www.pdfa.org

Blockchain, Threat or Opportunity?

Joris Schellekens
Software Engineer - iText

Joris Schellekens
Software Engineer
iText

The iText R&D team

Why?

- **Integrity**
  "The document has this exact content."

- **Authentication**
  "I created this document. And I can prove it."

- **Non-repudiation**
  "He created this document. And I can prove it."

Joris Schellekens
Software Engineer
iText

Why?

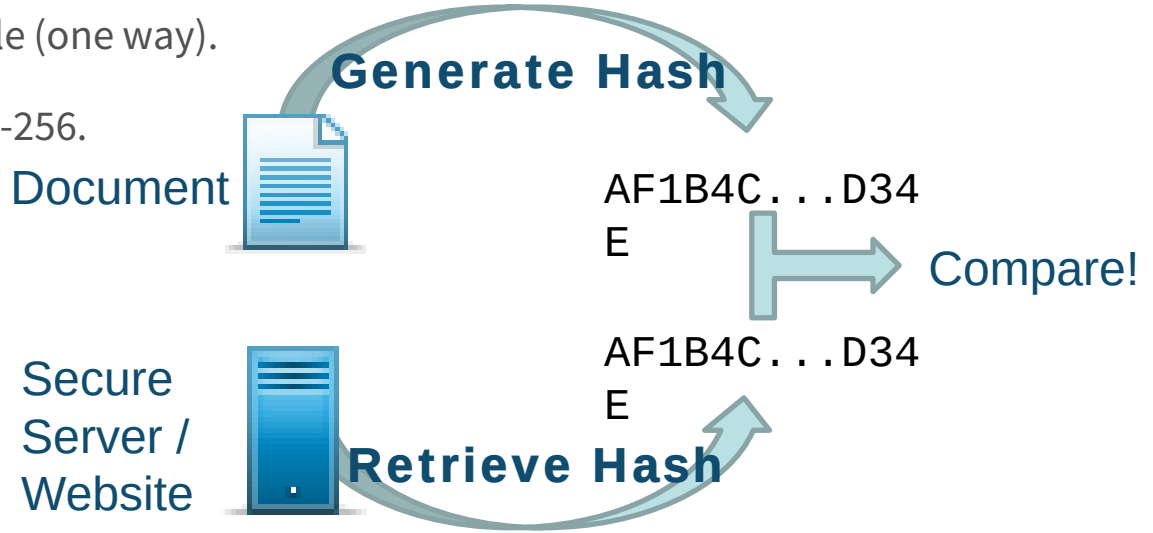
- *"Hey, I've created this hash on 10 Oct 2016: here is the transaction in the blockchain which contains the hash. I've created it according to this formula from this file."*

- Integrity
- Authentication
- Non-repudiation
- Timestamp

Joris Schellekens
Software Engineer
iText

Hashing

- Turns an arbitrary block of data into a fixed-size bit string.
- Used for verification of data integrity.
  - Any small change to input has huge effect on hash value.
- Non-reversible (one way).
- SHA-1 vs SHA-256.



Joris Schellekens
Software Engineer
iText

Encryption

- Using two separate but compatible keys to encrypt information.
  - Encrypt data

  - Sign data

- Can be decrypted => two-way.

Joris Schellekens
Software Engineer
iText

Relation to pdf

- Pdf documents can be digitally signed.
  - Requires Certificate Authority (centralized).
  - Requires timeserver (centralized).
  - Can not be signed in parallel.
  - Signatures live in the document.

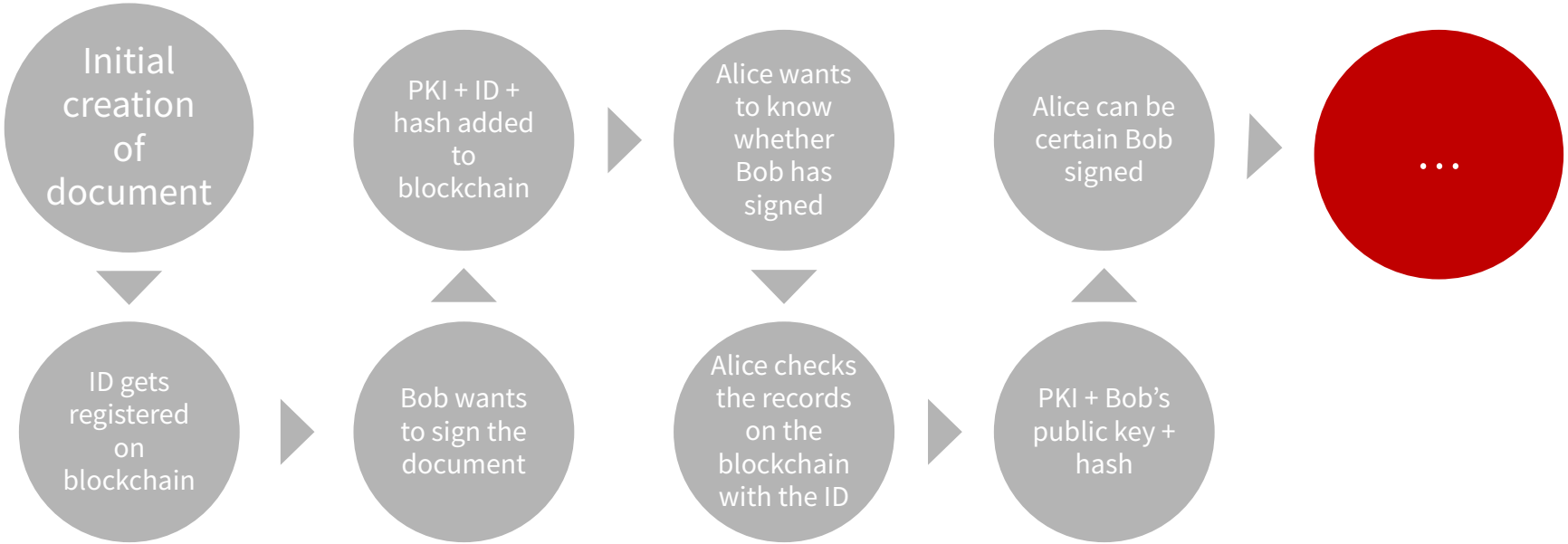
Joris Schellekens
Software Engineer
iText

Opportunities

- Data in a blockchain
  - Can be signed using known PKI – infrastructure.
  - Is automatically validated and timestamped.
  - Can be viewed by everyone.
  - Can live separately from the physical (real world) data it references.

Joris Schellekens
Software Engineer
iText

Our idea - high level



Joris Schellekens
Software Engineer
iText

Our idea - detail level

- Store meta-information of the pdf document on a blockchain:
  - ID,
  - hash (+ algorithm),
  - signature (+ algorithm),
  - fields that can be chosen by the end-user.
    - E.g. “currently awaiting feedback”, “asset has been checked by customs USA”, etc.

Joris Schellekens
Software Engineer
iText

Web of trust

Web of trust

- In cryptography, a web of trust is a concept to establish the authenticity of the binding between a public key and its owner.

  Source: Wikipedia

Joris Schellekens
Software Engineer
iText

Web of trust

- Bob can look up the public key of Alice
  - assuming public keys are truly publicly available,
  - or Alice can simply give Bob her public key.

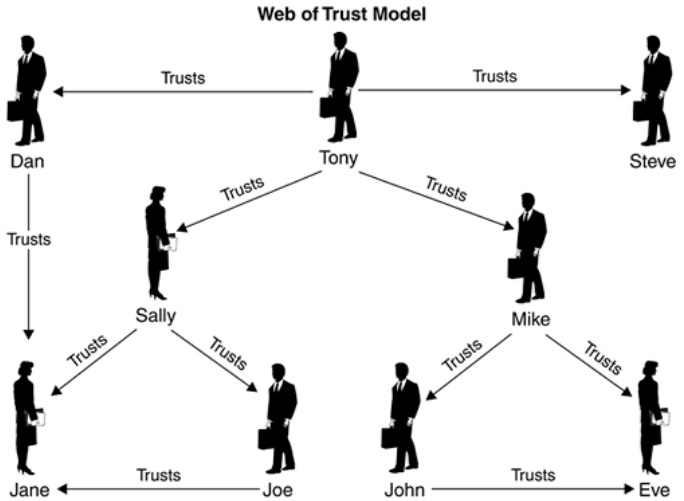
- Bob signs the public key of Alice with his private key.

- Other users can see all these records.
  - They can verify (using Bob's public key) that Bob has signed Alice's key.
  - This is considered as "Bob trusts Alice".

Joris Schellekens
Software Engineer
iText

Web of trust

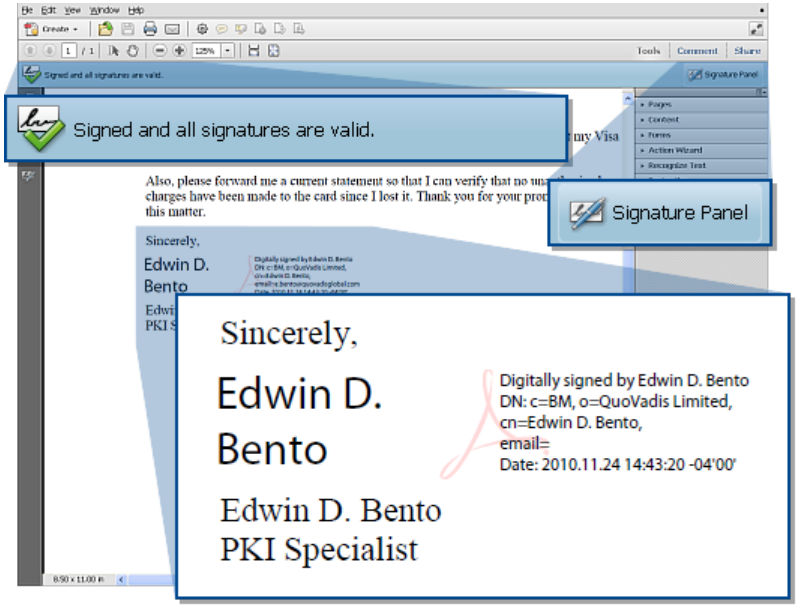
- This builds a graph where some nodes are connected by a “X trusts Y” relationship.
- The application built on top of this framework can then decide how to handle trusted vs. untrusted users.



Joris Schellekens
Software Engineer
iText

Web of trust

- Example



Joris Schellekens
Software Engineer
iText

Web **of trust**

- Extensions are possible.
- Add a status field “ACK” or “NACK”.
  - Now Bob can revoke his trust in Alice.
  - Only the most recent record is taken into account.
- Allows temporary trust (interim workers).

Joris Schellekens
Software Engineer
iText

Use case

Use case

Joris Schellekens
Software Engineer
iText

Use case

Joris Schellekens
Software Engineer
iText

Use case

Joris Schellekens
Software Engineer
iText

Roadmap

PDF community

A typical PDF company:

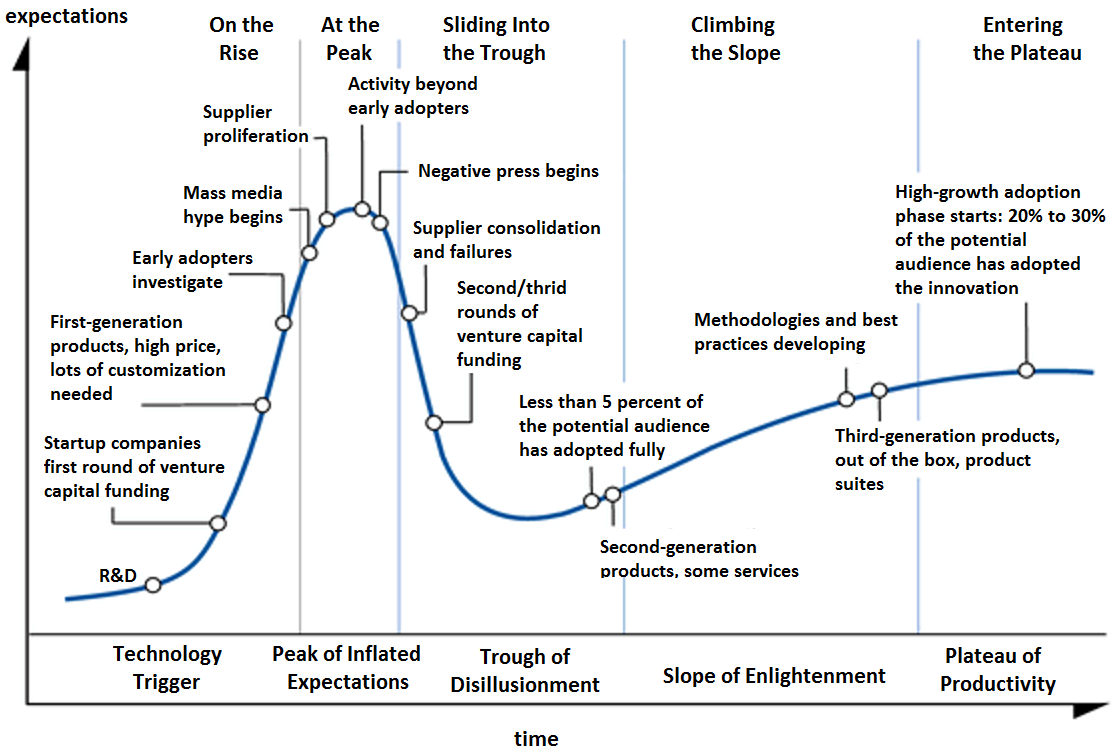
- Proven PDF experts.
- 20 years of experience with PDF (and related software)
- Members of ISO committee that sets PDF standards.
- highly trained (in a niche market).

Joris Schellekens
Software Engineer
iText

Blockchain community

- Substantial amount of investigation to be done.
- Patents with regards to blockchain-PDF interaction.
  - Everyone wants to be ‘the first’
- Loads of startups.
- Mutually beneficial cooperation:
  - They learn about the possibilities of PDF documents.
  - We learn about how blockchain can be used.

Joris Schellekens
Software Engineer
iText



Joris Schellekens
Software Engineer
iText

Community outreach

How can you help?

- **Gathering use-cases**
- **Working group within PDF association**
- **Specification (drafts)**

- **Pull request always welcome**
- **https://github.com/itext/i7j-pdfchain**

Joris Schellekens
Software Engineer
iText

Thank you! Any questions?

Joris Schellekens
Software Engineer
iText

Get in touch: joris.schellekens@itextpdf.com
Web site: www.itextpdf.com
Twitter: @itext