Crowe

Smart decisions. Lasting value.™

Blockchain overview and applicability to education and charitable institutions

The new technology will enable new models

David Uhryniak
Brian Zygmunt

September 2018

Housekeeping

- Please note that all of today's audio is being broadcast to your computer speaker
- Please submit questions through the Q&A function on your screen. Questions will be addressed at the end of the presentation.
- To download a copy of the presentation or access the resources connected to this session, please visit the resources icon at the bottom of your console

© 2018 Crowe LLP

CPE Details

CPE Credit

- Login individually to the session
- Minimum of 50 minutes on the session
- Successfully complete 3 of the 4 polling questions

NO CPE Credit

- Fail to successfully complete 3 of the 4 polling questions
- Viewing a recording of this session (CPE is only awarded for live sessions)

Upon completion of this program you will receive a post event evaluation

Your feedback is important

- CPE certificate of completion
- E-mailed within two weeks of upon successfully passing this program

© 2018 Crowe LLP

Crowe

Smart decisions. Lasting value.™

Blockchain overview and applicability to education and charitable institutions

The new technology will enable new models

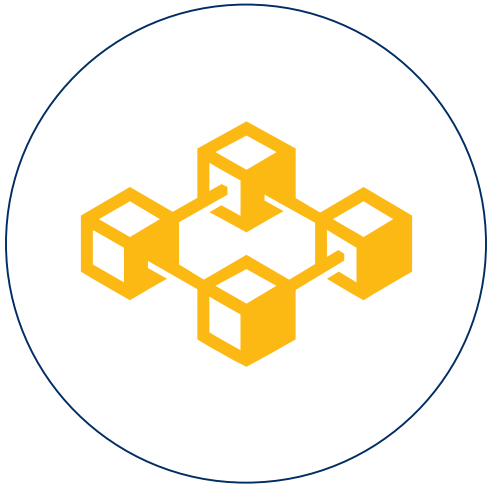
David Uhryniak

September 2018

Agenda

Insight into blockchain

Blockchain use cases in education and non-profit

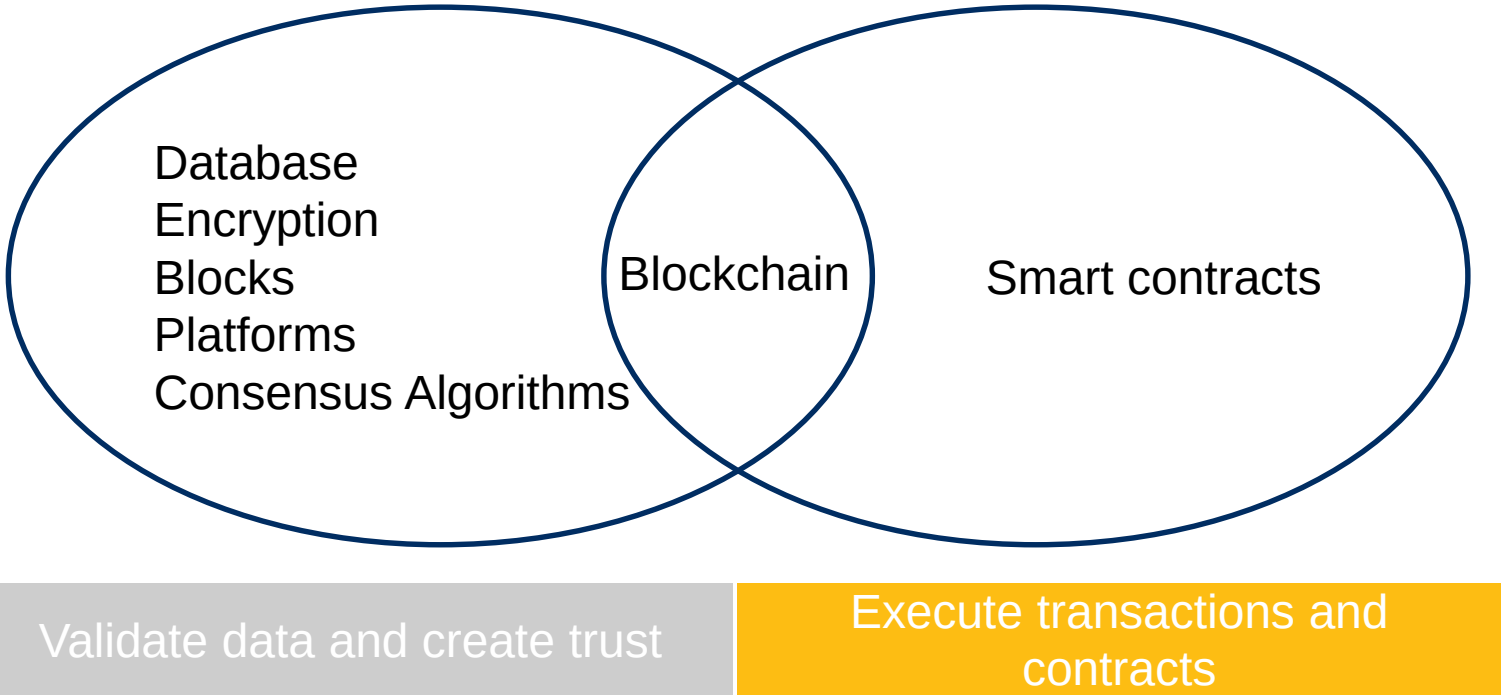


© 2017 Crowe Horwath LLP

Insight into blockchain

© 2018 Crowe LLP

Blockchain is a combination of technologies that enable transactions and contract terms to be executed without a central authority.



© 2018 Crowe LLP

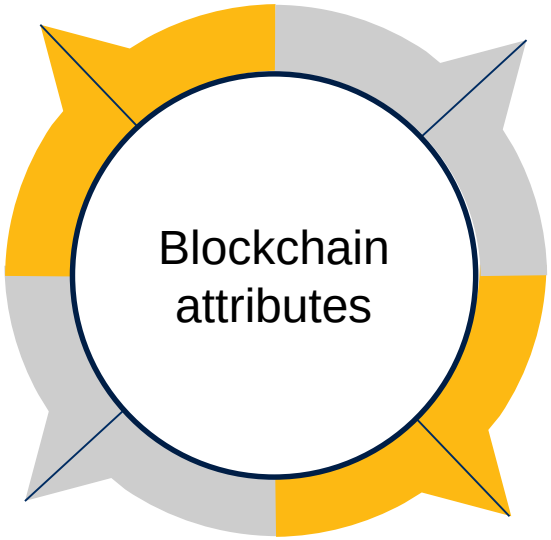
Blockchain characteristics make the technology unique.

Valid

Ensures transaction legitimacy, e.g. prevents double spending

Trust

Allows unknown parties to transact without a central clearinghouse or intermediary



Authentic

Ensures transaction originates from the account owner and is not duplicated

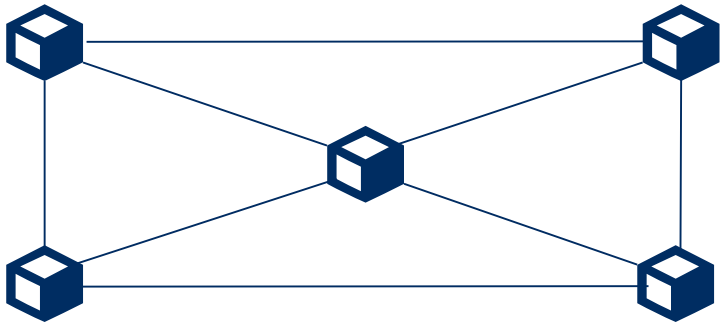
Immutable

Once written onto blockchain, the entry cannot be changed

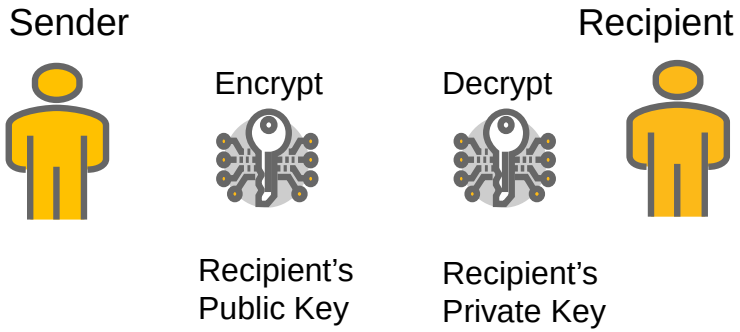
© 2018 Crowe LLP

What gives blockchain these characteristics?

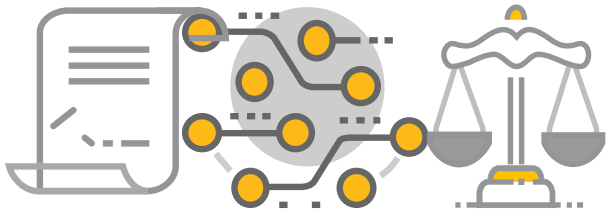
Distributed



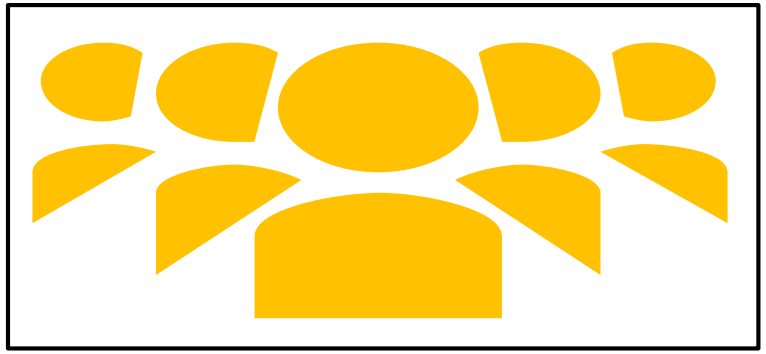
Cryptography



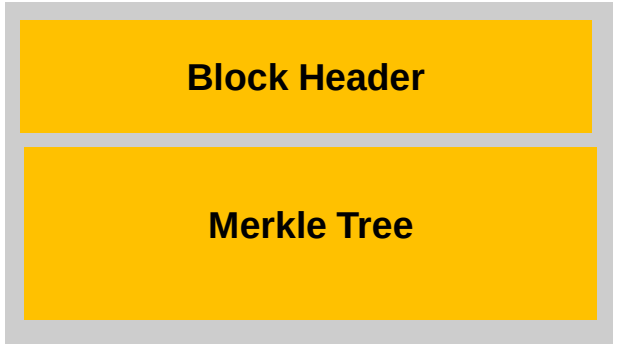
Smart contracts



Consensus



Block structure

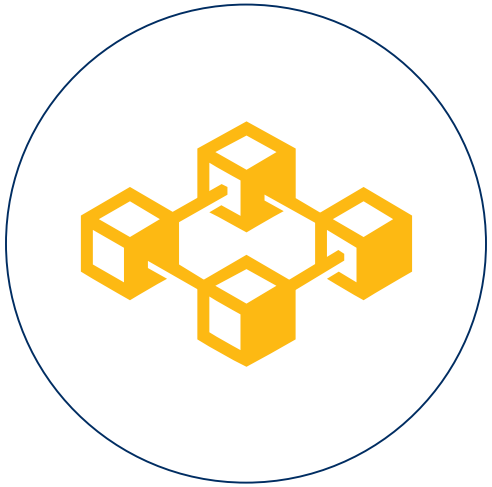


© 2018 Crowe LLP

Poll questions

My level of familiarity with Blockchain can best be described as:

a) I'm very familiar
b) I'm somewhat familiar
c) I'm familiar with cryptocurrencies but not the underlying Blockchain technology
d) I have no familiarity and hope to learn the basics today



© 2018 Crowe LLP

The block structure consists of two pieces, the header and the merkle tree.

Block structure

Block Header

Merkle Tree

Block Header

- *Block version number*
- *Time stamp*
- *Hash of the merkle root*
  - A hash of all the hashes in a block
- *Hash pointer*
  - Hash of the previous block
  - Hash of the data in the previous block
- *Nonce*
  - Random 32 bit number used to order outgoing transactions

Merkle Tree

- Cryptographic hashes of paired data
- Proves and maintains data integrity and validity
- Computationally easy and relatively fast
- Easily transmitted across networks

© 2018 Crowe LLP

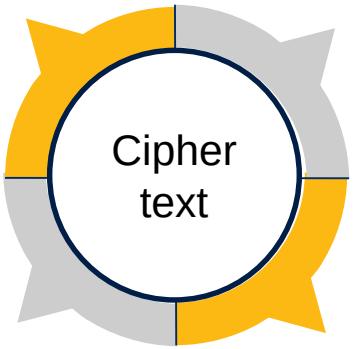
Public Key Encryption Infrastructure is the process of securely transmitting messages on blockchain between parties.

Send

Validate and encrypt

- Receiver public key
- Cryptographic hash of message
- Sender private key
- Signing algorithm
- Digital signature

Transmit



Recieve

Validate and decrypt

- Receiver private key
- Cryptographic hash of message
- Sender public key
- Verification algorithm
- Digital signature

© 2018 Crowe LLP

Defining cryptographic hash function and digital signatures.

Cryptographic hash function

- Deterministic
- Quick computation
- Pre-image resistance
- Small changes in the input change the hash output
- Collision resistant
- Puzzle friendly

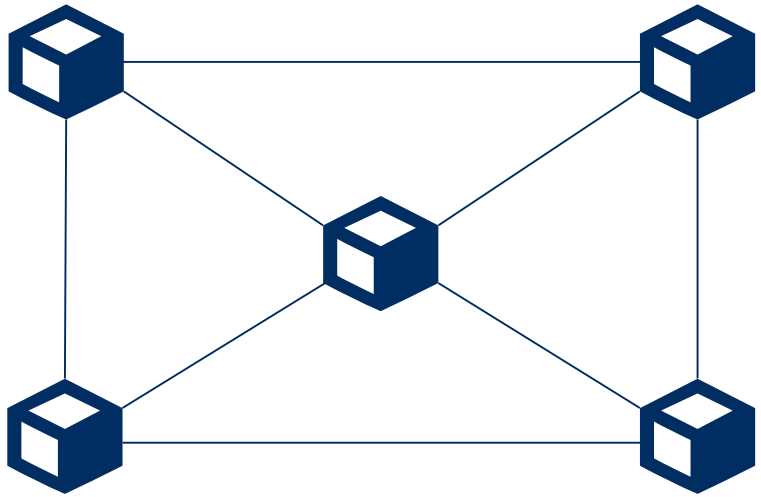
Digital signatures

- An algorithm that creates private and public keys, i.e., assymetric encryption
- A signing algorithm that combines data and private key to make a signature.
- A verifying algorithm that verifies signatures and determines authenticity based on the message, the public key and signature.

© 2018 Crowe LLP

The blockchain network is distributed among potentially hundreds of nodes (public) to a handful of nodes (private).

Distributed



Key points

Transparency

- Ensures all participants have the same version of the ledger; updates in real time.

Security

- Network redundancy, as there is not a single point of failure

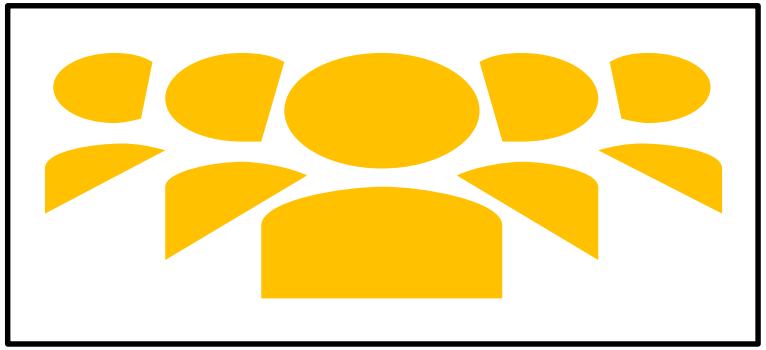
Access

- Public blockchain's (cryptocurrencies) are open to anyone.
- Private blockchain's (corporations), require permission to access.

© 2018 Crowe LLP

Consensus is determined by a network of nodes provides a guaranteed ordering of transactions and validates the block of transactions.

Consensus



Functionality

- Confirms the correctness of all transactions in a proposed block, according to endorsement and consensus policies.
- Agrees on order and correctness and hence on results of execution (implies agreement on global state).
- Interfaces and depends on smart-contract layer to verify correctness of an ordered set of transactions in a block.

Models*

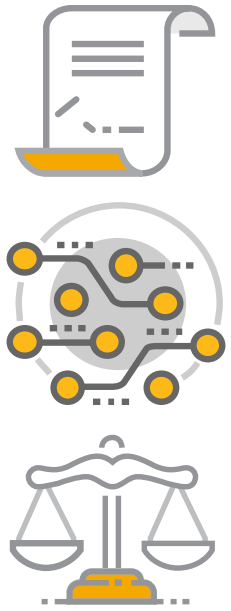
*list is not comprehensive

- Practical Byzantine Fault Tolerance
- Proof of Work
- Proof of Elapsed Time
- Proof of Stake

© 2018 Crowe LLP

Smart contracts are leveraged by to automate tasks, confirm information, and execute contracts.

Smart contracts



Types

Deterministic

The contract can be entirely executed within the code written on the blockchain.

Non-deterministic

For the code to be executed, input from an external source is required. This party is known as an “oracle”.

Functions

Legal

Smart contracts are legally binding nationally, though certain states are passing legislation to ensure legality.

Execute contracts

Contract terms can be coded into blockchain to quickly and efficiently ensure terms are met.

Automate tasks

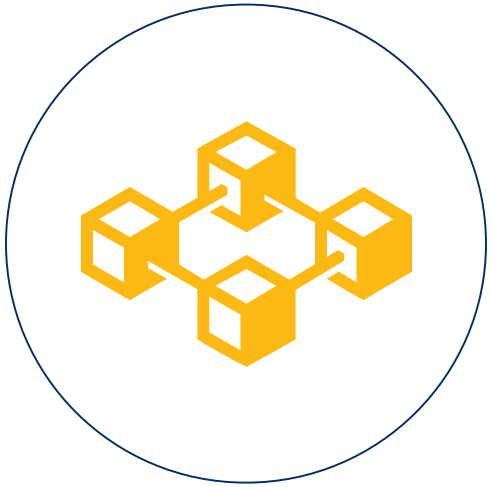
Many paper-based or manual-entry tasks can be coded into blockchain.

© 2018 Crowe LLP

Poll questions

My organization has been involved in a transaction(s) utilizing cryptocurrency

a) Yes
b) No
c) I don’t know

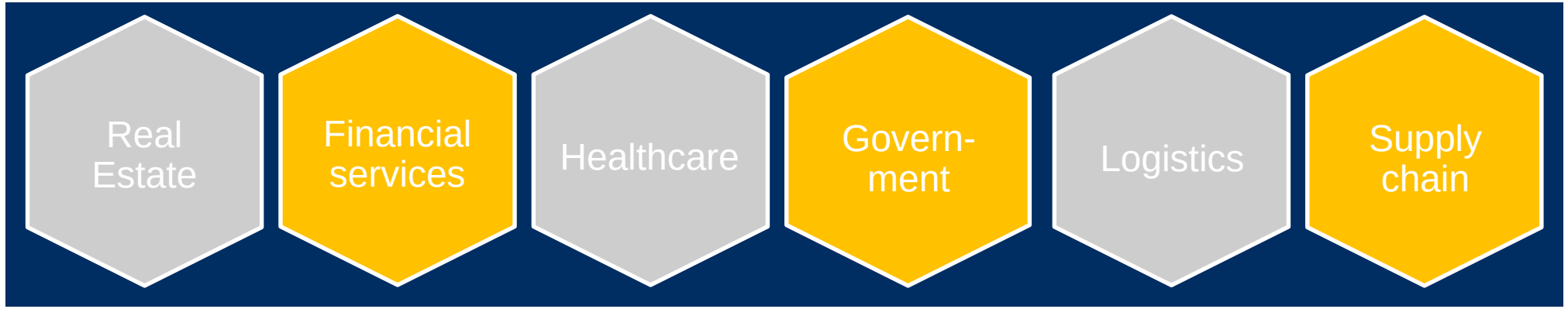


© 2018 Crowe LLP

Blockchain use cases in Education and Non-profit

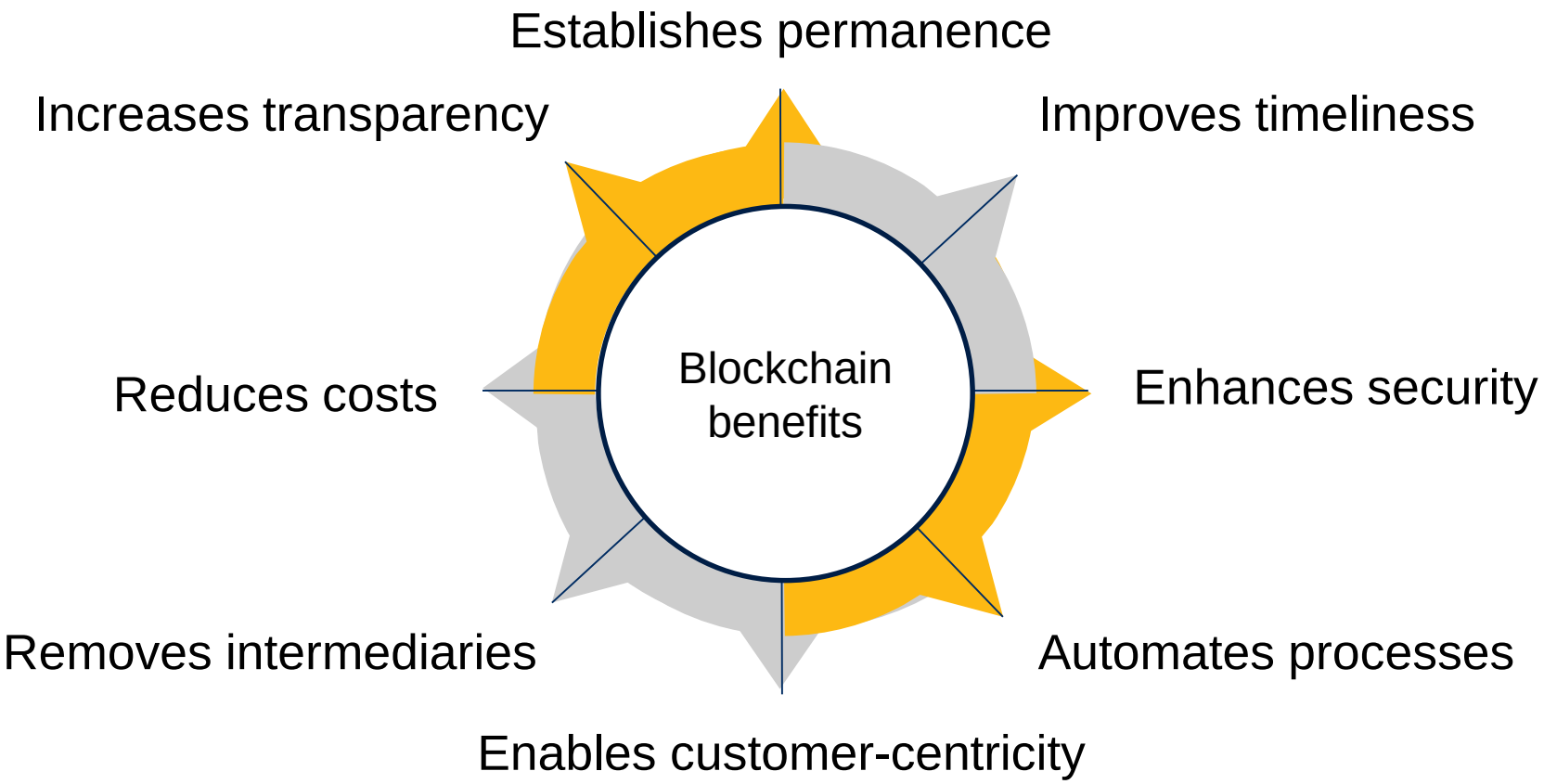
© 2018 Crowe LLP

Blockchain is now being applied to a wide range of business functions in multiple industries.



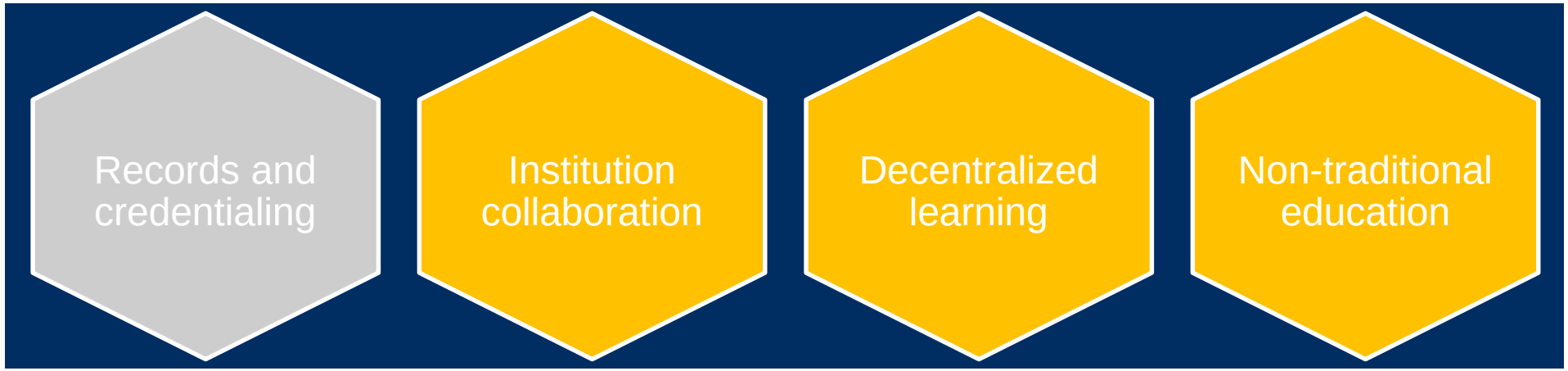
© 2018 Crowe LLP

Deploying blockchain offers multiple benefits.



© 2018 Crowe LLP

Blockchain is set to transform education to new models and offers enhancements to the current model.



© 2018 Crowe LLP

Blockchain is set to transform education to new models and offers enhancements to the current model.

UNIVERSITY of NICOSIA

https://verify.unic.ac.cy/verify

2018 – received title as the “Biggest contributer to the rise of blockchain” at the Blockchain Expo in Amsterdam

- First University to publish on blockchain all graduates diplomas

Certificate U111N1111 - Master Degree - 201707071234567.PDF is valid!

Transaction Id	bcbad90d35d04fe925682f239c004879331cbe177ed174b76262448d93e61d1f
Issuer	University of Nicosia
Address	1A94iDxxJijPvo8CjCWe4GLUfT6BGTWuUq
First Name	Konstantinos
Fathers Name	A
Last Name	Papadopoulos
Degree Type	Μεταπτυχιακό Δίπλωμα
Program of Study	Εκπαιδευτική Ψυχολογία
Date of Issue	12/6/2017

© 2018 Crowe LLP

The first blockchain-based university has been launched; leading universities are offering blockchain courses.

Traditional universities offer blockchain courses…

BLOCKCHAIN AT BERKELEY

ILLINOIS

Duke Blockchain Lab
Bringing Blockchain Technology to the Duke University Community

Stanford

GEORGETOWN UNIVERSITY
McDonough SCHOOL of BUSINESS

PRINCETON UNIVERSITY

coursera

NEW YORK UNIVERSITY
NYU STERN
LEONARD N. STERN SCHOOL OF BUSINESS

CORNELL BLOCKCHAIN

DIGITAL CURRENCY INITIATIVE
mit media lab

…as the transformative impact of blockchain is beginning

- Woolf University is the first institution to be entirely built and operated with blockchain

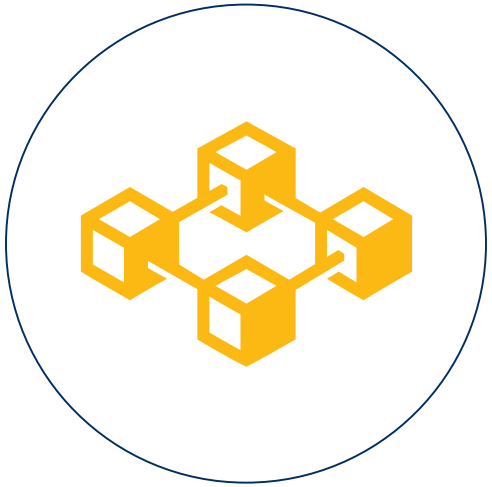
- Designed to address multiple issues in traditional education:
  - Tuition costs for students
  - Professor compensation
  - Return on Education
  - Increases liquidity in professor market

© 2018 Crowe LLP

Poll questions

Based on what I have learned about Blockchain, I can envision potential use cases for the technology that will improve existing business processes at my organization or impacting my organization

a) Yes
b) No
c) I don’t know



© 2018 Crowe LLP

Blockchain can provide the impoverished access to basic attributes that have never been possible and improve current non-profit models.

© 2018 Crowe LLP

Blockchain is being leveraged to provide ownership rights in countries where it had not previously been possible.

Transform current situations

Collaboration

MEDICI LAND GOVERNANCE

The World Bank

Issues

- Speculation often creates risk of illegtimate property siezure
- Prevents development of a real estate market
- Government cannot tax
- Certain ethnic groups or genders often cannot easily gain property ownership
- Invites fraud into system

Mission

- The companies will design, implement, and evaluate pilot programs to create blockchain PoC's and infrastructure to secure property rights.

https://www.marketwatch.com/press-release/overstockcom-blockchain-subsidiary-medici-land-governance-signs-agreement-with-world-bank-to-enhance-access-to-secure-land-rights-in-developing-countries-2018-08-01

© 2018 Crowe LLP

Start-ups are developing blockchain platforms for non-profit organizations.

Improve existing model

- "a blockchain platform that solves the major compliance issues of fund tractability, security, and fraud, while offering cost savings on the transactions"

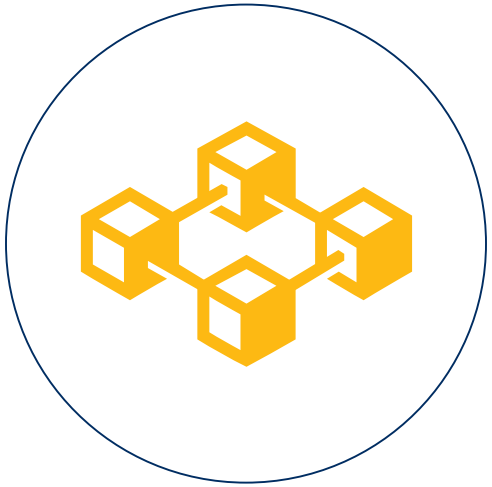
- "AidCoin is the ERC20 token that aims to become the preferred method to donate transparently through the Ethereum blockchain and to access the ecosystem of services provided by the AIDChain platform."

© 2018 Crowe LLP

Poll questions

My organization is actively exploring potential Blockchain use cases

a) Yes
b) No
c) I don’t know



© 2018 Crowe LLP

Thank You

David Uhryniak

Office 312-632-6573 | Mobile 224-374-3454

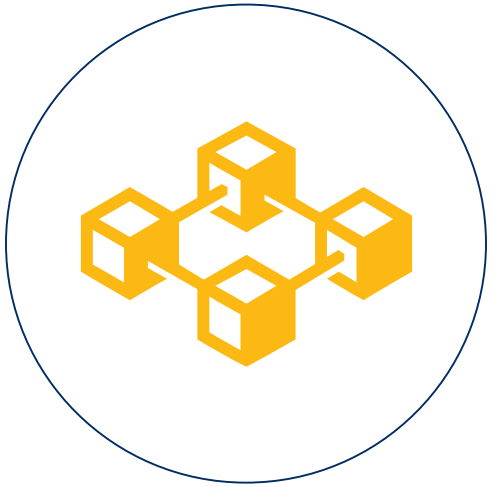
David.Uhryniak@crowe.com

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2018 Crowe LLP.

Poll questions

Would you like a Crowe professional to follow up with you regarding Blockchain and its potential impact on your business?

a) Yes, please call me
b) Yes, please send me a one-time email regarding Blockchain
c) No, please do not contact me
d) N/A



© 2018 Crowe LLP