Electronic Signatures and Similarities Between Blockchain

İBRAHİM DEMİRAL

ECZACIBAŞI BİLİŞİM A.Ş.

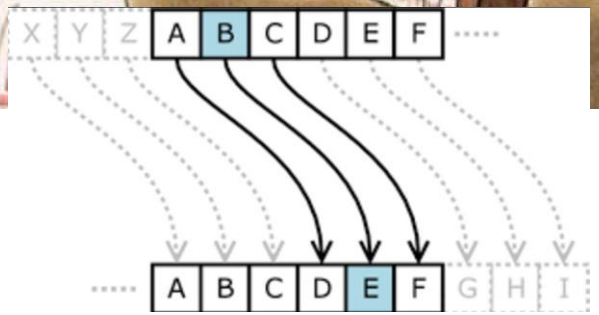
Dijital Transformation in Business Process

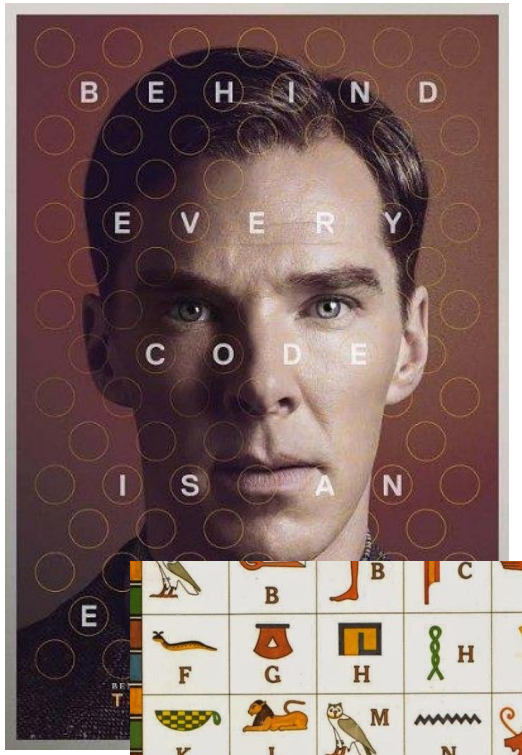
Cryptology

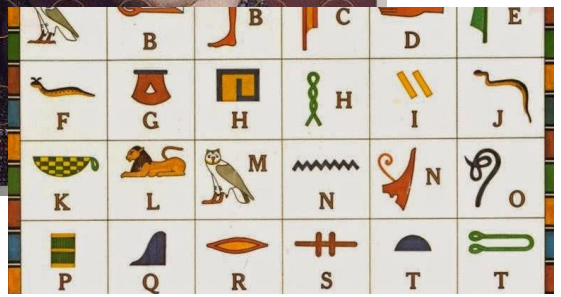
Cryptology (from Greek kryptós, "hidden, secret"; and graphein, "to write") is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

- Cryptography
- Cryptanalysis

History of Cryptology







History of Cryptology

Ancient Egypt

Skytale

Julius Caesar

Enigma

M-138-A Strip Cipher

NSA

Lucifer

TUBITAK UEKAE

Classic Encryption Algorithms

Classic Encryption Algorithms

Transposition

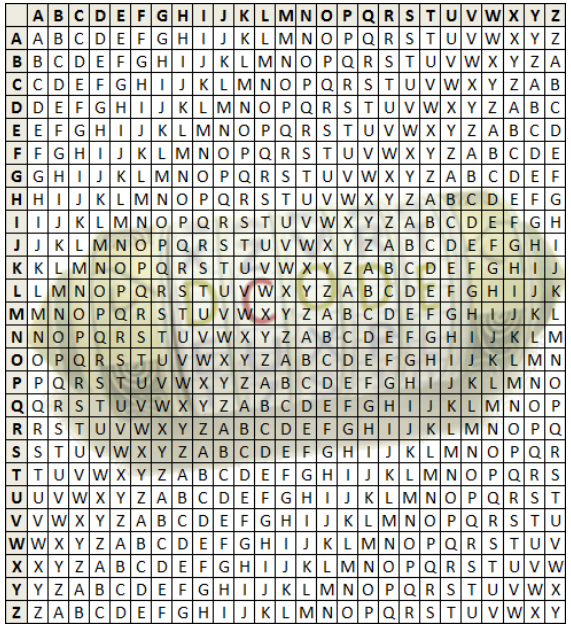
Substitution

- Monoalphabetic Substitution
- Polyalphabetic Substitution

Multiple – Letter Encryption

H E L O W
R D A B C
F G I J K
M N P S T
U V X Y Z

Key: Hello World



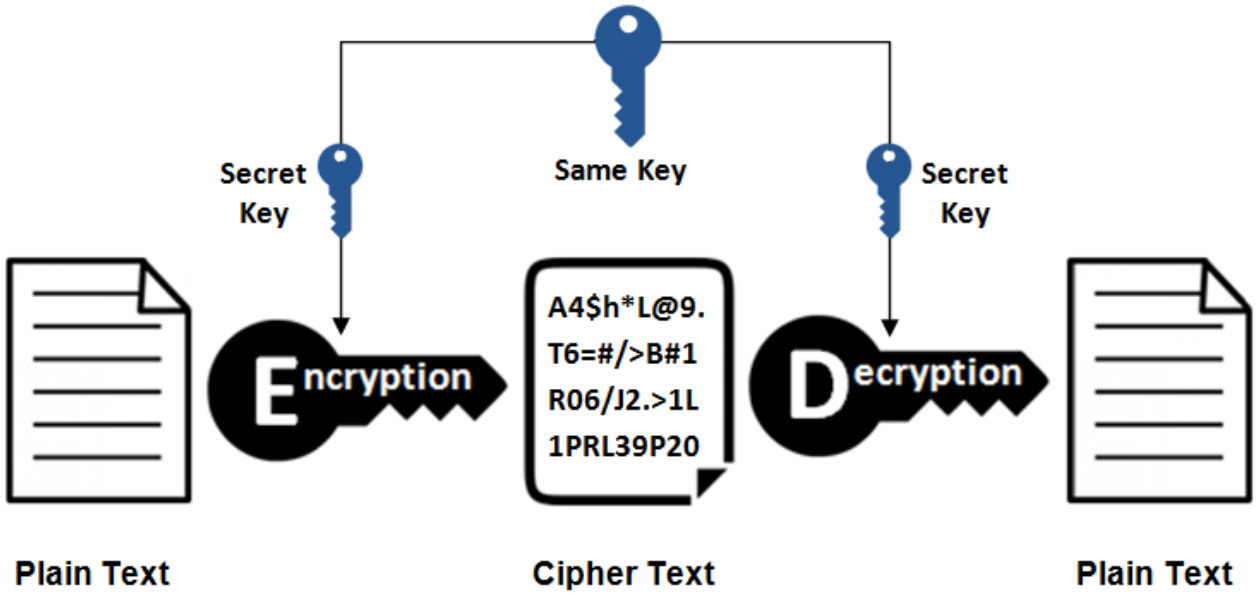
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Modern Encryption Algorithms

Symmetric and Asymmetric

Symmetric Key Cipher

This is the simplest kind of encryption that involves only one secret key to cipher and decipher information. It uses a secret key that can either be a number, a word or a string of random letters. It is a blended with the plain text of a message to change the content in a particular way. The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages



Symmetric Cryptography Algorithms

DES (Data Encryption Standard)

3DES (Triple DES)

AES (Advanced Encryption Standard)

Symmetric Key Cipher

Advantages:

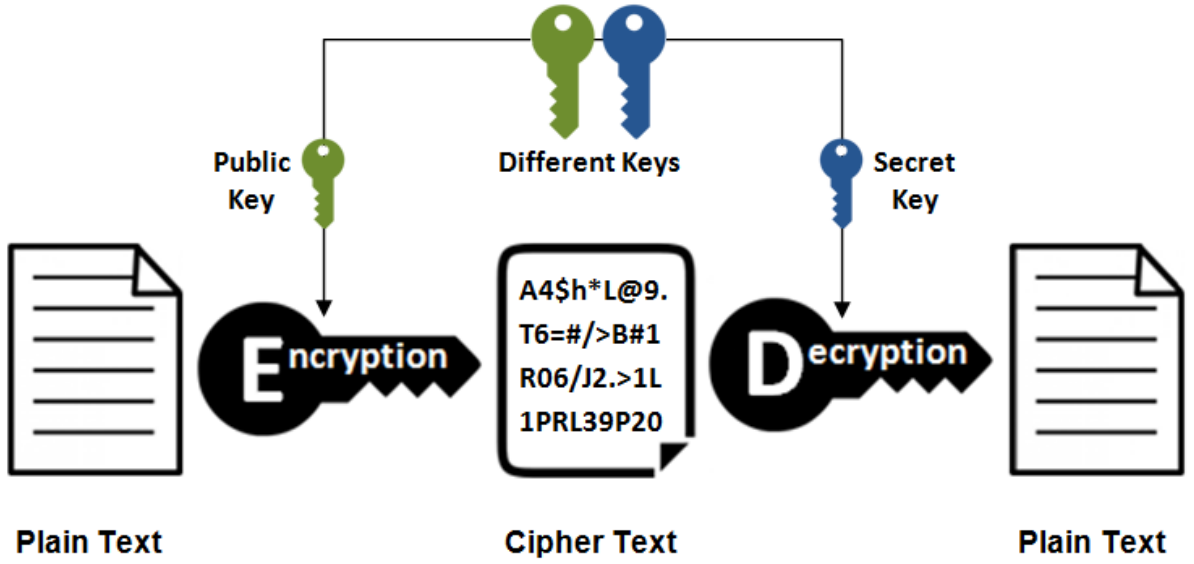
- Faster
- Key ciphers are small
- Encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the data, the chances of data being decrypted are null.
- A system only which possesses the secret key can decrypt a message

Disadvantages

- Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally
- Secret key must be kept secret.
- In big ecosystems, many keys are needed.
- In two way communications, secret keys must be changed

Public Key Cipher

Asymmetric encryption uses two keys to encrypt a plain text. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.



Asymmetric Cryptography Algorithms

Key Share Algorithms

- RSA, DH

Signing Algorithms

- DSA, ECDSA, RSA

Public Key Cipher

Advantages:

- Must keep only private key.
- Private/Public key pair can be kept longer according to usage
- These methods enable efficient digital signature mechanisms
- In big networks, necassary key number can be few

Disadvantages

- Slow
- Long key lengths.
- New.

Hashing Algorithms

Hashing

Hashing is generating a value or values from a string of text using a mathematical function. It is mainly used for two purposes

Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering.

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string so size of the sender’s data is reduced.

Properties

There is no classification as symmetric / asymmetric for the summarization algorithms. Hashing algorithms do not use keys.

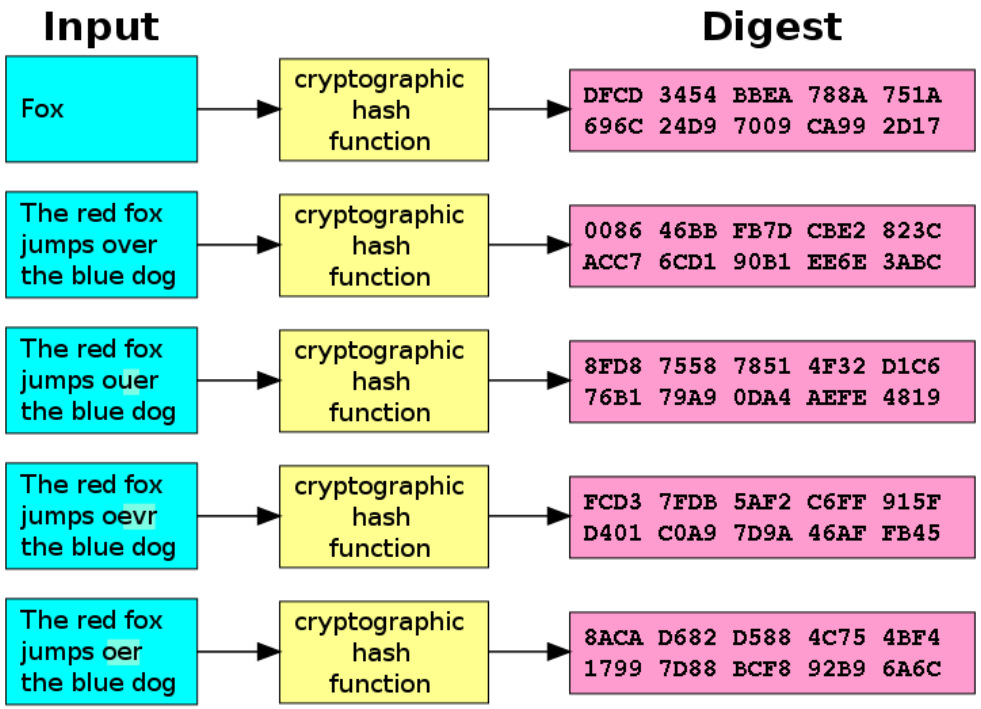
Hashing algorithms are one way. For this reason, from hashed data, the actual data can not be obtained. Strong algorithms should be used to guarantee the recycling

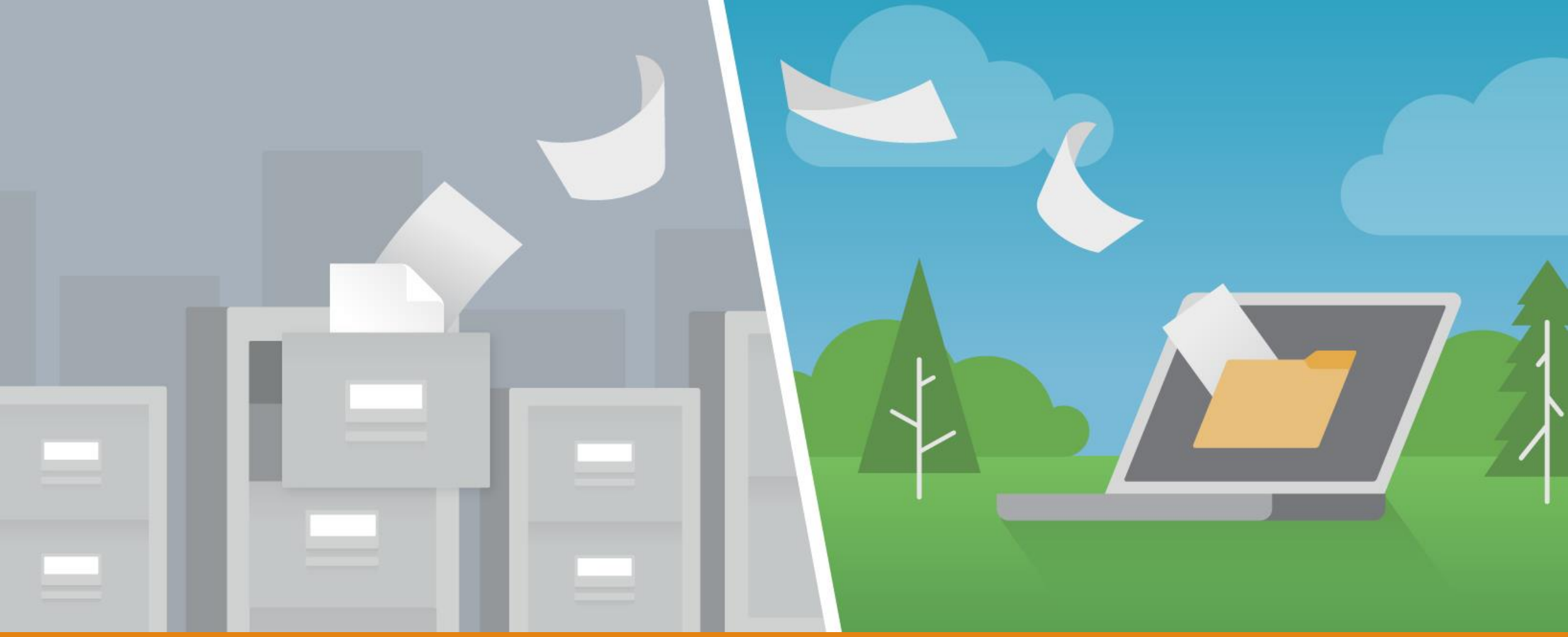
If the same text is processed with the same hashing algorithm, the same result is obtained every time. Integrity check can be performed for this reason.

With a powerful hashing algorithm, a small change in the text results in a large change in the output.

Hashing Algorithms

MD5, RIPEMD160, SHA1, SHA256, SHA384, SHA512, MACTripleDES, HMACSHA1





Digital Transformation

A greener world!!

What is Signature

A signature is a handwritten (and often stylized) depiction of someone's name, nickname, or even a simple "X" or other mark that a person writes on documents as a proof of identity and intent

Identity, Declaration, Will

What is Electronic Signature

An electronic signature, or e-signature, refers to data in electronic form, which is logically associated with other data in electronic form and which is used by the signatory to sign

An electronic signature is intended to provide a secure and accurate identification method for the signatory to provide a seamless transaction.

According to the Electronic Signature Law No. 5070, an electronic signature is an application that has the same legal validity as the wet signature we use in our daily lives.

E-Signature in Turkey

29 June 2001 working group

10 September 2002 Drafts

Started legally in 23 January 2004

Why?

Accelarating Processes

Digital Transformation

Increasing reliability

Authentication

Integrity

Irreversibility

Respect for the environment

How?

USB Token

HSM

Mobile Signature

Timestamp

CADES, PADES and XADES

SHA1, SHA256, SHA-384, SHA-512

Public Key Infrastructure (PKI)

Certificate Authority (CA)

What?

Document Signing

Banking Operations

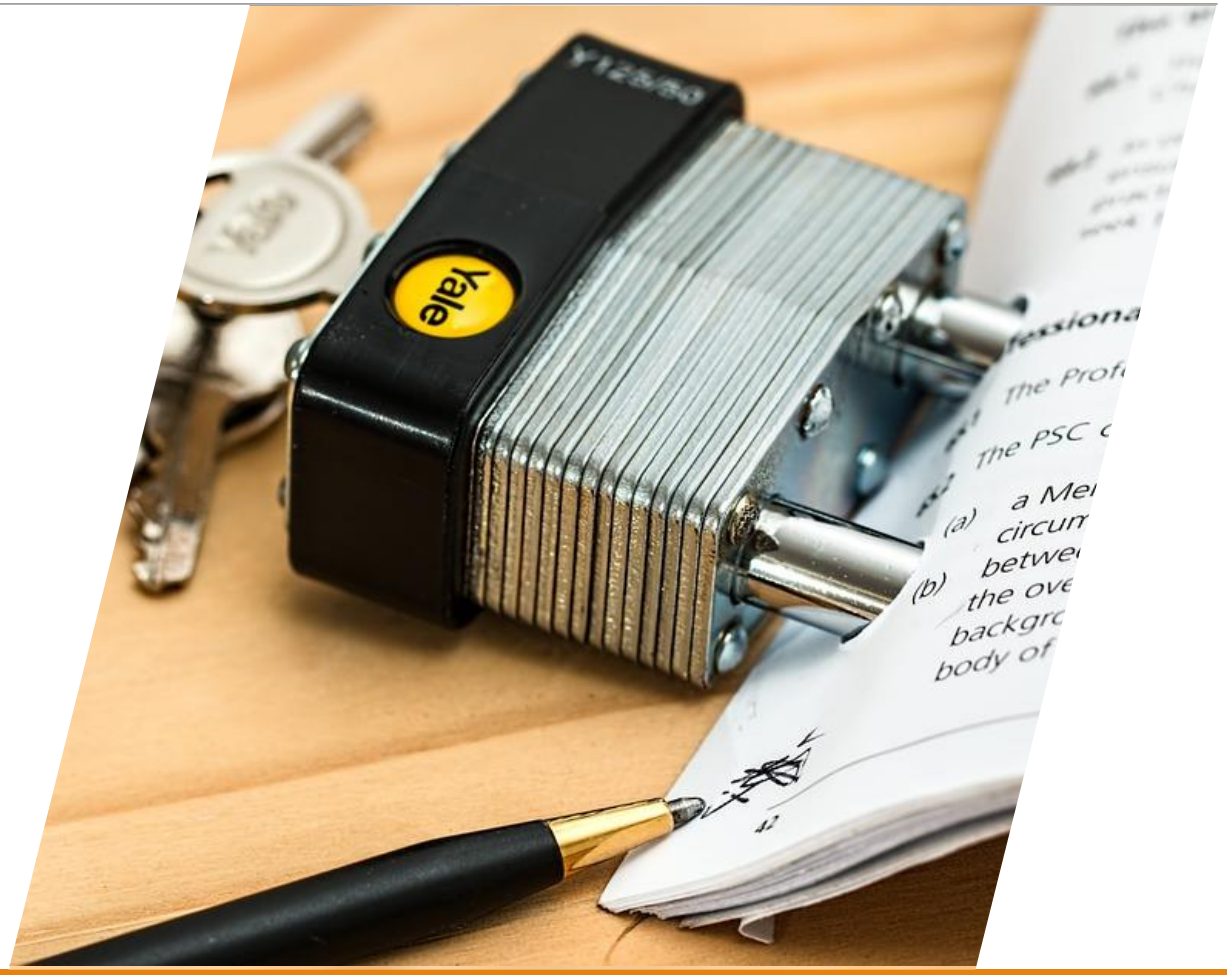
Contracts

KEP

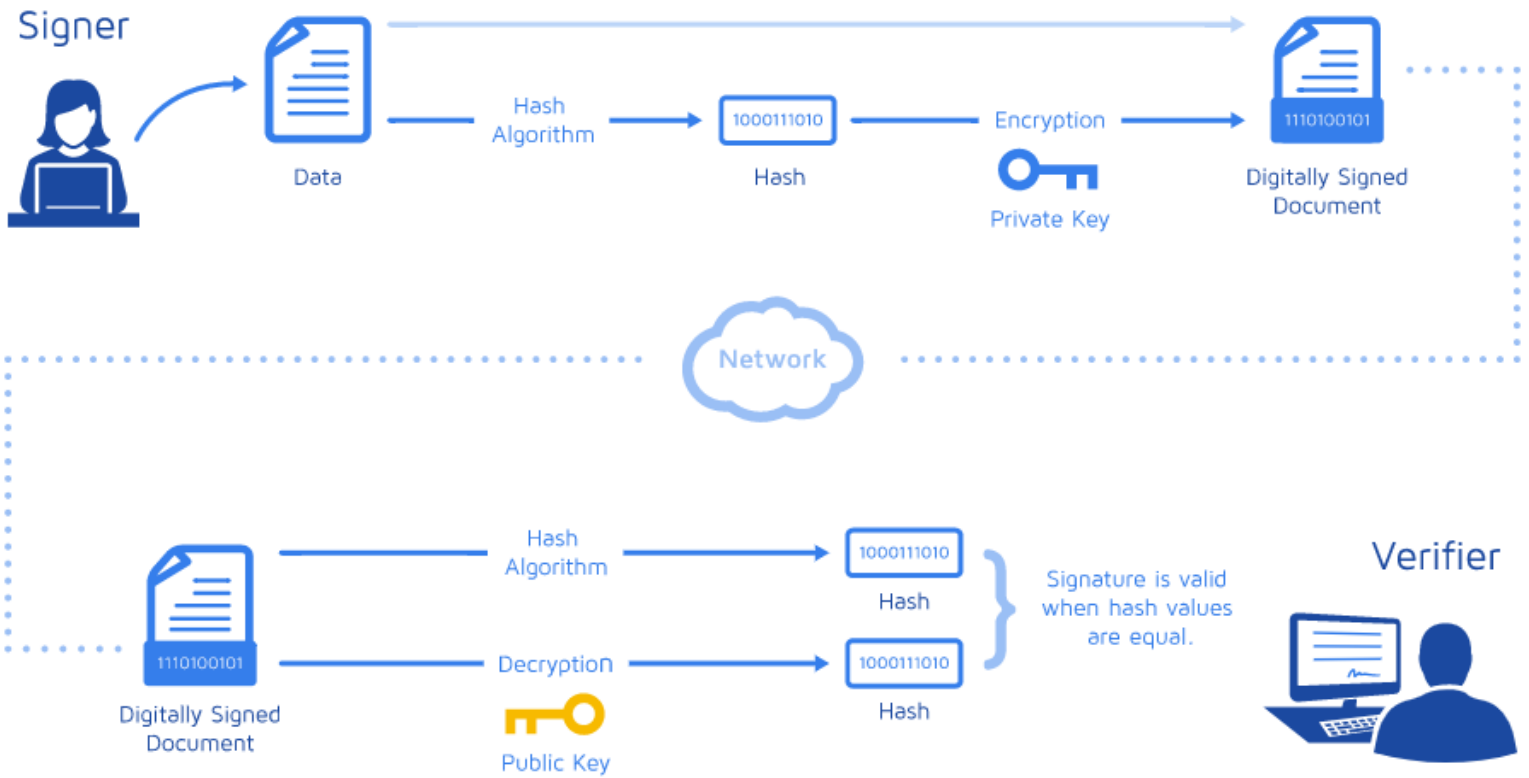
E-Goverment Applications

Inter-institutional communication

Orders



How it is work?



Neler Yapılabilir?

İmzala Gönder

Bank Payments

KEP

Board Desicion

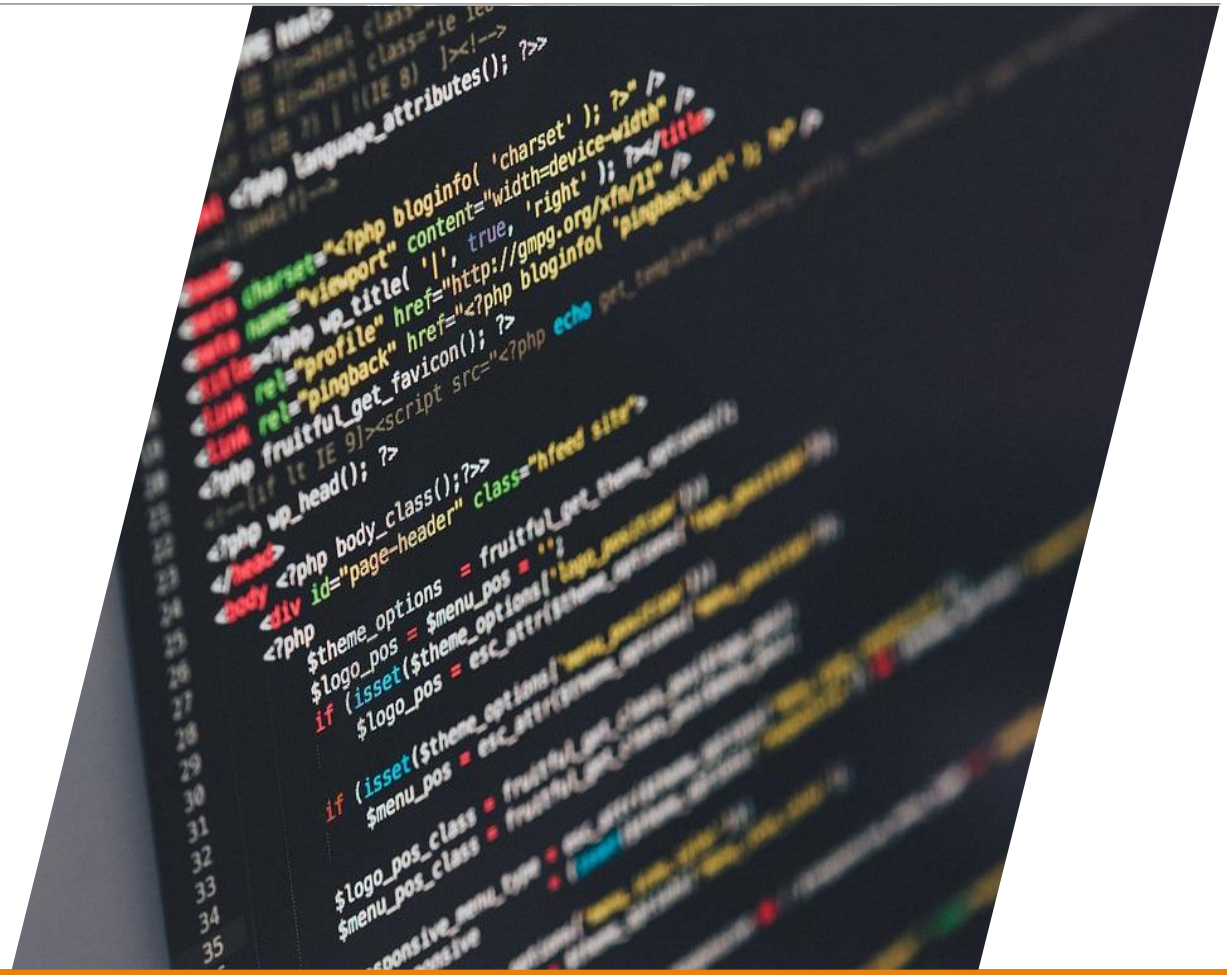
Law Contracts

Leasing Contracts

Expertise Reports

E-Distraint Application

E-Goverment Services



Statistics

Document statistics

- According to the Ministry of Forestry research in Turkey, approximately 140 sheets of paper consumed per person per day in an office.
- Managers spend 5-15% of their time to get information and 50% to search for information.
- A document is copied about 19 times on average.
- 90% of corporate memory is on paper.
- The cost of rebuilding a lost document is $ 220, the cost of finding a malfunctioning document is $ 120, and the cost of a document file is $ 30.

E-Signature statistics

- Turkey: 750K/month Signature
- 1M/month Verification

Sample Project: Mortgage Expertise Process

Our leading bank customer in retail banking

- Avarage expertise report page: ~80 pages
- Avarage cargo count for one report: 1,5 times
- Daily cargo cost: 600*5=3.000 TL
- Monthly page usage: 600*80*20=960.000 pages
- The average A4 page produced from a tree: ~73.000 pages
- Number of trees recovered in a month: ~13

BlockChain

What? Where to use?

Blockchain

We can define Blockchain as a distributed database that provides briefly an encrypted transaction. Blockchain technology, constructed from a chain model, which can be understood from its name, is traceable but not breakable, allowing to operate without being connected to a center. Thus, transactions can be carried out directly between the buyer and the seller and safely.

Blockchain Critical Application Areas

Smart contracts

Smart Assets

- Conservation and management of all assets of the person

Clearing and Settlement

- Entire network transactions are acknowledged in each new transaction

Payments

- No control over payments on one center

Digital Identity / Dijital Kimlik Yönetimi

- Identification and authorization of customers with digital identity management

Bitcoin

2008 Satoshi Nakamoto

2009 Bitcoin

Bitcoin BTC

1 BTC = 0.00000001 satoshi (100M satoshi)

Production limit 21 M Bitcoin

This year: Amount 16.143.025 BTC

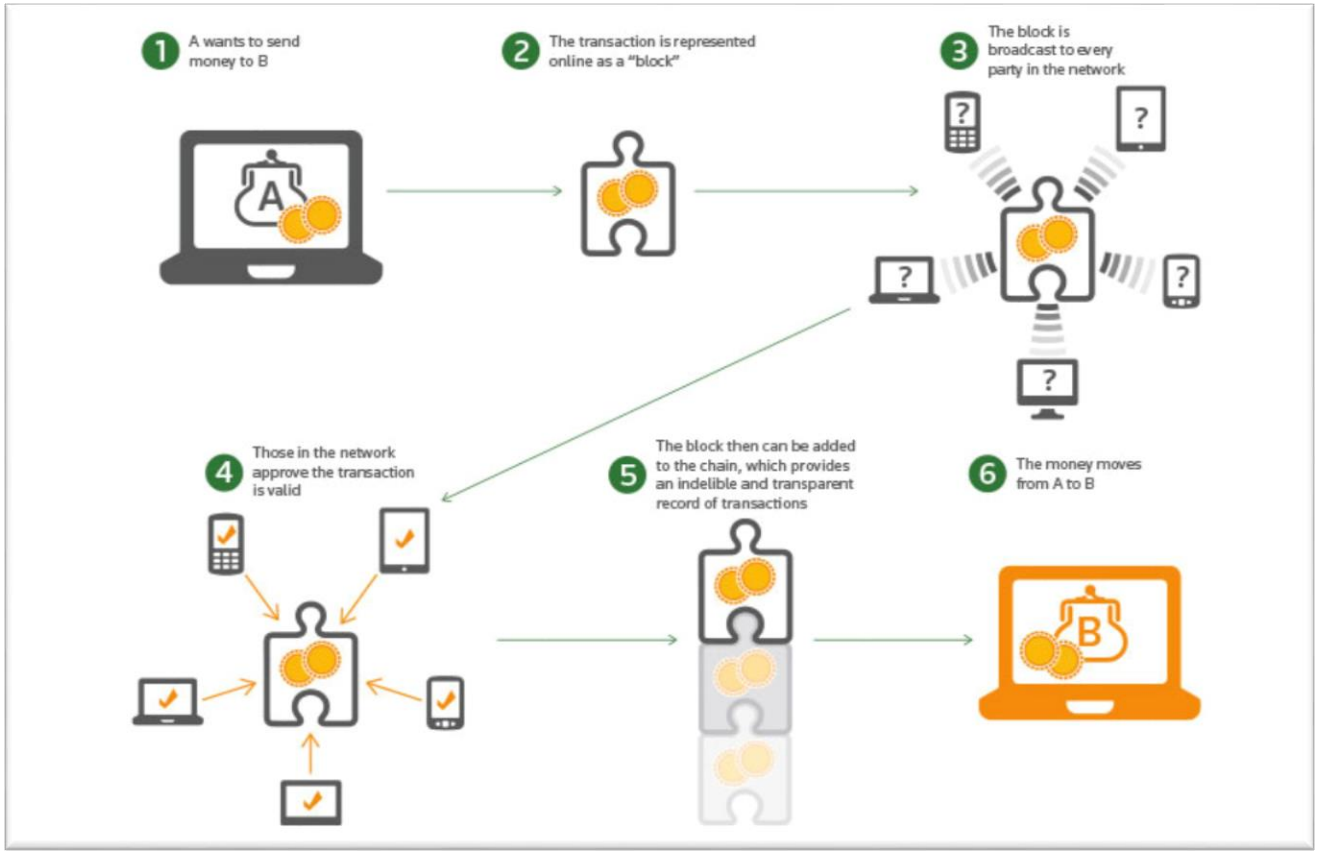
Bitcoin uses Blockchain technology

Blocks keeps all transactions from the beginning of Bitcoin

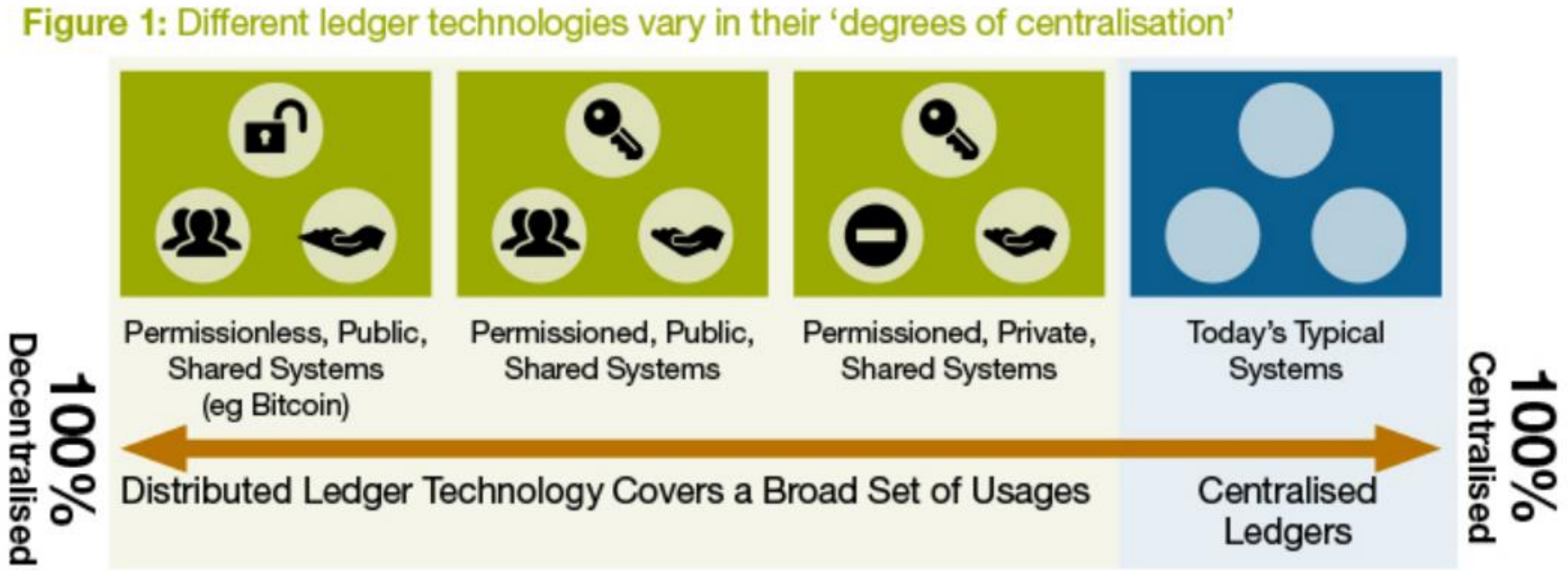
Start block – Genesis Block

BTC Exchanges

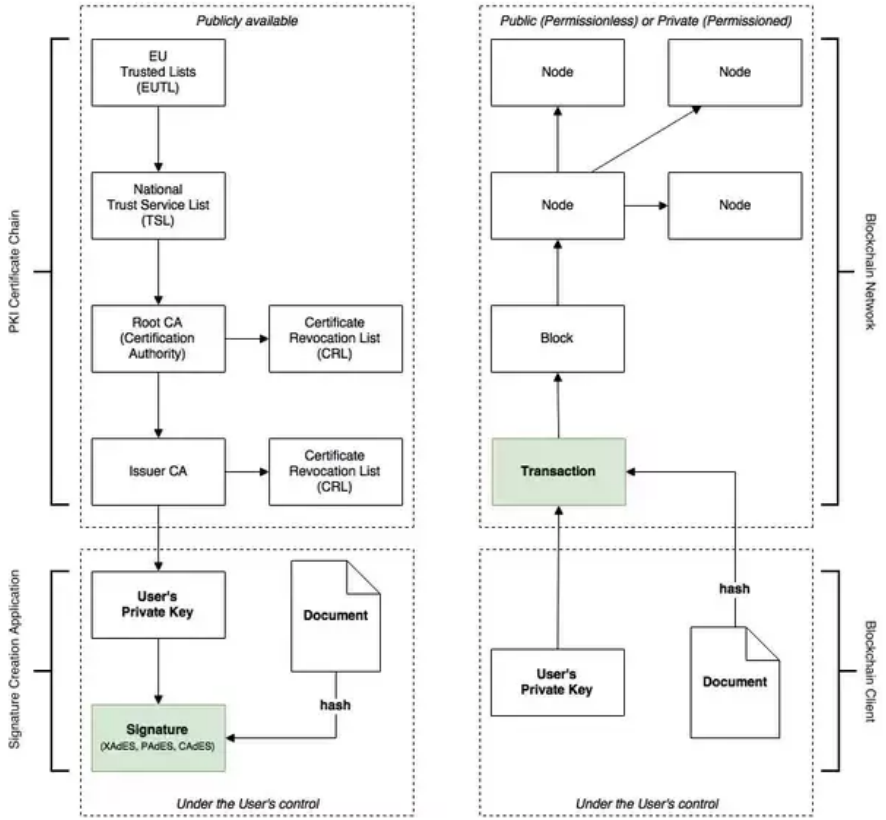
How Blockchain Works?



How Blockchain Works?



BlockChain vs Digital Signatures



BlockChain vs Digital Signatures

BC vs DS	*Blockchain (Public)*	Blockchain (Private)	Digital Signatures
Offline access	×	×	√
Validation independent from the infrastructure	×	×	√
Total transaction privacy	×	×	√
Infrastructure maintained by known/trusted entities	×	√	√
Fast (quick transaction validation)	×	√	√
Proof of identity	×	√ (possible)	√
Proof of existence (at a certain time)	√	√	√ (possible)

BlockChain vs Digital Signatures

BC vs DS	*Blockchain (Public)*	Blockchain (Private)	Digital Signatures
Proof of integrity (not tampered)	√	√	√
Signed data may remain undisclosed	√	√	√
Censorship resistant	√	×	√
Smart contracts available	√	√	×
Validation always available publicly	√	√	×
Impossible to delete a transaction	×	×	×

Teşekkürler

meetup.com/Istanbulflow