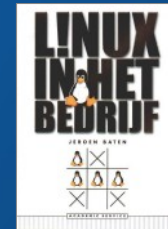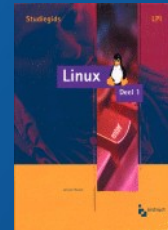# A new document workflow for the government

Who am I?

- Jeroen Baten
- Lifetime innovator
- Job title : IT Solutionist
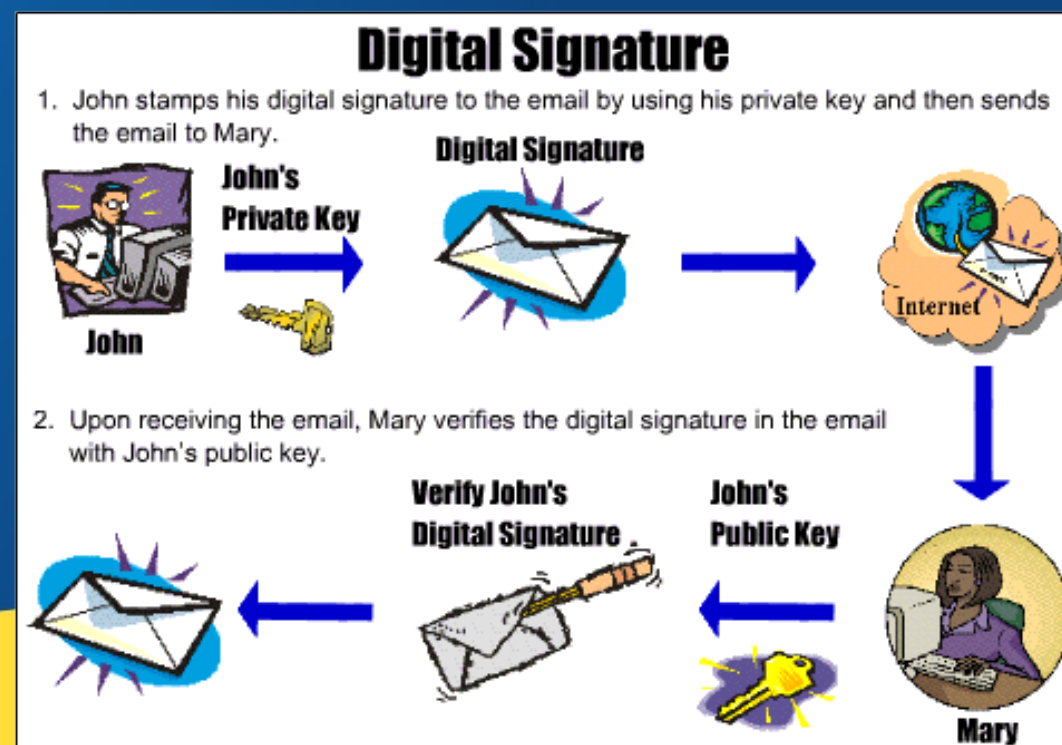
Who am I ? (in pics)

Government doc workflow

- Registration of birth, marriage, etc
- Notary registration of house ownership
- Judicial documents, judgements, etc
- And a lot more....

What is GPG

- Secure digital signature
- Public key encryption
- Secure email
- Verifiable signature

Digital Signature

1. John stamps his digital signature to the email by using his private key and then sends the email to Mary.

John's Private Key → **Digital Signature** → **Internet**

John

2. Upon receiving the email, Mary verifies the digital signature in the email with John's public key.

Verify John's Digital Signature ← **John's Public Key** ← Mary

Signature history

- 3000 BC: pictograms, no sigs
- 1069: First sig: "El sid"
- 1677: UK: Sigs, Statue of Frauds
- 1869: Telegraph: Digital Sigs
- 1980: Fax accepted as sig
- 1995: Digital money/DigiCash
- 2000: the rise of digital signature software
- 2008: Distributed blockchain

GPG Example

Hi,

This is not a really sensitive email, but
I bet you want to know that I really send it.
So, I will digitaly sign it for your verification.

Kind regards,
Jeroen

gpg --output email.sig --clearsign email.txt

----BEGIN PGP SIGNED MESSAGE----
Hash: SHA256

Hi,

This is not a really sensitive email, but
I bet you want to know that I really send it.
So, I will digitaly sign it for your verification.

Kind regards,
Jeroen
-----BEGIN PGP SIGNATURE-----

iQEcBAEBCAAGBQJaDvdkAAoJELRdI69H18RF
hwXgZzD6USUCf8EXGs/Dy8+noZoOXptaOfJUm
QKwICH7UI/ekwnGKl4rQ7f1hHB+ymo2Aje0YxBU
8dITuJ4OqQYxIFJp5eNXUdU8Enwhk1ULGQuLi
hqz7tx5tdr98jQMuI+OIm/qidgsVPCDCyY7r3rXD0
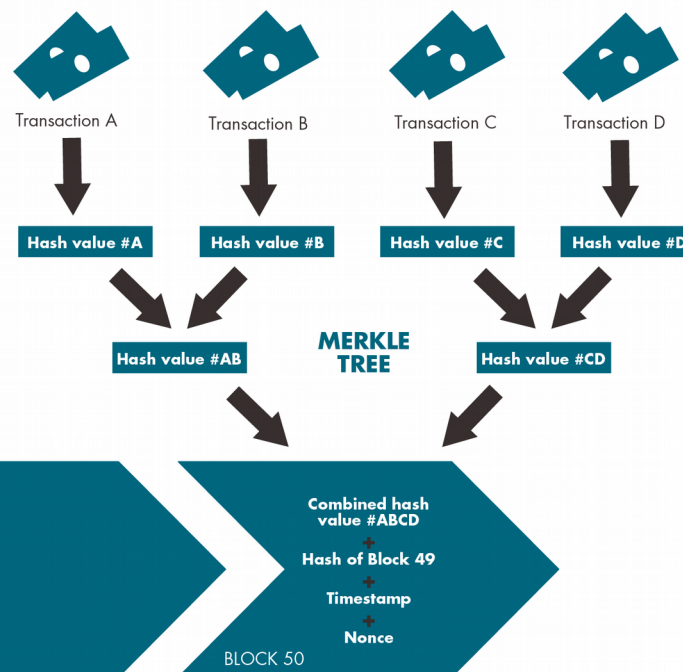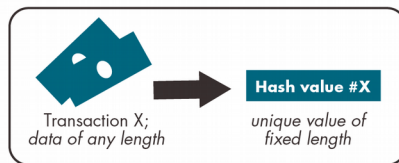bbc5Z777NiCv+O3eD7Z690qK0oevZvBrq7VSv1
=br3k
-----END PGP SIGNATURE-----

What is Blockchain

- Secure digital ledger

- A chain of blocks signed by the block before

- An append only database

HOW THE BLOCKCHAIN WORKS

Transaction X; data of any length → Hash value #X, unique value of fixed length

Transaction A → Hash value #A
Transaction B → Hash value #B
Transaction C → Hash value #C
Transaction D → Hash value #D

Hash value #AB   MERKLE TREE   Hash value #CD

Combined hash value #ABCD
+
Hash of Block 49
+
Timestamp
+
Nonce

BLOCK 48   BLOCK 49   BLOCK 50

Reproduction of an original figure in "The Great Chain of Being Sure About Things" by the Economist

Center for Global Development

The basic idea

- Use blockchain as a secure ledger
- Use GPG to sign documents
- Use open source MultiChain
- Add signed docs to the blockchain
- (Bitcoin: transactions of value exchange)

Demo time!

Questions for me?: jeroen@jeroenbaten.nl