INF 638
Cryptography & Cryptosystems

Section 7: Elements of Asymmetrical Cryptography

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

NORTHERN ARIZONA UNIVERSITY

INF 638: Cryptography & Cryptosystems

- 1- Motivation & Definitions
- 2- Elements of Number theory
- 3- Early Cryptographic methods
- 4- Symmetrical Cryptography: DES
- 5- Symmetrical Cryptography: AES
- 6- Quantum Cryptography: Key distribution
- 7- Elements of Asymmetrical Cryptography
- 8- Asymmetrical Cryptography: RSA
- 9- ECC Key Distribution
- 10- PKI & Digital Signatures
- 11- Hash Functions
- 12- Smartcards

NORTHERN ARIZONA UNIVERSITY

7-Asymmetrical cryptography

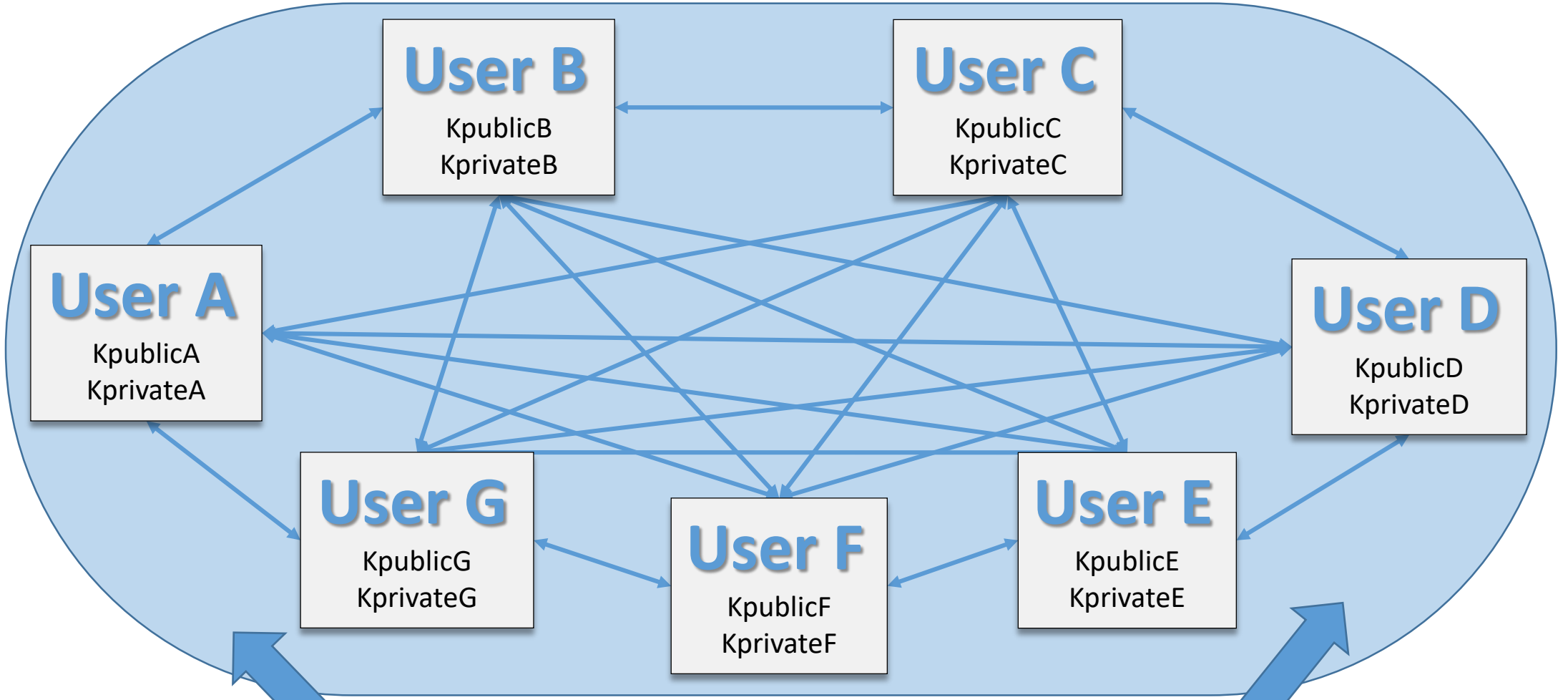
- 7-1 PKI
  - Cryptography
  - Services
- 7-2 Blockchains
  - Bitcoin
  - Hash/DSA
  - Attacks

History of Asymmetrical Cryptography

- Asymmetrical cryptography is also called PKI, Public Key Infrastructure.
- PKI represents the most significant advance in modern Cryptography
- Developed by ***Ralph Merkle***, ***Martin Hellman***, ***Whitfield Diffie*** in the early 70's
- Can accommodate a very large number of users operating independently
- Implementation based on the number theory – ***RSA***, ***ECC*** and others
  - Invert modulo
  - Theorem of Fermat-Euler
- Highly secure, but encryption/decryption is very slow

Presented
Chapter 1

Public key & Private key exchange

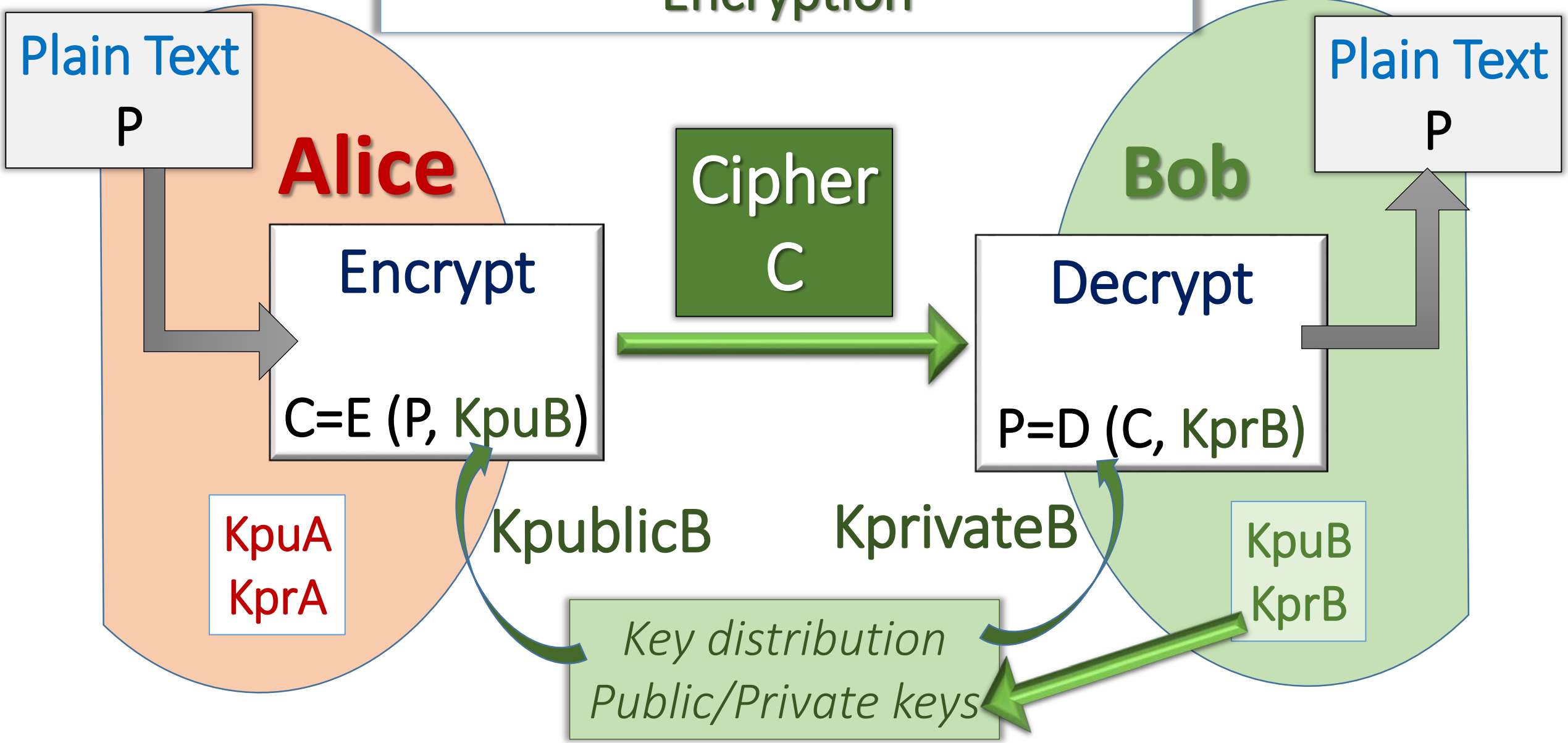


Public Key Exchange: $Kpublic_A$, $Kpublic_B$, $Kpublic_C$, $Kpublic_D$, $Kpublic_E$, $Kpublic_F$, $Kpublic_G$

Presented
Chapter 1

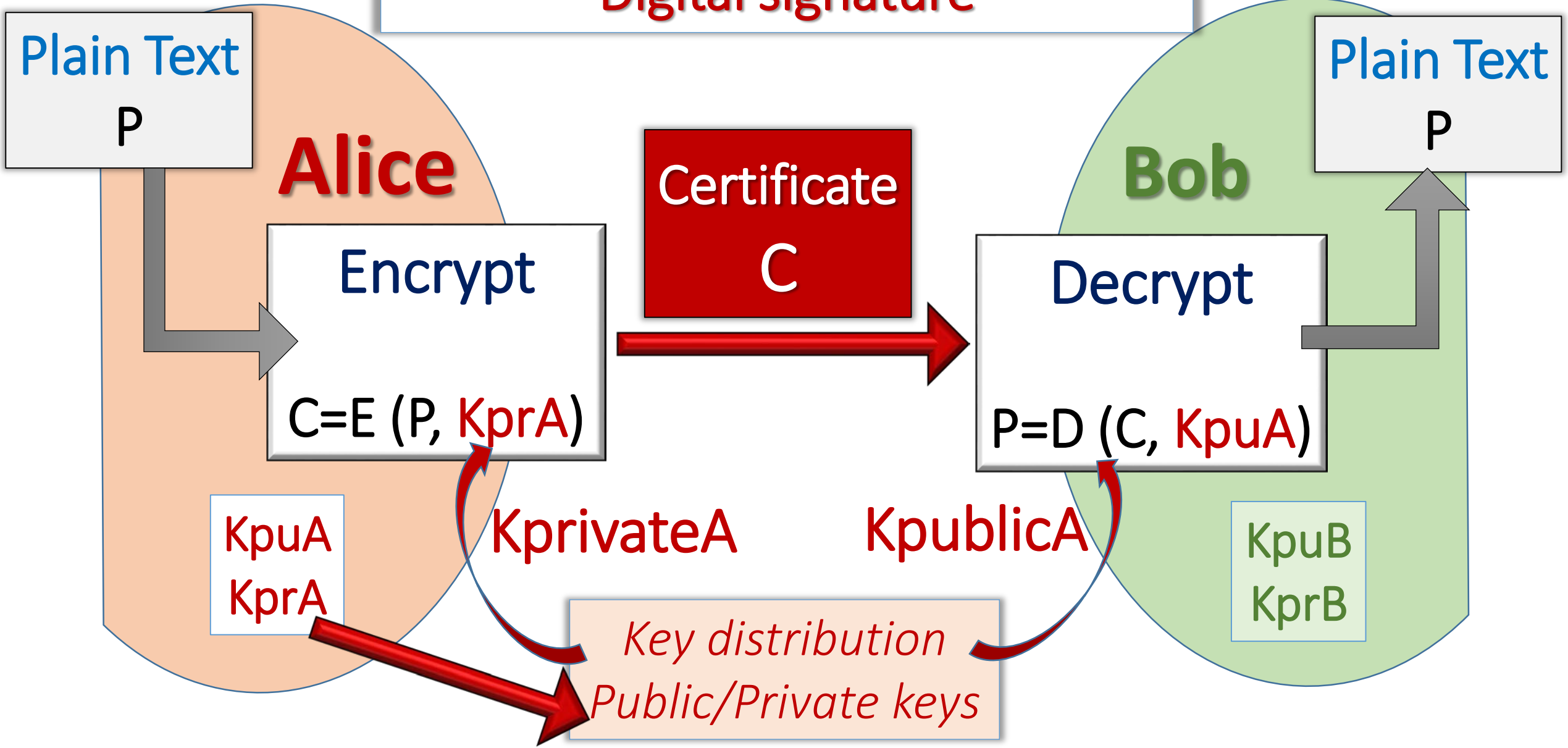
Asymmetrical Cryptography (RSA)

Encryption



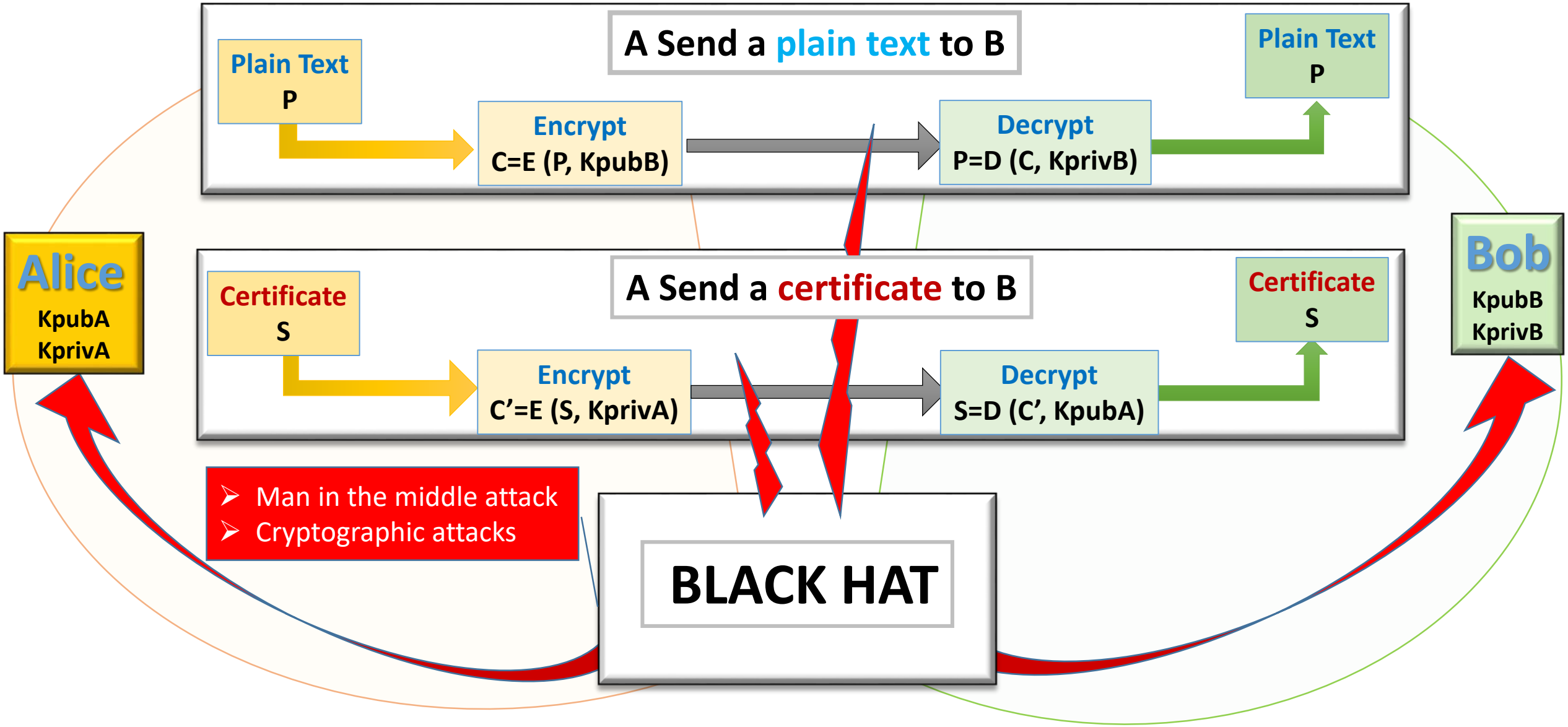
Presented
Chapter 1

Asymmetrical Cryptography (RSA)
Digital signature

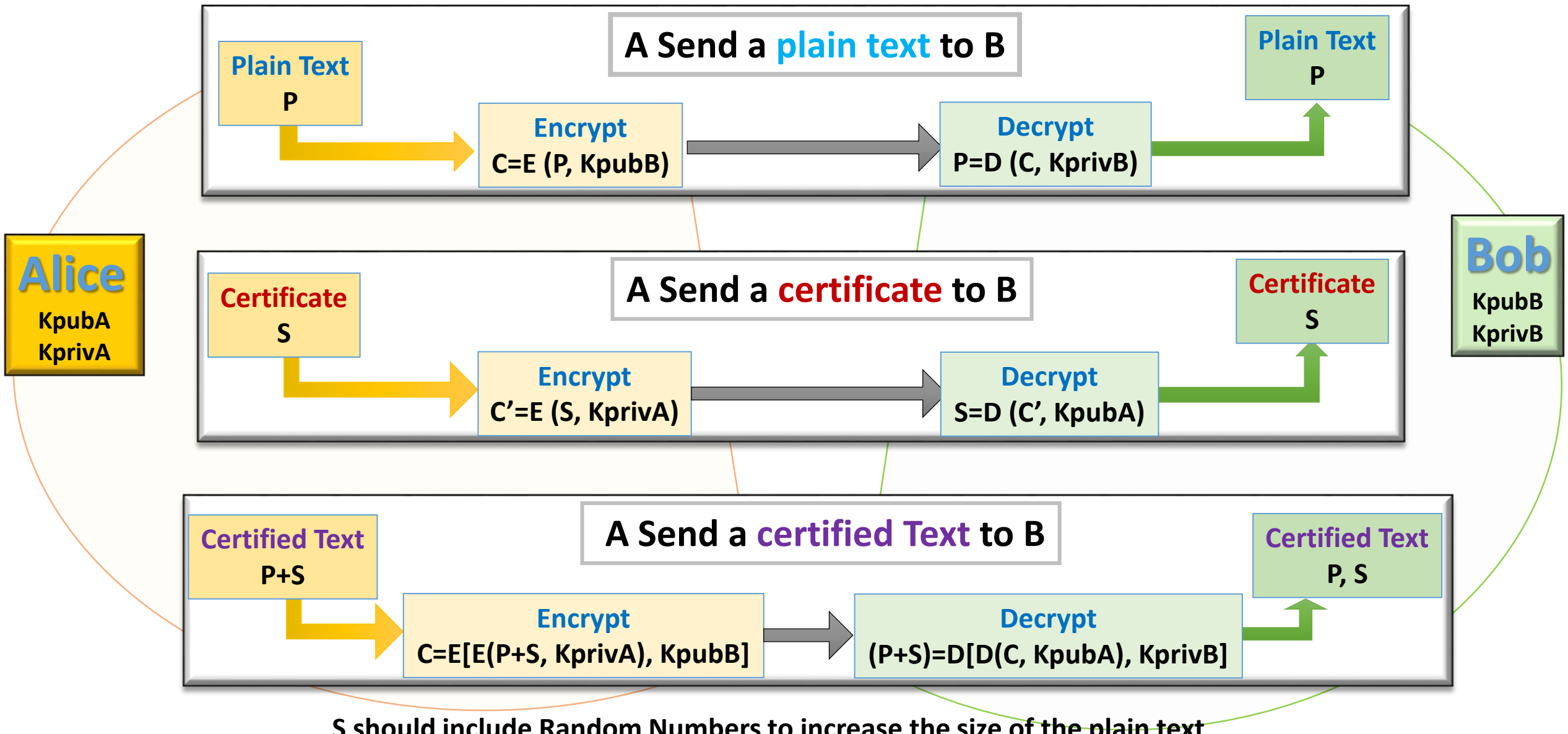


Presented
Chapter 1

Asymmetrical Encryption (ex RSA)

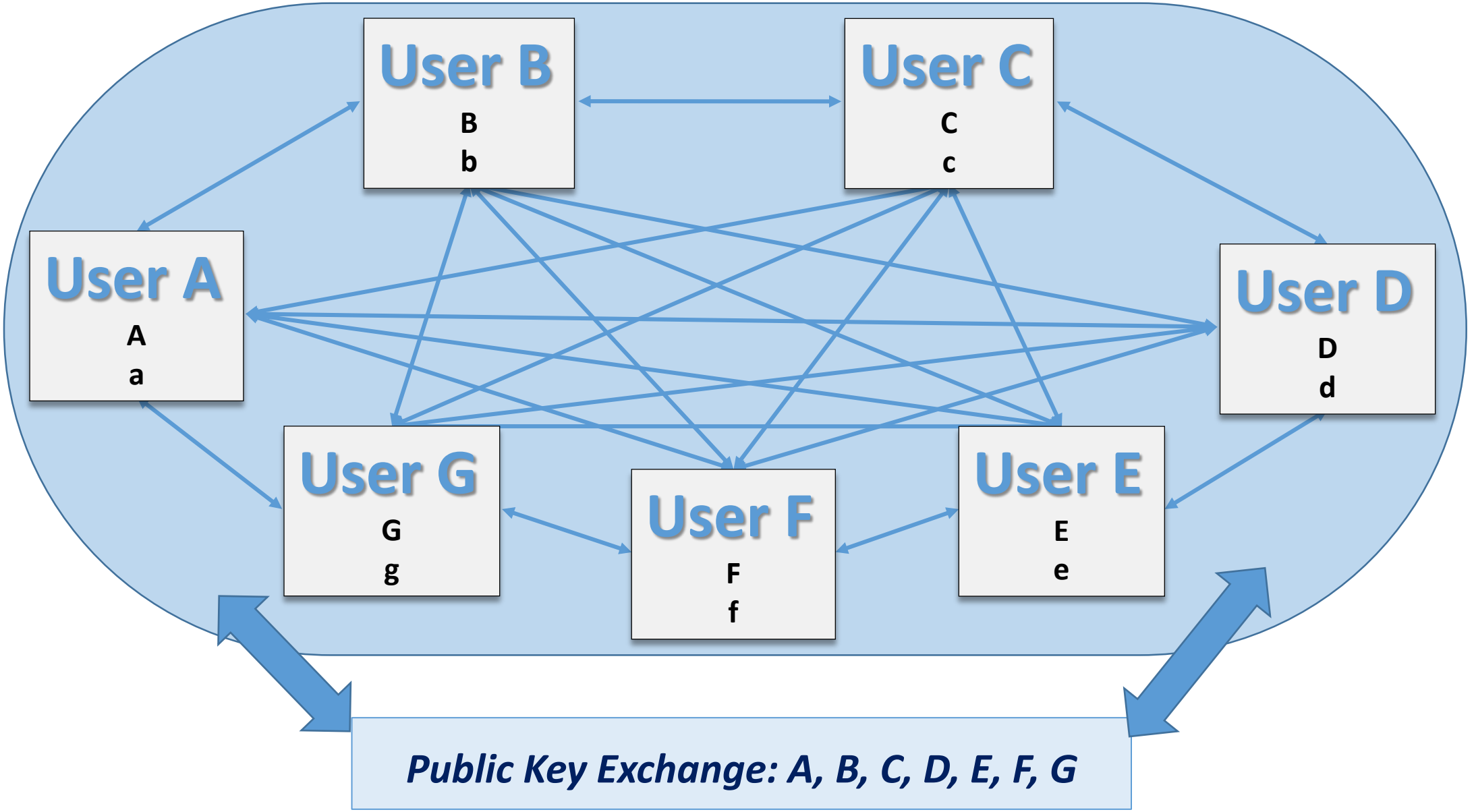


Asymmetrical Encryption (ex: RSA)



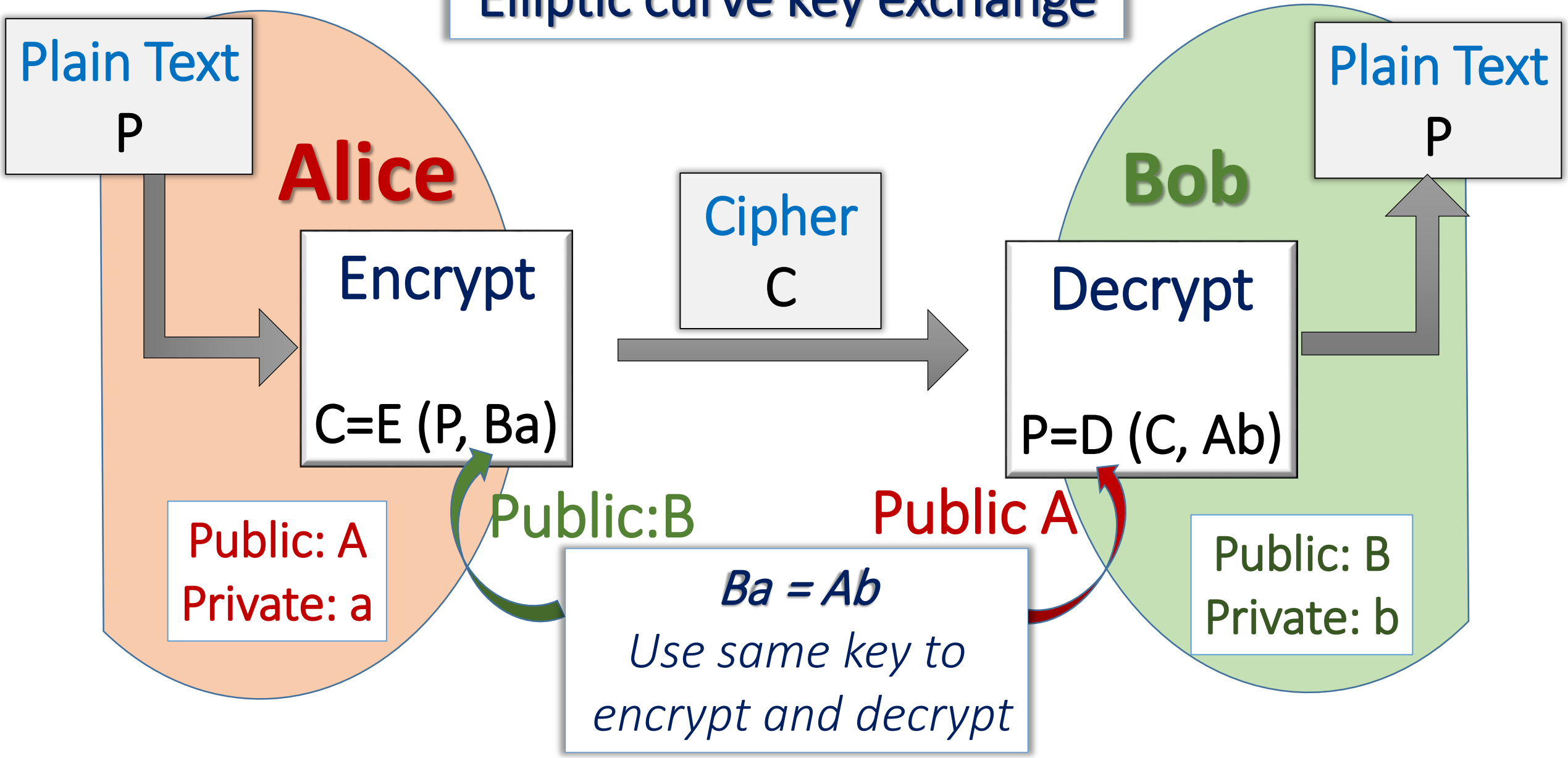
S should include Random Numbers to increase the size of the plain text

Public key & Private key: ECC



Presented
Chapter 1

Asymmetrical Cryptography
Elliptic curve key exchange



NORTHERN ARIZONA UNIVERSITY

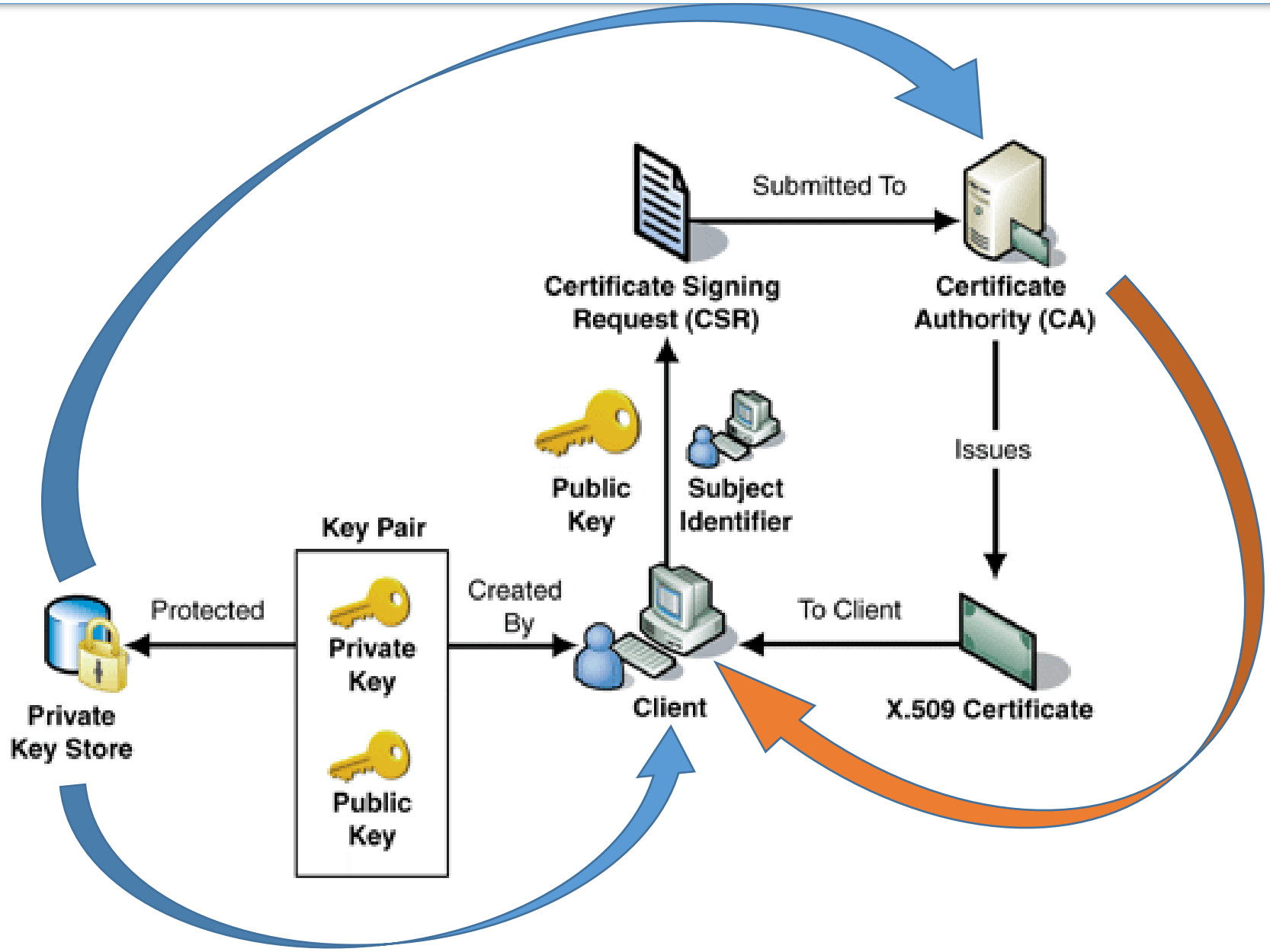
7-Asymmetrical cryptography

- 7-1 PKI
  - Cryptography
  - Services
- 7-2 Blockchains
  - Bitcoin
  - Hash/DSA
  - Attacks

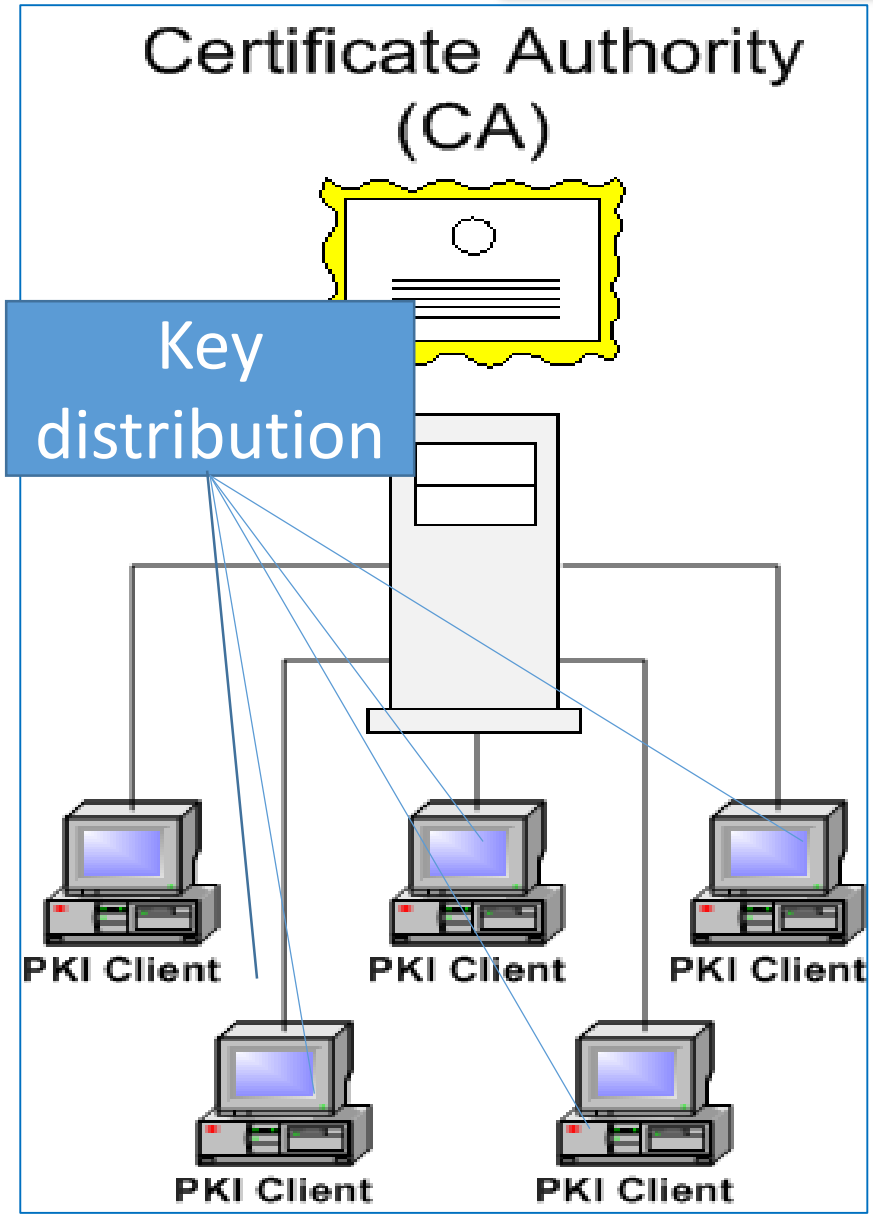
Security services

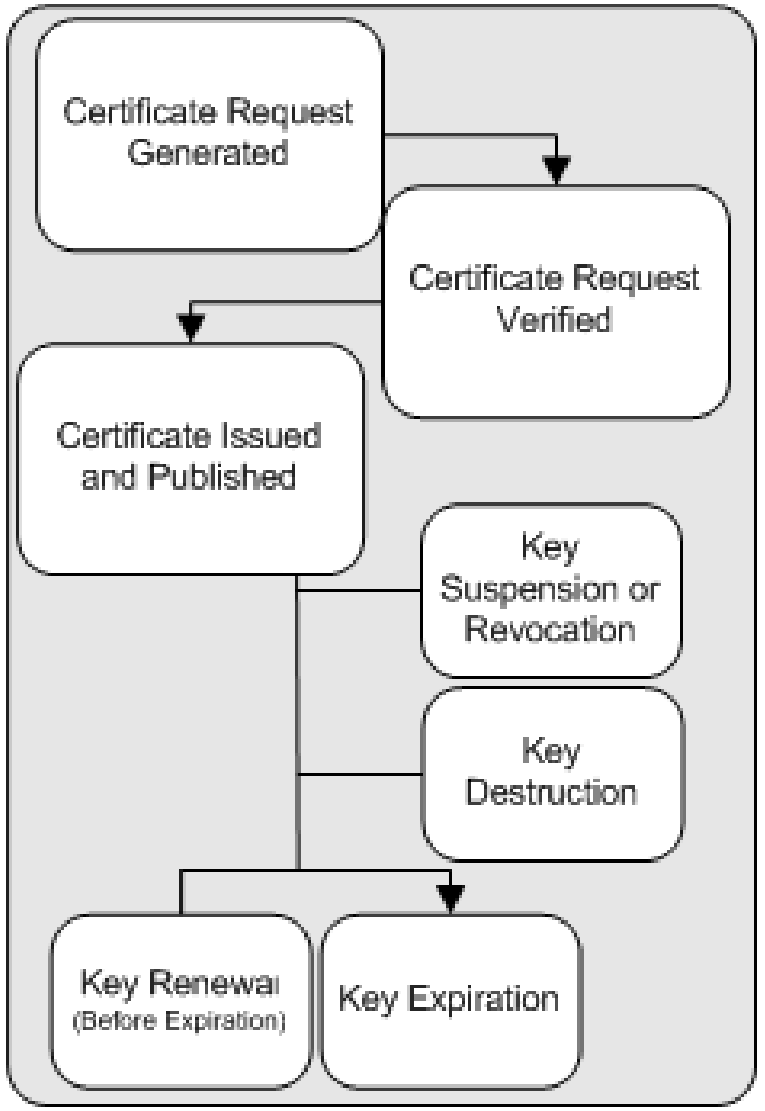
	Symmetrical	*Asymmetrical RSA Encryption*	*Asymmetrical RSA DSA*	*Asymmetrical ECC or RSA double E*
1- Confidentiality Information is kept secret from all but authorized parties	**Yes**	**Yes**	**No** The signature is "public"	**Yes**
2- Authentication The sender of the message is authentic	**?** Only if the sender is the only one with the key	**No** Anyone can encrypt with the public key	**Yes**	**Yes**
3- Integrity The message has not been modified during transmission	**Yes**	**No** Third party can Intercept the message	**Yes**	**Yes**
4- Non repudiation The sender cannot deny the creation of the message	**?** Only if the sender is the only one with the key	**No** This is not signed by the sender	**Yes**	**Yes**

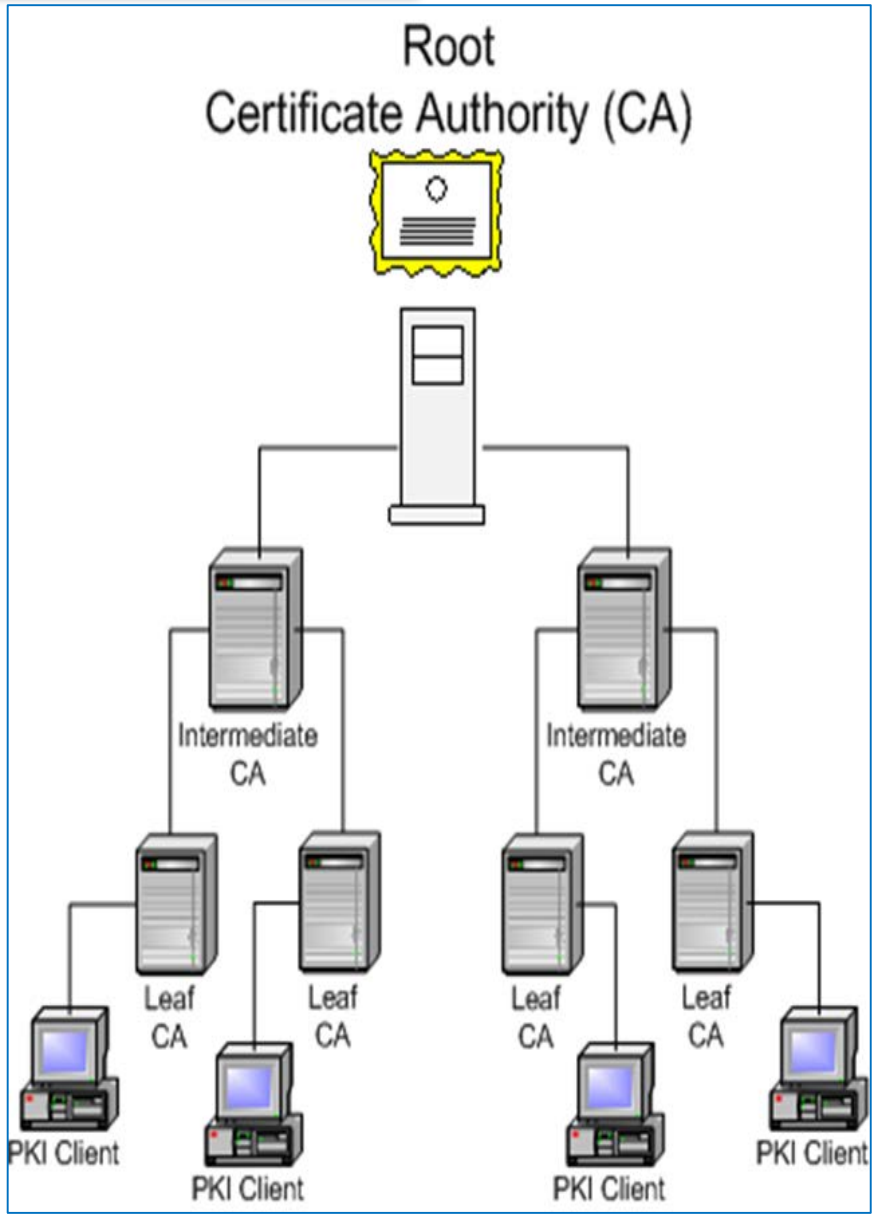
Key distribution: certificate authority (X.509 certificate)



Public Key Infrastructure (PKI):
Key Management and the Certificate Life Cycle







Key distribution with Smart Cards

Key distribution

Back-end Systems

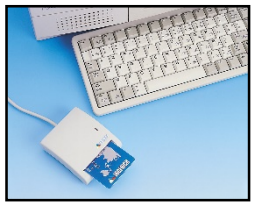
Card Personalization
Issuance

Post-Issuance
Transactions

Smart Card

Post-Issuance
Transactions

Accepting Devices



NORTHERN ARIZONA UNIVERSITY

7-Asymmetrical cryptography

- 7-1 PKI
  - Cryptography
  - Services
- 7-2 Blockchains
  - Bitcoin
  - Hash/DSA
  - Attacks

The hype around bitcoin

Cryptocurrencies & Bitcoin

What is cryptocurrency?

It is a digital currency that effectively employs *cryptography*:

Example: Bitcoin.

What is bitcoin?

" immutable and traceable record of ownership without intermediate (no single party trusted) in an environment of mistrust"

Invented by Toshi Nakamoto, 2008

From Bitcoin to blockchains

Bitcoin: a cryptocurrency created in 2008

Blockchain: a process of transacting and storing information on decentralized, distributed ledger

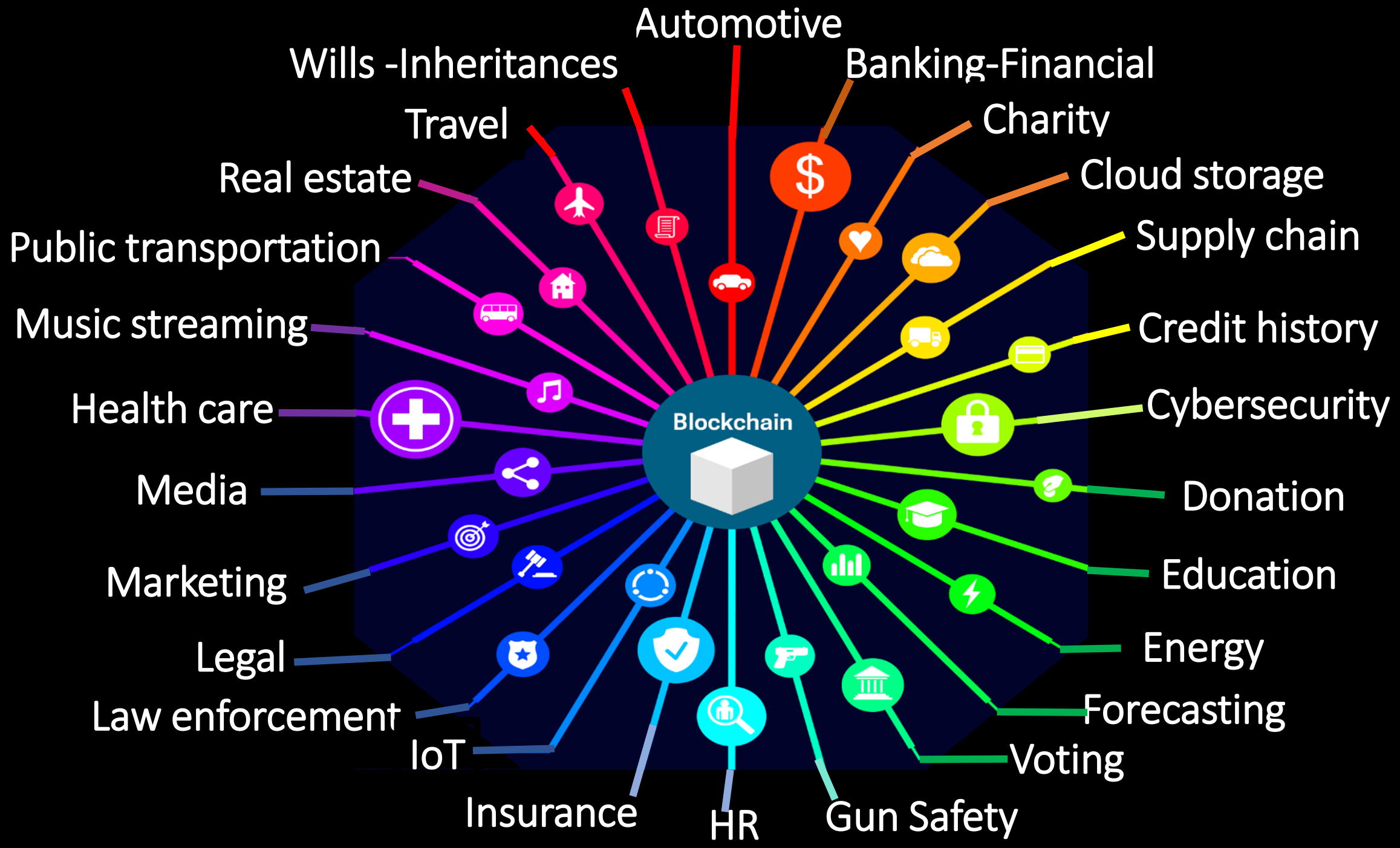
The blockchain **cryptography** is based on hashing functions and digital signature (DSA)

Hash: SHA2
DSA: ECC

The **regulation** of the bitcoin is based on the game theory: 51% rule

Strength of the blockchain technology

- Process of transacting and storing information
- Decentralized and distributed network
- Integrated network, updated in real-time with always-consistent data
- Ability to set rules for each blockchain: enforces compliance
- Tracing data from provenance to present to reduce disputes or discourage fraudulent activity
- Increased efficiency of industry processes, reduced auditing costs
- Consent, protection, and control of consumer/customer data
- High level of trust in repository of transactional data


Automotive
Wills -Inheritances
Banking-Financial
Travel
Charity
Real estate
Cloud storage
Public transportation
Supply chain
Music streaming
Credit history
Health care
Cybersecurity
Blockchain
Media
Donation
Marketing
Education
Energy
Legal
Law enforcement
Forecasting
IoT
Voting
Insurance
HR
Gun Safety

Cybersecurity in Blockchain & Bitcoin

- **Authentication** → Public Key Crypto: Digital Signatures - ECC (§9 & 10)
  - Am I paying the right person? Not some other impersonator?
- **Integrity** → Digital Signatures and Cryptographic Hash (§11)
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- **Availability** → Broadcast messages to the P2P network
  - Can I make a transaction anytime I want?
- **Confidentiality** → Pseudonymity
  - Are my transactions private? Anonymous?

Cryptography behind the bitcoin

The Technology Behind BTC

- Hashing (double-SHA256, RIPEMD-160)
- Proof-of-work (hashcash proof)
- Dual key encryption (Elliptical Curve Digital Signature Algorithm, Merkle Trees)
- Peer-To-Peer Networking (similar to IRC Internet Relay Chat)

NORTHERN ARIZONA UNIVERSITY

7-Asymmetrical cryptography

- 7-1 PKI
  - Cryptography
  - Services
- 7-2 Blockchains
  - Bitcoin
  - Hash/DSA
  - Attacks

Bitcoin Whitepaper – 2008.10.31*

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest

How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

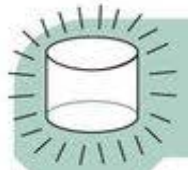
WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJL1ybLCWrfDpN.

CREATING A NEW ADDRESS



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

Each address has its own balance of bitcoins.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

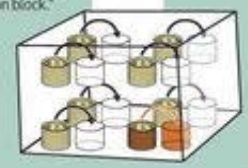
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

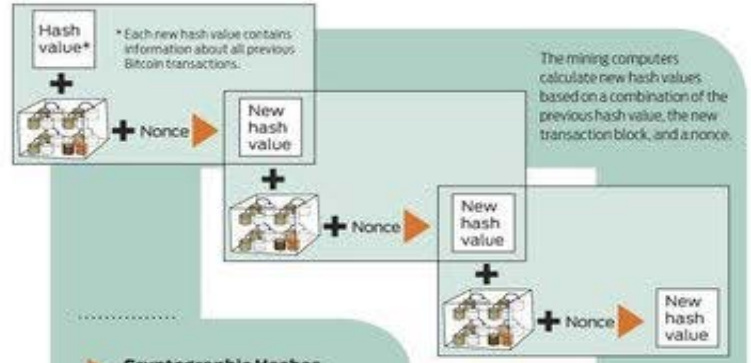
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

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



The miners' computers are set up to calculate cryptographic hash functions.



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

Cryptographic Hashes

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

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all evil	486c 6be4 6dde...
The root of all evil	b8db 7ee9 8392...

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ???	0000 0000 0000 ...

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

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

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—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.

JOSHUA J. MOLINO, BRANDON PALACIO & ANDY KIRKPATRICK

Basic architecture

- Any person can generate a pair of ***public-private*** cryptographic keys to create the equivalent of a bank account, dubbed a ‘Bitcoin address’.
  It uniquely identifies the owner of an account.
- Person A sends X amount of Bitcoins to Person B, with a ***blockchain***.
  Similar to what a typical bank ledger contains.
- At its core, a Bitcoin address is a numbered bank account, but without a bank and or any ties to the identity of the owner.

Financial transactions with bitcoin

- The **Blockchain** gets recorded on a ledger – *use hashing*

  This transaction holds the origin of funds (inputs) as a Bitcoin address and the destination (outputs).

- To ensure the ownership, the whole transaction file is **digitally signed** with a *private key* by the user sending the funds (the customer in our case). The signature along with *public key* are enclosed in the transaction.

  This allows anyone to validate the transferred Bitcoins are really owned by the sender.

- **Total privacy!!!**
  - Though the origin of funds address is derived from the enclosed public key, no one knows the identity of the owner.
  - The same goes for the destination, which is represented by another Bitcoin address.

Bitcoin: How to get started?

(1) Create your own account

a) Prove that you are a legitimate person: Name, Residence, proof of residence...
b) You get verified for bitcoin purchase
c) The apps get downloaded to your PC/phone with public/private keys

(2) Organize your wallet

a) Inventory of all transactions: amount, date, receivers/senders
b) Receive validation of all transactions

(3) Buy or Sell with bitcoins

a) Use your credit card when needed
b) Trade your bitcoins
c) Get additional bitcoins

Bitcoin: Prepare the wallet

Price Converter | **Paper Wallet** | TX Lookup | Faucet | Verify | Spend

English | Español | Français | ελληνικά | italiano | Deutsch
Česky | Magyar | 日本語 | 简体中文 | Русский | português

Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet | Vanity Wallet | Split Wallet | Wallet Details

Generate New Address | Print

Bitcoin Address

SHARE

17zLsfgZUv5TjoZRauKHcza8KF8aXNb3zf

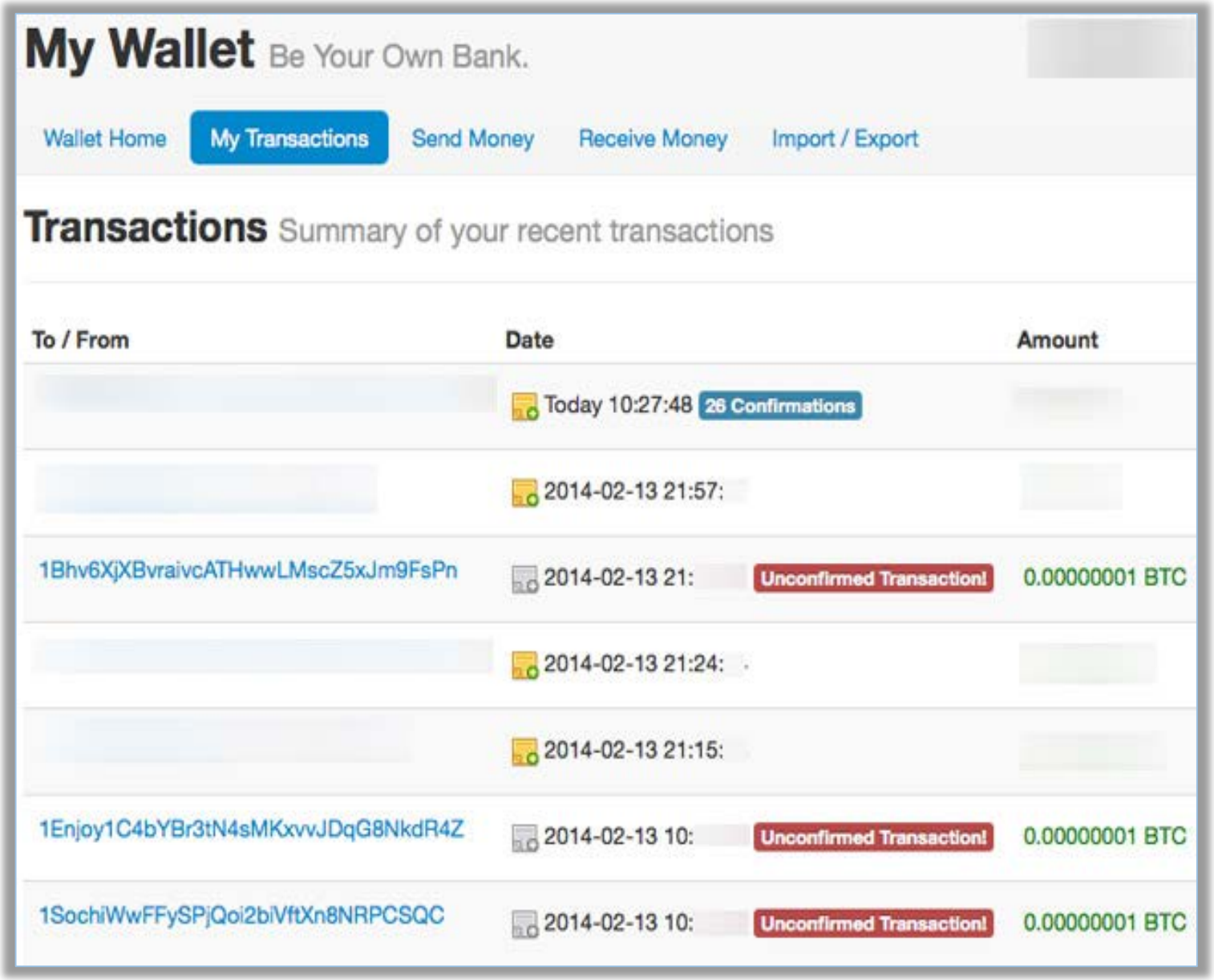
Private Key

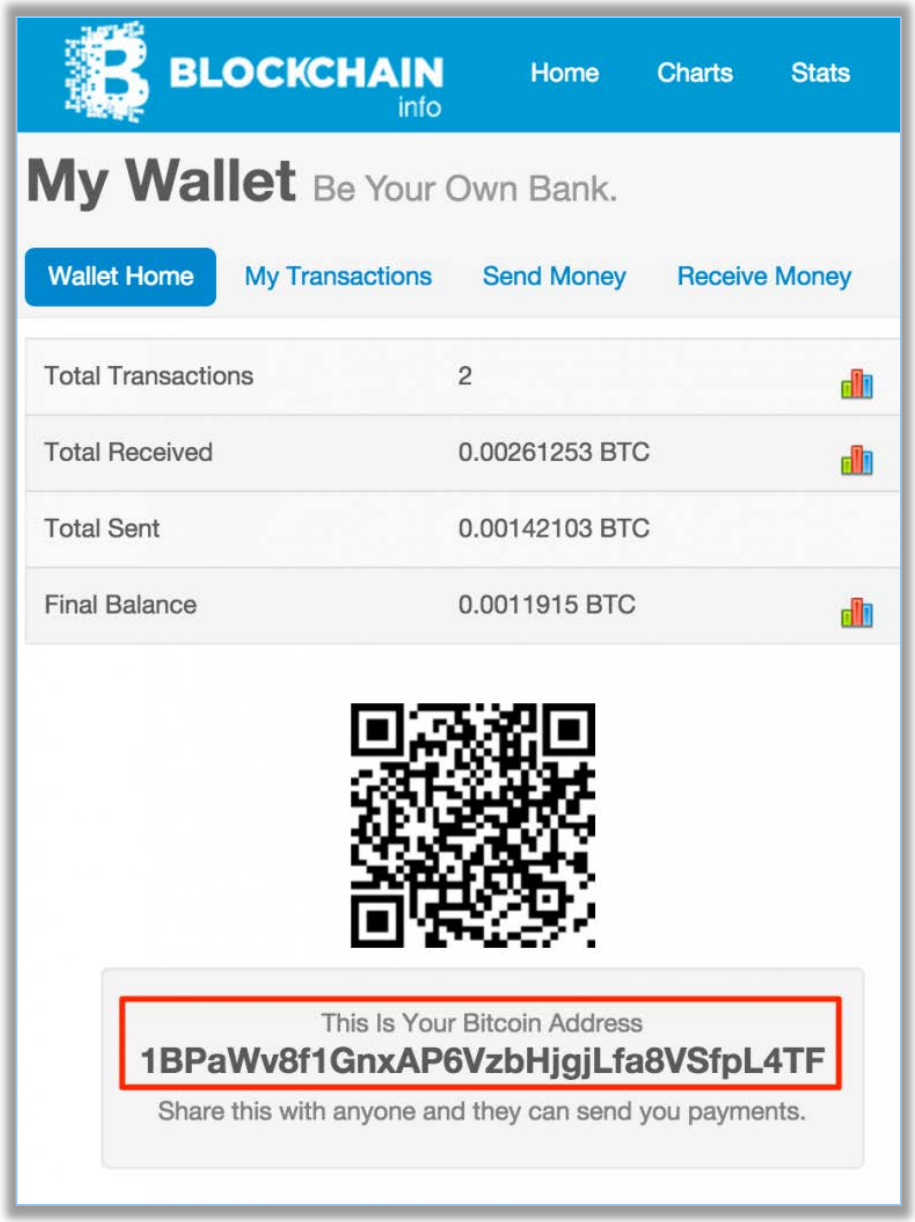
SECRET

KxfHv8oFQ5S7q5a9keBzFWrdrfU9L7bi4AUw5v3LDnSgJQMvXqz1

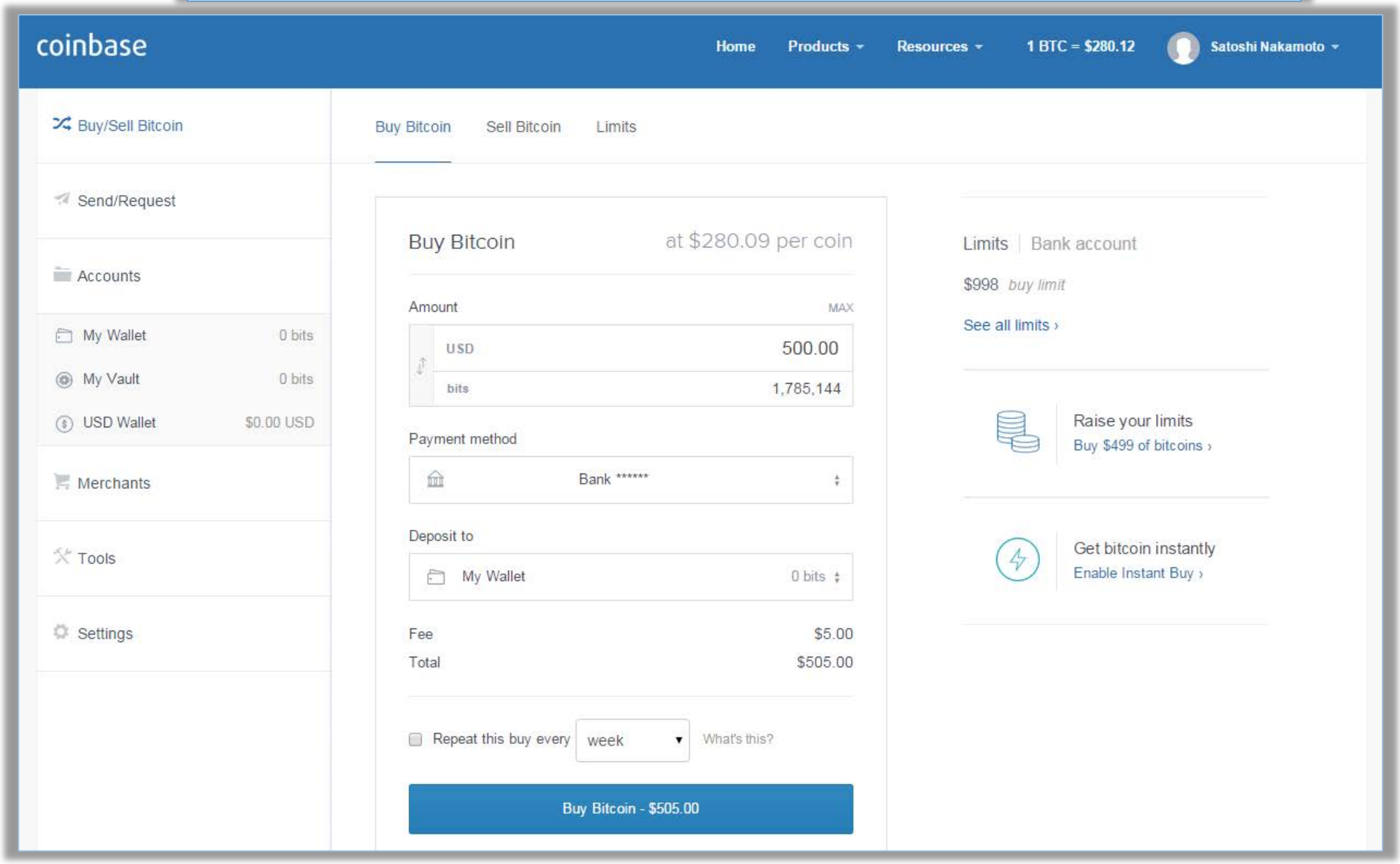
A Bitcoin wallet is as simple as a single pairing of a Bitcoin address with its corresponding Bitcoin private key. Such a wallet has been generated for you in your web browser and is displayed above.

Example of wallets

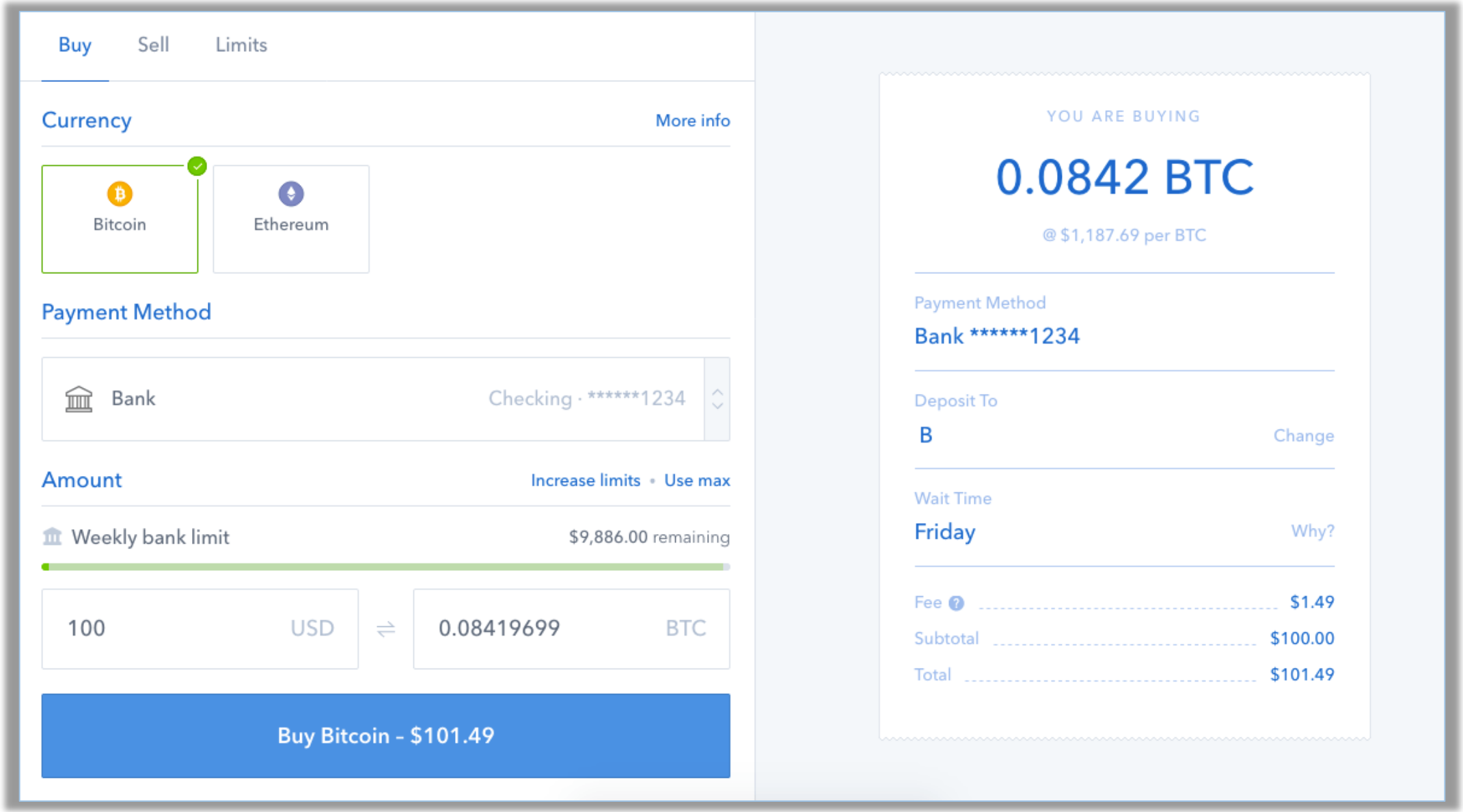




Buy Bitcoin with credit card



Buy cryptocurrencies with credit card



Buy bitcoins using Paypal with US Dollar (USD)

LocalBitcoins.com user wishes to sell bitcoins to you.

Price: 12,273.98 USD / BTC

Payment method: Paypal

User:

(feedback score 100 %, see feedback)

Trade limits: 8 - 1,200 USD

Location: United States

Payment window: 90 minutes

This seller requires SMS verification before you can make a purchase.
Proceed to phone number verification here.

Terms of trade with

★PLEASE READ BEFORE OPENING A TRADE★

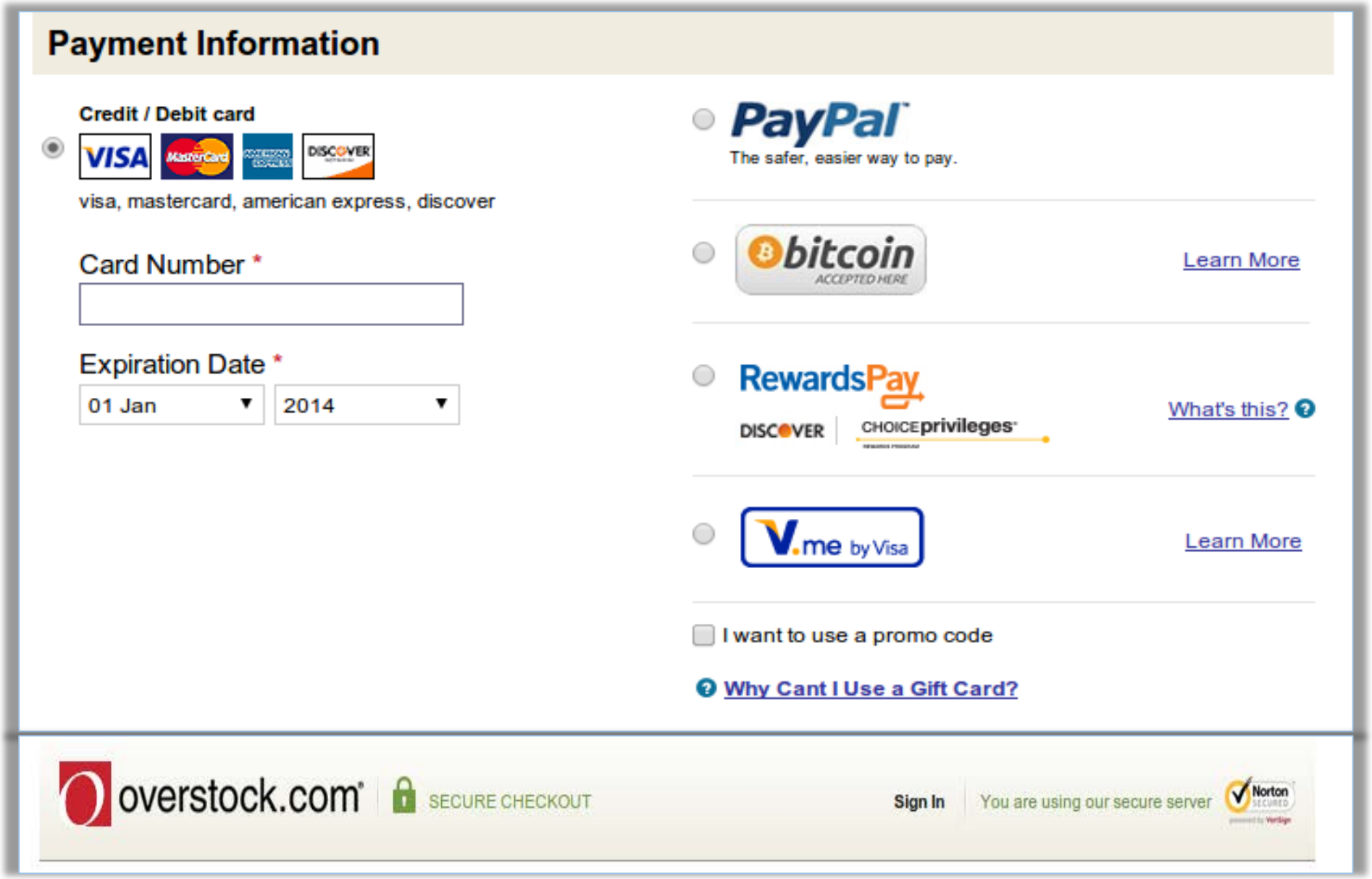
★★★Opportunity for customers without (NO) reputation★★★

★★★No matter how many trades you have, you will have to comply with all the rules and once your account is verified by me, I can selling you without being verified★★★

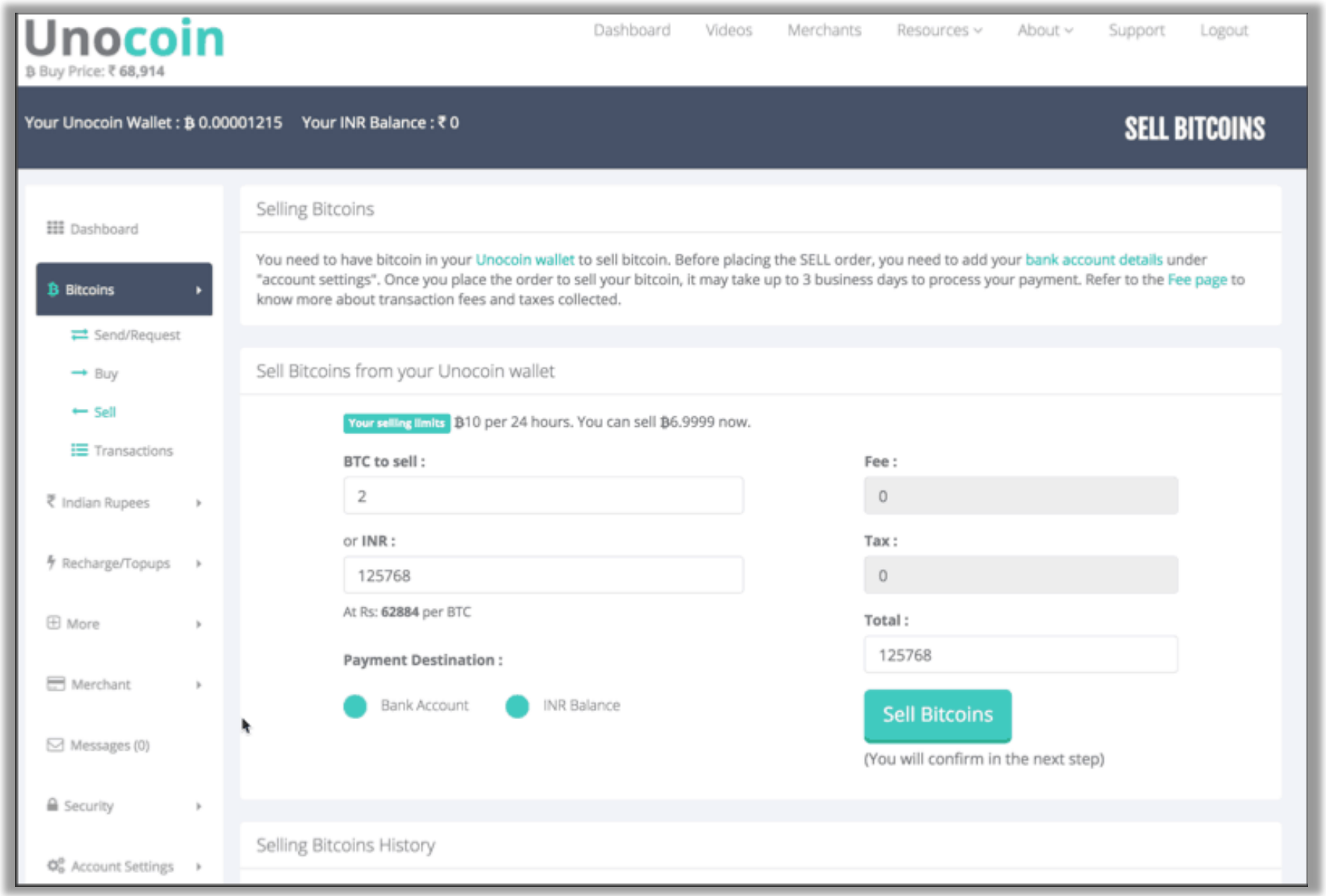
-----Honesty is my Policy to open a trade-----

1-Proof of ID (Passport, Driver license or ID Card) (IN HIGH QUALITY)

Bitcoin can replace credit card



Sell Bitcoin with your wallet



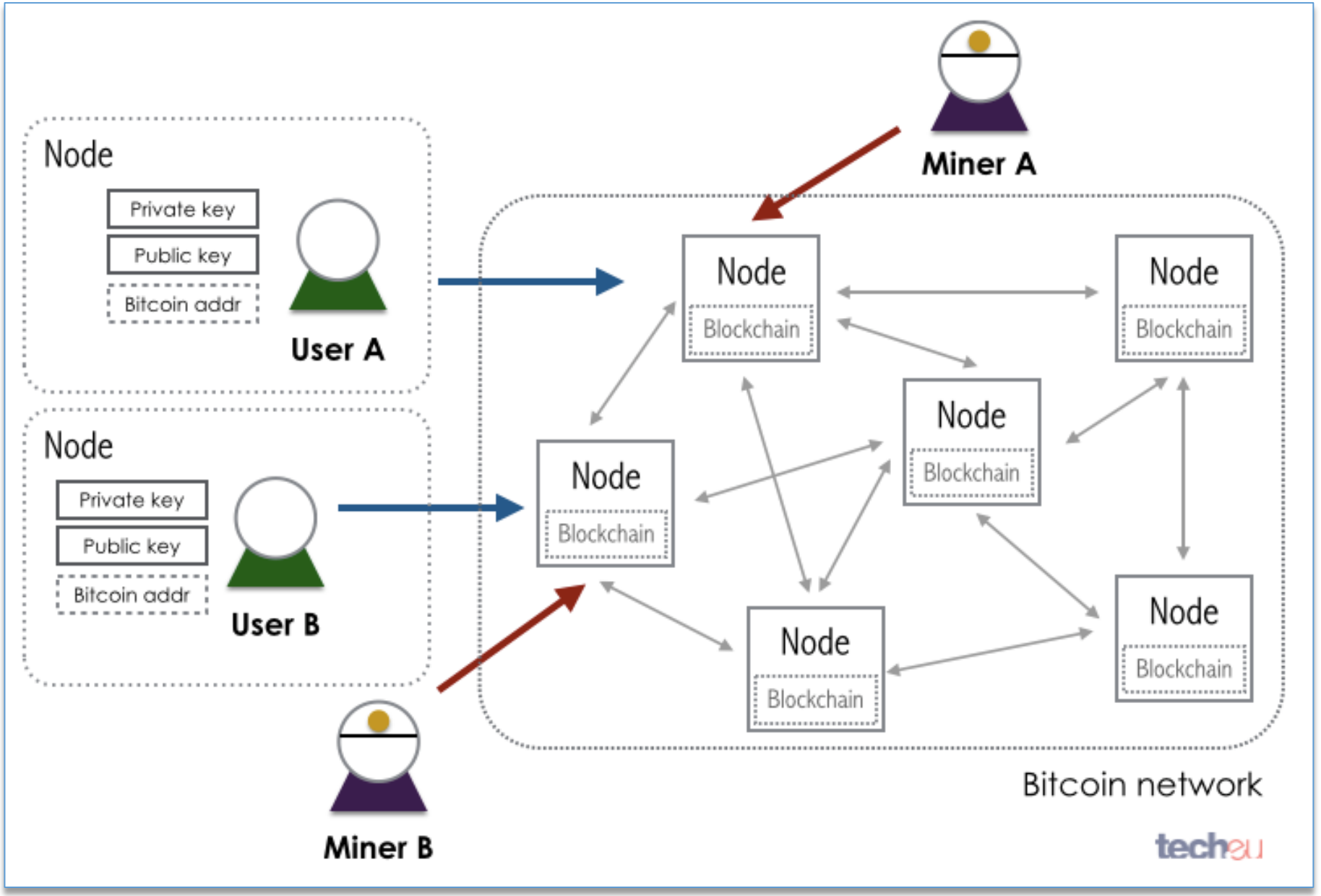
Purchase / Exchange Bitcoins

In addition to mining bitcoins, they can be acquired from an exchange!

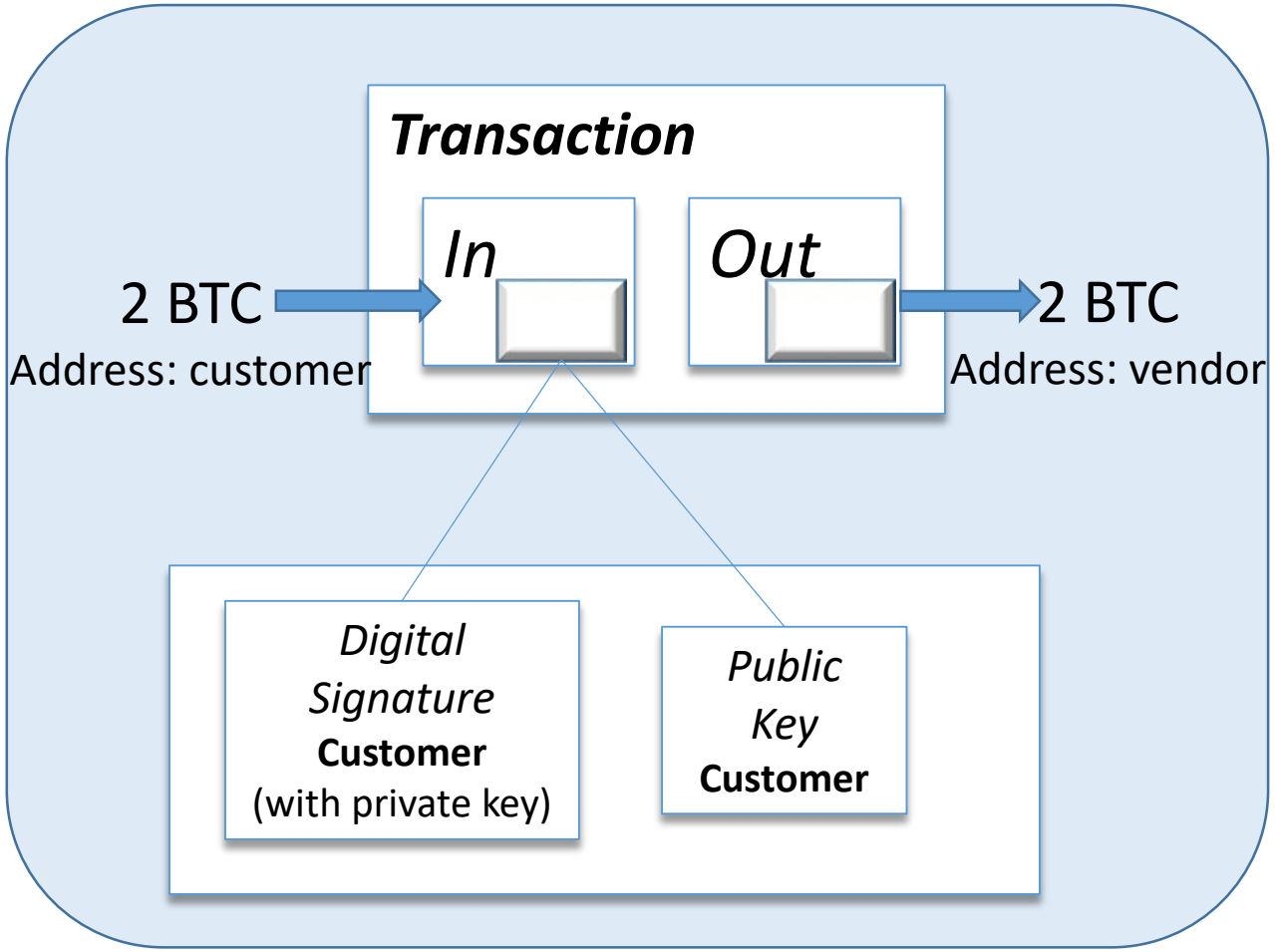
Merchants Accepting Bitcoin

- Overstock.com
- Newegg.com
- Microsoft XBOX Network
- Telsa Motors
- Time Inc (publisher)
- Virgin Galactic
- Wordpress
- BitPay claims 44,000 merchants!
- http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html

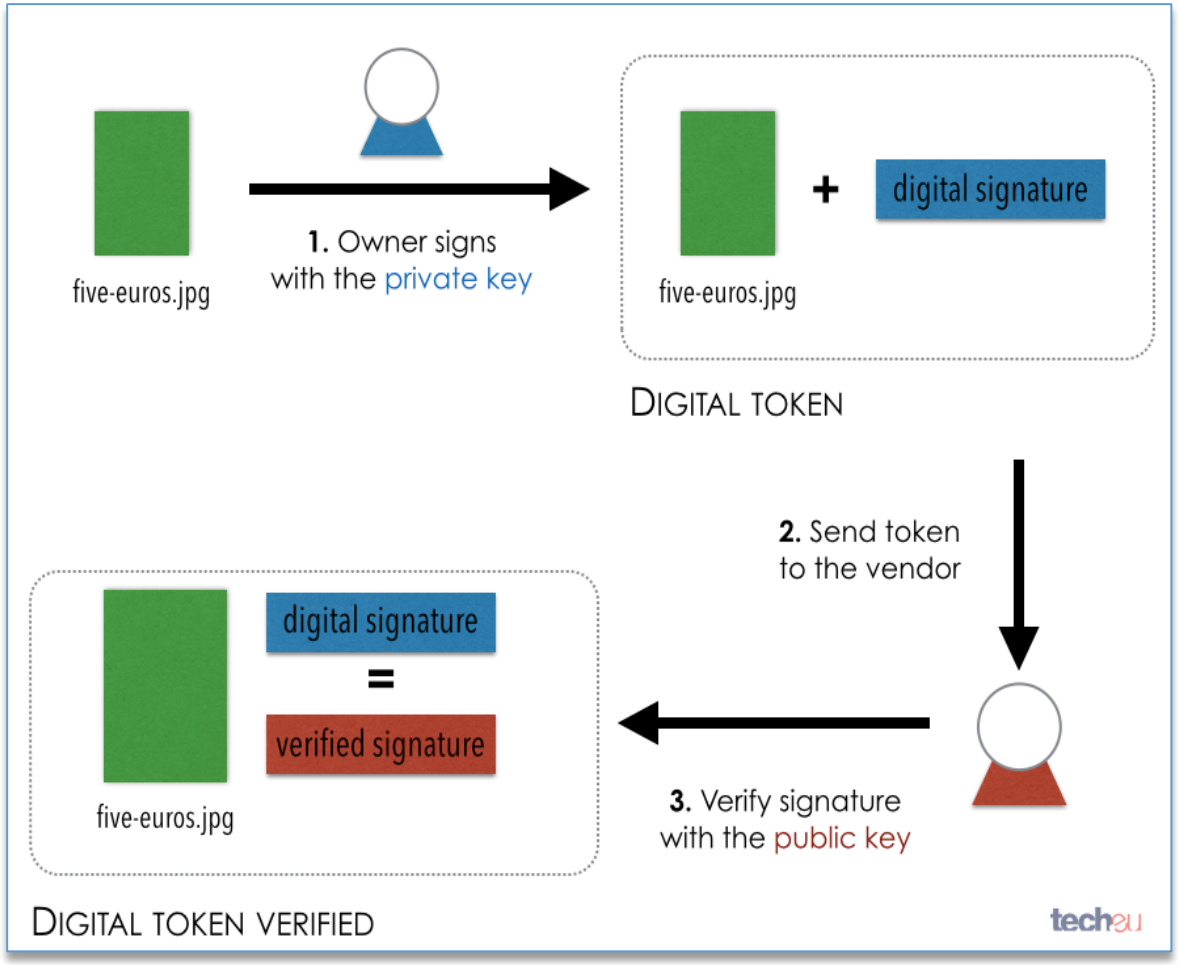
Overview of the Bitcoin network



Example of Financial transactions with bitcoin

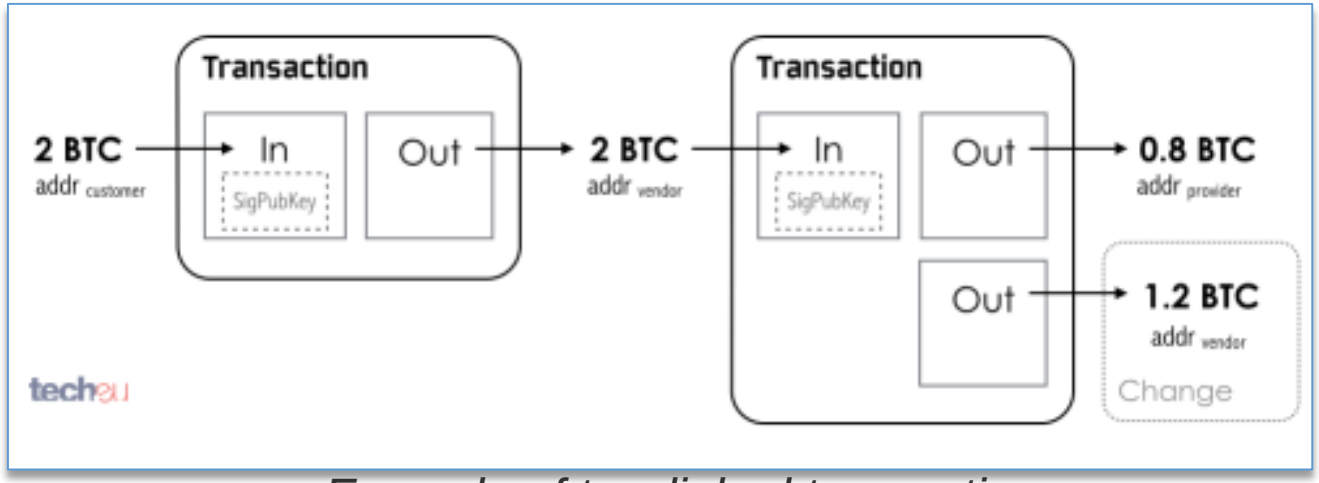


An example of a simple Bitcoin transaction

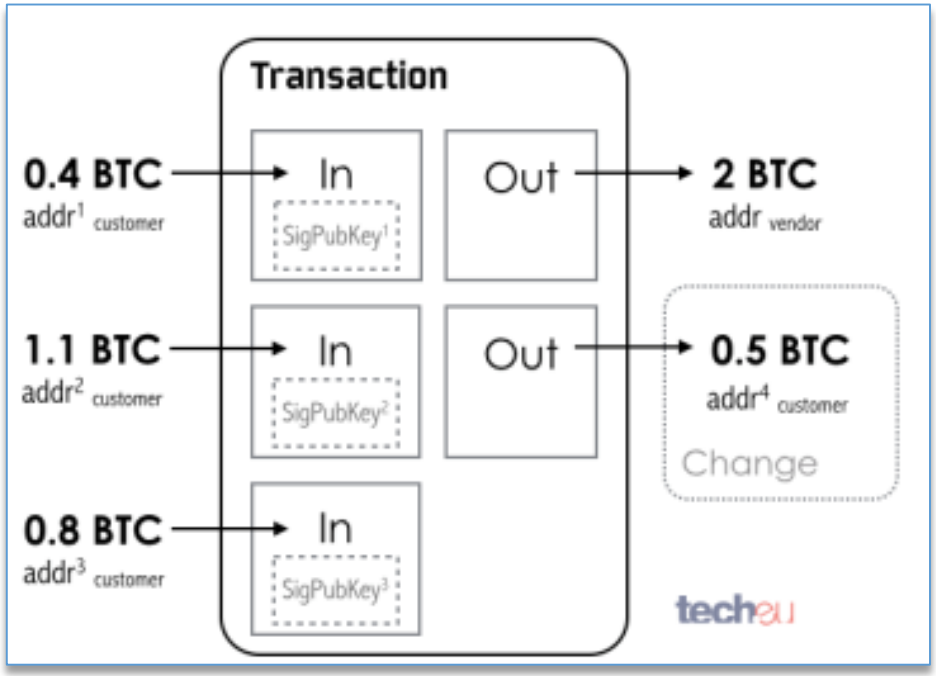


Verification of the ownership of a digital token

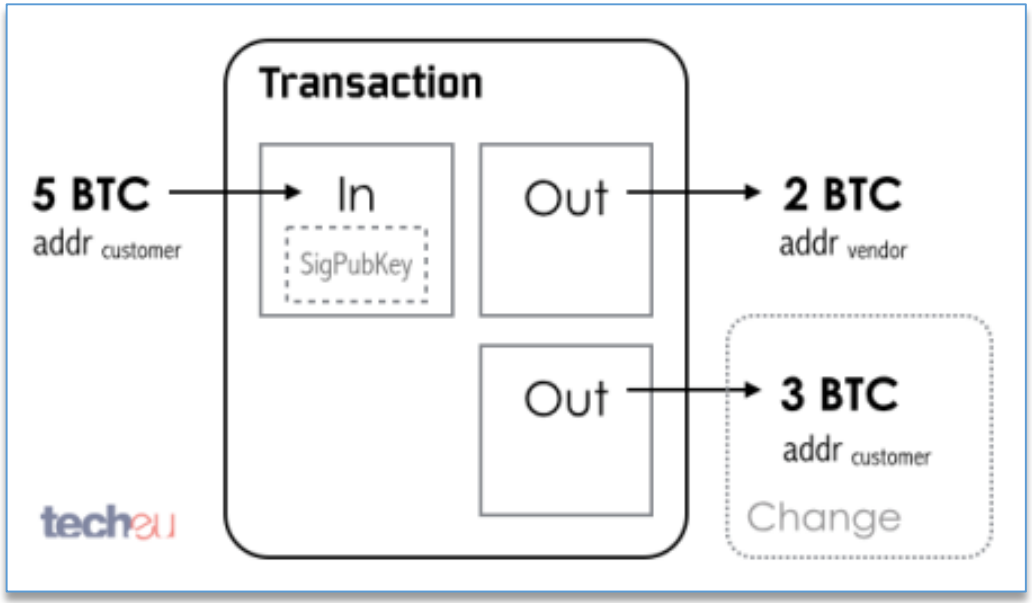
Examples of transactions with bitcoin



Example of two linked transactions

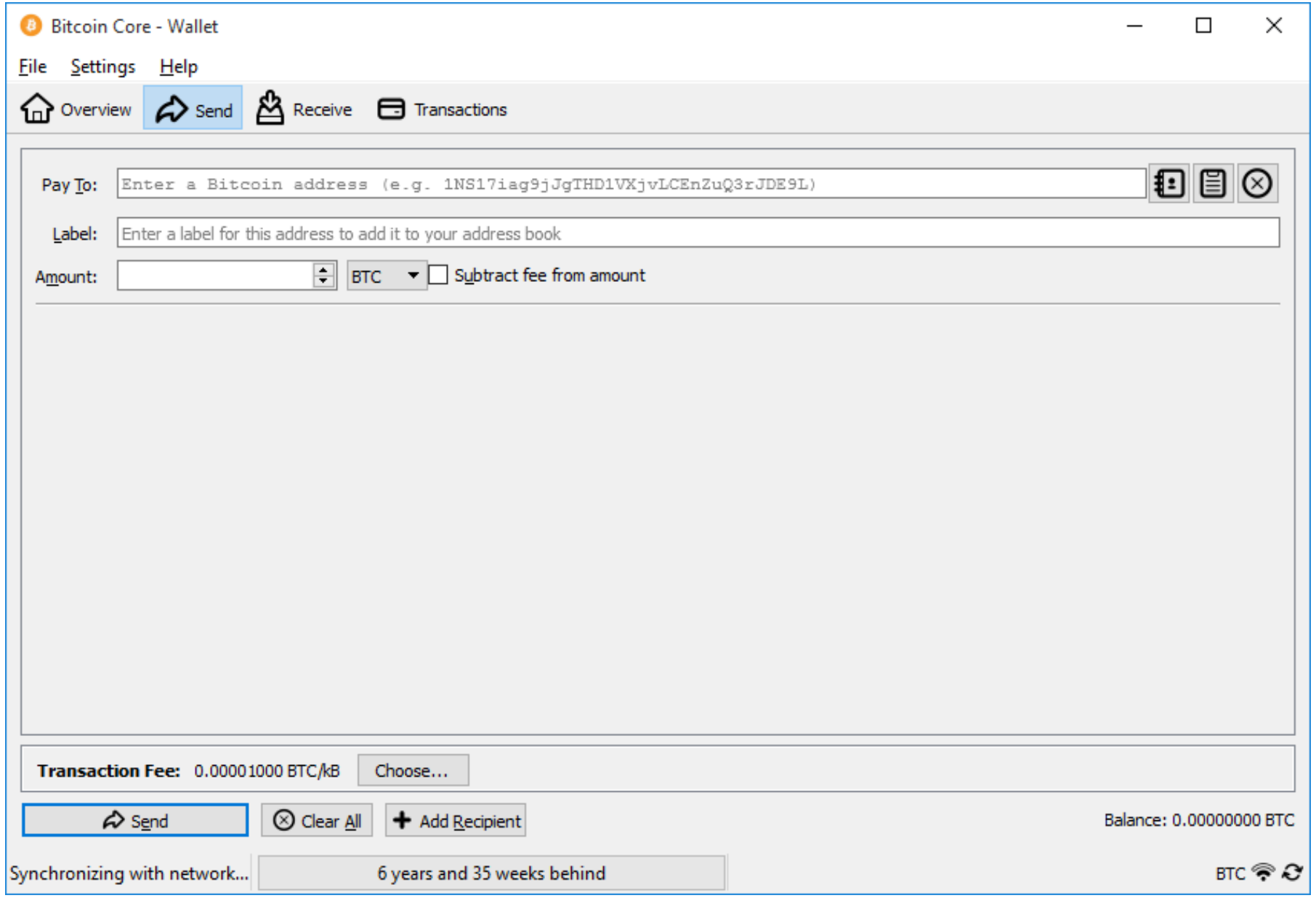


A multiple input-multiple output Bitcoin transaction



Single input-multiple output Bitcoin transactions

Send Bitcoins



Who prints it?

No one. This currency isn't physically printed by a central bank. Some argue central banks are unaccountable to the population and can simply produce more money to cover the national debt, thus devaluing their currency.

Instead, bitcoin is created digitally, by a community of people anyone can join. Bitcoins are '**mined**', using computing power in a distributed network.
This network also processes transactions made with the virtual currency, effectively making bitcoin its own payment network.

NORTHERN ARIZONA UNIVERSITY

7-Asymmetrical cryptography

- 7-1 PKI
  - Cryptography
  - Services
- 7-2 Blockchains
  - Bitcoin
  - Hash/DSA
  - Attacks

Hash based transaction for the bitcoin

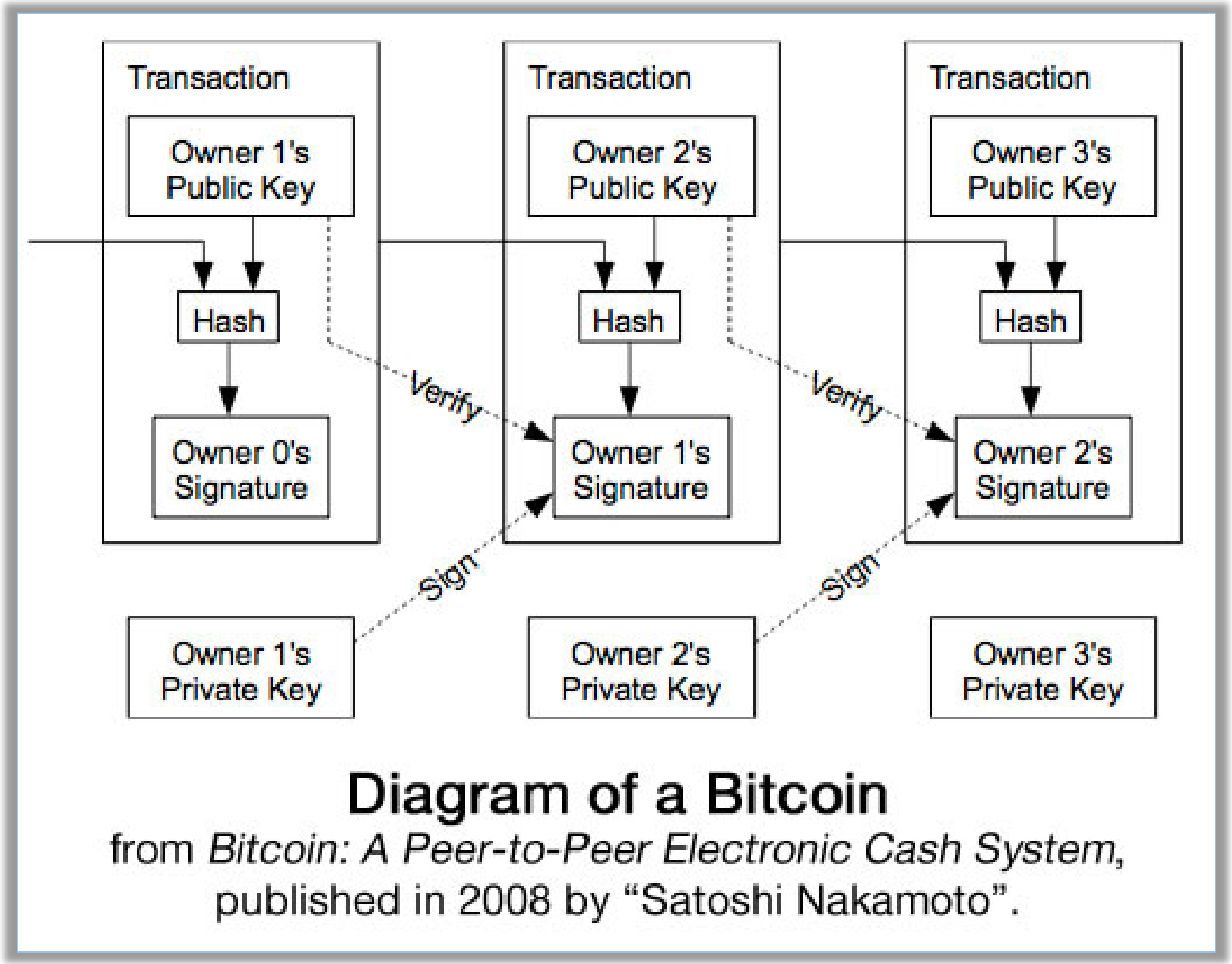
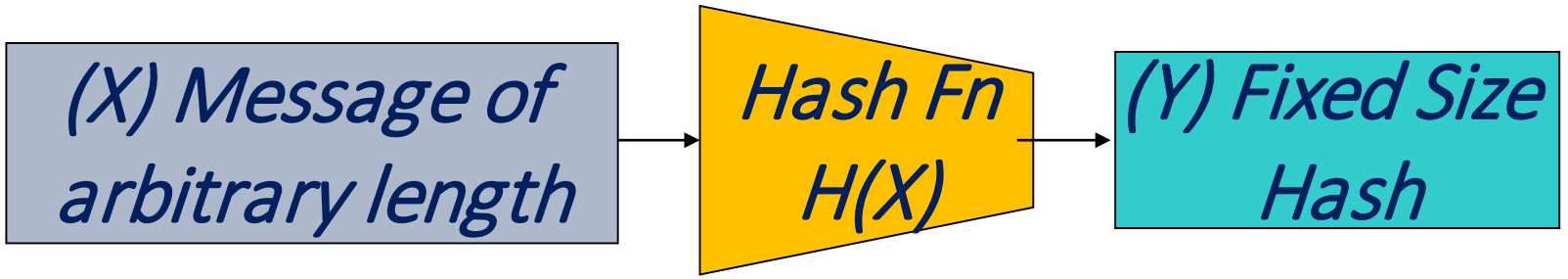


Diagram of a Bitcoin

from *Bitcoin: A Peer-to-Peer Electronic Cash System*, published in 2008 by "Satoshi Nakamoto".

Cryptographic Hash Functions

- Consistent:
  hash(X) always yields same result
- One-way:
  given Y, hard to find X s.t. hash(X) = Y
- Collision resistant:
  given hash(W) = Z, hard to find X such that hash(X) = Z



SHA-256 Hash Function

SHA-256 Hash Function

Generates 256 bit output irrespective of the size (or length) of input.

Collision resistant - two inputs will "never" generate the same output.

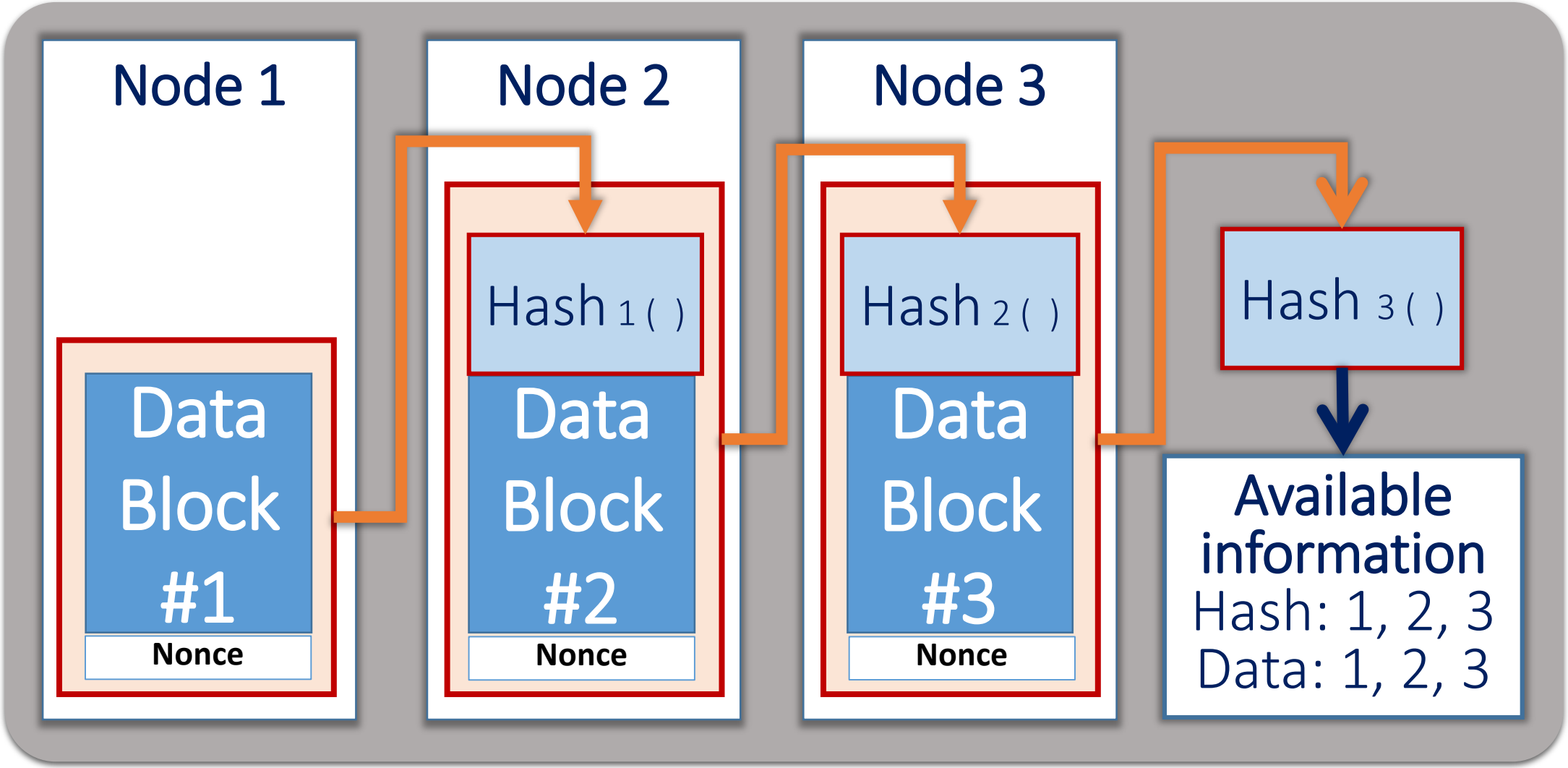
Hash("prithwis")
1b18b866382f05d8698ebcb8eae7c8811b3a988e7112503c1ecc9aacd9cc63e8

Hash("prithwish")
4486d9ef726a5a4a559f24cce58480968a4527004cfb7ceb8cf6fccbef2886bc

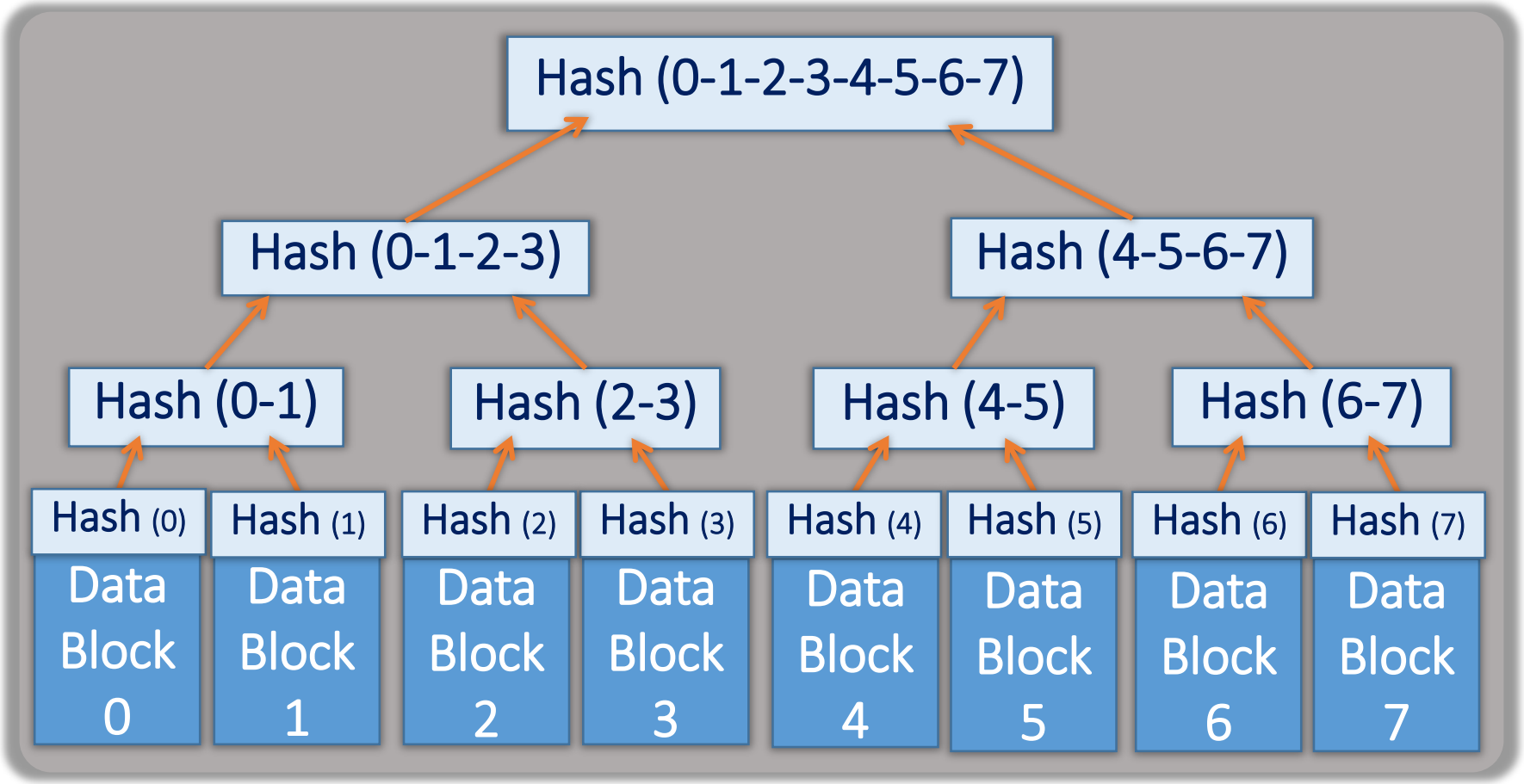
Hash("Our price bid is Rs 2,00,000")
62b72cda490d54e56ac0978d263906ef892b6449c1175ebf0af839c7f99e772f

Hash(pm.jpg) <- a full image file
af9493c777bcb88e57fb3e08cf05807d117f945fdffc932f3deddcc82835b385

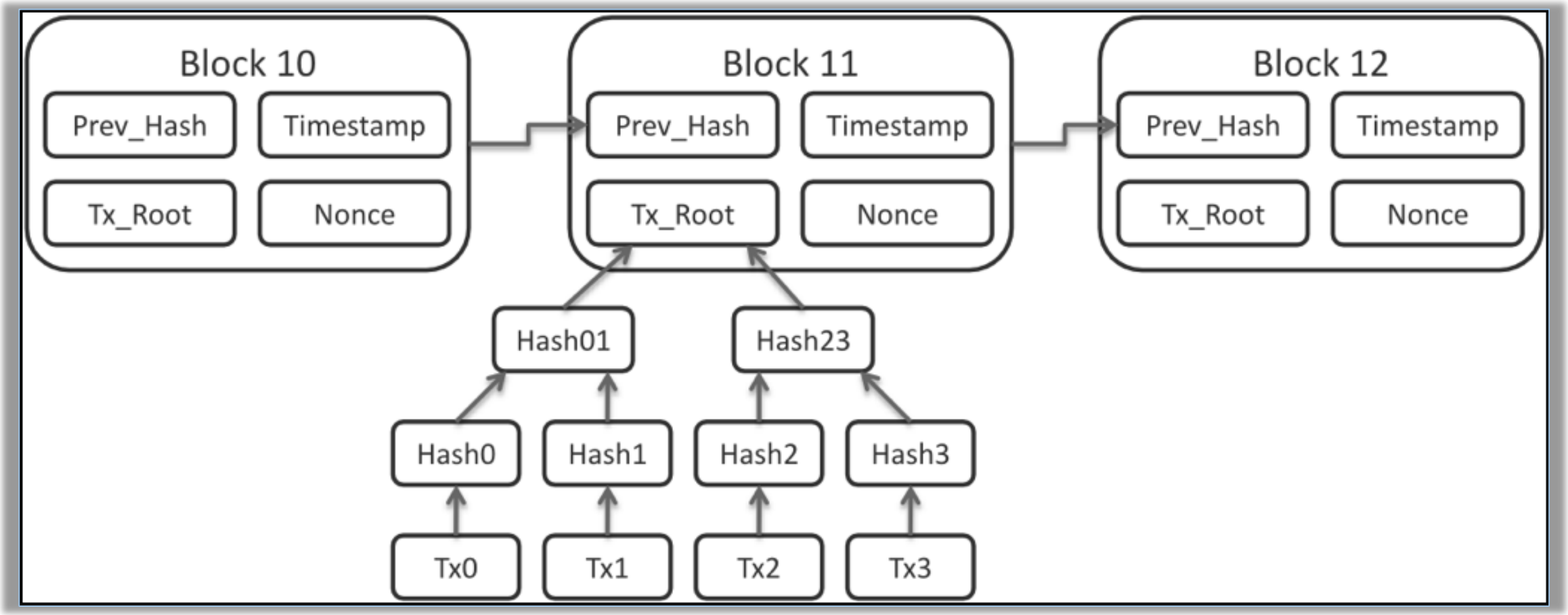
Hash Pointer



Merkel Tree


Hash (0-1-2-3-4-5-6-7)
Hash (0-1-2-3)
Hash (4-5-6-7)
Hash (0-1)
Hash (2-3)
Hash (4-5)
Hash (6-7)
Hash (0)
Hash (1)
Hash (2)
Hash (3)
Hash (4)
Hash (5)
Hash (6)
Hash (7)
Data Block 0
Data Block 1
Data Block 2
Data Block 3
Data Block 4
Data Block 5
Data Block 6
Data Block 7

Use of Merkel Tree to secure blockchains



Anatomy of a Block

Block #404234

Summary	
Number Of Transactions	459
Output Total	3,812.78908631 BTC
Estimated Transaction Volume	815.7381711 BTC
Transaction Fees	0.1059914 BTC
Height	404234 (Main Chain)
Timestamp	2016-03-25 15:52:47
Received Time	2016-03-25 15:52:47
Relayed By	BitFury
Difficulty	165,496,835,118.23
Bits	403088579
Size	704.855 KB
Version	4
Nonce	311538175
Block Reward	25 BTC

Hashes	
Hash	000000000000000000221e92ec5f42f4ccf8ba7ad71020e9dcbeed3f5e484b2f8
Previous Block	000000000000000000060e89871b8a2e9a769ec031ac3fc1da24d00886d5a8f256
Next Block(s)	000000000000000000005687e47a1fa3936b3c7eca894920b30d4904f42faa1df75
Merkle Root	3bef11b868b850a27ca176d8c4a5fb465f71771f9b46ba272dbf6f53d4e1550b

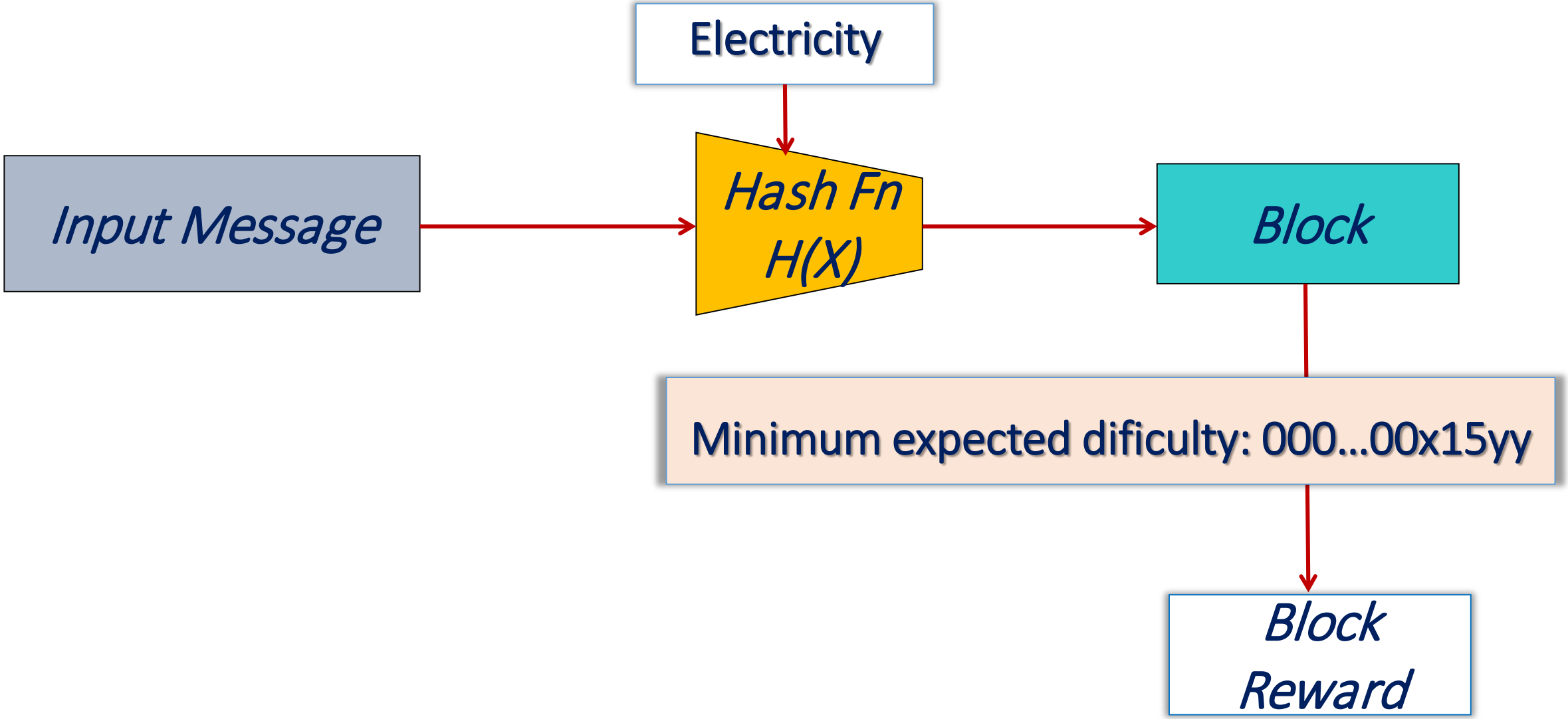
Network Propagation (Click To View)

Block Transactions

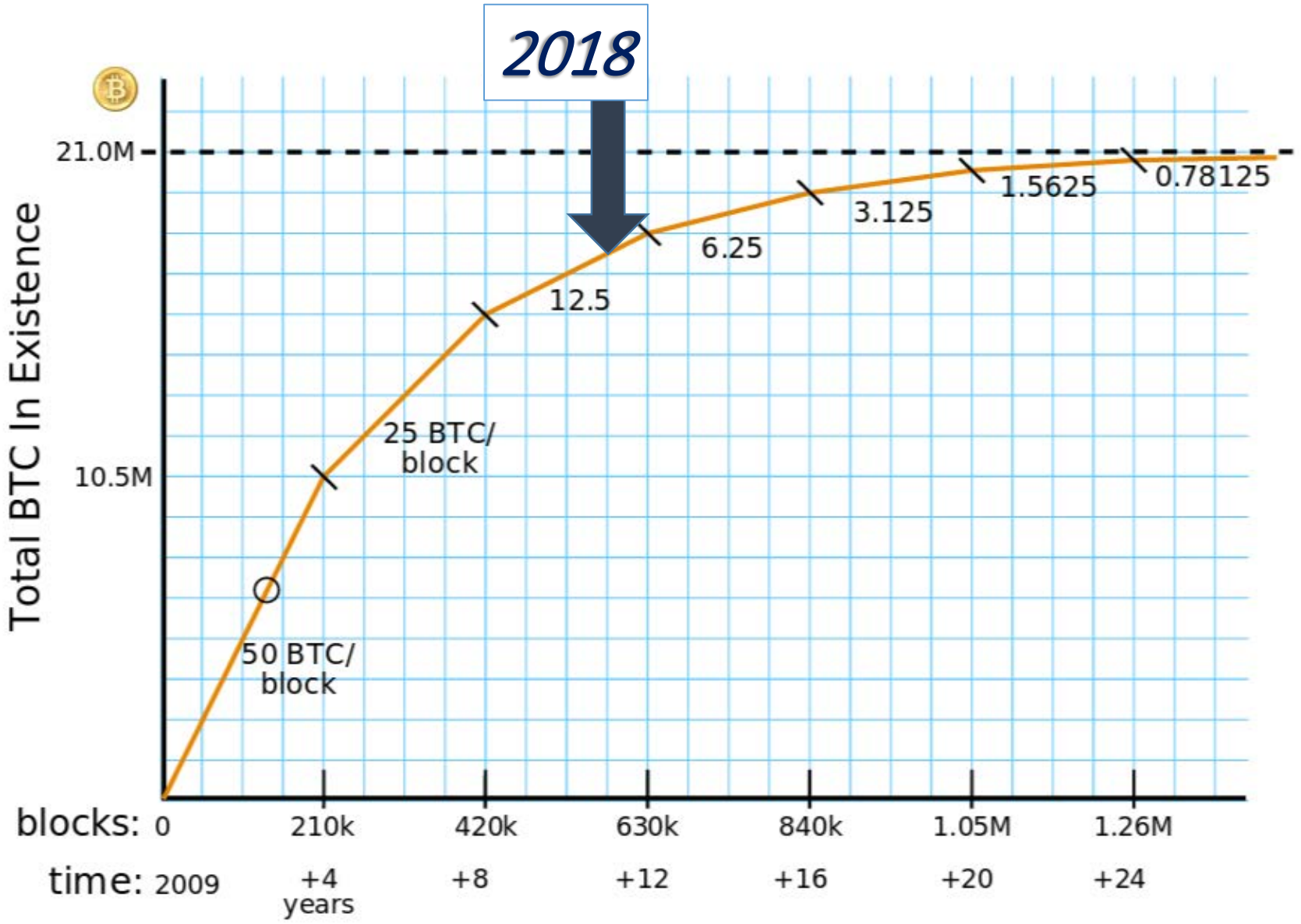
Transactions

4d0452c4fe98178875ede72319ca3162389edd43a22690ebcd49938bbcffd37c			2016-03-25 15:52:47
No Inputs (Newly Generated Coins)		1DrK44np3gMKuvc... (Bitfury)	25.1059914 BTC
			25.1059914 BTC
ed93695feee71a0d115d84e3bfbd759eebc03c3f707b9fdfec6fed3514d204ec			2016-03-25 15:51:26
1BJaAgMK9F31HpTB8yePe69zEqR6cTg9eS		1Lie2o1tAjKxHgRMkFVmJZUMgFbsjummks	1.1269325 BTC
			1.1269325 BTC
53cd4fbc48378eb686873f0f8b1d5cc34dfd0099bcc4cfb46069649fb18fe0e7			2016-03-25 15:51:55
17wLMV3wgDFCn4LQxQsDLrD6KvvVMZSuBi		15PUBY3omSex2kkBNBfEwextZvhRWYevNA 17zLoiL1EEdHkgdpNuagG1vq7Fa6UMyK2h	8.7 BTC 3.37028336 BTC
			12.07028336 BTC

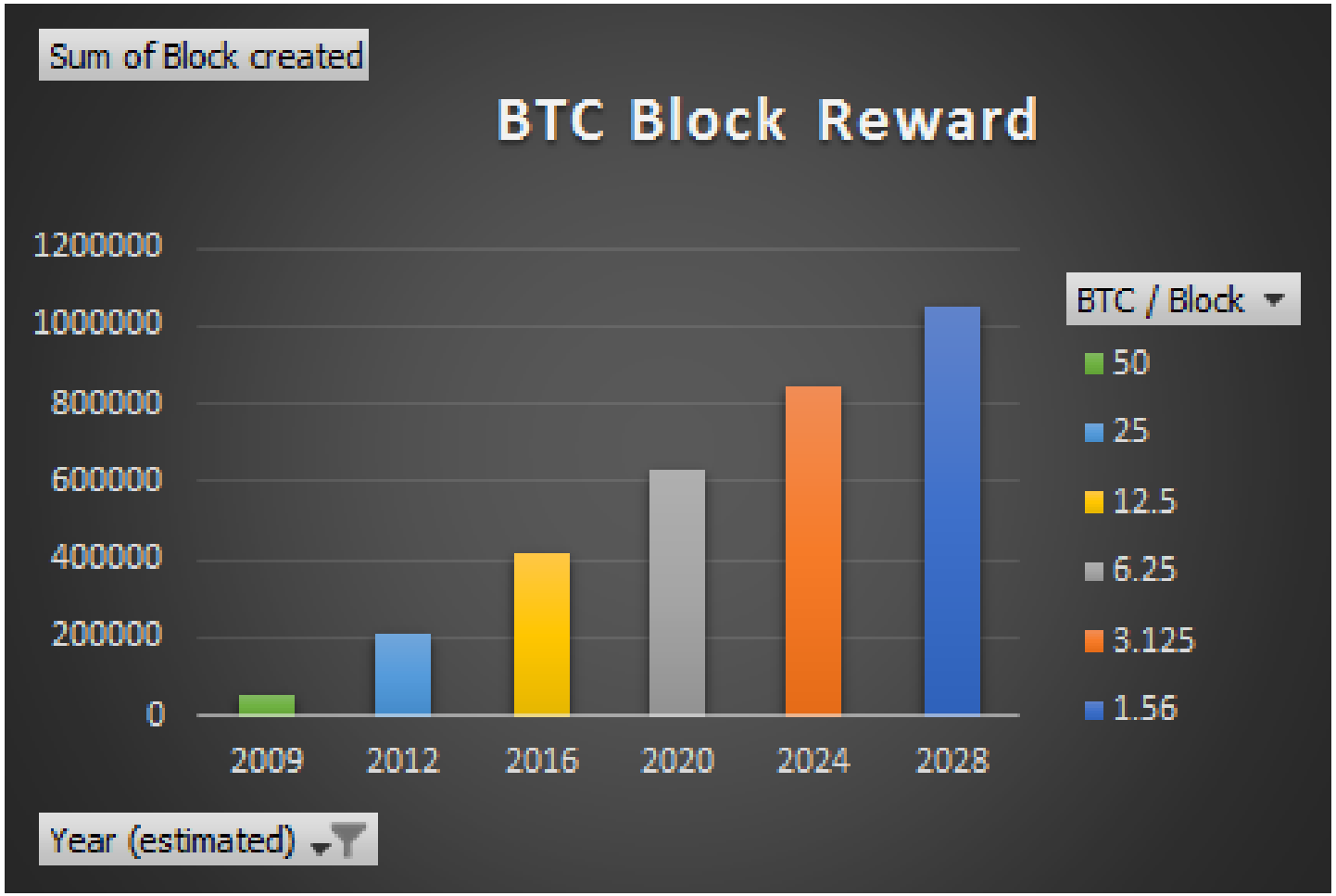
Bitcoin mining technology



Mining opportunities overtime

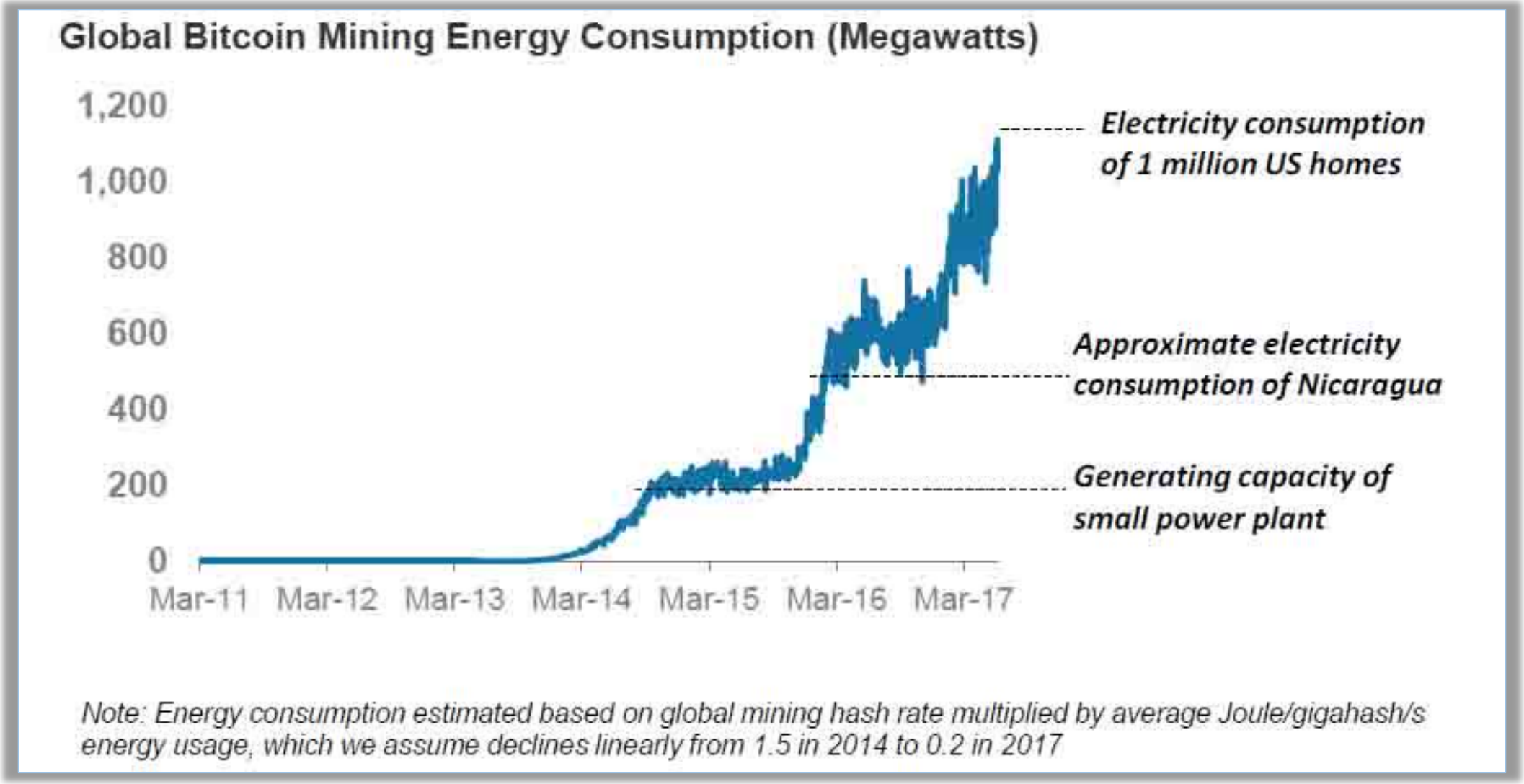


Mining rewards overtime



Year (estimate)	Block created	BTC / Block	Reward Era
2009	52560	50	1
2010	105120	50	1
2011	157680	50	1
2012	210240	25	2
2013	262800	25	2
2014	315360	25	2
2015	367920	25	2
2016	420480	12.5	3
2017	473040	12.5	3
2018	525600	12.5	3
2019	578160	12.5	3
2020	630720	6.25	4
2021	683280	6.25	4
2022	735840	6.25	4
2023	788400	6.25	4
2024	840960	3.125	5
2025	893520	3.125	5
2026	946080	3.125	5
2027	998640	3.125	5
2028	1051200	1.56	6
2029	1103760	1.56	6
2030	1156320	1.56	6

Energy needed to mine bitcoins



Mining In Mongolia

Bitcoin mining hardware

ASICMINER BLOCK ERUPTER
BY THE NUMBERS

Hash Rate: 330 MH/s
PCB Temp: 125°F / 51°C
Weight: 2.1 Ounces

Power Usage: 500 - 510 mA, 2.5 w
Heat Spreader Temp: 136.5°F / 58°C
Cost: 1.05 BTC / $184.00
Break Even Point: 30 / 50 weeks

Interface: Standard USB
Dimentions: 3" x 1.4" x 0.5"
MHash/Sec/$: 1.79

Comes in 4 different colours

bitcoin

CRYPTO DRILLING

$5,689^{00}

ETH ZEC miner case
12GPU 2PSU

- 1-9 Pieces
US $60.00
- 10-999 Pieces
US $58.00
- >=1000 Pieces
US $55.00

Capacity:
128GB16GB256GB
All 10 Options
Color:
-+
Shipping fee:
US $ 227.49 to United States by Express FedEx IE
Lead Time:
1 day(s) after payment received

Digital Signature

1- Alice initiate the transaction

Create a hash with a unique number

2- Alice create a digital signature with private key

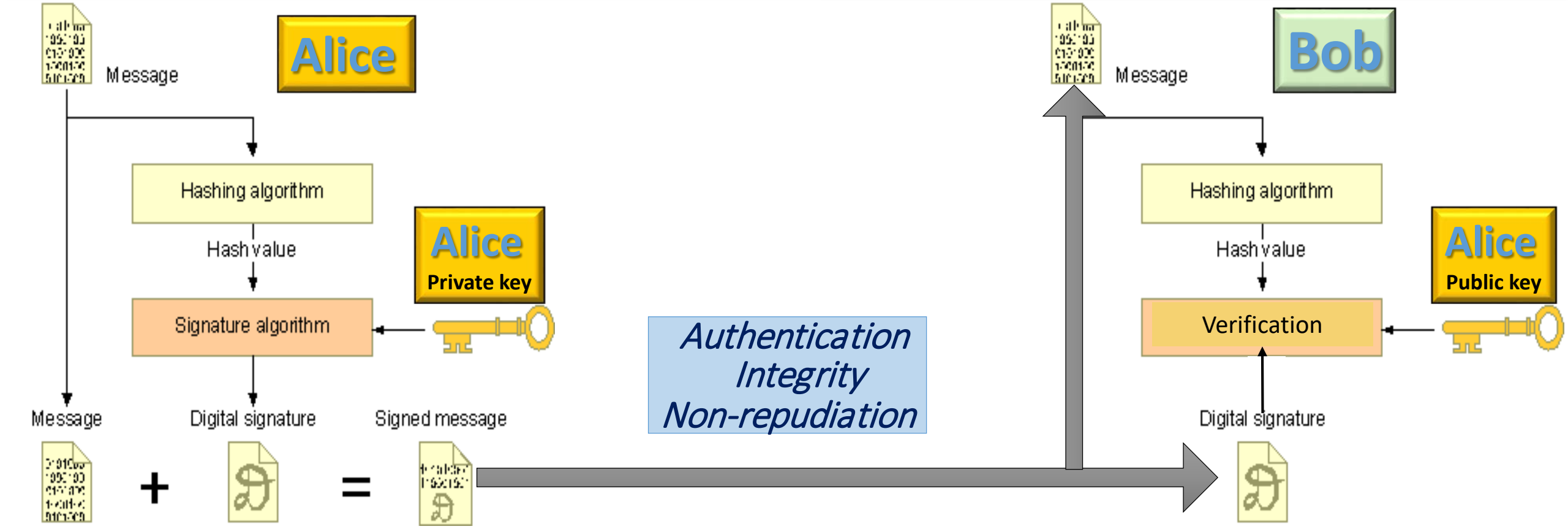
To prove that the message is authentic

1- Bob read the hash

Information is accepted: sell/buy the bit coin

2- Bob read the signature

Verify that the message is authentic



NORTHERN ARIZONA UNIVERSITY

7-Asymmetrical cryptography

- 7-1 PKI
  - Cryptography
  - Services
- 7-2 Blockchains
  - Bitcoin
  - Hash/DSA
  - Attacks

Bad Uses for Good Technology

- Bitcoin has had its fair share of “bad press”
- Silk Road
  - An online anonymous marketplace for “censorship-free” commerce
  - Ross Ulbricht’s trial starts this week
- Bitinstant
  - Charlie Shrem plead guilty to aiding money laundering
- MT-GOX
  - aka “Magic The Gathering Online eXchange”
  - 700,000 coins “missing”
- Neo & Bee
- Bitstamp

Black Markets

Silk Road: US$14M in Revenue in 2012

Welcome! | Silk Road

http://ianxz6zefk72ulzz.onion/index.php

silk road darknet

Most Visited | Learn more about Tor | The Tor Blog

Are you using Tor? | list of TOR sites silkroad - Goo... | TORDIR - Link List | Welcome! | Silk Road

Silk Road

anonymous marketplace

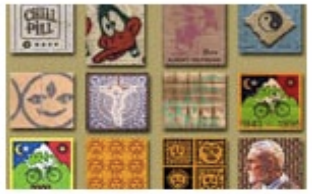
Welcome

messages(0) | orders(0) | account(฿0) | settings | log out

(0)

Shop by category:

- **Cannabis(203)**
- **Ecstasy(35)**
- **Psychedelics(127)**
- **Opioids(39)**
- **Stimulants(68)**
- **Dissociatives(9)**
- **Other(197)**
- **Benzos(43)**



1 hit of LSD (blotter)
฿0.58

1/8 oz high quality cannabis
฿2.05

1 g pure MDMA (white)
฿1.28

Step-by-step:

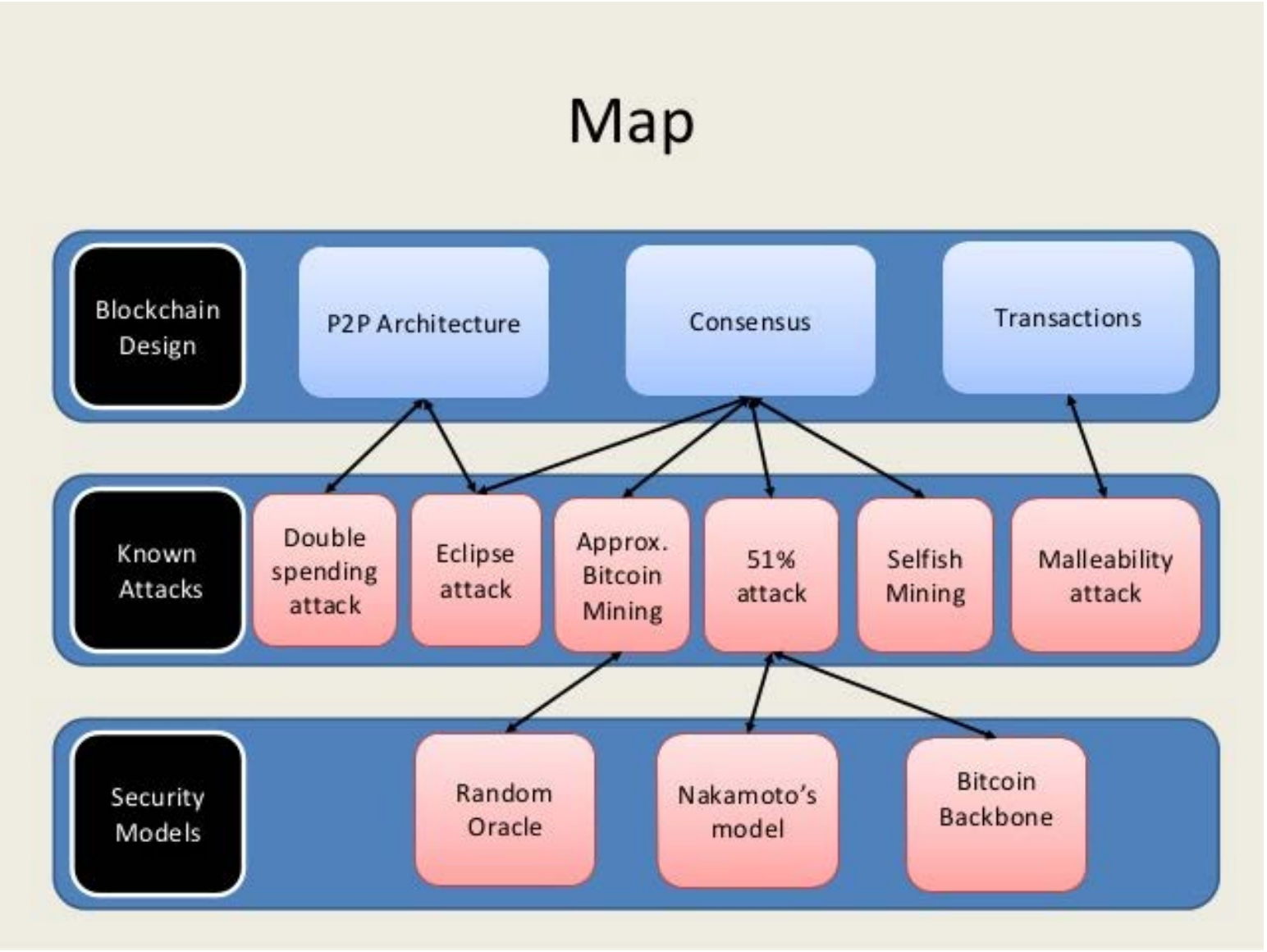
1. Get **anonymous money**
2. Buy something here
3. Enjoy it when it arrives!

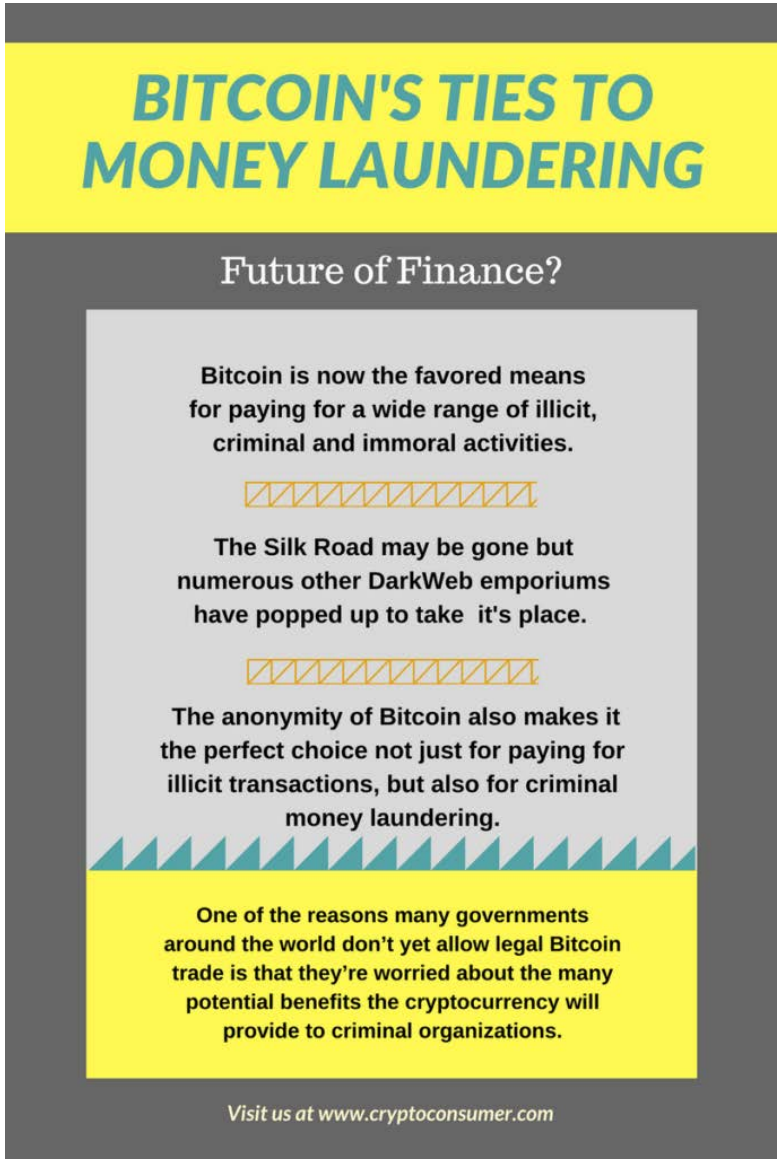
Vacation mode. Important info for **sellers**...

recent feedback:

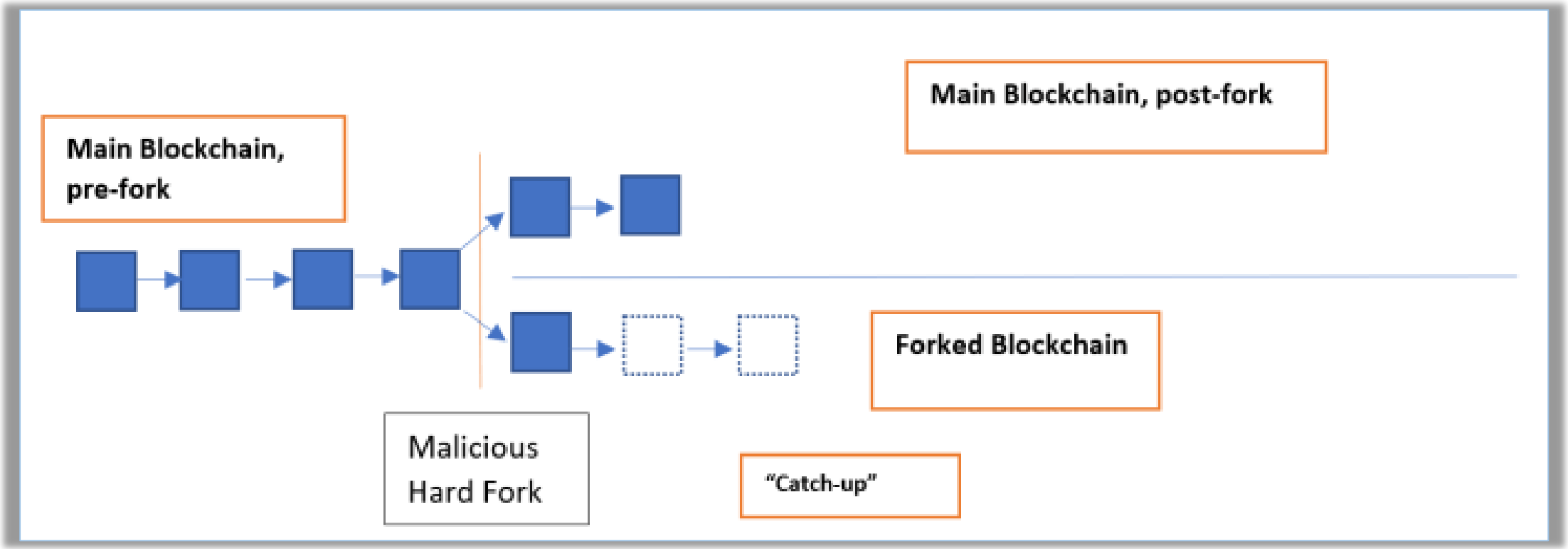
seller	rating	feedback	
1UP of Canada(97)	4 of 5	amazing weed. the only reason this is not a 5 is because the package was so tightly double vaccuum sealed that the product was flattened, which I know is necessary for security but it still decreases quality	**item**
CaliforniaSunrise	5 of 5	Fast shipping. Nice packaging. I haven't tried the chocolate yet, but it looks tasty! Smooth transaction.	**item**
Rook	5 of 5	all good! thanks so much!	**item**
illy	5 of 5	Very friendly. Fast Shipping. Great packaging.	**item**
somatik	5 of 5	Order arrived quickly and as described. Thanks!	**item**
gamely54	5 of 5	No issue at all, I officially recommend this seller. Now go forth and purchase from him!	**item**
mellowyellow	5 of 5	Item arrived quickly and as described, good communication. This guy's legit.	**item**
dirtysouf(100)	5 of 5	looks good	**item**

Known attacks

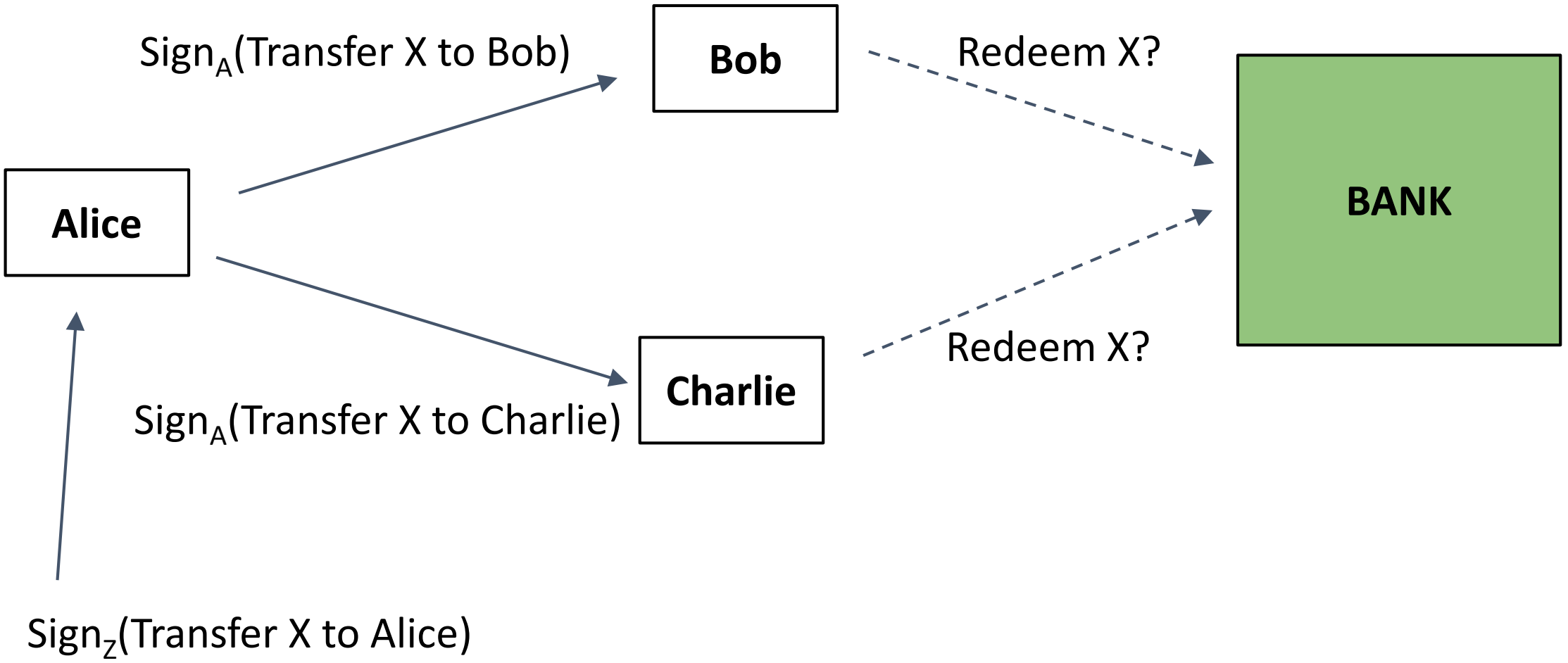




Double spending attack

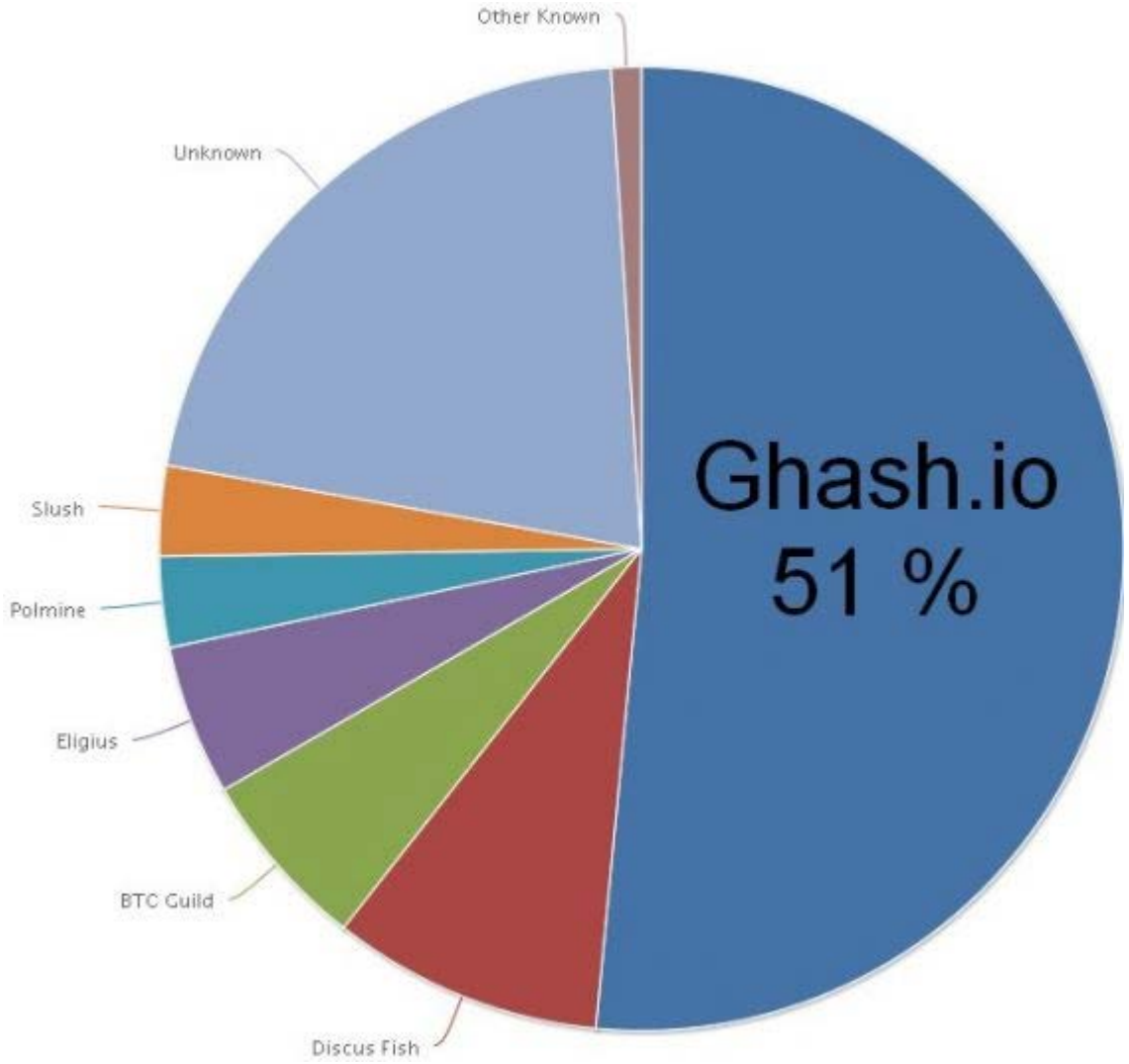


Double spending: why ecash is hard



JB

51% attack


Other Known
Unknown
Slush
Polmine
Eligius
BTC Guild
Discus Fish
Ghash.io
51 %

NORTHERN ARIZONA UNIVERSITY

Summary

- 1- Bitcoin cryptography is strong
- 2- ECC is fine, but will be compromised by QC
- 3- SHA hashing is strong
- 4- Anonymity creates an anonymity problem
- 5- Crypto-currencies have the potential to replace current financial infrastructures

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

Safeguarding: Proof of Work

Of course, there's still a trust issue with the Bitcoin network. If miners are the real validators of the transactions, then any single entity owning enough miners could potentially subvert the Blockchain. With ownership of the network, old transactions could be manipulated and even open up the possibility of double spending.

To avoid this, Bitcoin introduced a safeguard mechanism called Proof of Work (PoW), a small mathematical problem every miner has to solve before sending a block back to the node. PoW is designed so it takes miners, on average, 10 minutes to complete.

The computing power and randomness required to obtain the solution of the problem prevents having rogue agents fully controlling the Blockchain. Essentially, the more computer power you own, the faster you can compute the PoW.

But there's a catch: Every 2016 blocks (around two weeks), the network checks how fast the miners have worked. If they've mined blocks faster than expected, it means the miners have increased their computational power.

To prevent this from happening and tipping the balance, the network modifies the difficulty of the PoW and increases it so the average time to solve it remains at 10 minutes.

If mining a block costs computational power, then why would anyone want to do it? Well, miners are rewarded with Bitcoins. Originally, for every block, miners would be awarded 50 Bitcoins plus any transaction fees. This reward is called a coinbase transaction.

Coinbase transactions introduce new Bitcoins into the system, control the inflation of the currency and, at the same time, deter any attempt to subvert the network. The system is designed under a controlled supply – this means that every four years, the mining reward gets halved.

The role of Blockchain

The original Bitcoin paper highlighted two major goals behind the design of the cryptocurrency: 1) To create a digital currency preventing the double spending problem 2) To achieve the first goal without a centralized third-party financial institution.
In previous attempts to build digital currencies, the ledger was always stored by a centralized third-party. Bitcoin circumvents this by deploying a peer-to-peer network of shared ledgers. Every client in the Bitcoin network owns a copy of Blockchain, which is public and accessible to anyone in the network allowing unprecedented transparency to the currency.

The Bitcoin network is made out of interconnected clients, called full clients or nodes, that are in charge of validating any transactions received. Once validated, the clients broadcast the transaction to neighbouring until each one in the network has a copy of it. Instead of storing the transactions as they are, Blockchain bundles them into what is dubbed a 'Bitcoin block'. Once a block is created, it will be broadcasted to all the other nodes so everyone can update their Blockchain. Each block is then linked to the previous block, creating a chain that can be traced to the first block ever created – the 'genesis block'.

Users in charge of creating these blocks are called 'miners' and the process, unsurprisingly, is called 'mining a block'.
In the early days, every client in the network was a miner. Currently, miners have dedicated clients that connect to the Bitcoin network with specific protocols. Once a transaction gets bundled into a block and is accepted by a large majority of the network, it is considered official. Once a node receives a block from a miner, it will add it to its local Blockchain and broadcast it to the rest of the network. As we can see below, each block can contain any number of transactions.