New Kids on the Blockchain:
RIM Blockchain Applications Today & Tomorrow

Q. Scott Kaye, Partner, *Rimon Law*

John Isaza, *Information Governance Solutions, LLC*

AGENDA

- What is Blockchain?
  - How it works
  - Forming it
  - Distribution
  - Immutability
- Application of Blockchain to Information Governance
  - Benefits of using it
  - Application to contracts and signature authentication
  - Application to metadata capture
  - Time stamp management and security
  - Evidence preservation
  - Records preservation

2

Part I

WHAT IS BLOCKCHAIN?

WHAT IS BLOCKCHAIN?

(And why should we care?)

A Blockchain is simply a digital, decentralized, distributed LEDGER.

LEDGERS

Techno revolution using 13th Century Tools

A ledger is just a set of data ordered by rules.

Ledgers confirm:

- Ownership- Property records
- Identity-Birth, Death, Corporate Existence
- Authority – Bank accounts, Access lists
- Status- Citizenship, Voting rolls
- Money – Bitcoin!

The oldest European ledger is a Florentine Bank Ledger from 1211. There are even older ledgers going back to 4th and 5th centuries in ancient cultures.

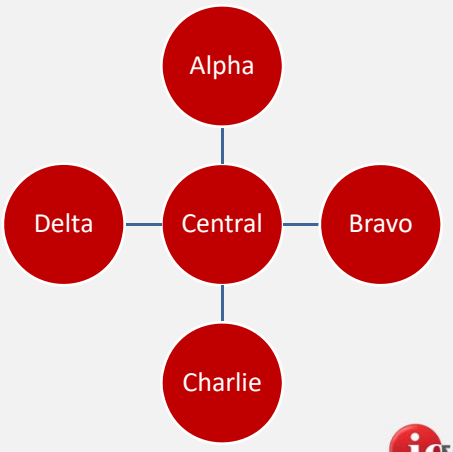
5

CENTRALIZED AUTHORITY

Who maintains the ledger?

The easiest example is a money transfer. Central, the bank, maintains the ledger. If Alpha wants to transfer money to Charlie it requests the bank to debit its account and credit Charlie's account on Central's ledger.

We are dependent on a central authority to establish trust between participants.



6

WHAT IF THE BANK FAILS?

The reliability of a digitized ledger is solely dependent on the organization that maintains the ledger.

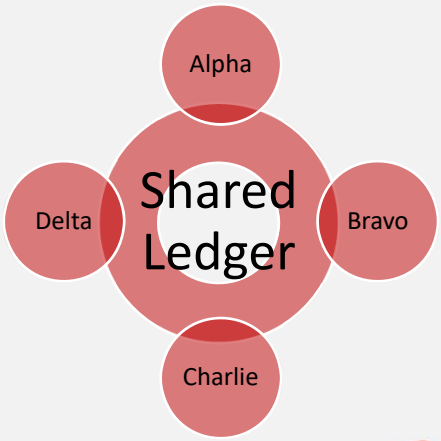
7

DECENTRALIZED NETWORK

Who maintains the ledger?

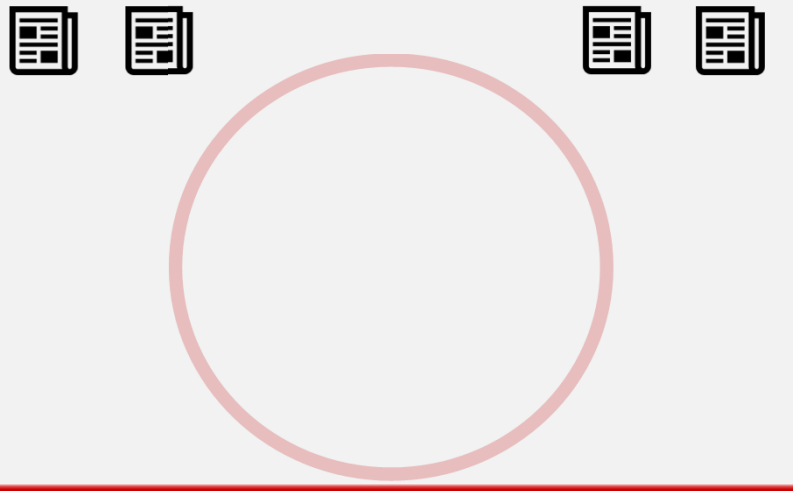
Is there a way to maintain a ledger among ourselves without a central authority?

With three or more participants you can distribute the ledger among the participants which does not rely on a trusted central authority.



8

THE FIRST BLOCK IN THE CHAIN



9

HOW CAN THAT POSSIBLY WORK?

- Each participant would start with a blank ledger.
- When Alpha wants to transfer money to Bravo, Alpha announces it to the group.
- All participants mark the transaction on their personal ledgers. This continues to happen with each participant announcing transfers until a ledger page is full.
- Now the page needs to be certified and stored. This is often called mining and the certificate code is found by "hashing" which simply means using cryptography to solve a complex problem which generates a magic word.

10

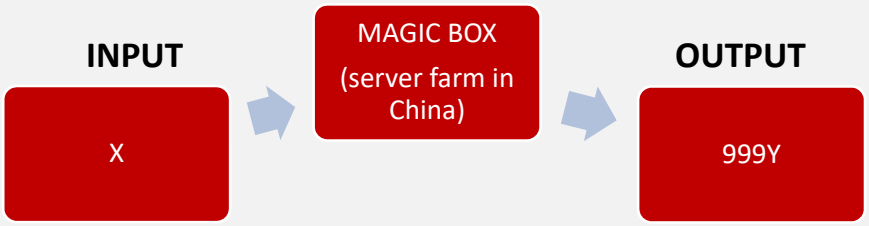
FORMING THE BLOCKCHAIN

How it works:

1. Transaction Request
2. Verification Que
   - Either instantly validated or placed in a que for determination if valid based on rule set
3. Validation of Block by **Proof of Work**
   - Solving a mathematical puzzle based on a block header
   - Answer is found by **Mining**
     - brute force computing to find a variable which satisfies a network agreed protocol
     - Other types of Validation – **Proof of Stake**
       - a person can mine or validate block transactions according to how many coins he or she holds.
4. Distribution of Validated Blocks

11

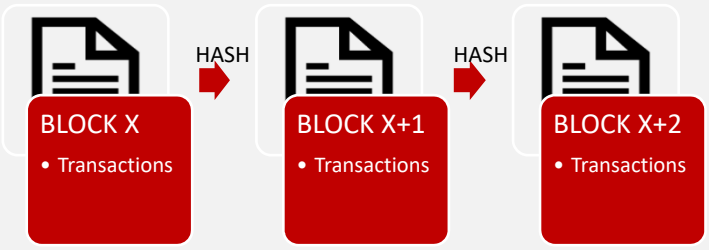
VALIDATION- PROOF OF WORK



- Find a X input for an output that satisfies network protocols.
- Key Feature- Provided the output, its extremely difficult to determine the input- but provided the input the output is extremely easy to determine.

12

DISTRIBUTION



Each block is identified by a hash- typically a 256-bit number created by an fixed algorithm and contains a **header**, **reference to the prior block** and **transactions**.

13

DISTRIBUTION

- After the Miner solves the puzzle to validate the block, the block is distributed to participants.
- The Miner is rewarded with additional access, additional tokens, or some other network privilege.

14

IMMUTABLE

Each block's hash function relies on all prior block hash functions so no one participant can go back and change an earlier transaction as it would then create an alternative chain which would be rejected by the majority.

15

Database vs. Blockchain

Do I need a Blockchain?

↓

Probably Not

www.AskVirgo.com 16

DATABASE vs. BLOCKCHAIN

BLOCKCHAIN

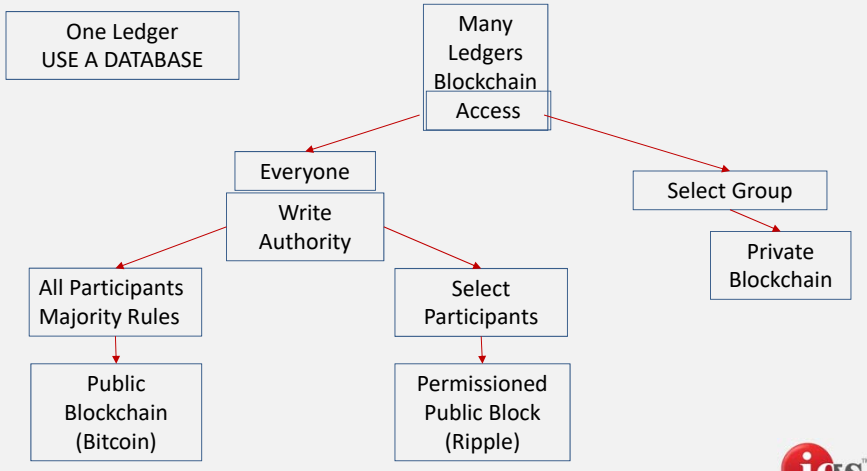
Fixed rules about the transactions that are tied to the transactions themselves.

DATABASE

Rules are set at the database level not the transactions

17

DATABASE vs. BLOCKCHAIN



18

EX of BLOCKCHAIN APPLICATIONS

- **Everledger**- Identification of diamonds by digitizing attributes and laser-inscribed serial numbers onto a blockchain. Include a digital passport to record and verify its transaction history.
- **Codel-** Records corporate actions on blockchain with digital notary software.
- **SETling-** privately funded venture to develop and deploy a specialist blockchain to all financial market participants to settle securities transactions on a peer-to-peer basis.

19

EX of BLOCKCHAIN APPLICATIONS (cont'd.)

- **Bitcoin** is a medium of exchange created and stored on a blockchain using encryption to create, control and verify the transfer of Bitcoins.
- **Bitcoin** goes beyond replicating physical cash in a digital world as it is fully independent of any bank or government.
- **Bitcoin's** blockchain can handle about 20,000 transactions per hour, with up to an hour's latency before a transaction can be trusted.

20

Part II

APPLICATION OF BLOCKCHAIN TO RECORDS AND INFORMATION GOVERNANCE

21

SOCIAL SCIENCES AND HUMANITIES RESEARCH COUNCIL OF CANADA

Survey findings presented on October 24, 2016:

- Blockchain technology is fundamentally a recordkeeping technology, as much as it is a value transfer technology.
- Many current and proposed applications of blockchain technology aim to address recordkeeping challenges; that is, they offer a new form of records storage, use, maintenance or control of records.
- Blockchain records must be managed as legal evidence alongside other records in order to meet business and societal purposes.

22

BENEFITS OF USING BLOCKCHAIN

- Immutability & Verification
- Redundancy
- Transparency
- Security
- Establishes trust among multi-party transactions when trust does not exist
  - Trust is identity and authority

23

IMMUTABILITY & VERIFICATION

Multiple actors and parties to transactions may keep separate ledgers that are updated upon validation of a new transaction.

Blockchain allows these ledgers to be verified by the block headers and proof of work, which also prevents any changes to earlier data by a single party.

24

REDUNDANCY

Multiple copies of the same ledger avoid a single or even multiple points of failure.

Using blockchain also reduces the cost and complexity of maintaining multiple backups of conventional databases

25

TRANSPARENCY & SECURITY

Every party can verify every record once the block is validated. Accordingly chain of custody and assurances that the data has not been changed or modified is built into the system.

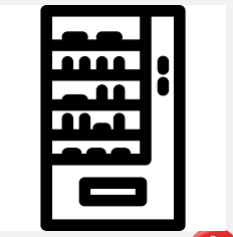
Access control is granted using “keys” to unlock the actual data in the transactions. Using a key a authorized party can view the transactions. Keys can be conditional and only function under certain circumstances.

26

SMART CONTRACTS

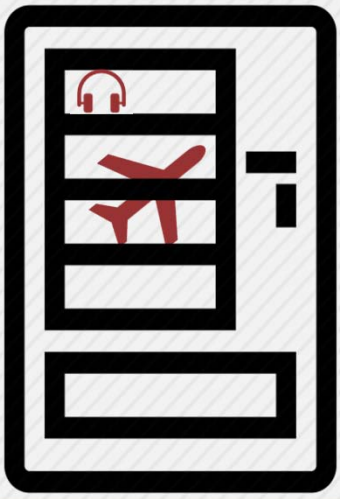
Nick Szabo in 1996 coined the phrase Smart Contract defined as a "*computerized transaction protocol that executes terms of a contract*." What does that really mean though?

- Think of a Smart Contract like a vending machine.
- When you put your $2.00 into the machine do you trust the machine to give you a soda?



27

SMART CONTRACTS (cont'd.)



Would you trust a vending machine to buy a $50 pair of headphones?

How about to lease a $2 million airplane?

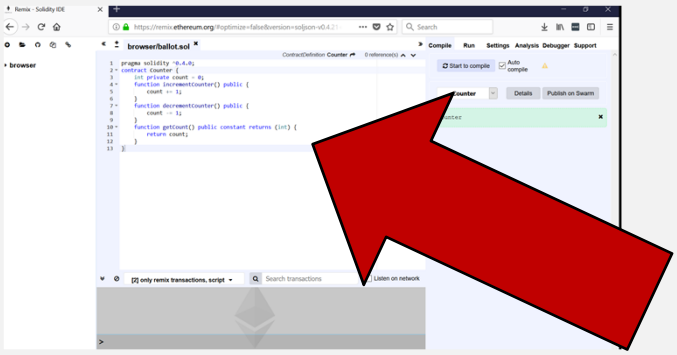
28

SMART CONTRACTS (cont'd.)

- Smart Contracts provide trust among participants who would otherwise not trust each other
- Smart Contracts are simply code running at a certain blockchain address waiting for a person or another Smart Contract with which to interact
- Smart Contracts reside in an application layer running on top of a blockchain (e.g. Ethereum)
- Initial Coin Offerings (ICO) use Smart Contracts to distribute tokens to investors

29

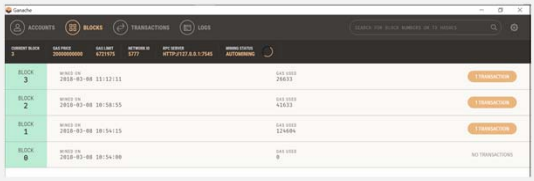
SMART CONTRACTS (cont'd.)



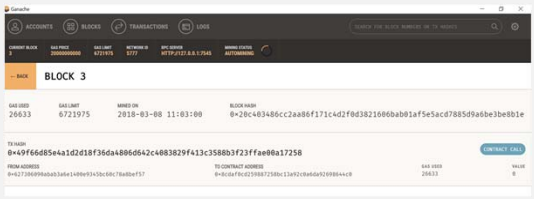
Example of a Smart Contract

30

SMART CONTRACTS (cont'd.)



Private Blockchain showing four completed blocks



Details of Block 3

SMART CONTRACTS (cont'd.)

Not for just commerce!

Incorporating Smart Contracts into Record Keeping and Information Governance can:

- Automate intake procedures
- Provide real-time recordation of any event on an immutable blockchain
- Allow access at many different levels or even upon the occurrence of certain triggering events
- Trigger additional actions depending on the type and substance of a new record

SIGNATURE AUTHENTICATION

- In a paper records environment, the creator of a record states ownership of the document, or assents to an agreement articulated in the document, by signing or countersigning it.
- From the records manager's perspective, the document is the property of the party that signed it. The signature is synonymous with the document.
- In a digital records environment, we have digital signatures. Public key infrastructures (PKIs) are the established repository for the storage of signatures.
- Blockchain presents an alternative platform for the preservation of digital signatures.

33

METADATA CAPTURES

- Records in the form of documents will not generally be stored in the blockchain.
- Blockchain simply carries a chain of transactions with it and continually replicates these, which is voluminous.
- Documents themselves cannot be contained in the chain.
- The metadata in the chain, on the other hand, is itself a record that needs to be managed, such as the programmatic rules driving the contracts or the instances of the contracts.
- Recordkeeping is integrally connected to the blockchain.

Cumming, K. & Findlay, C. (2016). Report on blockchain: Applications and implications. *Recordkeeping Roundtable*. Retrieved from https://rkroundtable.org/2016/04/03/report-on-blockchain-applications-and-implications/.

34

STANDARDS IMPACTED BY BLOCKCHAIN

- *ISO 18492:2005 - Long-term preservation of electronic document-based information*
- *ISO 14721:2012 (OAIS – Open Archival Information Systems)*
- *ISO 15489-1:2016 – Management and control of records with their metadata*

35

TIMESTAMPING: RFC 3161 / ANSI X9.95

- Existing standards, such as RFC 3161 and ANSI X9.95, require trusted third parties, or digital notaries to administer timestamps. These parties are known as Time Stamping Authorities (TSAs).
- RFC 3161 sets out the respective formats for which TSAs receive requests for a timestamp and the TSAs' response (RFC 3161).
- ANSI X9.95 also deals with time stamping of documents, but with an emphasis on the security of financial transactions (ANSI, 2012).
- RFC 3161 defines a timestamping service as a proof mechanism "that a datum existed before a particular time".
- The point behind this mechanism is to enable the archivist to verify that any digital signatures, coming under the archivist's jurisdiction in a *fonds*, had been created within the validity date of the public key certificate (RFC 3161, 2001).

S. Thompson, "The Preservation of Digital Signatures in the Blockchain," University of British Columbia iStudent Journal, Vol. 3 (Spring 2017).

36

RECORDS PRESERVATION

- Blockchain generates and keeps metadata about people, rules and transactions.
- They may be supported by documents or other information that exist outside the chain.
- The metadata is the core record and it will need management.
- Therefore, the recordkeeping processes of appraisal, preservation and accessibility have a core role to play in the blockchain.

Cumming, K. & Findlay, C. (2016). Report on blockchain: Applications and implications. *Recordkeeping Roundtable*. Retrieved from https://rkroundtable.org/2016/04/03/report-on-blockchain-applications-and-implications/.

37

Thank You!

Q. Scott Kaye –
Q.Scott.Kaye@RimonLaw.com
John Isaza –
John@InfoGovSolutions.com

38