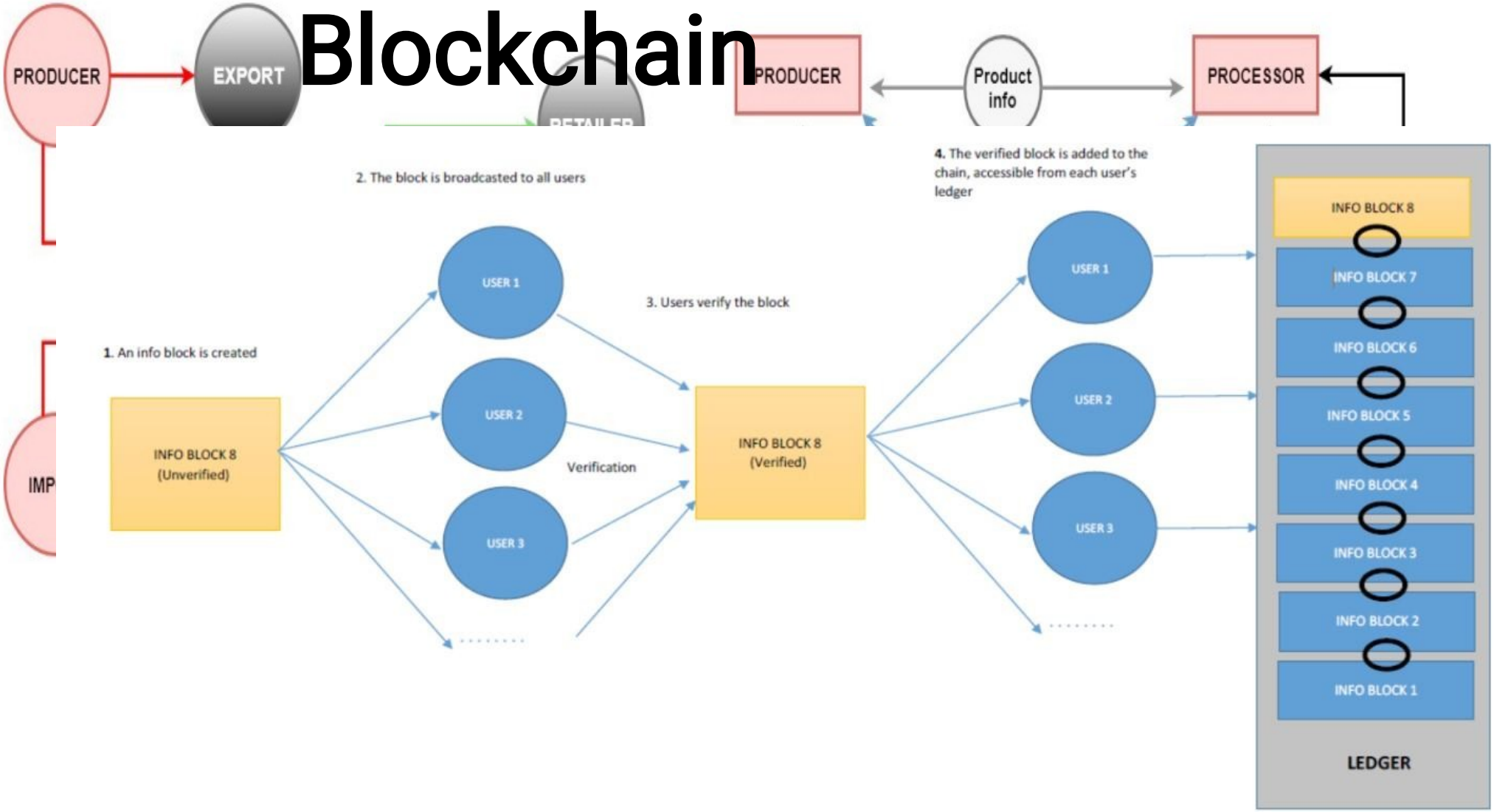
Common Class: Block Chain

How use of Blockchain can provide benefits to supply chain industry?

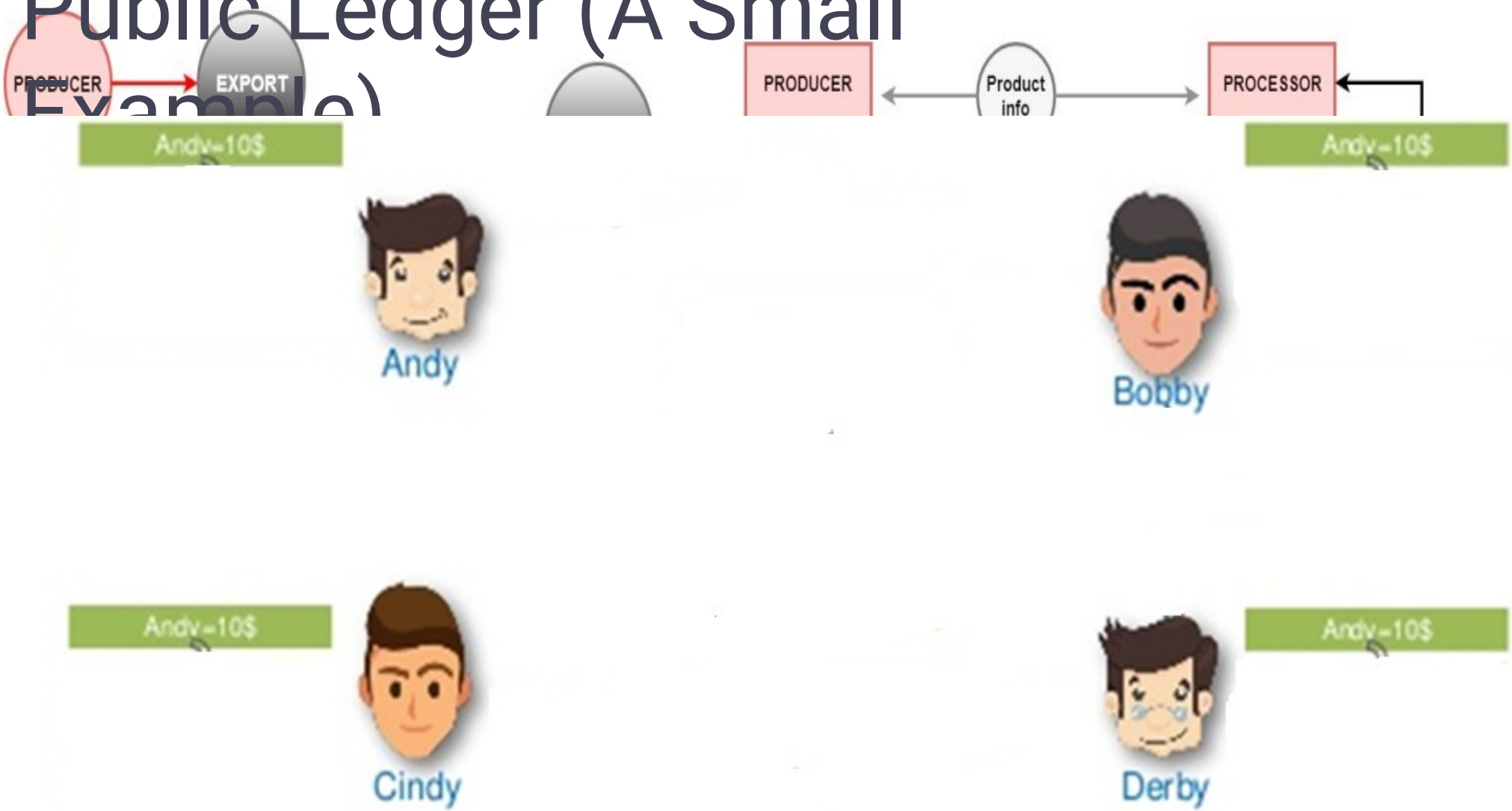
Blockchain



- Largely manual processing
- Regulatory compliance
- Reconciliation burden

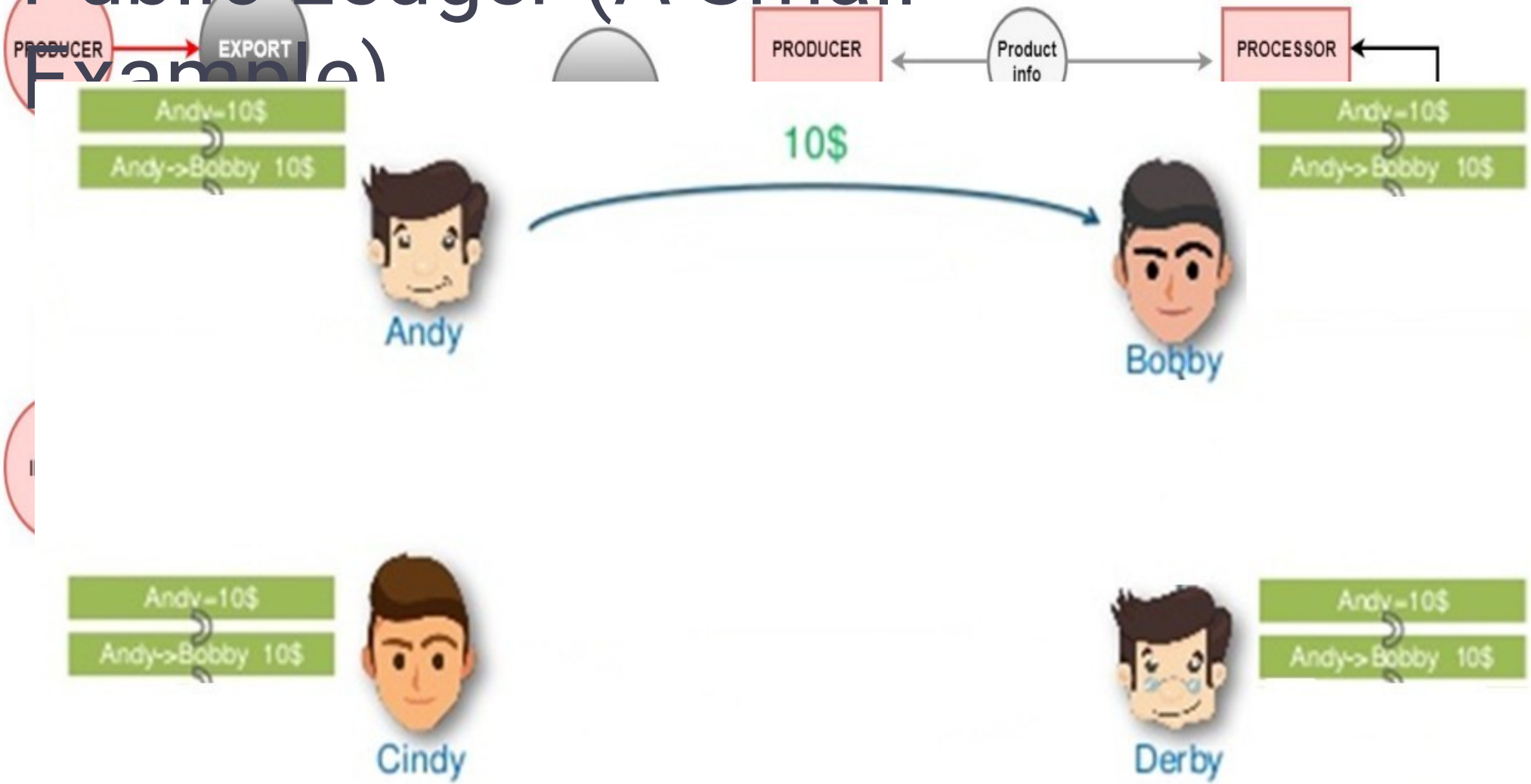
- Digitalized means quicker
- Tamper-proof data is easily verifiable
- Single shared source of truth

Public Ledger (A Small Example)



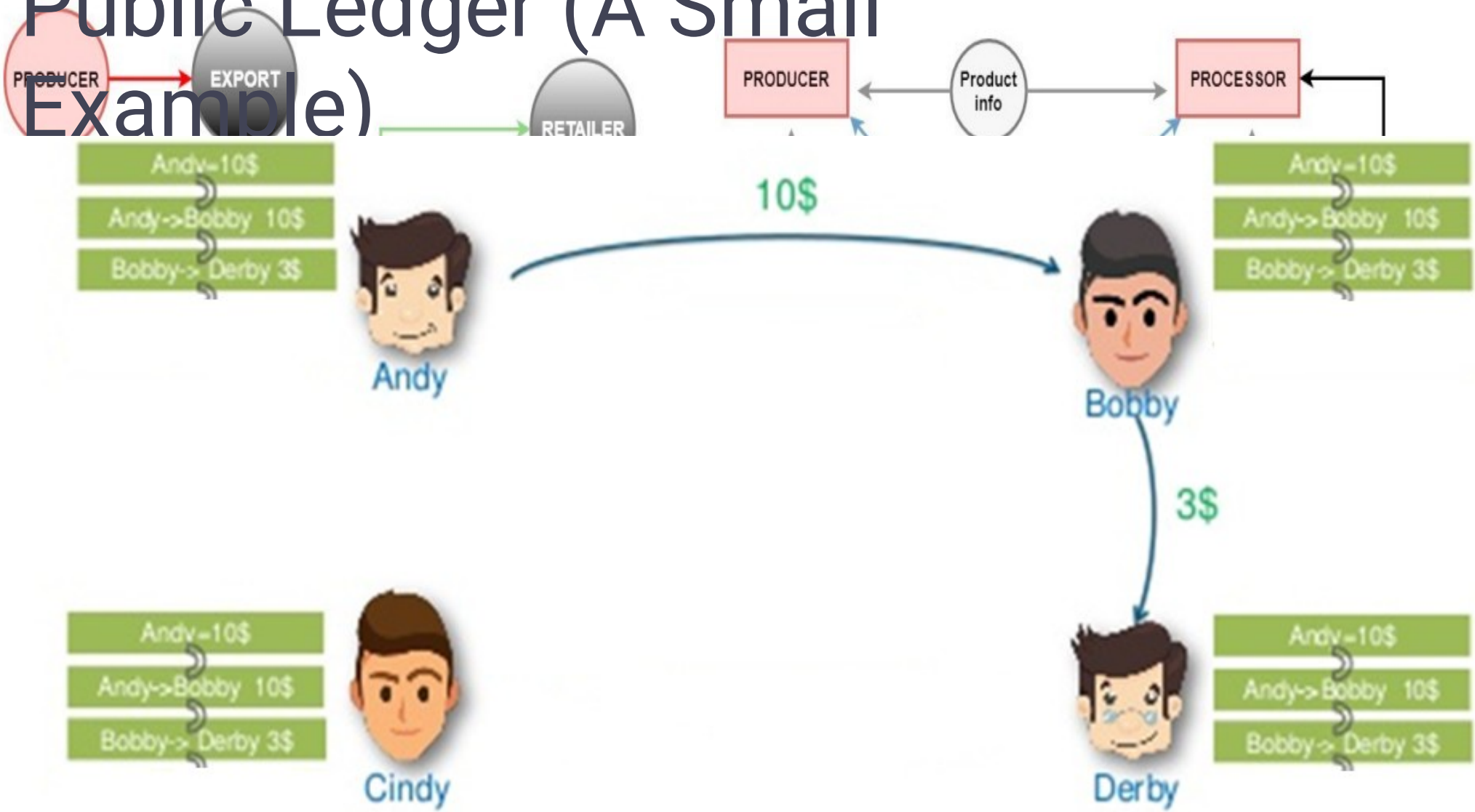
Lack of responsiveness	Near real-time
Largely manual processing	Digitalized means quicker
Regulatory compliance	Tamper-proof data is easily verifiable
Reconciliation burden	Single shared source of truth

Public Ledger (A Small Example)

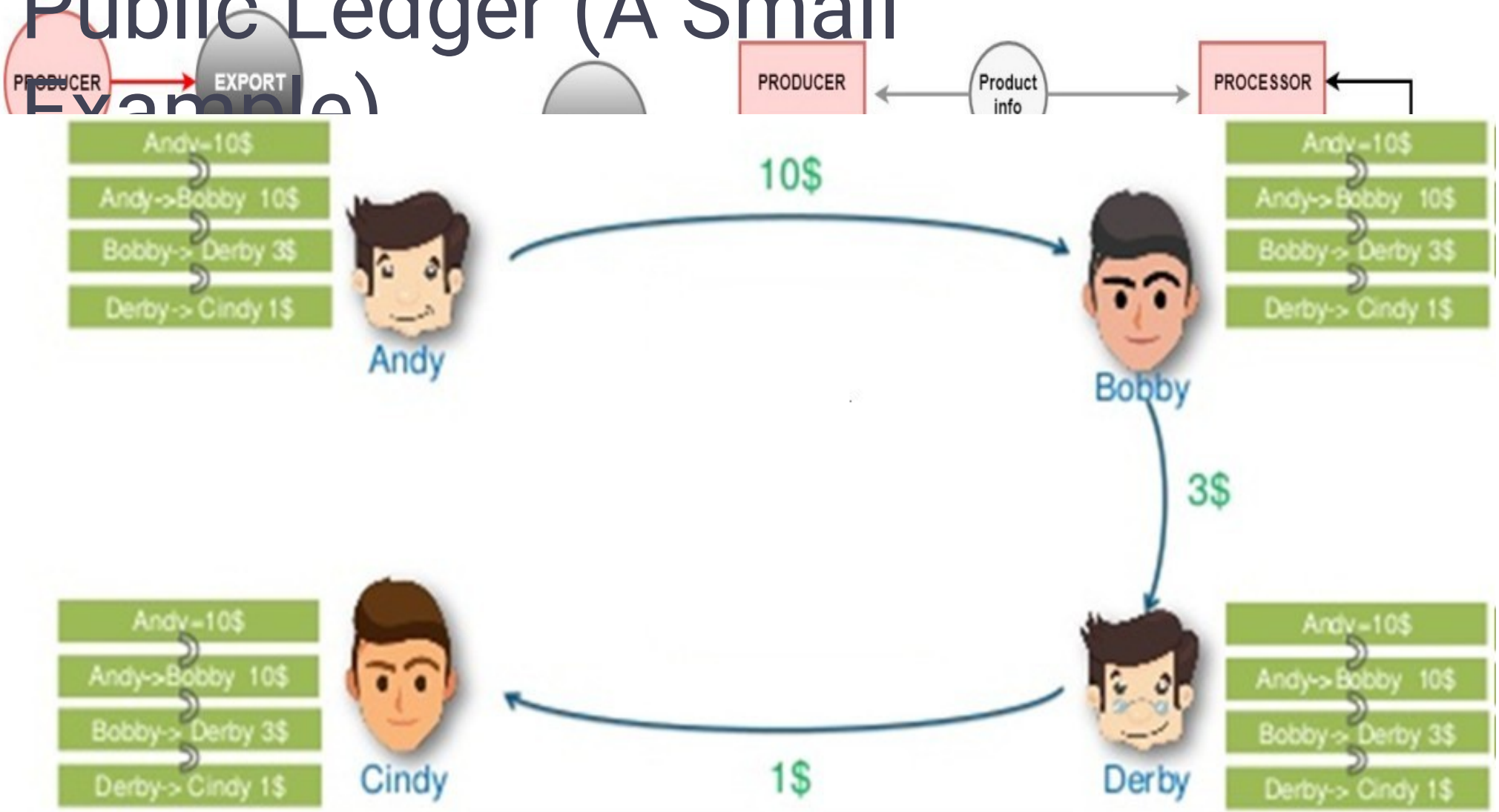


Lack of responsiveness	Near real-time
Largely manual processing	Digitalized means quicker
Regulatory compliance	Tamper-proof data is easily verifiable
Reconciliation burden	Single shared source of truth

Public Ledger (A Small Example)

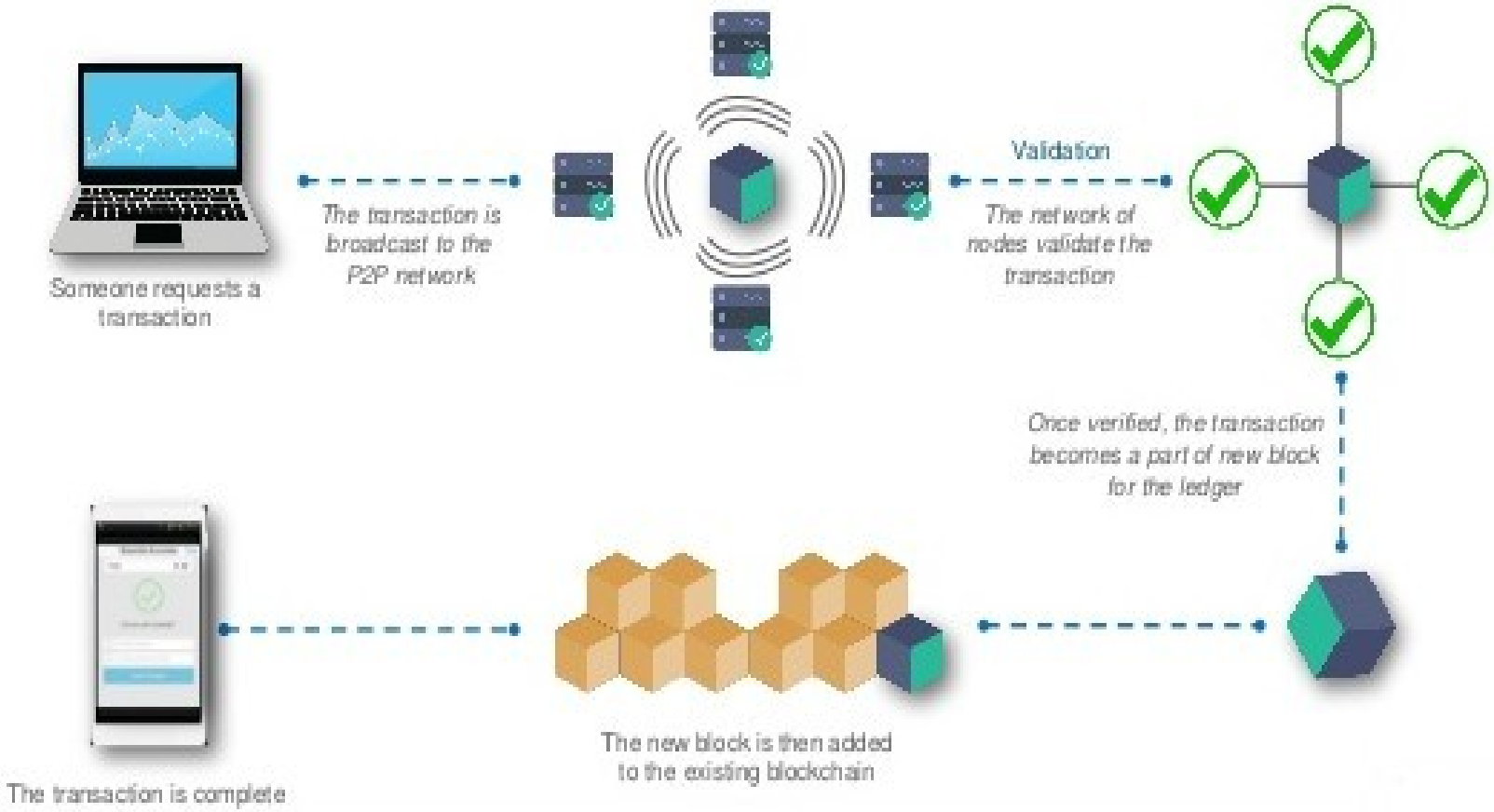


Public Ledger (A Small Example)



Lack of responsiveness	Near real-time
Largely manual processing	Digitalized means quicker
Regulatory compliance	Tamper-proof data is easily verifiable
Reconciliation burden	Single shared source of truth

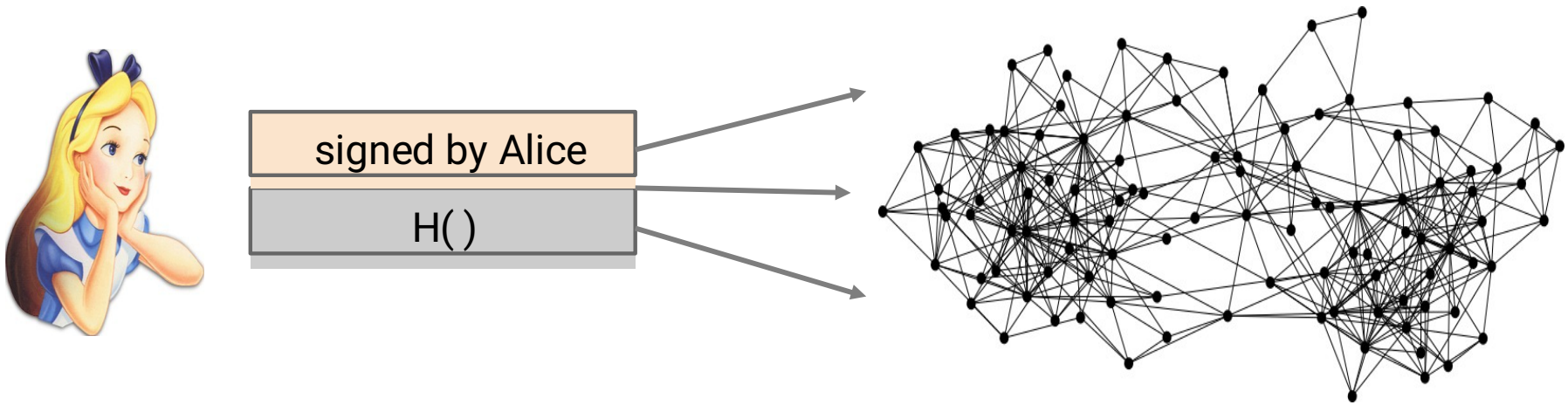
How Blockchain Works?



Block chain example: peer-to-peer system

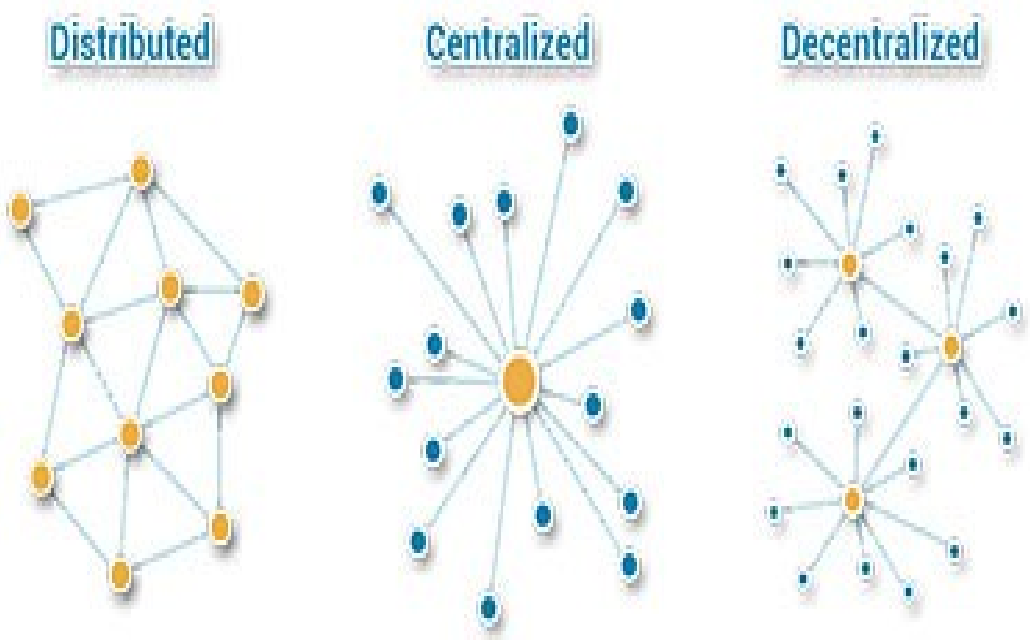
When Alice wants to perform an action

she broadcasts the action information as a transaction to all nodes in the networks



Block Chain in SCM

-
-
-



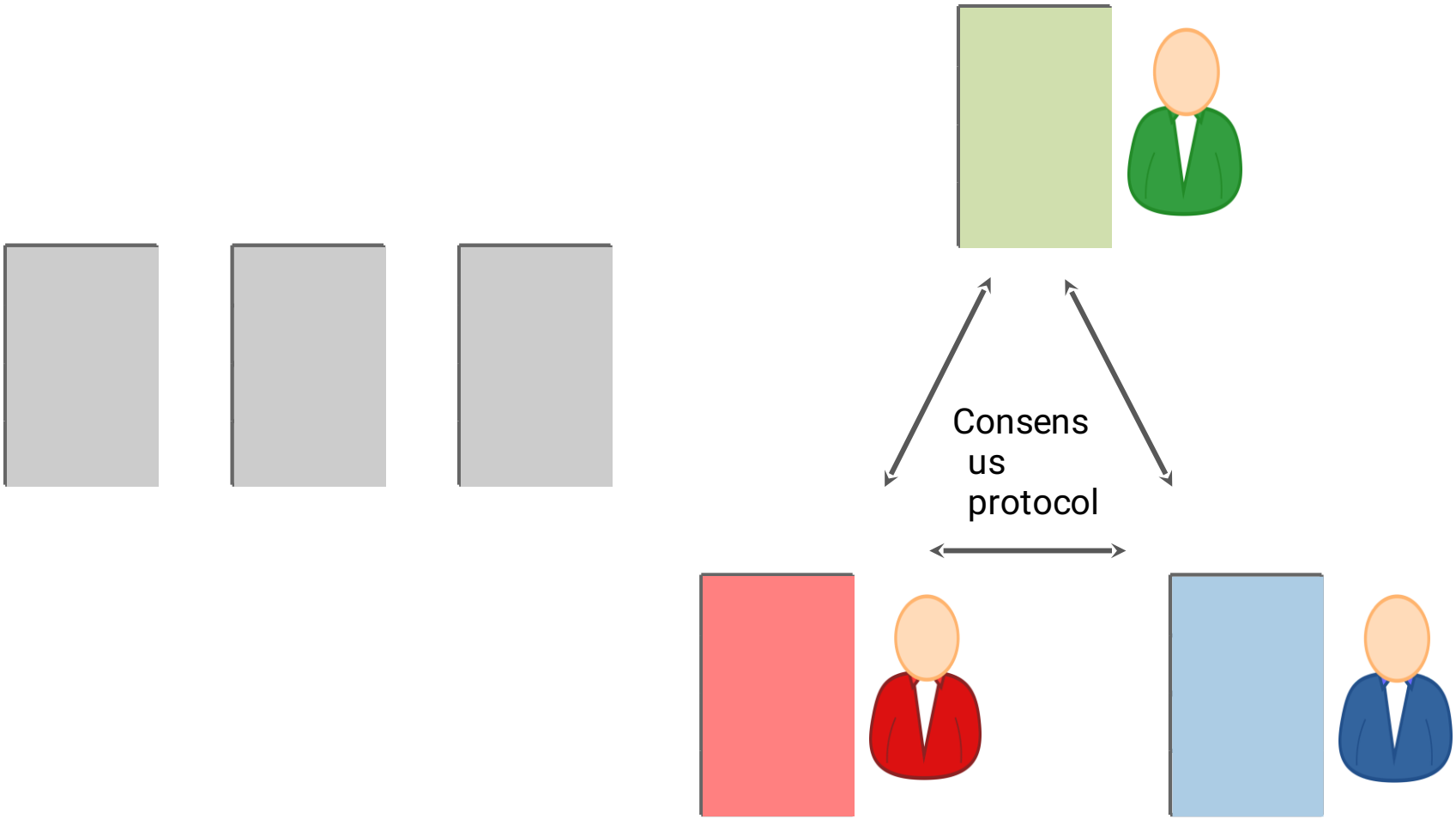
How consensus could work

At any given time:

- All nodes have a sequence of blocks of transactions they've reached consensus on

- Each node has a set of outstanding transactions it's heard about

How consensus could work



Why consensus is hard

Nodes may crash
Nodes may be malicious

Network is imperfect

- Not all pairs of nodes connected
- Faults in network
- Latency

No notion of global time

Features and advantages

Features and advantages

How the Blockchain helps Supply Chain industry

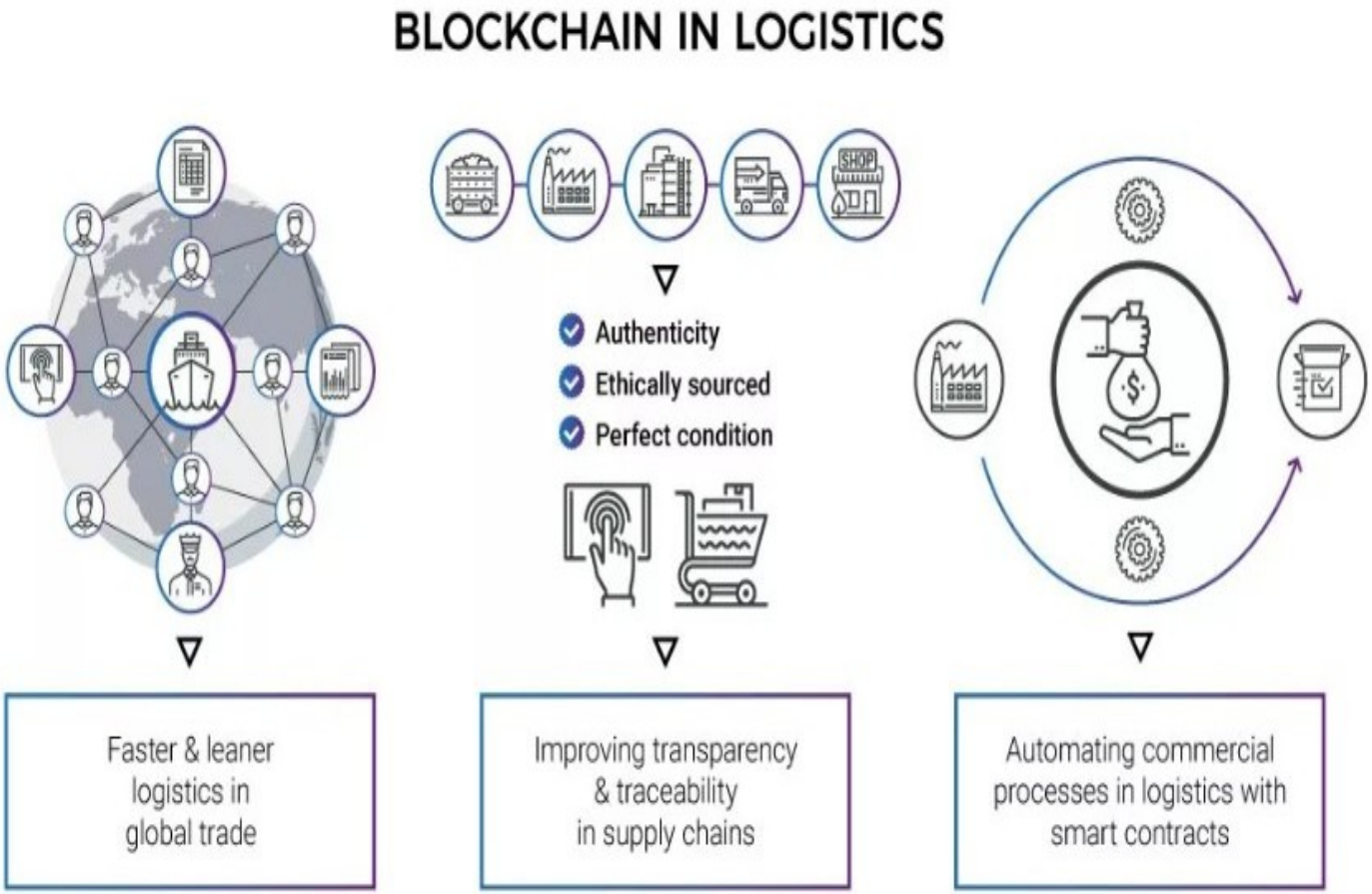
Recommendation

Recommendation

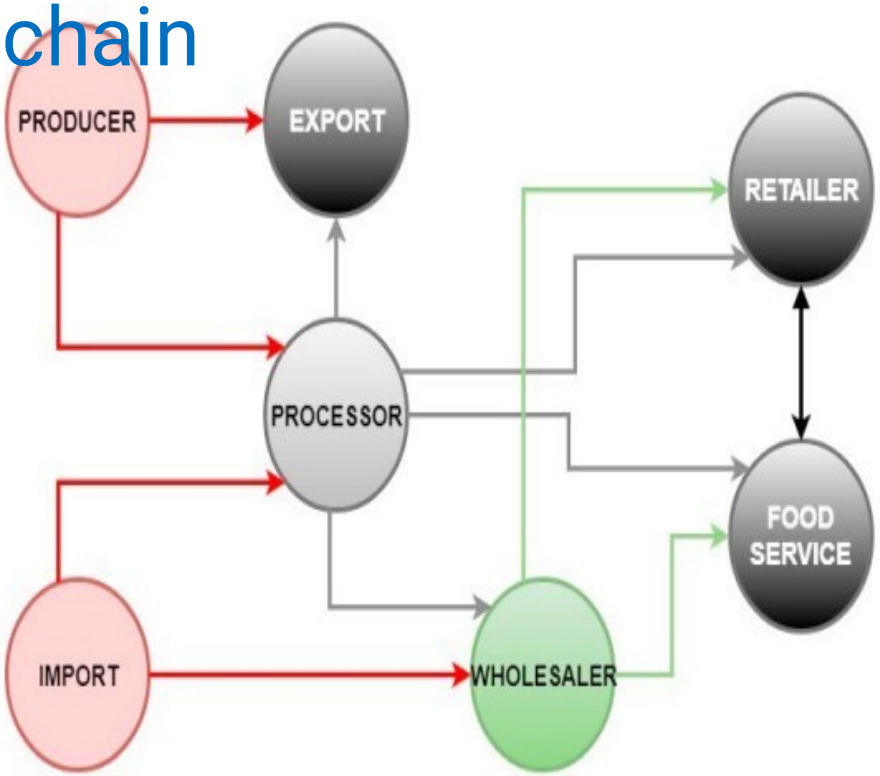
Conclusion

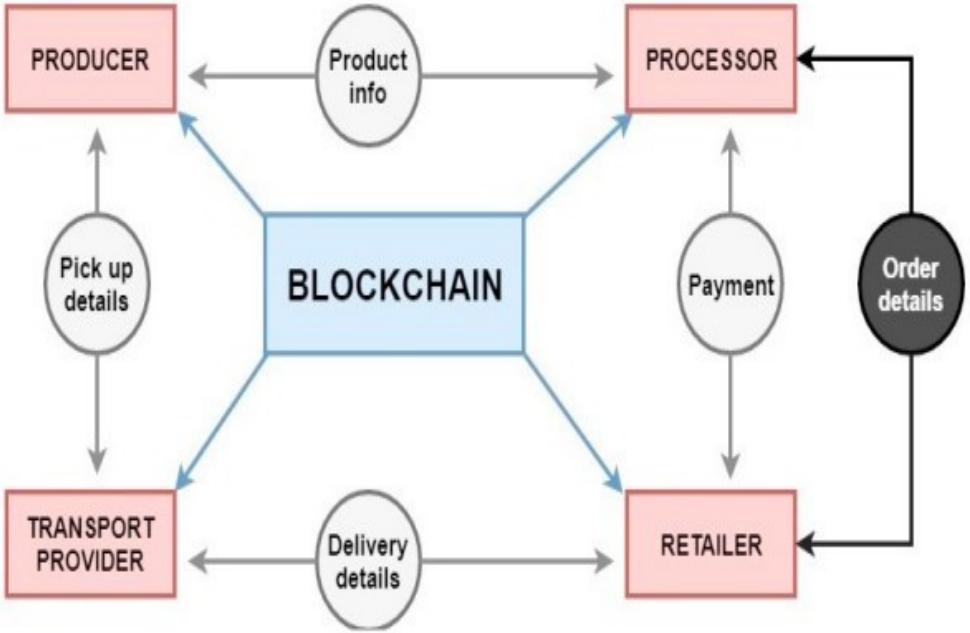
Block Chain in Logistics

According to the World Economic Forum, reducing supply chain barriers could increase global gross domestic product (GDP) by nearly 5% and global trade by 15%.



Traditional Methods challenges addressed by Block chain





Issues with traditional supply chains

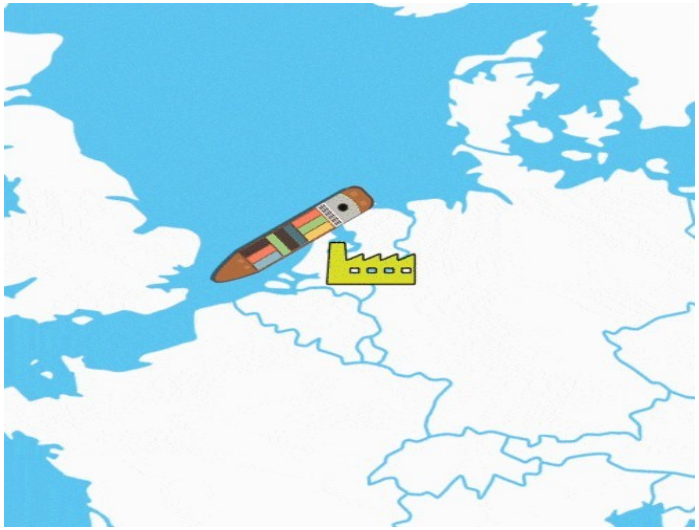
- Lack of traceability
- Risks involved with multiple stakeholders
- Lack of responsiveness
- Largely manual processing
- Regulatory compliance
- Reconciliation burden

How blockchain could address these problems

- Audit trail for all transactions
- Immutable - secure against undesired changes
- Near real-time
- Digitalized means quicker
- Tamper-proof data is easily verifiable
- Single shared source of truth

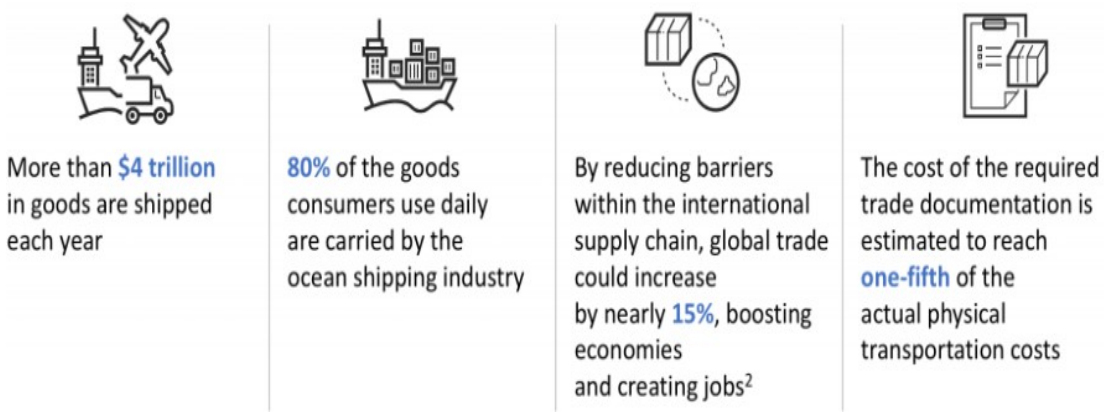
Case Study of Maersk and IBM

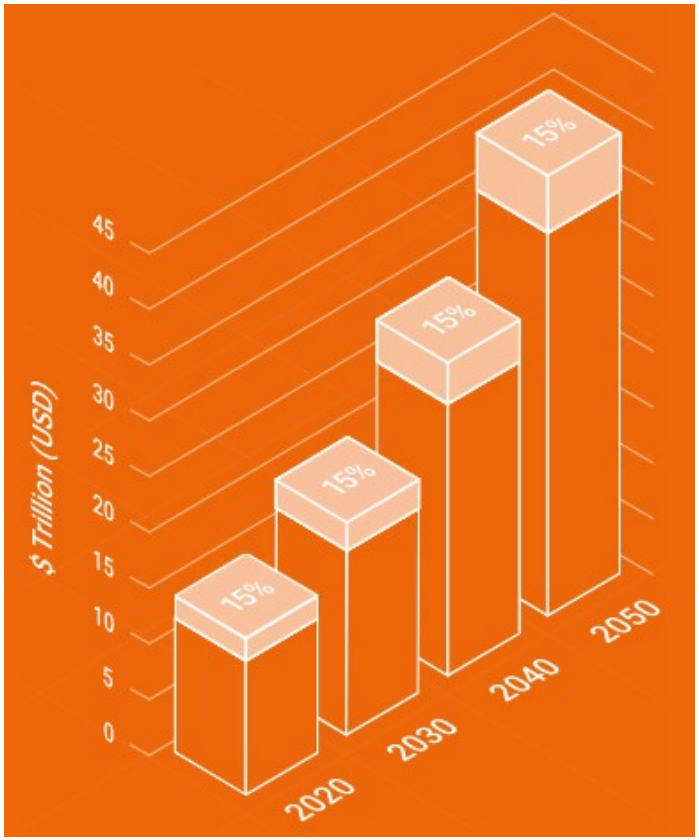
Both companies intended to develop the fully integrated secure and efficient system using block chain technology.



Current industry challenges

Current global trade at USD $1.8 trillion annually with potential savings from more efficient process of ~10%.





Present situation In Maersk: Highly inefficient and burdened by paper- based processes

Complex, cumbers ome

Inconsis tent, Blind

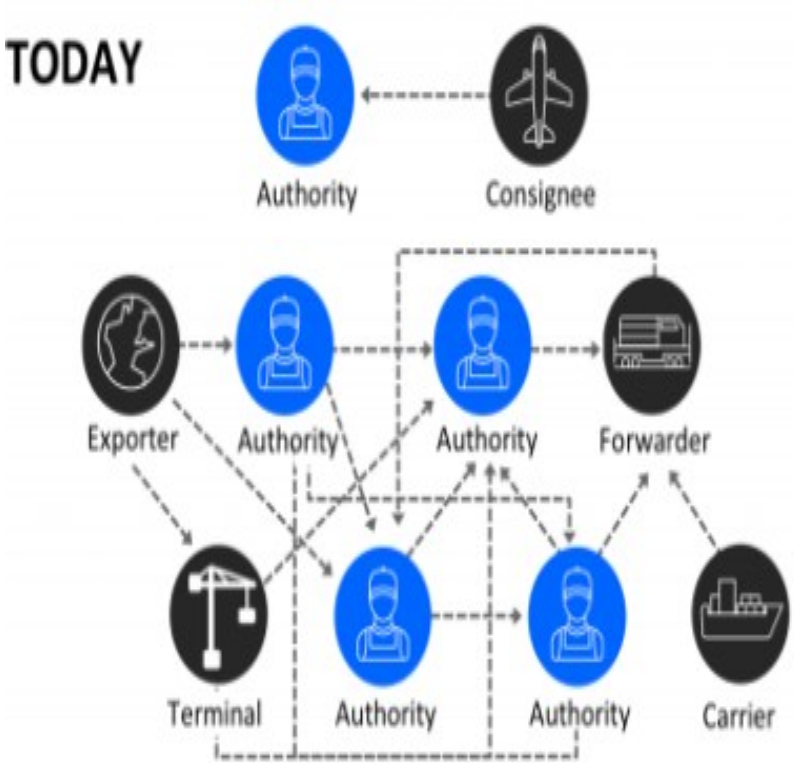
Manual, Time-consumin

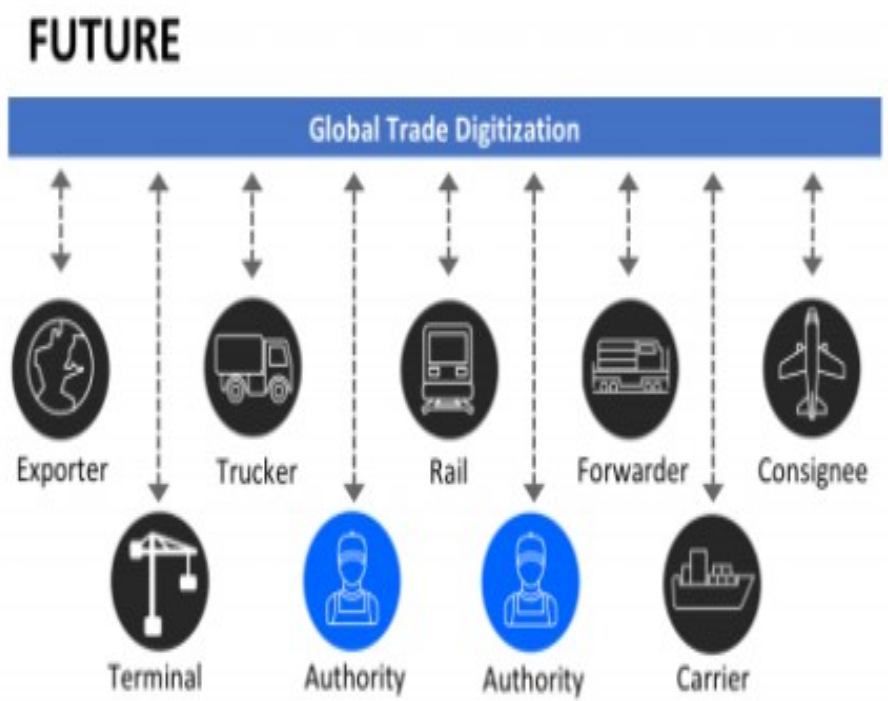
Fast, Secure ccess

Single source of the Truth

Trusted cross organizational workflows

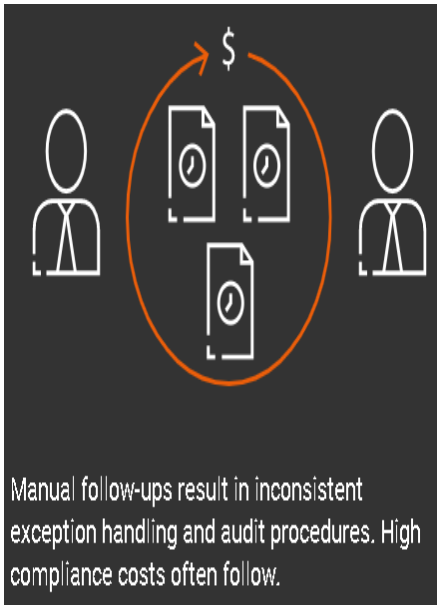
Better Risk assessment





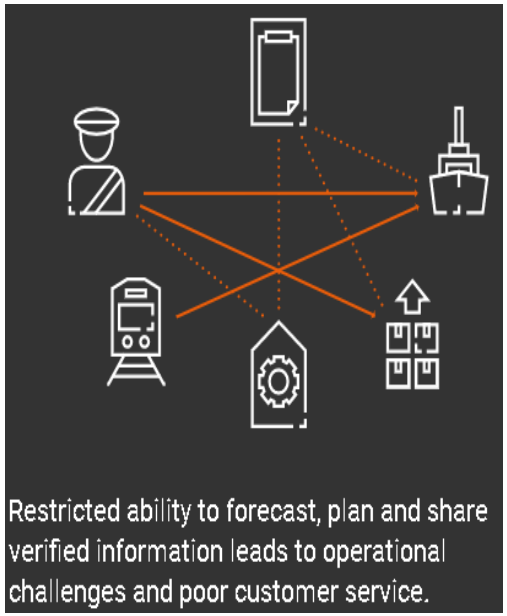
Challenges with global trade

Data is Trapped in organizational Silos



Time consuming Processes

Custom clearance is time consuming and not transparent



Operational Complexity and costly

Maersk and IBM Actors considered in framework

Ports and Terminals	**Provide** information about the disposition of shipments within the boundaries of the port / terminal **Benefit from** pre-built connections to shipping lines and other actors, end-to-end visibility across shipping corridors, and real-time access to more information to enrich port collaboration and improve terminal planning
Ocean Carriers	**Provide** information about the disposition of shipments across the ocean leg **Benefit from** pre-built connections to customers and ports / terminals around the world and real-time access to end-to-end supply chain events
Customs Authorities	**Provide** information about the export and import clearance status for shipments into and out of the country **Benefit from** more informed risk assessments, better information sharing, less manual paperwork, and easier connections to national single window platforms
Freight Forwarders / 3PL	**Provide** the transportation plan, inland transportation events, information on intermodal handoffs, and document filings **Benefit from** pre-built connections to the ecosystem, improved tools for customs clearance brokerage function, and real-time access to the end-to-end supply chain data to improve effectiveness of track-and-trace tools
Intermodal Transport	**Provide** information on the disposition of shipments carried on trucks, rail, barges, etc. **Benefit from** improved planning and utilization of assets (e.g., less queuing) given real-time access to end-to-end supply chain events for shipments
Shippers	**Engage** with the solution as a consumer of the shipping information events and paperless trade capabilities **Benefit from** a streamlined and improved supply chain allowing for greater predictability, early notification of issues, full transparency to validate fees and surcharges, and less safety stock inventory

Benefits to actors(shippers/cargo owners)

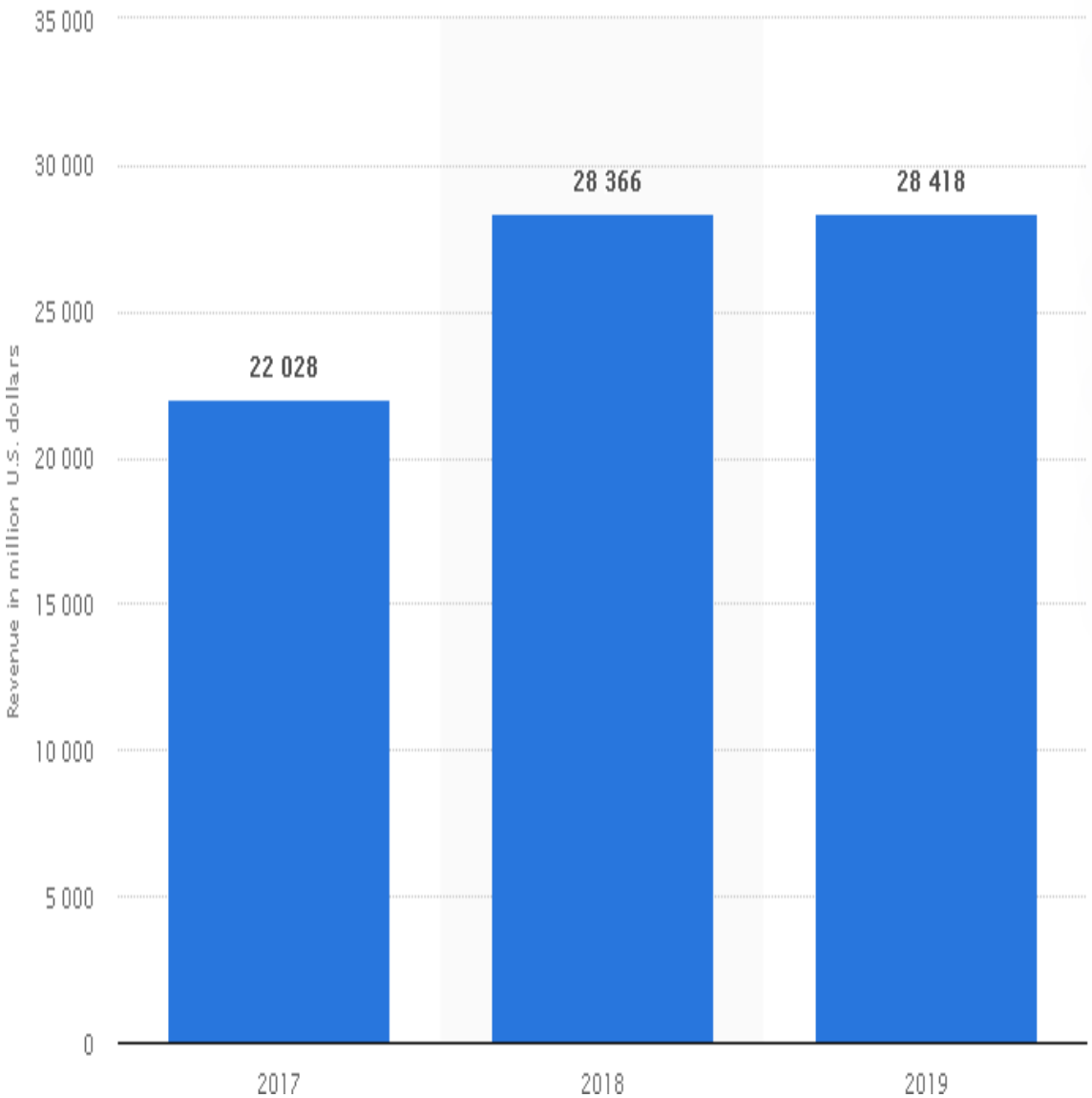
Problems	Solutons
Excessive capital tied up in inventory	Reduces the need to maintain safety stock by providing greater visibility and predictability in the supply chain
High administrative costs for managing supply chain transactions	Eliminates manual processes
Lack of trust regarding the fees on freight invoices	Full, trusted visibility on the end-to-end journey of a shipment
High IT costs for integrating with service providers	Single, standards-based publish/subscribe interface for obtaining visibility data
High compliance costs for international trade transactions	Eliminates the need to hand-carry physical paper forms to obtain stamps
Border delays due to lost/ erroneous paperwork	Improves document turnaround times
High costs charged by customs brokers and freight forwarders for clearance services	Simplified process and workflow-driven compliance policies

Financial benefits Maersk achieved using Block chain

Reduced cost of paper work: On an average the cost of paper work for international transport and clearance is about 15-20% of the cost of delivery. Using Block chain these costs were reduced by 70%-90% depending on the participating actors.

Reducing shipping time: Time were reduced by 40% from USA due to speeding workflow.

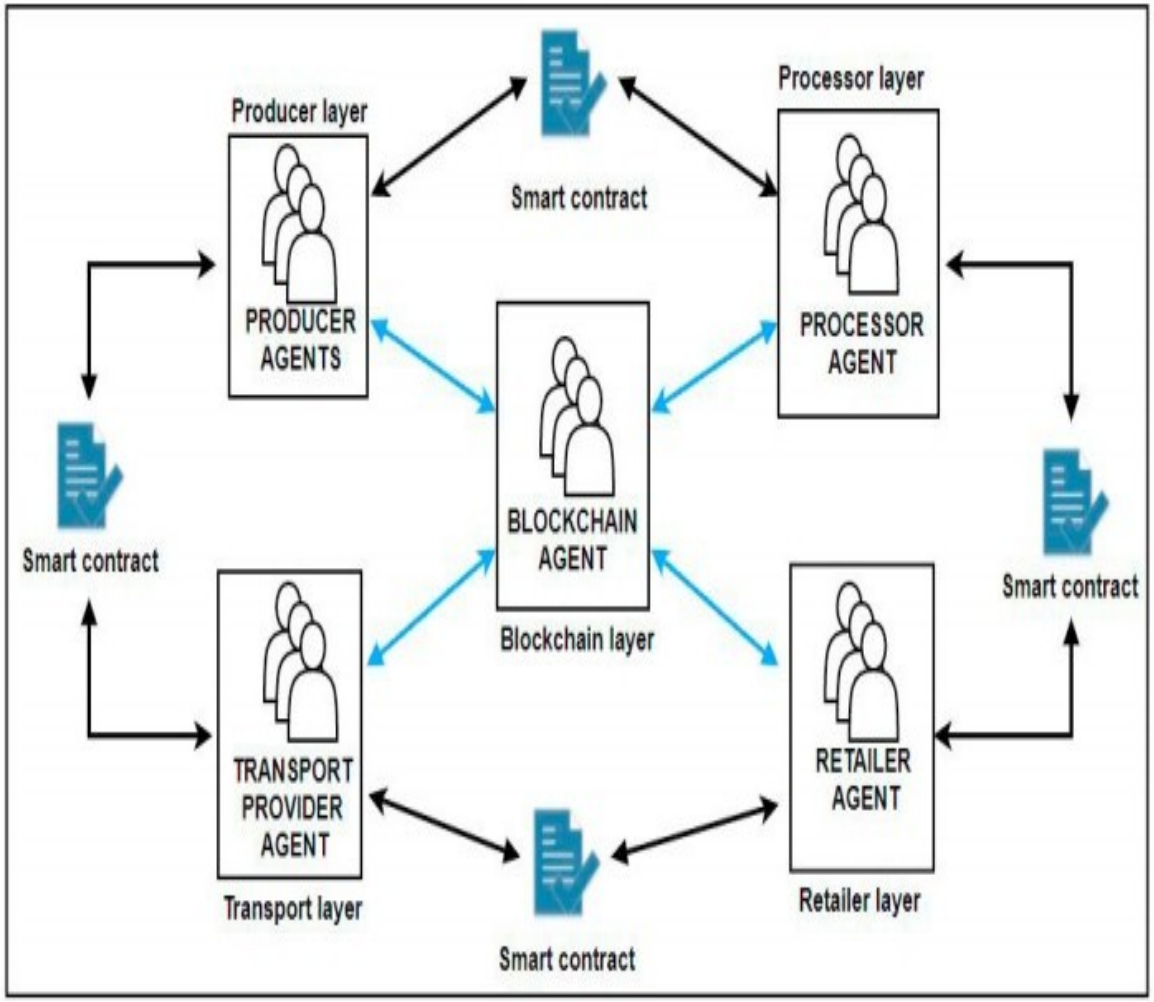
Reducton in number of steps: due to transparency of block chain technology the number of steps in operational question



Maersk's ocean segment revenue in FY 2017 and FY 2019 ("Maersk Ocean: revenue 2017-2019 | Statista", 2020)

How Block chain Disrupt the Supply Chain?

- Decentralization
- **Distributed ledger**
- Database stored in chronological order
- Immutability
- Accessibility
- **Security**
- **Transparency**
- Auditability
- Traceability
- Quick response time
- Smart contracts



How Block chain benefits the Supply Chain?

- Eliminates the fraud
- Quickens up the pace of tracking Improves
- inventory management Reduces the courier cost
- Lessens the paperwork
- Better monitoring of shipment

References

Cryptography

Yet it may roundly be asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.

EDGAR ALLAN POE, THE GOLD BUG

Learning Objectives

Upon completion of this material, you should be able to:

- Explain the basic principles of cryptography, both symmetric and asymmetric encryption (and one-way hashes)
- Describe the operating principles of the most popular tools in the area of cryptography
- List the major protocols and algorithms used for secure communications
- Discuss the nature and execution of the dominant methods of attack used against cryptosystems

Topics

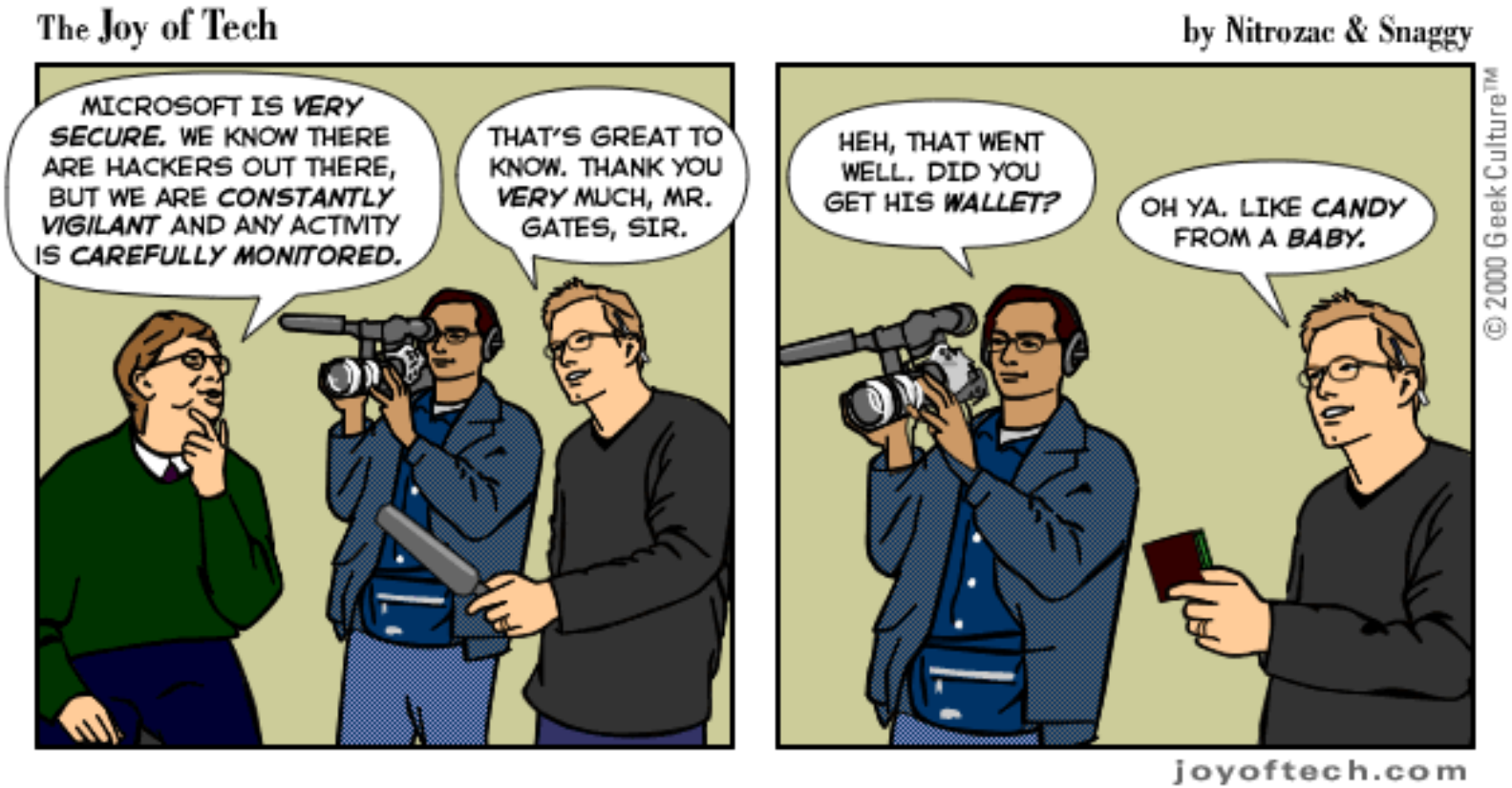
- Terminology
- Cipher types
  - Substitution ciphers
  - Transposition ciphers
  - Exclusive OR
  - Hash functions
- Encryption algorithms
  - Symmetric
  - Asymmetric
- Tools
  - Digital signatures, digital certificates, PKI (Public Key Infrastructure)
  - Diffie-Hellman
- Cryptanalysis

Introduction

- Cryptography: process of making and using codes for the secure transmission of information
- Encryption: converting original message (plaintext) into a form unreadable by unauthorized individuals (ciphertext).
- Decryption: converting the encrypted message into the original message using authorized information
- Cryptanalysis: process of an “adversary” obtaining original message from encrypted message with only partial information
- Cryptology: science of encryption; combines cryptography and cryptanalysis (AMTH 387)

Foundations of Cryptology

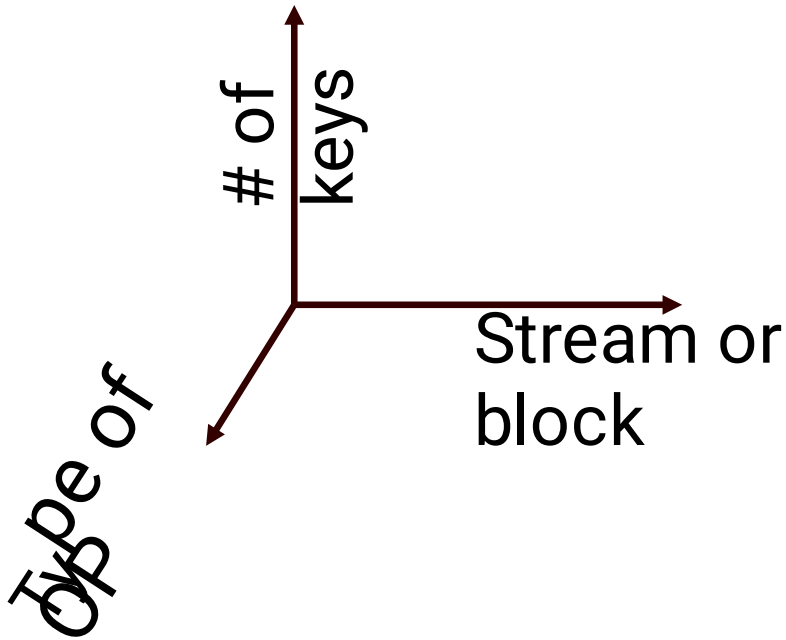
- Encryption is essential to securing digital data and modern ciphers are intended to be very hard to crack
- However, sometimes the biggest vulnerability is not what you expect.
  - What is the biggest vulnerability in E-Commerce?



Categorizing of Encryption

1. Plaintext can be encrypted through bit (or character) **stream** or **block** cipher method
   - Stream cipher: each plaintext bit transformed into cipher bit one bit at a time (or character by character)
   - Block cipher: message divided into blocks (e.g., sets of 32- or 128-bit blocks) and each is transformed into encrypted block of cipher bits using algorithm and key
2. Another category is number of keys – usually one or two (single or dual key / symmetric or asymmetric)
3. Third category: Type of operations – substitution, transposition, XOR (non-encrypting mathematical transforms, "proprietary method")

Encryption Methods



- Substitution – character, stream, shift forward by one to encrypt, shift back to decrypt
  - This is a test
  - Uijt jt b uftu

Cipher Methods

- Substitution cipher: substitute one value for another
  - Monoalphabetic substitution: uses only one alphabet for ciphertext Uijt jt
  - Polyalphabetic substitution: more advanced; uses two or more alphabets (sets of symbols)
  - Vigenère cipher: substitution cipher that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets
    Ujlw ..

TABLE 8-2 The Vigenère Square

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Cipher Methods (continued)

- Transposition cipher: rearranges values within a block to create ciphertext

this

isse cret

- Exclusive OR (XOR): function of Boolean algebra; two bits are compared (still used today)
  - If two bits are identical, result is binary 0
  - If two bits not identical, result is binary 1

TABLE 8-3 Exclusive OR Operations

Bit 1	Bit 2	Exclusive OR result
0	0	0
0	1	1
1	0	1
1	1	0

Network Reconnaissance Tool

eth0: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

Cryptographic Hash Functions

- Publically known mathematical algorithms that generate a fixed-length message summary/ digest used to confirm message identity and confirm no content has changed (for integrity)
- It is intended to be computationally infeasible to
  - generate a message that has a given hash
  - modify a message without changing the hash
  - find two different messages with the same hash
    - strong collision resistant property

Cryptographic Hash Functions

- Used in many password verification systems
- Use of keys not required; message authentication code (MAC – hash encrypted with symmetric key), may be attached to a message

- Examples:
  - md5 produces a 128 bit hash
  - SHA-1 produces a 160 bit hash

Strong collision vulnerabilities

Cryptographic Algorithms

- Often grouped into two broad categories, symmetric and asymmetric; today's popular cryptosystems use hybrid (encapsulated) combination of symmetric and asymmetric algorithms
- Symmetric and asymmetric algorithms distinguished by number and types (shared vs. public/private) of keys used for encryption and decryption operations
  - Symmetric is called 'secret key' or conventional cryptography
  - Asymmetric is called 'public key' cryptography

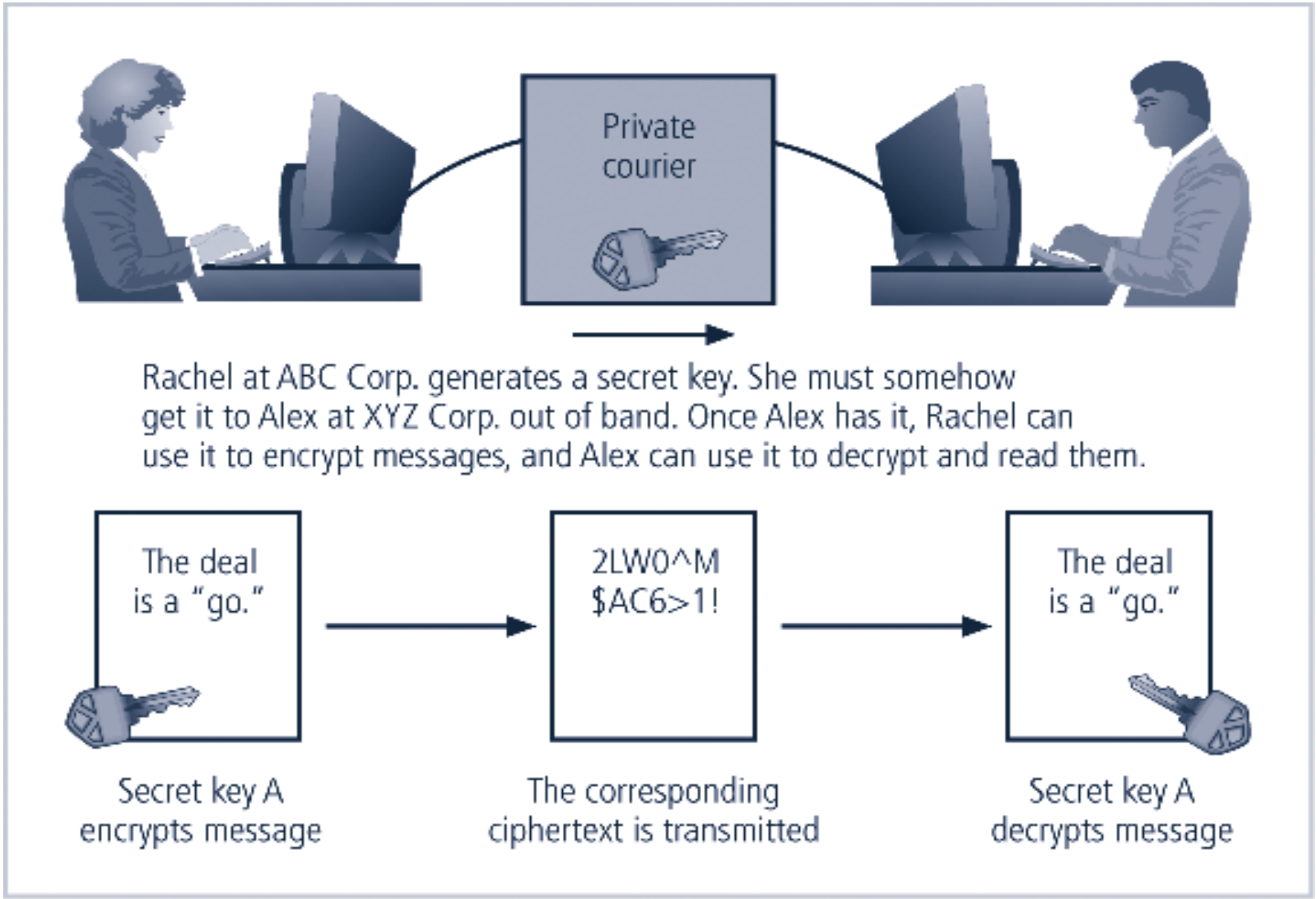


FIGURE 8-3 Example of Symmetric Encryption

Symmetric Encryption Algorithms

- Symmetric encryption: uses same “secret key” to encode and decode message
  - Encryption methods can be extremely efficient, requiring minimal processing [hardware, software implementations]
  - Both sender and receiver must possess encryption key
  - If either copy of key is compromised, the encryption is no longer secure
  - Key distribution problem: if key is used too often, it is susceptible to cryptanalysis – how to securely distribute new key (concerns: data spills/key leakage and sample size to attack)

Symmetric Encryption

- Data Encryption Standard (DES): popular symmetric cryptosystem
  - 64-bit block size; 56-bit key
  - Adopted by NIST in 1976 as federal standard for encrypting non-classified information
- Triple DES (3DES): created to increased security while being somewhat compatible with DES
  - Increases effective key size by using 2 or 3 keys
  - ciphertext = EK3(DK2(EK1(plaintext)))
- Advanced Encryption Standard (AES) replaced DES (as federal standard), 3DES in 2001 (built by community)
  - Can use 128, 192 or 256 bit key (or longer)

Encryption Key Size

- When using ciphers, size of key is very important
- Strength of many encryption applications and cryptosystems measured by key size
- For cryptosystems, security of encrypted data is not dependent on keeping encrypting algorithm secret
- Cryptosystem security depends on keeping the key(s) secret

TABLE 8-7 Encryption Key Power

Number of Bits in Key	Odds of Cracking: 1 in	Estimated Time to Crack*
8	256	.000032 seconds
16	65,536	.008192 seconds
24	16,777,216	2.097 seconds
32	4,294,967,296	8 minutes 56.87 seconds
56	72,057,594,037,927,900	285 years 32 weeks 1 day
64	18,446,744,073,709,600,000	8,090,677,225 years
128	3.40282E+38	5,257,322,061,209,440,000,000 years
256	1.15792E+77	2,753,114,795,116,330,000,000,000,000, 000,000,000,000,000,000,000 years
512	1.3408E+154	608,756,305,260,875,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000, 000,000,000 years

[NOTE] *Estimated Time to Crack is based on a general-purpose personal computer performing eight million guesses per second.

Table has been updated in the 4th edition

Cryptographic Algorithms - Asymmetric

- Asymmetric encryption (public-key encryption)
  - Uses two different but related keys; either key can encrypt or decrypt message
  - If Key A encrypts message, only Key B can decrypt
  - Useful to have one key serve as private key and the other serve as public key
- More computationally intensive than symmetric
- Can be used for authentication as well as confidentiality

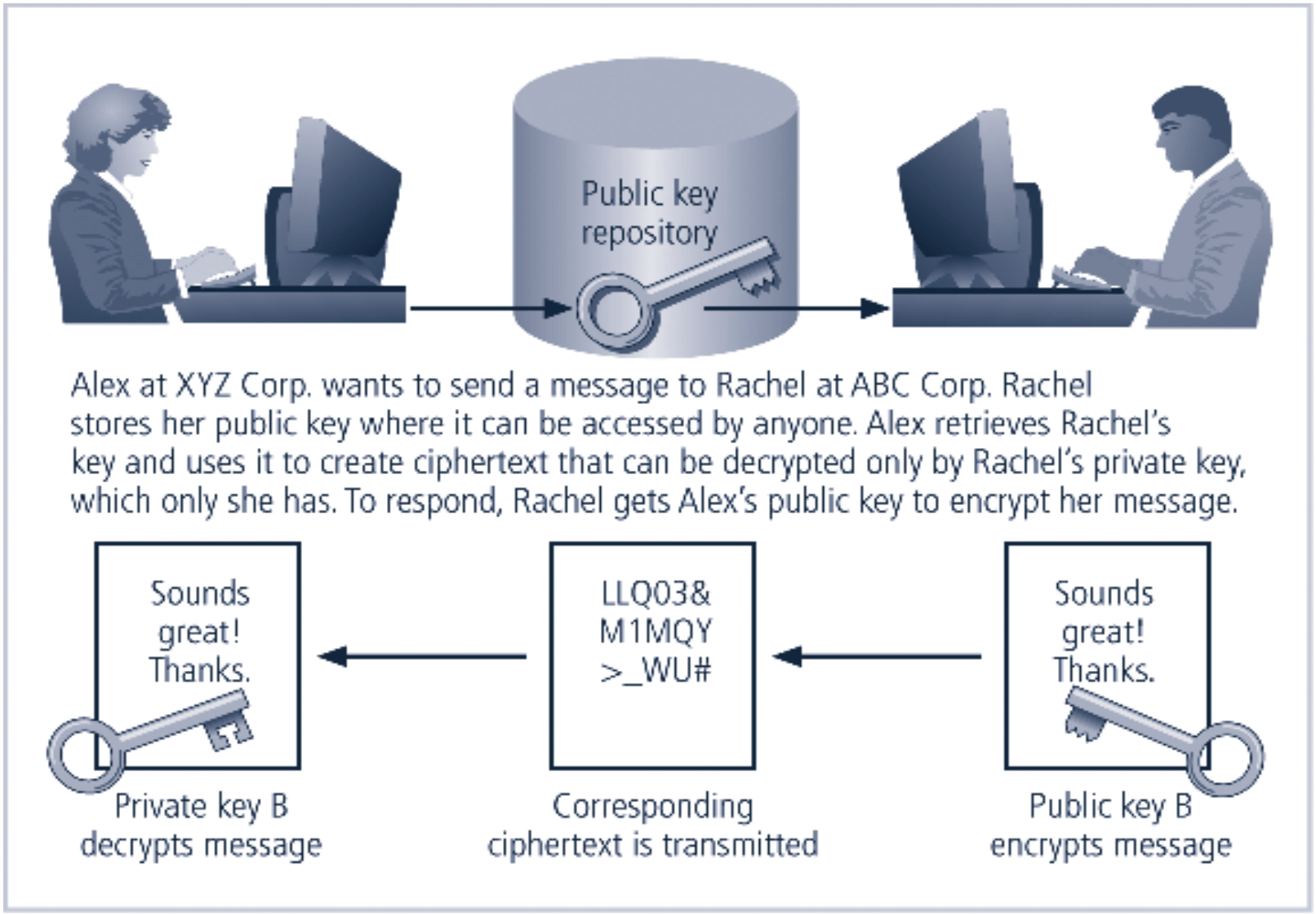
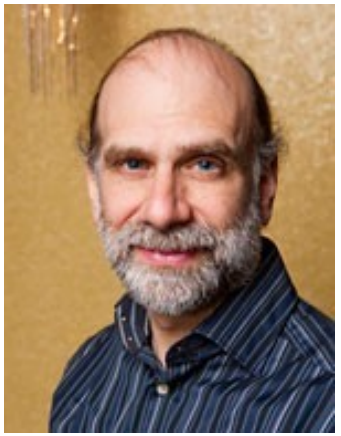
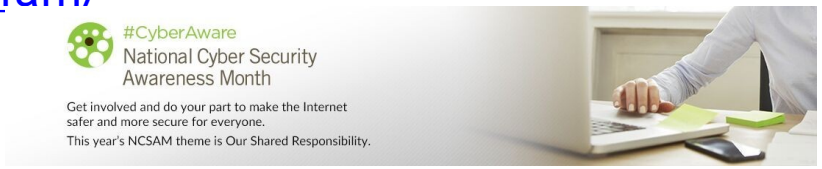


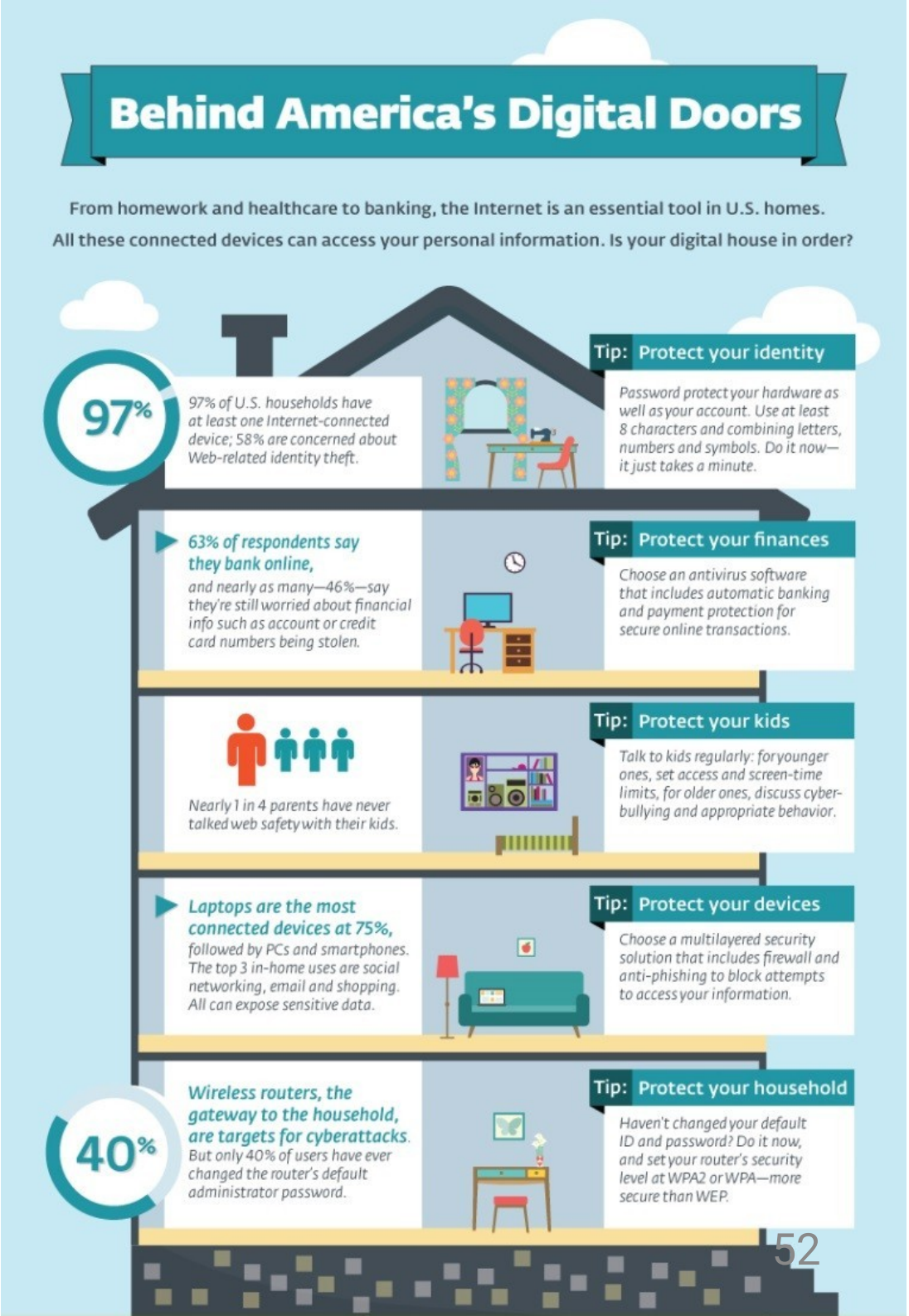
FIGURE 8-4 Example of Asymmetric Encryption



Useful References

- Staysafeonline.org
- Eff.org
- https://www.schneier.com/crypto-gram/





Public Key Encryption

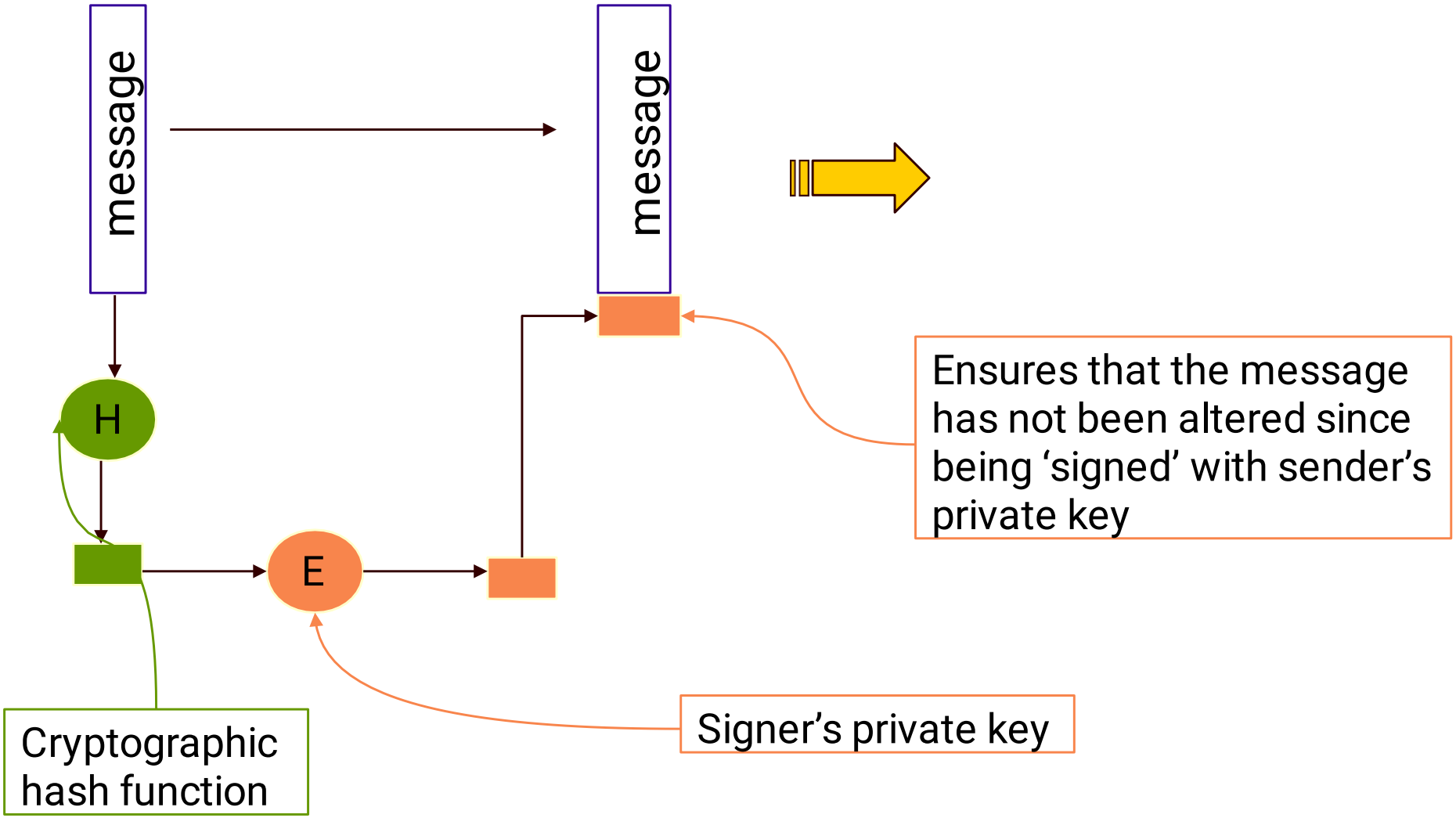
- How would Alex and Rachel use public key encryption to ensure authentication as well as confidentiality?
  - That is, when Alex gets the message, how can he be sure it came from Rachel?

Features of Block Chains
--Digital Signatures
--Digital Certificates
--Hashing
--Encryption

Digital Signatures

- Additions to messages so that the message can be mathematically proven to be authentic
  - Assuming private key has not been compromised
- Created in response to rising need to verify information transferred using electronic systems
  - May be recognized as a legal signature in U.S.
- Asymmetric encryption processes used to create digital signatures
  - Digital signature is a hash encrypted with a private key

Digital Signature Idea



Why We Need Digital Certificates

- The problem with the public key cryptography scheme and digital signature idea so far discussed is, what if someone tampers with the public key repository?

Digital Certificates

- Electronic document containing public key value and identifying information about entity that controls key
- Digital signature attached to certificate's container file to certify file is from entity it claims to be from
- A CA such as Verisign creates a public- private key pair for you and puts the public key in a digital certificate.
- Signed with Certificate Authority's private key – your browser has CA's public key

Digital Certificate Example

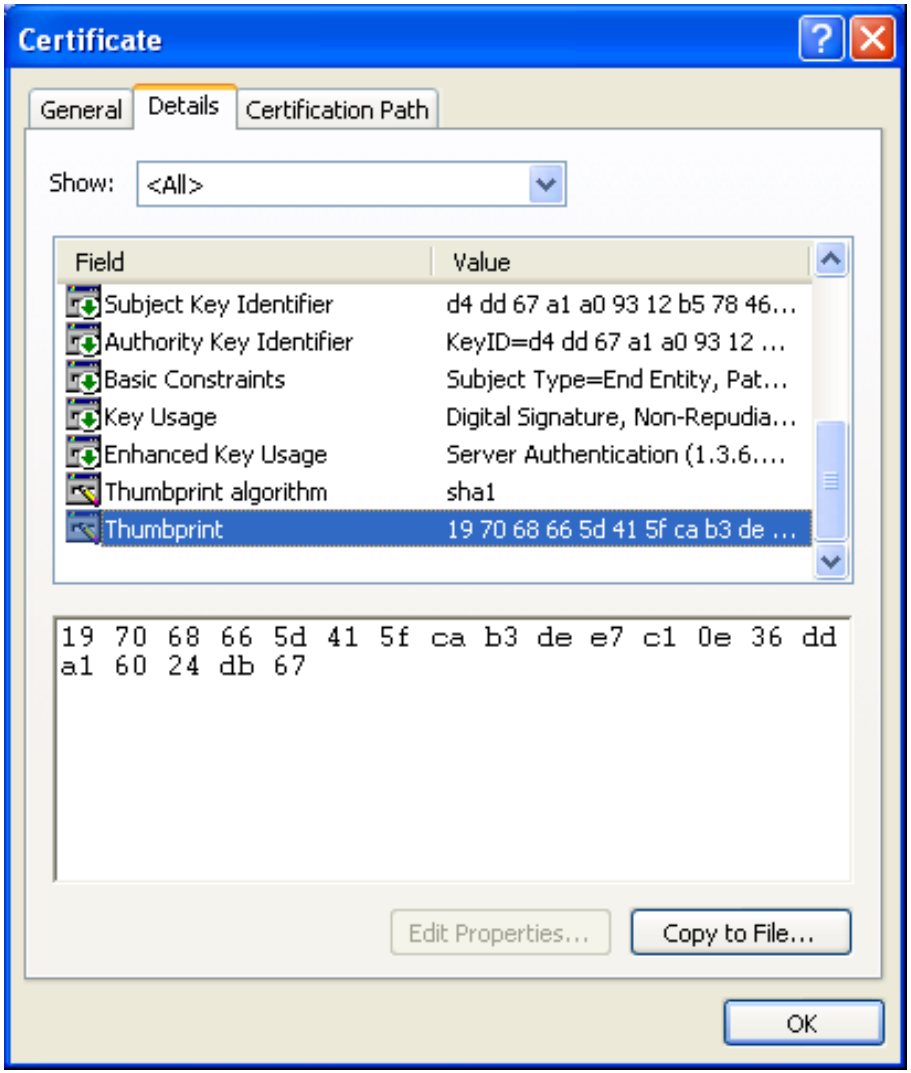


TABLE 8-8 X.509 v3 Certificate Structure[10]

Version
Certificate Serial Number
Algorithm ID ■ Algorithm ID ■ Parameters
Issuer Name
Validity ■ Not Before ■ Not After
Subject Name
Subject Public Key Info ■ Public Key Algorithm ■ Parameters ■ Subject Public Key
Issuer Unique Identifier (Optional)
Subject Unique Identifier (Optional)
Extensions (Optional) ■ Type ■ Criticality ■ Value
Certificate Signature Algorithm
Certificate Signature

Signature is hash of certificate encrypted with private key of CA

Cryptographic Tools, PKI

- Public Key Infrastructure (PKI): integrated system of software, encryption methodologies, protocols, legal agreements (CPS), and third-party services enabling users (relying parties) to communicate securely
- PKI systems based on public-key cryptosystems; include digital certificates and certificate authorities (CAs)
  - Two CA's were compromised in 2011 (Diginotar)
  - Browsers prepopulated with trusted roots
- Equifax, GlobalSign, DigiCert, GoDaddy and Verisign are "Root CA's" and must pass audits by external security firms

Cryptography Tools (continued)

- PKI protects information assets in several ways:
  - Authentication
  - Integrity
  - Privacy
  - Authorization
  - Nonrepudiation

Hybrid Cryptography Systems

- Asymmetric encryption more often used with symmetric key encryption, creating hybrid system
  - Conventional encryption is faster
  - Don't want to "overuse" a key.
  - PKI or digital certificates used to agree on symmetric 'session' key
- Diffie-Hellman Key Exchange method: means for secure distribution of secret keys; provided foundation for subsequent developments in public-key encryption

Diffie Hellman Key Exchange

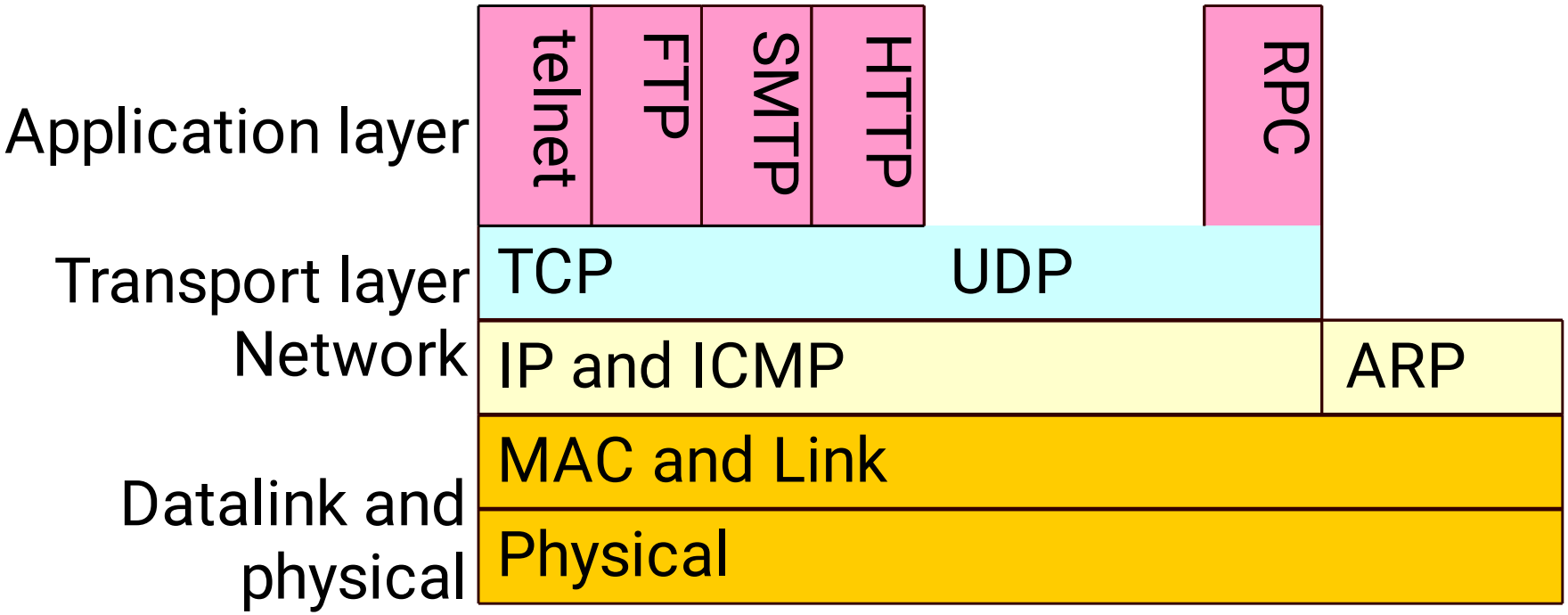
- Alice and Bob want to agree on a secret key but have only an insecure communications channel.
- They agree on a finite cyclic group and a generating element of that group.
  - Usually a multiplicative group of integers modulo P, where P is a large prime number and a generating element G.
- They must assume the attacker knows P and G and any message they exchange.
- Alice and Bob each choose a secret integer, a and b
  - Alice sends Bob G^a mod P
  - Bob sends Alice G^b mod P
- Both compute G^{ab} mod P which will be their secret key

Steganography

- Process of hiding information; in use for a long time
- Most popular modern version hides information within files appearing to contain digital pictures or other images
- Some applications hide messages in .bmp, .wav, .mp3, and .au files, as well as in unused space on CDs and DVDs

- Secure Socket Layer (SSL) protocol: uses public key encryption to secure channel over public Internet; operates at the Transport layer
- Transport Layer Security (TLS) replaces SSL and also uses asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity
- Secure Hypertext Transfer Protocol (S-HTTP): extended version of Hypertext Transfer Protocol; provides for encryption of individual messages between client and server across Internet using a virtual connection
  - S-HTTP is the application of SSL over HTTP (application and transport layer work together)
  - Variation of the more popular HTTPS

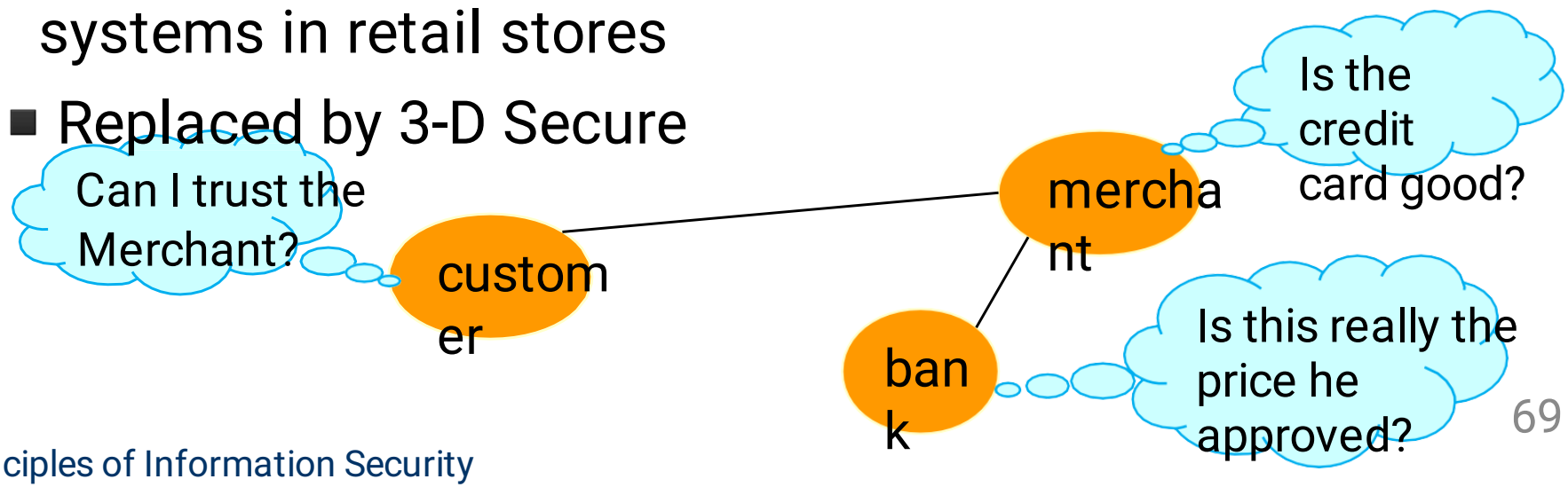
Internet Protocol Layers



Protocols for Secure Communications (continued)

- Securing e-mail with S/MIME, PEM, and PGP
  - Secure Multipurpose Internet Mail Extensions (S/MIME): builds on Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication
  - Privacy Enhanced Mail (PEM): proposed as standard to function with public-key cryptosystems; also uses 3DES symmetric key encryption
  - Pretty Good Privacy (PGP): can use several different ciphers for message encoding

- Secure Electronic Transactions (SET): developed by MasterCard and VISA in 1997 to provide protection from electronic payment fraud
- Uses RSA for key exchange and DES to encrypt credit card information
- Provides security for both Internet-based credit card transactions and credit card swipe systems in retail stores
- Replaced by 3-D Secure



- Securing Wireless Networks with WEP, WPA and WPA2
  - Wired Equivalent Privacy (WEP): early attempt to provide security with the 802.11 network protocol
    - Used RC4 in an insecure way
  - Wi-Fi Protected Access (WPA): created to resolve issues with WEP (but had to be similar for compatibility reasons)
  - WPA2 is the real solution; uses AES
- Bluetooth: de facto industry standard for short range wireless communications between devices; can be exploited by anyone within approximately 30 foot range, unless suitable security controls are implemented

Protocols for Secure Communications (continued)

- Securing TCP/IP with IPSec (network layer)
  - Internet Protocol Security (IPSec): open source protocol to secure communications across any IP-based network
  - IPSec designed to protect data integrity, user confidentiality, and authenticity at IP packet level
  - IPSec combines several different cryptosystems: Diffie-Hellman; public key cryptography; bulk encryption algorithms; digital certificates
  - IPv6 starting to be used since they ran out of addresses

- Pretty Good Privacy (PGP): hybrid cryptosystem designed in 1991 by Phil Zimmermann

- Combined best available cryptographic algorithms to become open source *de facto* standard for encryption and authentication of e- mail and file storage applications
- Freeware and low-cost commercial PGP versions are available for many platforms
- PGP security solution provides six services: authentication by digital signatures; message encryption; compression; e-mail compatibility;

  segmentation; key management

TABLE 8-11 PGP Function[15]

Function	Algorithm	Application
Public key encryption	RSA/SHA-1 or DSS/SHA-1	Digital signatures
Conventional encryption	3DES, RSA, IDEA or CAST	Message encryption
File management	ZIP	Compression

PGP can use Digital Envelopes

- First, the message itself is encoded using symmetric encryption, and then this session key to decode the message is encrypted using the recipient's public key.
- This technique overcomes one of the problems of public- key encryption, which is that it is slower than symmetric encryption. Because only the key is protected with public-key encryption, there is very little overhead.

Attacks on Cryptosystems

- Attacks on cryptosystems fall into four general categories

1. Man-in-the-middle: get plaintext/ciphertext pair or trick-you-into-revealing-the-key
2. Correlation attacks and statistical analysis
3. Dictionary attack: for short phrases or passwords where the cryptosystem is known
4. Timing attack: deduce info from timing patterns

WHEEL OF FORTUNE
BIG MONEY

Man-in-the-Middle Attack

- Anytime an attacker intercepts messages of two legitimate parties to trick them into accepting his message as legitimate.
- Intercept transmission of public key or insert known key structure in place of requested public key
- From victim's perspective, encrypted communication appears to be occurring normally, but in fact attacker receives each encrypted message, decodes, encrypts, and sends to originally intended recipient
- Establishment of public keys with digital signatures can prevent traditional man-in-the-middle attack

Correlation Attacks and Classical Cryptanalysis

- Collection of brute-force methods that attempt to deduce statistical relationships between structure of unknown key and ciphertext
- Differential and linear cryptanalysis have been used to mount successful attacks
- Correlation attacks can only be used on certain stream ciphers where some of the plaintext is known or can be guessed

Dictionary Attacks

- Origin of phrase: Attacker encrypts every word in a dictionary using same cryptosystem used by target
- Dictionary attacks can be successful when the ciphertext consists of relatively few characters (e. g., usernames, passwords)
- UNIX password file:
  - Your password is not stored as clear text
  - your password is used as a key to encrypt a known value which is stored.
  - Vulnerable to dictionary attacks

Timing Attacks

- Attacker eavesdrops during victim's session; uses statistical analysis of user's typing patterns and inter-keystroke timings to discern sensitive session information
- Can be used to gain information about encryption key and possibly cryptosystem in use
- Information does not break encryption but adds to knowledge that can be used in other attacks

Summary

- Key management is not so much management of technology but rather management of people
- Cryptography and encryption provide sophisticated approach to security
  - Encryption converts a message into a form that is unreadable by the unauthorized
- Many tools are available and can be classified as symmetric or asymmetric, each having advantages and special capabilities

Summary (continued)

- Strength of encryption tool is dependent on key size but even more dependent on following good management practices
- Cryptography is used to secure most aspects of Internet and Web uses that require it, drawing on extensive set of protocols and tools designed for that purpose
- Cryptosystems are subject to attacks that fall into four categories

Terms to Know

- Plain text, ciphertext, substitution, transposition
- Vigenere, Vernam
- DES, Triple DES, AES, RSA
- Hash function, message digest
- Symmetric or secret key encryption
- Asymmetric or public key encryption
- SSL, PGP, IPSec
- Digital signatures, PKI, Certificate authority