How Blockchain could revolutionize documents

PDF Days, Washington DC, January 29, 2017

iText: The Past, Present, and Future

- 1998: first java PDF library, written by 1 person (Bruno Lowagie)
- 2000: complete rewrite of the library
  - Continuous development by a thriving open source community
- 2008: first company; today known as iText Group (Belgium)
  - Mission: to enable a paperless world, pushing the limits of digital document interactivity
  - Goal: The “dematerialization” of paper; help companies evolve from paper to digital
- 2009: dual licensing business model, based on the AGPL
  - 2009: iText Software Corp. (US)
  - 2011: iText Software BVBA (Belgium)
  - 2015: iText Software Asia Pte. Ltd (Singapore)
- Our initial goal is on the verge of being accomplished:
  - Digital invoices: legally binding in many countries,
  - NARA: paperless in 2023,
  - …
- 2016: Question: what’s next? What could threaten our further growth?
  - “Dematerialization of the document”

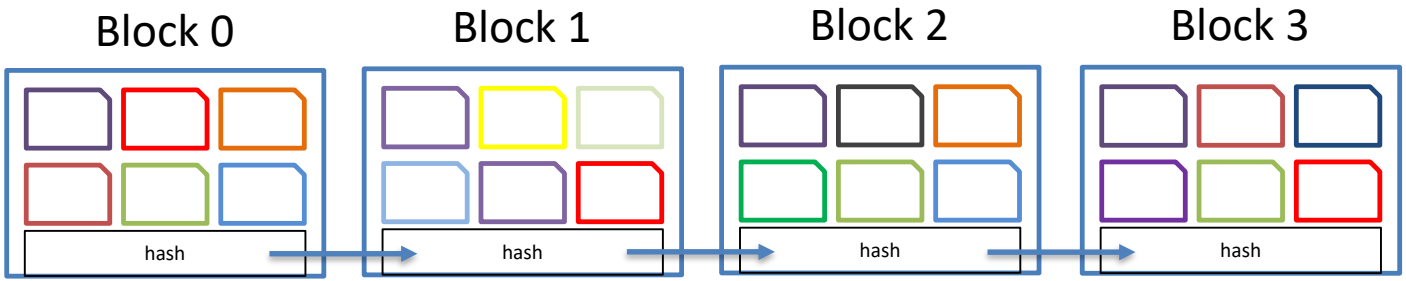
Competitive threats to PDF technology

- **Question:** what could be the end of PDF?
  - Other document formats: XPS? Not successful; ePub? Dying; HTML 5: the future threat?
    - But the purpose of HTML 5 (publications) is different from the purpose of PDF (documents)
    - And we're working on "Next-Generation PDF" (as discussed during the PDF Days in Berlin)
  - Other technologies; e.g. Distributed Ledger Technology (DLT)
- **Answer:** competing technology is a greater threat to PDF than competing formats
  - Boarding a plane, processing a payment,… it's all done in an app! No documents needed!
  - What about the Document of Record (DoR)?
    - What is more important in an automated world?
      Data that can easily be processed by machines, or documents that require human interpretation?
      PDF/A-3 could be a combination of both, but who will guarantee that PDF and data are consistent?
  - Data can be secured using DLT, e.g. blockchain.
  - Blockchain is:
    - A distributed database
    - That serves as an irreversible and incorruptible repository
    - For permanent records

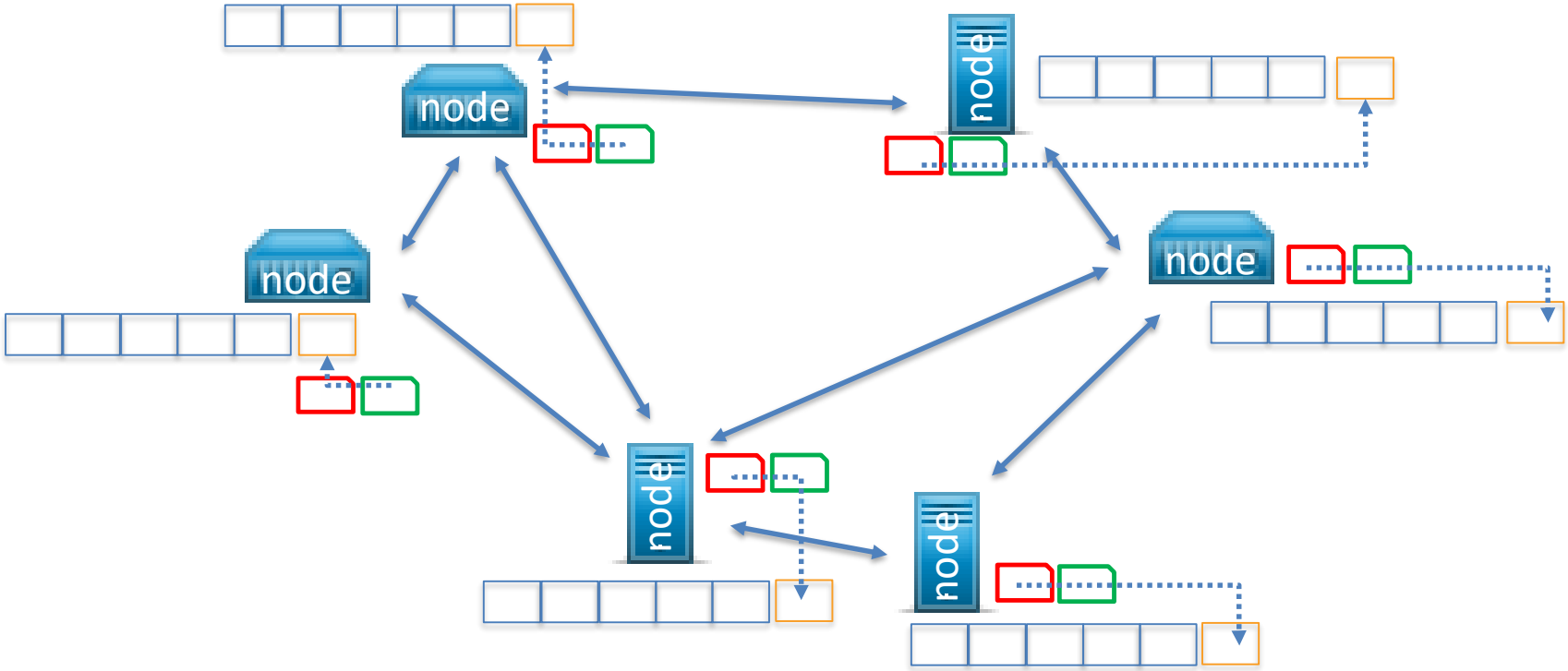
Blockchain

- Basic concept
- Example smart contract
- Example digital signature

What is a blockchain?



Distributed Ledger Technology



Example: smart contracts

Predefined Contract

- All counterparties agree on the terms (e.g. terms & conditions for a sale)
- Known conditions for execution (e.g. 10% down-payment; full payment upon delivery)
  - Expressed in source code stored in the blockchain

Events

- An event triggers contract execution
- An event can refer to:
  - The initiation of a transaction (e.g. a down-payment)
  - Information that is received (e.g. a parcel is received)

Execute

- Terms of contract dictate movement of value based on conditions met
  - E.g. a down-payment: a parcel is sent in the real world
  - E.g. a parcel is received: the payment is processed

Settlement

- On-chain assets: e.g. cryptocurrency (for instance “paid with Bitcoin”)
- Off-chain assets: e.g. the parcel (for instance “a work of art”)
  - The value bearing item resides outside (“off”) the blockchain; It has a digital counterpart in the blockchain (e.g. identified using an RFID tag)
  - Lifecycle events of the item are mirrored in the blockchain: the blockchain contains the “rights” (e.g. owner’s claim to a work of art)

Example: digital signatures

- Not every agreement can be captured in code
- Privacy can be an issue:
  - In a public blockchain, aliases are used and info can be encrypted, but that's not 100% waterproof
  - In a private blockchain, there's more security, but not all partners are necessarily trusted
- Innovative integration approaches and benefits:
  - Store a digital signature of a PDF document in the blockchain (instead of in the file itself)
    - Using the double PDF ID as the ID for the record (related documents have the first part in common)
    - A (signed) hash of the document (to verify the integrity)
    - Metadata, such as the status of the document (e.g. Quote request, Quote, PO, Invoice, Paid invoice)
    - One or more URLs indicating how to obtain the document (e.g. from a secure vault)
  - There are several advantages:
    - Documents can be signed in parallel; the concept of a timestamp is inherent to blockchain
    - Automated processes can keep track of the workflow
    - The existence of newer versions of a document can easily be detected
    - Link rot can easily be avoided by adding a new record each time a URL changes
    - LTV can easily be achieved by renewing the signature

Use cases

- Industries
- Use case 1: marriage certificates
- Use case 2: invoices
- Use case 3: sales workflow

Industries

Moody's Investors Service (MIS) released a report “Credit Strategy -- Blockchain Technology: Robust, Cost-effective Applications Key to Unlocking Blockchain's Potential Credit Benefits” identifying 25 top blockchain use cases, from a list of 120.

Exhibit 6

Selected Potential Blockchain Use Cases

Financial Institutions	Corporates	Governments	Cross-industry
International payments	Supply chain management	Record management	Financial management & accounting
Capital markets	Healthcare	Identity management	Shareholders' voting
Trade finance	Real estate	Voting	Record management
Regulatory compliance & audit	Media	Taxes	Cybersecurity
Anti-money laundering & know your customer	Energy	Government & non-profit transparency	Big data
Insurance		Legislation, compliance & regulatory oversight	Data storage
Peer-to-peer transactions			Internet of Things

Source: Moody's Investors Service

Use case 1: marriage certificates

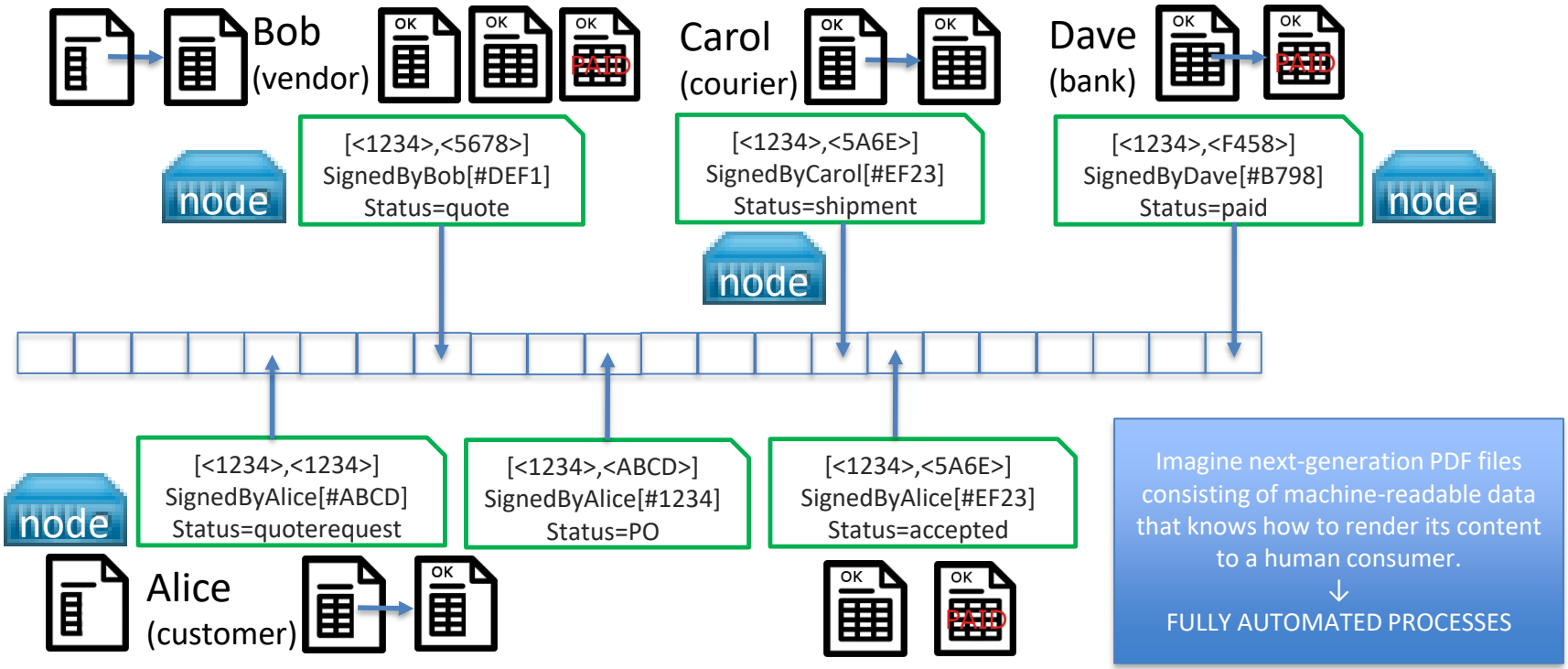
- An agreement that can't be captured in source code (no smart contract)
- Contains private data, such as names of the spouses, birth dates, etc.
- It is often forged, e.g. in the context of naturalization of spouses

- Solution:
  - Create the marriage certificate in two copies:
    - one for the spouses (they can store it in a safe place; or just keep the id),
    - one for the appropriate county office (in a secure document vault).
  - The county office registers all "active" marriage licenses in the blockchain on a regular basis
  - The certificate of the spouses can at all times be verified in the blockchain
    - If the spouses only have the ID, the document can be retrieved from the secure vault by key-holders

Use case 2: invoices

- Image that every vendor registers / signs each invoice in the blockchain:
  - What is stored? The document ID, the identity of the vendor, the hash signed by the vendor
  - What is not stored? The amount to be paid, the identity of the buyer, the invoice details
- Benefits for the buyer:
  - Is the vendor who he claims to be?
    - Avoid fake invoices. Check if the vendor has a license to sell. Check if a vendor paid all taxes.
  - When was the invoice registered on the blockchain?
    - Avoid backdated invoices
  - Was the invoice tampered with?
    - Avoid forged invoices (e.g. intercepted invoices of which the wiring information was changed)
- Benefits for the government:
  - Check how many invoices a vendor created:
    - if a company declares only 800 invoices, and the government finds a 1000, there's a problem
  - Check if all paid invoices were actually registered in the blockchain
    - If a company declares a 1000 invoices, and 200 aren't accounted for, there's a problem
  - Not all invoices have to be verified for integrity; a sample check might be sufficient

Use case 3: sales workflow



Conclusion

- PDF could become the document / data container format of choice for blockchain:
  - Store signatures for “human” contracts and private documents,
  - Ensure the integrity, authenticity, non-repudiation, and long-term validation,
  - Fully automate workflows.
- This makes blockchain not a threat, but a great opportunity for PDF