **danger of robbery**.



# Early Commercial Paper



- As Medieval trade routes became more widely used, **merchant banking** arose.
- People of means **stored value** (their money) with merchant bankers.
- In turn, merchant bankers issued **redeemable notes** and **letters of credit**.

# Earliest Stock and Bond Market

- The Dutch merchant guilds were the first to establish and widely use **central registries** for the recording of exchange transactions, **issuing certificates** and **redeemable instruments**.



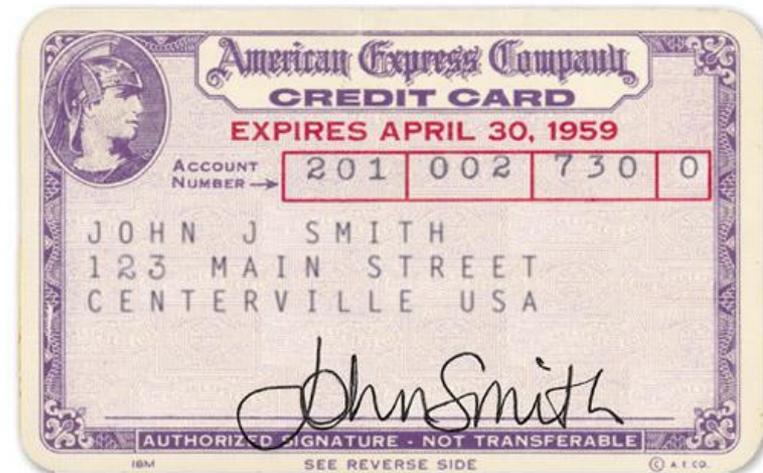
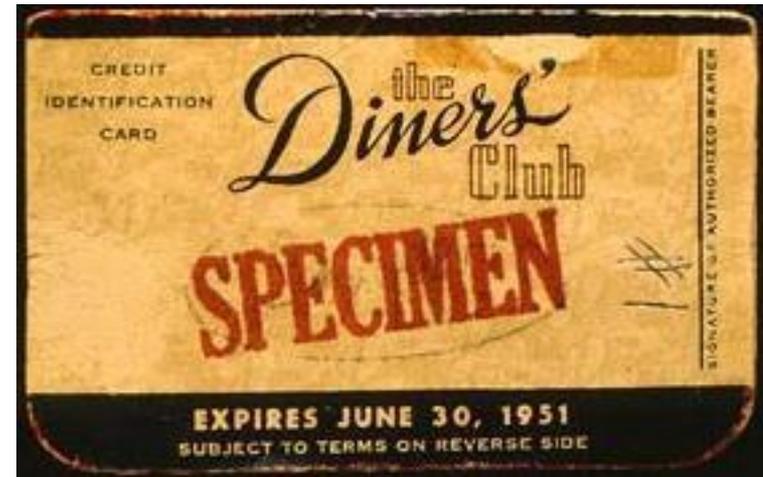
# The Checking Account



- The check as we know it was invented in 1870 to avoid double taxation on state banks.
- A check is a **payment order** drawn on a demand deposit account of a bank.
- It may **negotiated by endorsement**.

# The Early Credit Card

- Diners Club, followed shortly by American Express, were the first credit cards.
- They were dependent on restaurant, hotel, and merchant membership.



# The Proprietary Bank Credit Card



- Then came the proprietary bank credit card.
- Banks using this payment system were dependent upon restaurant, hotel, and merchant membership.
- This was limited to the largest banks.

# Visa and MasterCard Systems

- Then came Visa and MasterCard, which relied on membership by issuing banks.
- This greatly expanded the participation of most banks and credit unions in the issuance of credit cards, either as issuers or as resellers.



# The Bank Debit Card



- Then we saw the advent of the bank debit card.
- With the help of Visa and MasterCard, the bank debit card has become ubiquitous, eclipsing the check and cash as the most common form of payment.

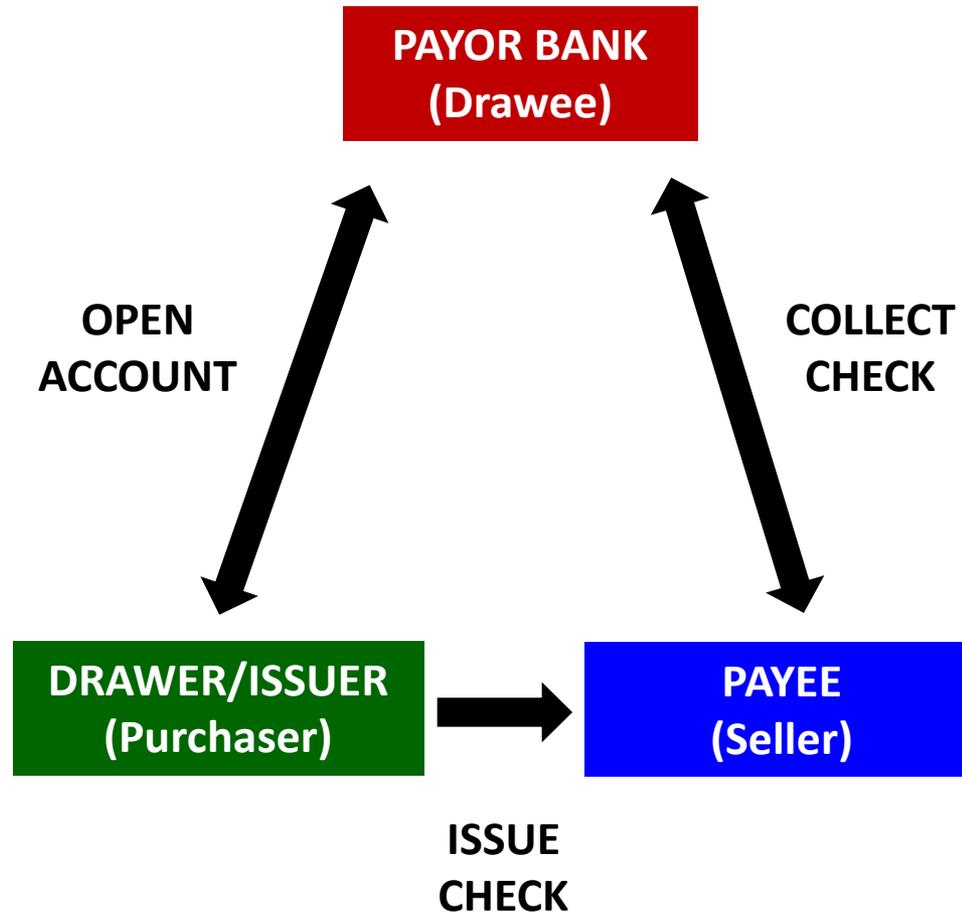


# The Prepaid Debit Card

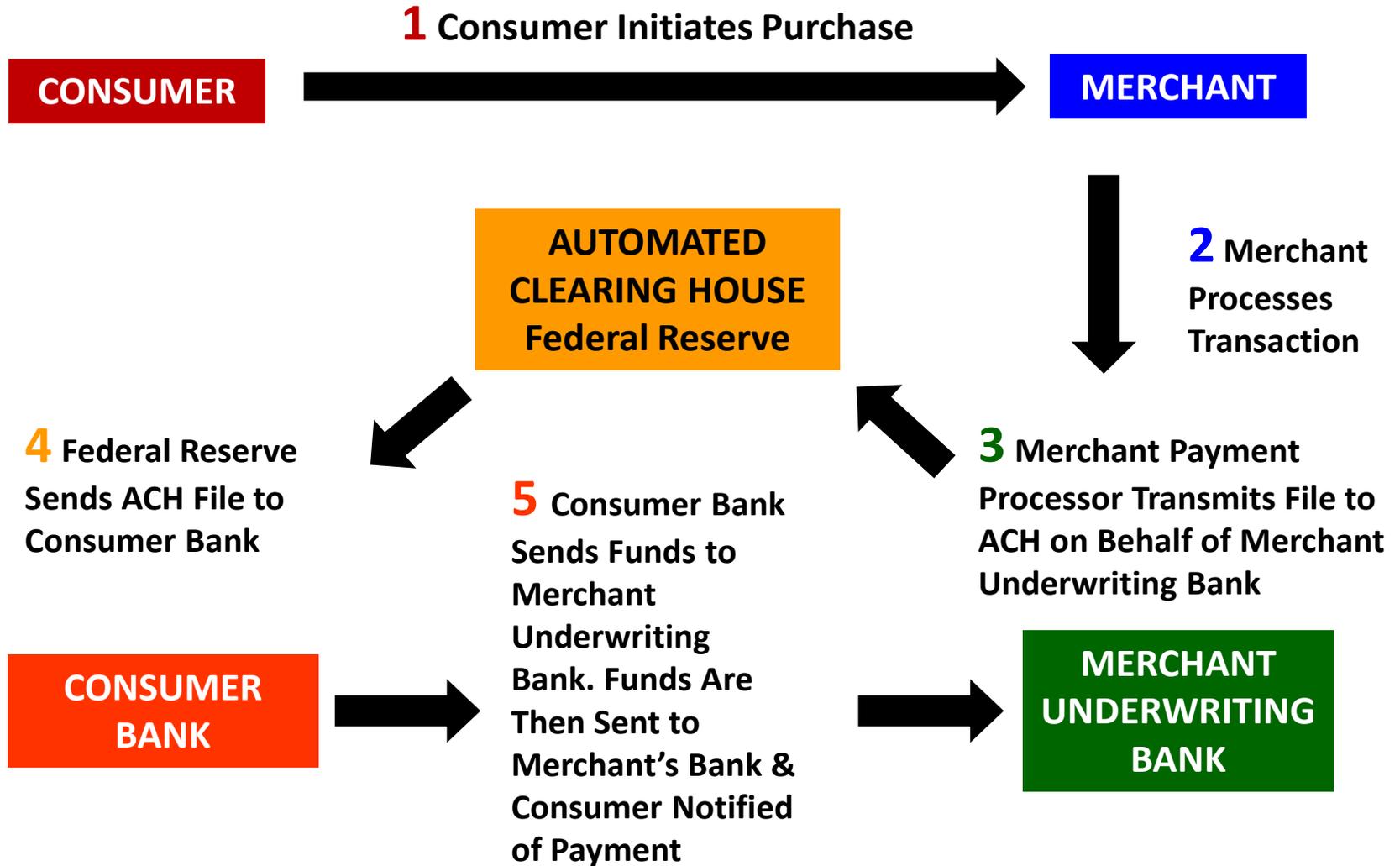
- As a substitute for cash – often for those consumers lacking or not wanting to use a bank account – the pre-paid debit card (**stored value card**), issued by banks and backed by the Visa and MasterCard networks, is becoming a significant percentage of the payments market.



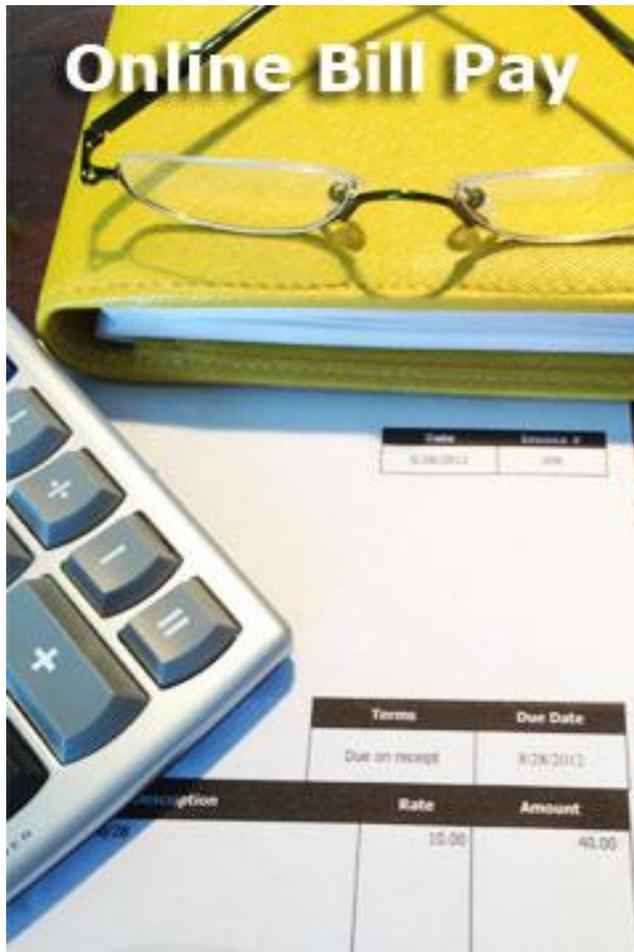
# Check Negotiability and Clearance



# Debit Card ACH



# Online Bill Pay Authorization



- Usually this involves giving your bank **authorization** to draw on your account to pay bills using the ACH process.
- Or it may involve going online and paying your credit card balance through your card issuer's **pre-authorized access** to your bank account.

# Summary of Legacy Payment Systems

- Each of the legacy payment systems is dependent on **non-repudiation** as a basis of trust.
- Decentralized legacy systems rely on **negotiability** (**endorsement**) as a trust model.
- Other legacy systems rely on a combination of a **central clearinghouse** and decentralized processing.

**clearinghouse**  
**negotiability**  
**endorsement**  
**non-repudiation**

The World of Emerging Payment Systems

# FIRST GEN E-COMMERCE PAYMENT SYSTEMS

# What Is Money Transmission?

- **Federal Registration as Money Transmitter: 31 U.S.C. §5330**
- **Unlawful Money Transmission: 18 U.S.C. §1960**
- **Uniform Money Services Act: RCW 19.230.010 & WAC 208-690-010**  
“Money transmission” means receiving money or its equivalent value to transmit, deliver, or instruct to be delivered the money or its equivalent value to another location, inside or outside the United States, by any means including, but not limited to, by wire, facsimile, or electronic transfer. Money transmission does not include the provision solely of connection services to the internet, telecommunications services, or network access. Money transmission includes selling, issuing, or acting as an intermediary for open-loop stored value devices and payment instruments, but not closed-loop stored value devices.



# Starbucks® App



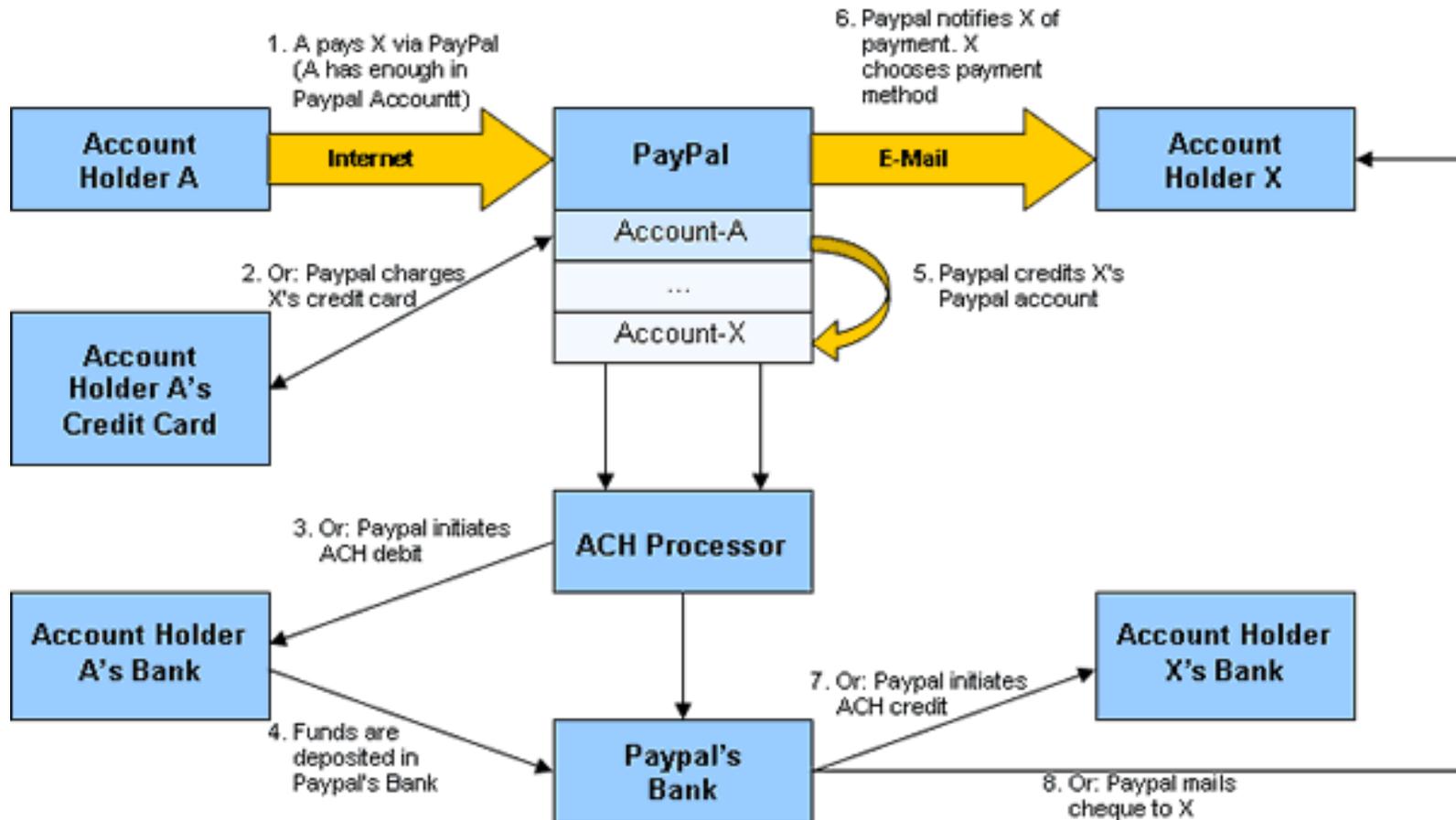


# Merchant App



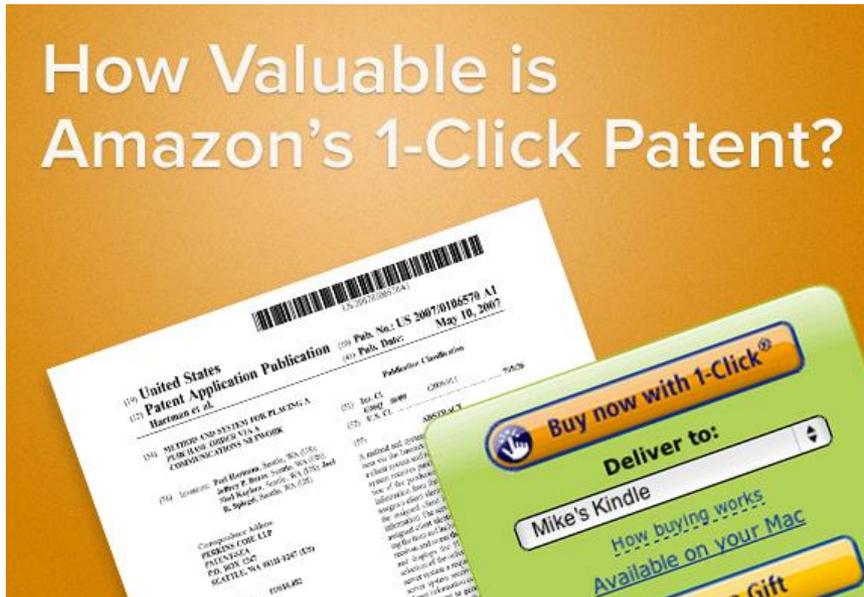


# Operational Model



# amazon.com® 1-Click® & Mobile Wallet

How Valuable is Amazon's 1-Click Patent?



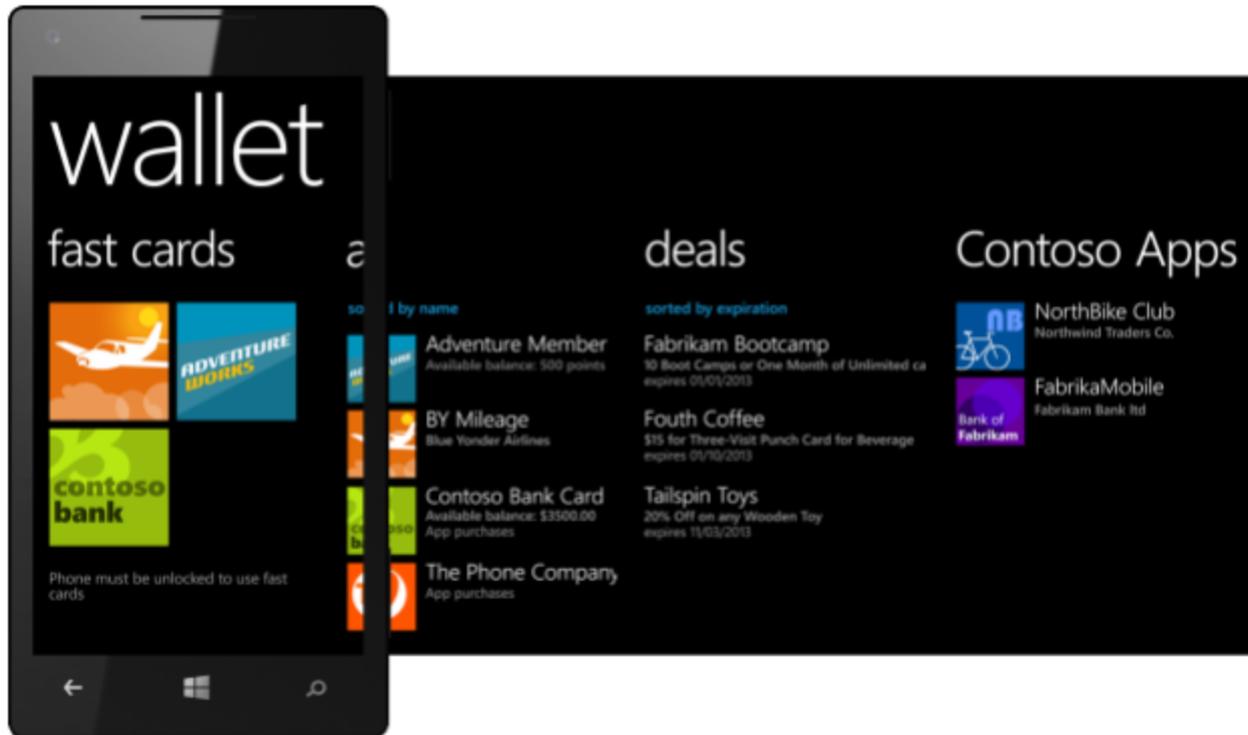


# Google wallet





# Microsoft Wallet



# Apple Pay



The World of Emerging Payment Systems

**NEXT GEN E-COMMERCE:  
REDEFINING “PAYMENT” & “MONEY”**

# Multi-Factor Authentication



**Something  
you know.**

+



**Something  
you have.**

+



**Who you  
are.**

+



**Where  
you are.**

---

**FFIEC Guidance**

**Authentication in an Internet Banking Environment**

**FIL-103-2005**

**October 12, 2005**

# Symmetric v. Asymmetric Encryption

**Encryption** is the process of encoding messages or information in such a way that only authorized parties can read it. This does not of itself prevent interception, but denies the message content to a would-be hacker.

**Plaintext** is encrypted using an encryption algorithm, generating **ciphertext** that can only be read if decrypted.

**Advanced Encryption Standard (AES)** is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES employs **symmetric-key algorithms**, which uses the same keys for both **encryption of plaintext** and **decryption of ciphertext**. The keys represent a shared secret between two or more parties that can be used to maintain a private link. The requirement that both parties have access to the same secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key cryptography.

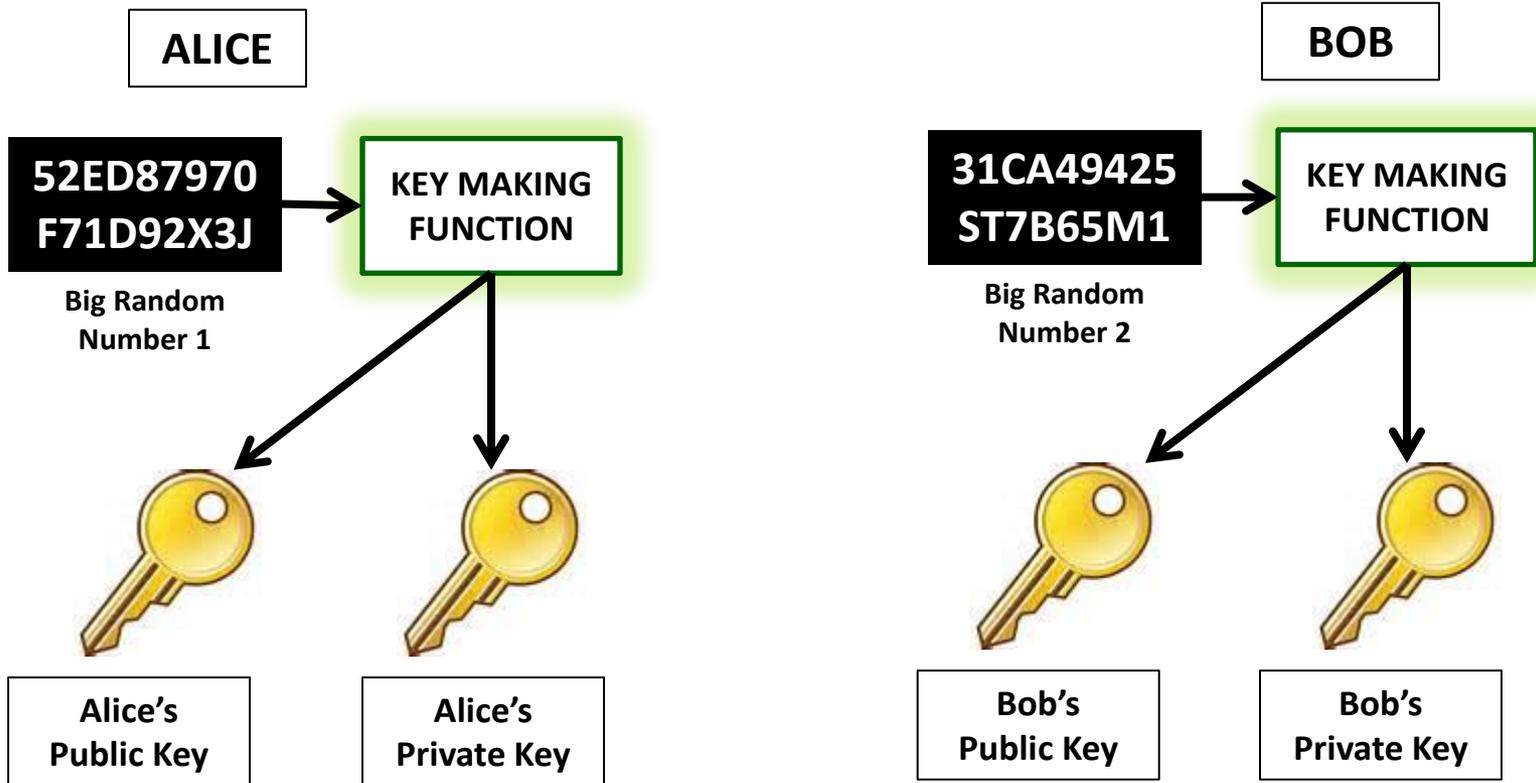
**Public-key cryptography**, also known as **asymmetric-key cryptography**, requires two separate keys, one of which is **secret** (or **private**) and one of which is **public**. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt ciphertext or to create a digital signature. The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other.

# Certification Authority

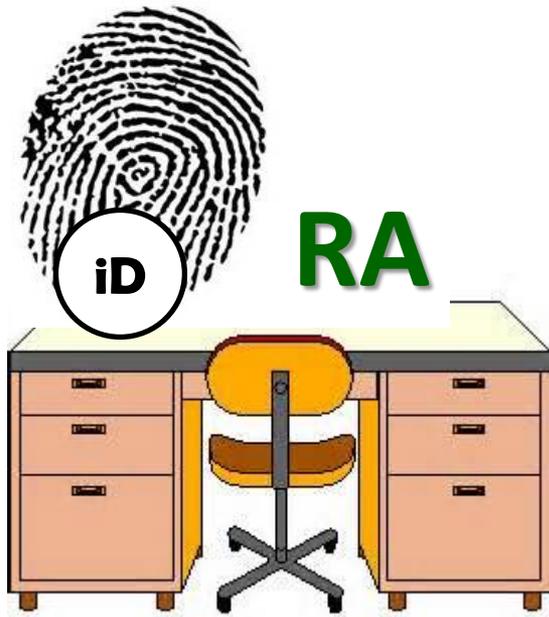
- A ***certificate authority*** issues a digital signature certificate containing a public key and a private key.



# Paired Key Encryption



# Registration Authority



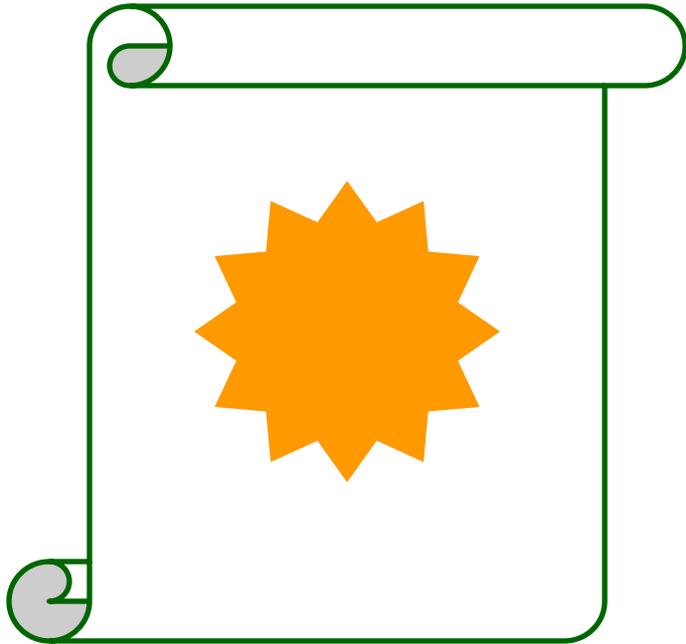
- A ***registration authority*** verifies the identity of users at the request of a certification authority.

# Public Key Repository

- A verification authority or *public key repository*— a secure location in which to store and index keys and which a recipient of a digital signature can verify and rely upon the identity of the sender.



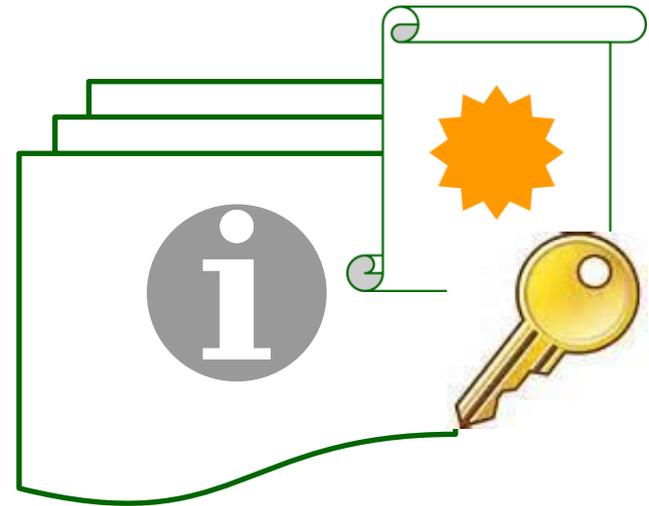
# Digital Signature Certificate



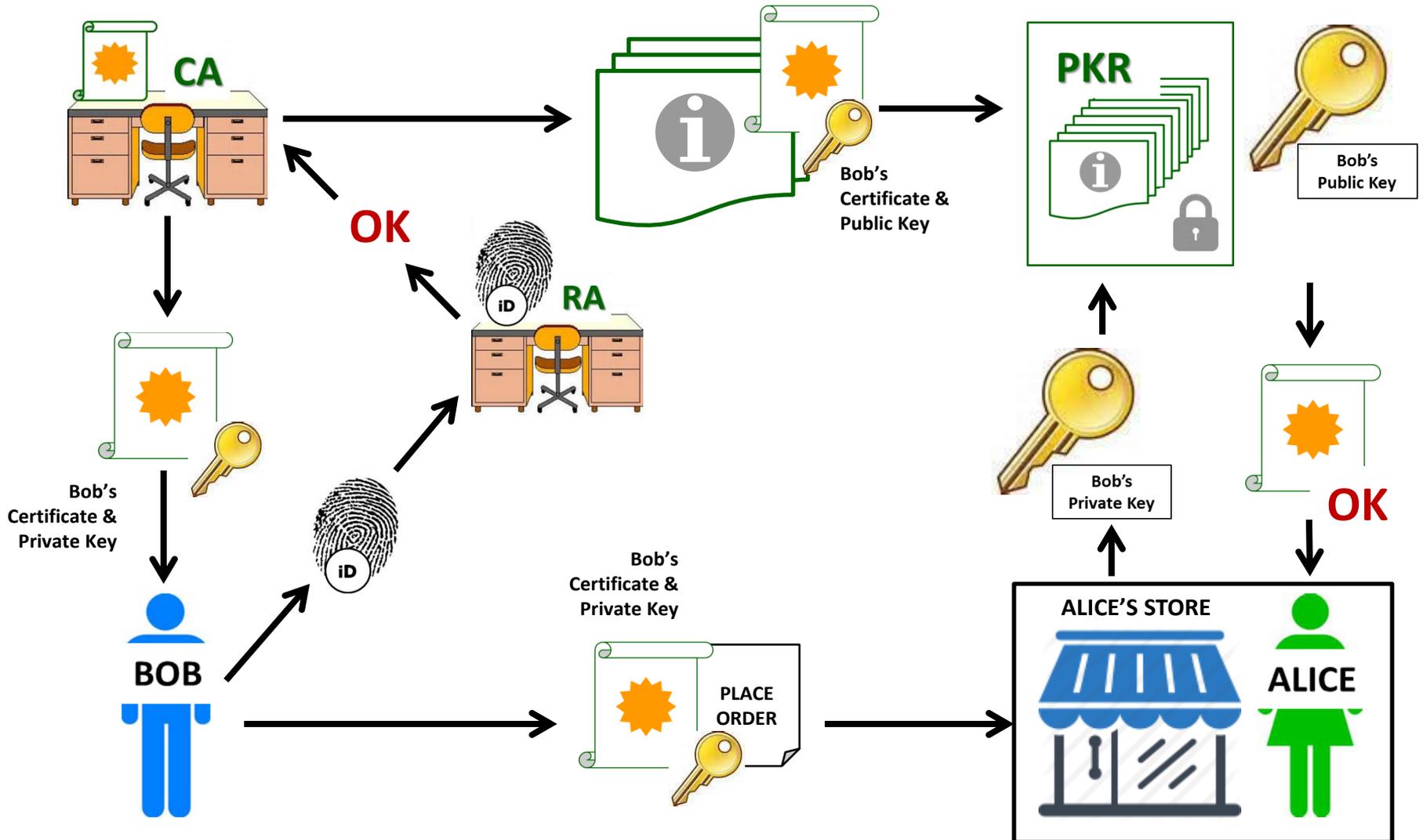
- A ***digital signature certificate***, which authorizes use of a ***private key*** and often contains a policy which sets forth what the user and recipient of a digital signature may rely upon.

# Storing the Certificate

- The information about the digital signature certificate containing the *public key* is then transmitted to the public key repository for safekeeping and for access by recipients of digital signatures.



# Model of a Public Key Infrastructure



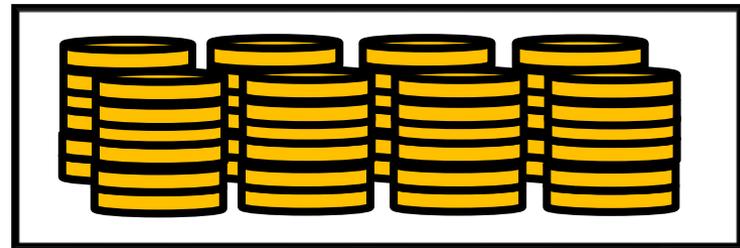
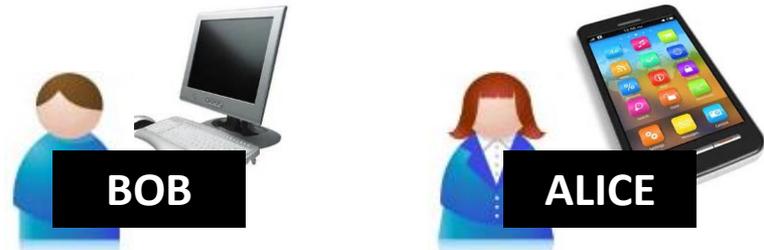
# Bitcoin



- Bitcoin was supposedly invented by **Satoshi Nakamoto**, who published his invention in 2008 and released it as open-source software in 2009.
- The system is **peer-to-peer**.
- The theory is that users can transact directly **without needing an intermediary** to establish trust and non-repudiation.

# Wallets & Addresses

- Bob and Alice both have **Bitcoin wallets** on their computer or smartphone.
- Wallets are files that provide access to multiple **Bitcoin addresses**.
- An address is a **string of letters and numbers**.
- Each address has its own balance of Bitcoins.



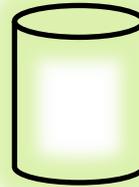
# How Does a Bitcoin Transaction Work?

## WALLETS & DEVICES



Bob and Alice both have Bitcoin wallets on their computers or devices.

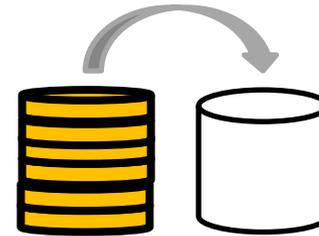
## CREATING A NEW ADDRESS



Alice creates a new Bitcoin address for Bob to send his payment to.

## SUBMITTING A PAYMENT

Bob tells his Bitcoin client that he would like to transfer the purchase amount to Alice's address.



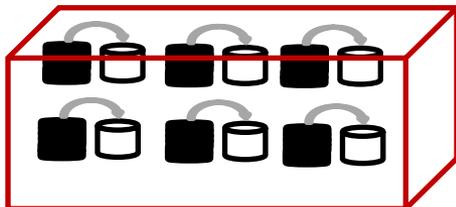
## VERIFYING THE TRANSACTION

Their computers bundle the past 10 minutes into a new "transaction block."



Their computers are set up to calculate **cryptographic hash functions**.

**Bitcoin Miners**



# How Does a Bitcoin Transaction Work?

## VERIFYING THE TRANSACTION

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length called hash value. Even tiny changes in the original data drastically change the resulting hash value. And it is essentially impossible to predict which initial data set will create a specific hash value.

The end **is** near. ▶

1HULMwZEPkJEPv . . . .

The **end** is near. ▶

AFT12tkRk985Aht . . .

The end **is near**. ▶

4dnW05gSVk71dU . . .

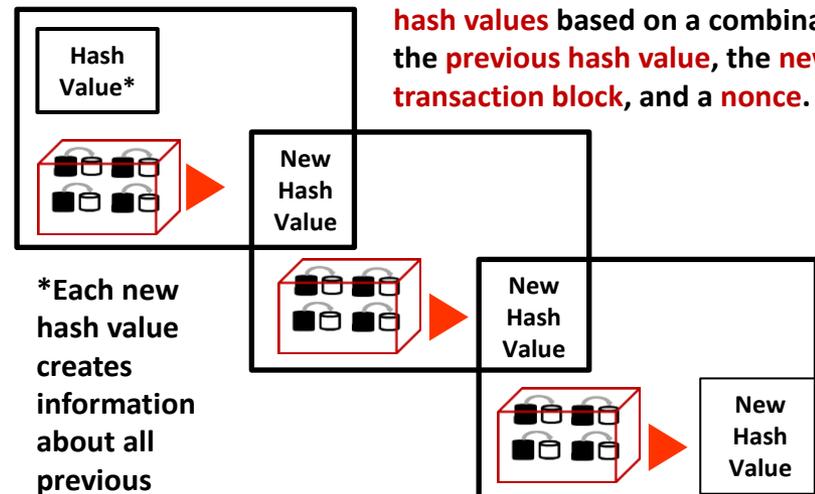
**Nonces:** To create different hash values from the same data, Bitcoin uses “nonces.” A nonce is just a random number that is added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The end is near ?????

0000 0000 0000 . . . . .

Creating hashes is computationally trivial, but the Bitcoin ecosystem requires that the new hash value have a particular form – specifically, it must start with a certain number of zeros.

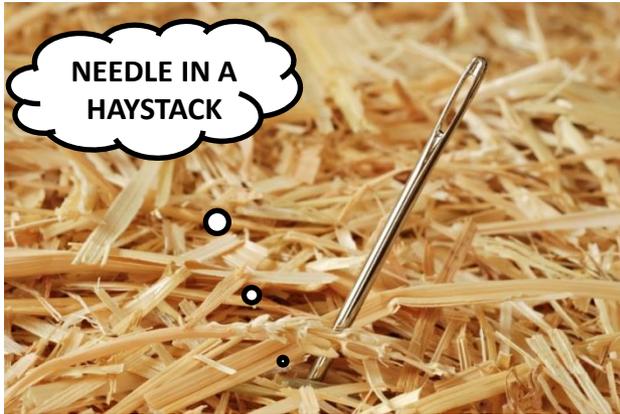
The mining computers calculate **new hash values** based on a combination the **previous hash value**, the **new transaction block**, and a **nonce**.



\*Each new hash value creates information about all previous Bitcoin transactions

# How Does a Bitcoin Transaction Work?

## VERIFYING THE TRANSACTION

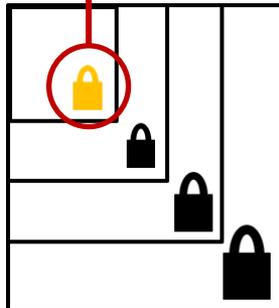


The miners – Huey, Louie, and Dooeey – have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they are forced to generate many hashes with different nonces until they happen upon one that works.



## TRANSACTION VERIFIED

As time goes on, Bob's transfer to Alice gets buried beneath other, more recent transactions. For anyone to modify the details, s/he would have to modify Louie's work – because any changes require a completely different winning nonce – and then redo the work of all the subsequent miners. Such a feat is nearly impossible.



Each block includes a "coinbase transaction" that pays out Bitcoins to the winning miner. A new address is created in Louie's wallet with a balance of newly minted Bitcoins.

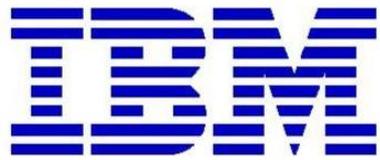


The World of Emerging Payment Systems

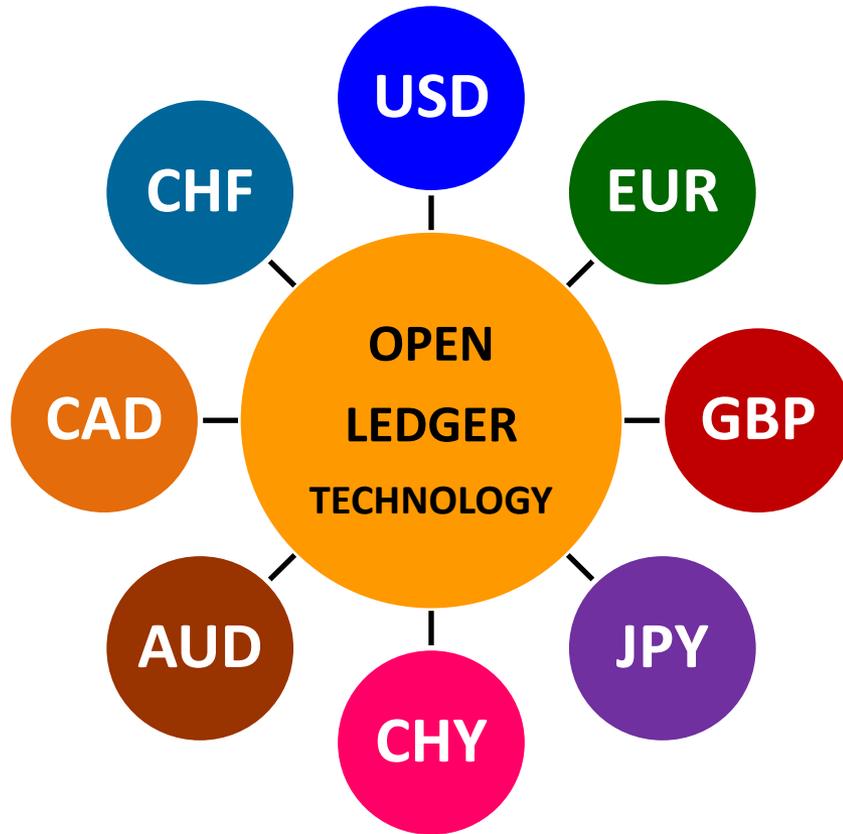
**WHAT LIES AHEAD**

# What Will Be the New Paradigm?



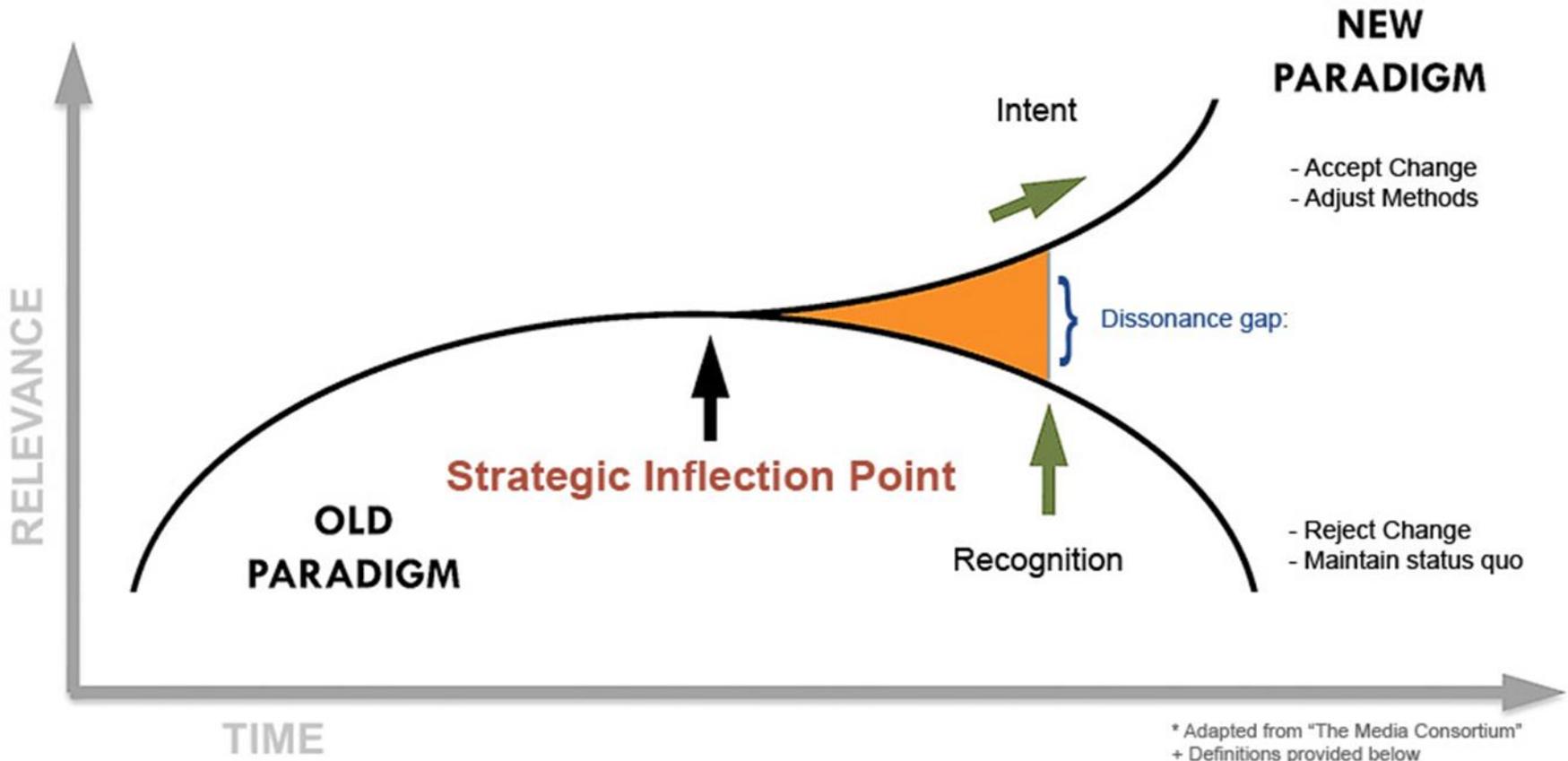


# to Adopt “Blockchain”

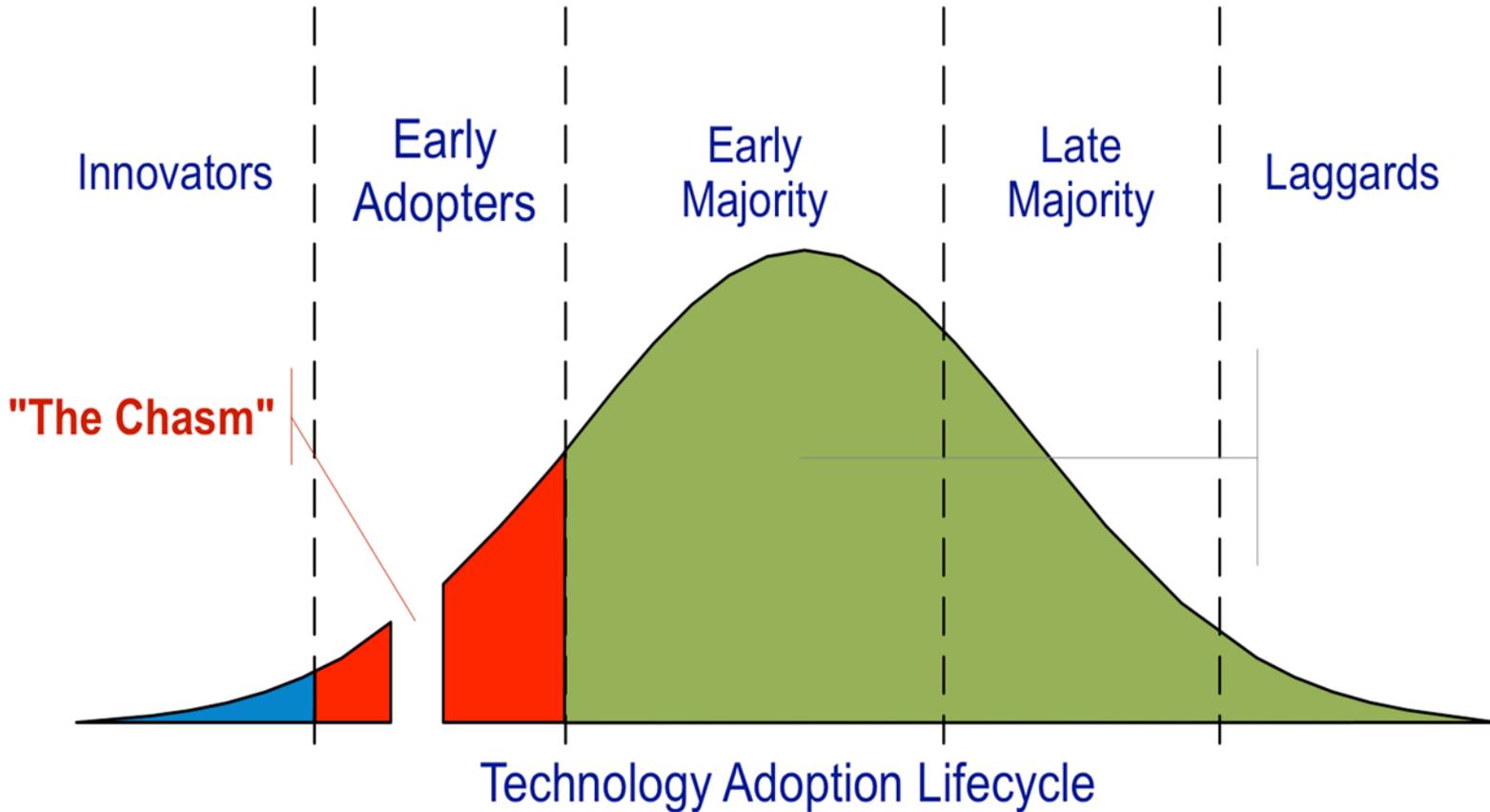


- IBM creating digital cash/payments system with Bitcoin technology – “Bitcoin without the Bitcoin.”
- Transfer cash or make payments instantaneously without a bank or clearing party.
- Unlike bitcoin, this digital currency system would be *controlled by central banks*.
- Linked to regular bank account using wallet software.

# We Are at an Inflection Point!



# Timing of Adoption?



# Contact Information

**Joseph M. Vincent**

**Director of Regulatory & Legal Affairs**

**Washington State Department of Financial Institutions**

**(360) 902-0516**

**[Joseph.vincent@dfi.wa.gov](mailto:Joseph.vincent@dfi.wa.gov)**