BLOCKCHAIN: ACCOUNTING AND ACADEMIC IMPLICATIONS OF BLOCKCHAIN

Presentation subject to change in topic, order and content

The Phenomena, the Fad and the Fallacies

ERIC E. COHEN

COHEN COMPUTER CONSULTING

SAN FRANCISCO, SEPTEMBER 13, 2018

ABOUT YOUR SPEAKER

Eric E. Cohen

Eric Cohen is a co-founder of **XBRL** and the chief architect of its initial standardization work in transactional and detailed data space: the *Global Ledger (XBRL GL)*. He serves as a Domain Coordinator for the **United Nations** CEFACT Accounting and Audit Domain.

As a national Expert to **ISO** standardization projects in *Audit Data Collection* and *Blockchain and Distributed Ledger Technologies*, he hopes to facilitate the development of continuous audit, the establishment of the electronic, seamless audit trail, and building the foundations for auditing in a Blockchain/Distributed Ledger environment. He leads the ISO study on interoperability issues for blockchain.

His consultancy, **Cohen Computer Consulting**, began in 1992 to help organizations cope with, and benefit from, accounting and audit technology. *Cohen Computer Consulting* was one of the original 13 organizations that started XBRL. After a brief 17 year hiatus, he is now again focusing on accounting software implementations, as well as Audit Data Standards, Blockchain, Continuous Audit, Data Level Assurance and XBRL. As he is fond of saying, "At Cohen Computer Consulting, we turn 'computerese' into 'computer-ease'".

Mr. Cohen is a member of the American Institute of Certified Public Accountants and the New York State Society of Certified Public Accountants. He appreciates a long history of collaboration with the academic community. A selective bibliography of his publications can be found at his web site.

Cohen Computer Consulting
Website: http://www.computercpa.com
E-mail: eric.e.cohen@computercpa.com
Phone: +1-559-4-XBRL-GL (+1-559-492-7545)

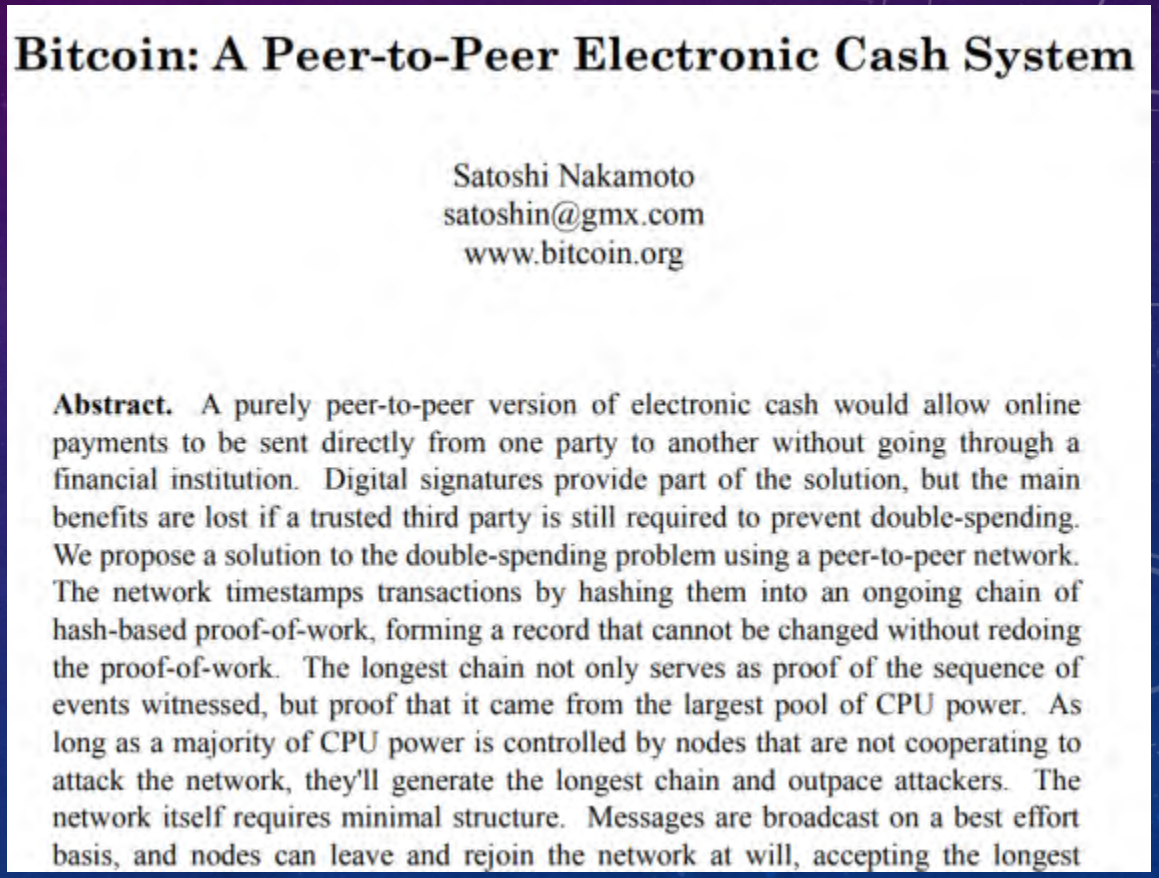
GETTING SOME THINGS OUT OF THE WAY

- Bitcoin and blockchain/distributed ledger technologies backgrounder
- The Phenomena, the Fad and the Fallacies; getting us together on some things

DID BLOCKCHAIN BEGIN WITH BITCOIN IN 2008?

October 31, 2008

https://bitcoin.org/bitcoin.pdf



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest

Data Network Architectures, Standards,

Start-up fields time-stamp system

Company unveils first electronic file validation software.

BY ELLEN MESSMER

Chatham, N.J.

Start-up Surety Technologies, Inc. this month began shipping desktop computer software that gives corporations a way to electronically notarize and time-stamp important documents.

Companies commonly have paper documents certified by notaries in order to prove the document's authenticity. The Surety Technologies software, used in conjunction with its Internet-based archive service, for the first time gives companies a way to notarize documents electronically over a network through the Digital Notary System.

With the Digital Notary client software for Windows or Unix running on their desktop computers, users can compress and time-stamp a file employing a mathematical algorithm, called a "hash."

Each time-stamped document's hash is as unique as a fingerprint, so only the identical document would produce the

Surety Technologies

"The Surety software for Windows works well as a single workstation implementation, but we want to make it server-based within the corporation so we can validate documents by integrating the Digital Notary System into Lotus Notes," said Gary Kuehlanz, manager of advanced technology at American Cyanamid.

The firm has an array of research data that must be notarized to substantiate patent claims, he said.

"Our scientists have to manually submit the test scripts and other documents to be witnessed by another individual under the federal rules of evidence," he noted. "The paper is getting out of hand, and we'd like to use the computer as the witness instead."

Stuart Haber, chief scientist and cofounder of Surety Technologies, said a LAN-based version of the software and an application program interface tool kit will be ready by March.

The Windows and Unix-based versions of the Digital Notary System, which cost

The fragmentation and data compression feature then takes over, break- add the new features for free.

©Prestcom: (514) 443-2909.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Chain of Blocks goes back 25 years!

DOES BLOCKCHAIN IMPACT/OBSOLETE ACCOUNTANTS?

Blockchain technology has the potential to impact all recordkeeping processes, including the way transactions are initiated, processed, authorized, recorded and reported. Changes in business models and business processes may impact back-office activities such as financial reporting and tax preparation. Independent auditors likewise will need to understand this technology as it is implemented at their clients. **Both the role and skill sets of CPA auditors may change as new blockchain-based techniques and procedures emerge.** For example, methods for obtaining sufficient appropriate audit evidence will need to consider both traditional stand-alone general ledgers as well as blockchain ledgers. Additionally, there is potential for greater standardization and transparency in reporting and accounting, which could enable more efficient data extraction and analysis. Blockchain technology could bring new challenges and opportunities to the audit and assurance profession. **While traditional audit and assurance services will remain important, a CPA auditor's approach may change**. Just as the audit and assurance profession is evolving today, with audit innovations in automation and data analytics, **blockchain technology may also have a significant impact on the way auditors execute their engagements**. Moreover, CPAs may need to broaden their skill sets and knowledge to meet the anticipated demands of the business world as blockchain technology is more widely adopted.

https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf

“BLOCKCHAIN MAKES AUDITORS OBSOLETE; IT IS SELF-AUDITING”

Valuation
Existence
a**L**location
Occurrence
Completeness
class**I**fication
unde**R**standability
Accuracy
Presentation
cu**T**off
Obligations
Rights

SHOULD EVERYONE SHOULD BUY CRYPTO TODAY?

- FOMO
- HODL
- DYOR
- ATH, ATL
- Whale
- ASHDRAKED, REKT
- *Eric is a REVERSE INDICATOR*

Most terms are humorous; not understanding *one* of these terms means you lose money.

- **Fork** – If you held Bitcoin at 8/2014, how may altcoins would you also hold? (https://en.wikipedia.org/wiki/List_of_bitcoin_forks)

https://cryptocurrencyfacts.com/a-list-of-upcoming-bitcoin-forks-and-past-forks/

7/15/2016	8/1/2017	10/24/2017	2/28/2018	9/13/2018
1 Bitcoin @ 7/15/2016	1 Bitcoin (BTC)	1 Bitcoin (BTC)	1 Bitcoin (BTC)	1 Bitcoin (BTC)
	1 Bitcoin Cash (BCH)	1 Bitcoin Cash (BCH)	1 Bitcoin Cash (BCH)	1 Bitcoin Cash (BCH)
		1 Bitcoin Gold (BTG)	1 Bitcoin Gold (BTG)	1 Bitcoin Gold (BTG)
			1 Bitcoin Private (BTCP)	1 Bitcoin Private (BTCP)

Bitcoin, Forks and Altcoins

	7/15/2016	8/1/2017	10/24/2017	2/28/2018	9/13/2018
BTC	660.00	2,900.00	5,900.00	11,000.00	
BCH		380.00	320.00	1,200.00	
BTG			140.00	115.00	
BTCP				60.00	
Total	$ 660.00	$3,280.00	$ 6,360.00	$12,375.00	

THERE'S A LOT OF CONFUSION

- "'The' Blockchain"
- Blockchain <> Distributed Ledger … or is it?
- Anarchy tool or regulatory tool?
- New means of financing/equity?
- Teams and whitepapers or F/S?
- Blockchain or Block chain (terminology)
- Nakamoto vs beyond

- **Fungible tradeable assets** vs direct identification (FT, FNT, ERC20/ERC721)
- Permissionless/permissioned
- Public/private

- Decentralized/centralized
- Proof of Work/Proof of Stake
- Mining/Consensus

IS IT ALL ABOUT BITCOIN?

- Generally fungible – no collectible coins or tokens
- Tied to tangible? Story of Tether
- Exchanges: e.g., Coinbase
- Manage your own
  - Handing over the keys?

Equity

Coins and Tokens

Utility

Security

DIGITAL ASSETS

Cryptocurrencies: 1590 • Markets: 11262 • Market Cap: $249,756,983,453 • 24h Vol: $10,135,720,844 • BTC Dominance: 42.3%

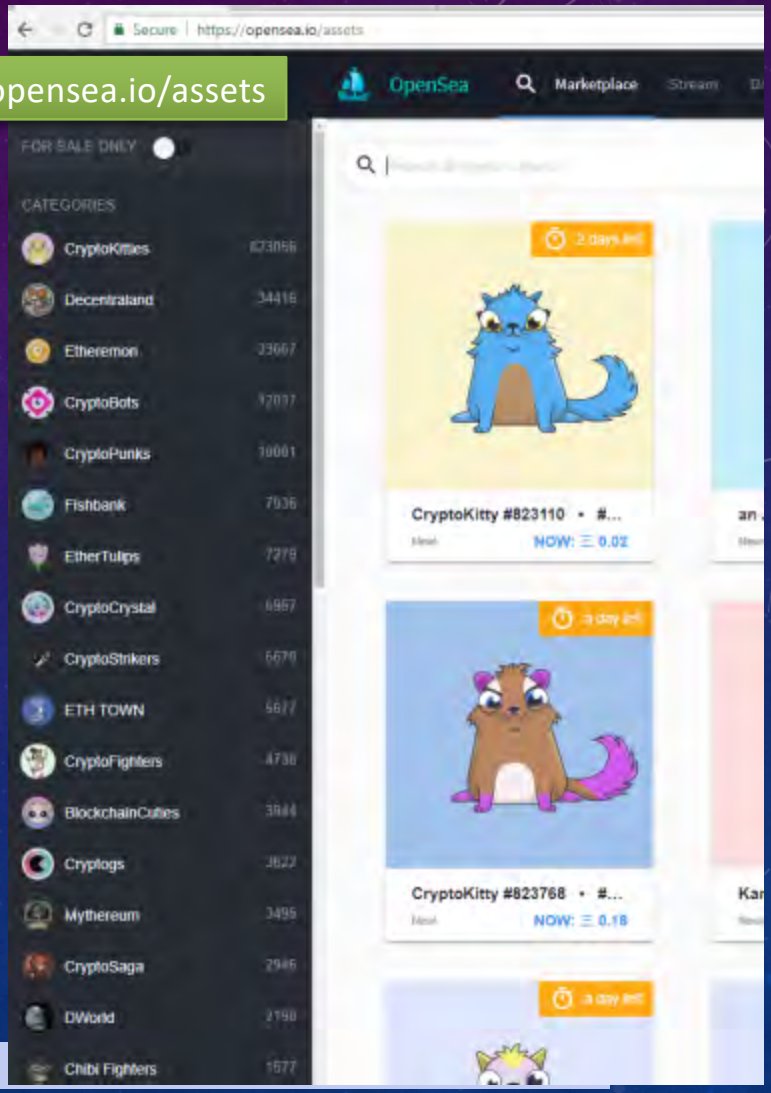
Top 100 Cryptocurrencies By Market Capitalization

Cryptocurrencies ▾ | Watchlist | USD ▾ | Next 100 → | View All

*#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$105,627,329,094	$6,170.92	$3,198,400,000	17,116,950 BTC	-1.93%	
2	Ethereum	$44,536,321,011	$443.94	$1,293,350,000	100,320,134 ETH	-3.94%	
3	Ripple	$18,417,019,311	$0.469079	$169,982,000	39,282,084,448 XRP *	-2.68%	
4	Bitcoin Cash	$12,467,289,916	$724.64	$334,515,000	17,204,900 BCH	-4.65%	
5	EOS	$6,999,348,724	$7.81	$595,935,000	896,149,492 EOS *	-5.82%	
6	Litecoin	$4,538,160,800	$79.41	$259,823,000	57,148,696 LTC	-4.25%	
7	Stellar	$3,606,660,527	$0.192251	$28,714,000	18,760,165,235 XLM *	-3.03%	
8	Cardano	$3,376,041,636	$0.130213	$30,936,900	25,927,070,538 ADA *	-4.34%	
9	IOTA	$2,722,132,983	$0.979350	$39,582,400	2,779,530,283 MIOTA *	-4.15%	
10	Tether	$2,693,802,265	$0.995073	$1,861,15			
11	TRON	$2,600,291,792	$0.039549	$87,971,100	65,748,111,645 TRX *	-6.73%	
12	Monero	$2,043,848,672	$126.40	$30,413,800	16,169,177 XMR	-1.47%	

Coinmarketcap.com

https://opensea.io/assets



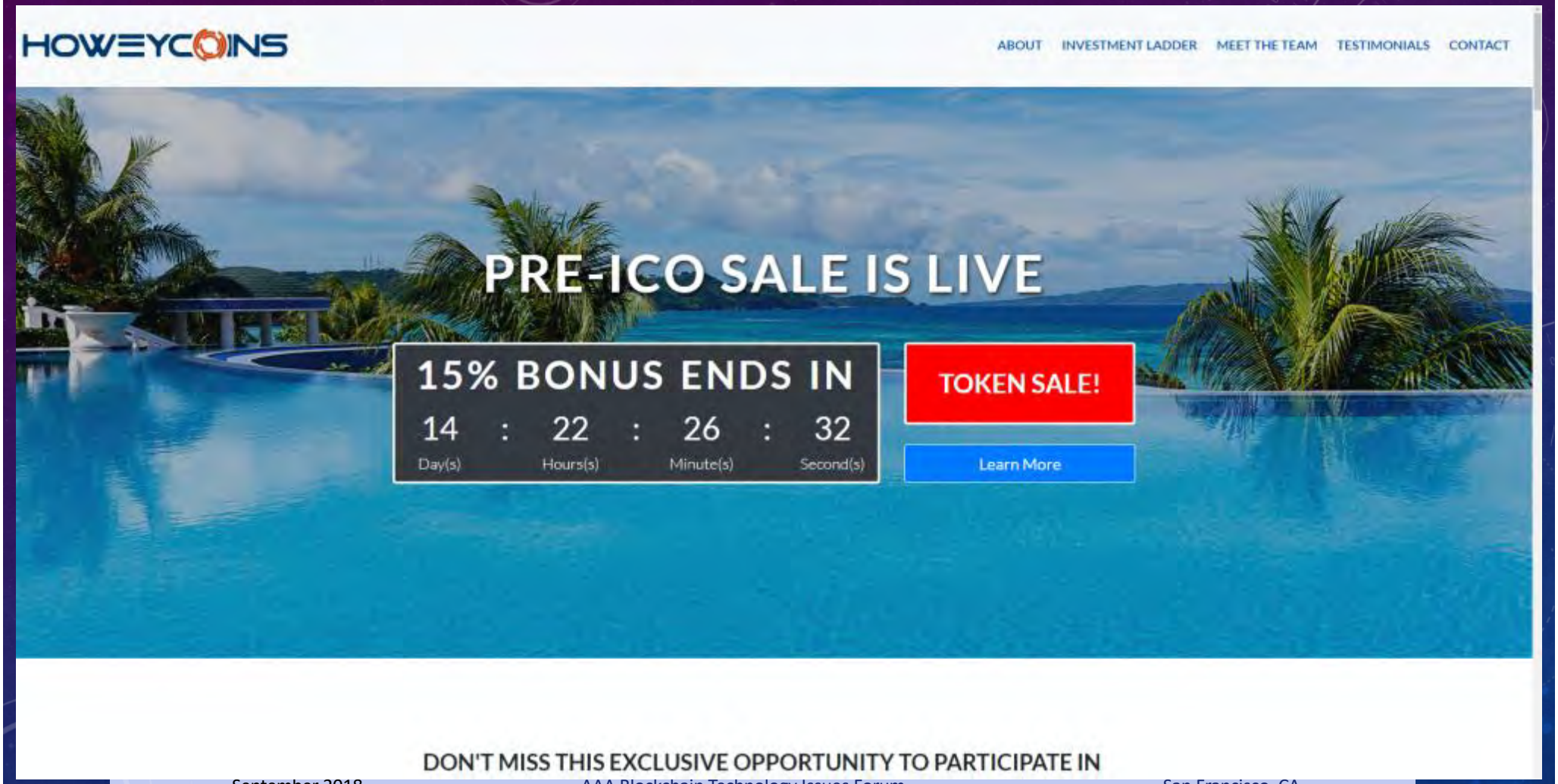
Forum

IS IT EASY TO INVEST AND MANAGE YOUR OWN ASSETS?

- With custodial accounts (they hold they keys), you do not have access to your assets except through them; many attacks and losses
- With non-custodial or direct holdings:
  - No one else can help you if you lose track of them; the strength of the security is a “weakness”
  - Your unfamiliarity with managing assets in these matters means someone else could use guesswork, social engineering or other relatively simple means of taking your assets from you
  - No one has any idea how much of the assets are left without anyone having access to them

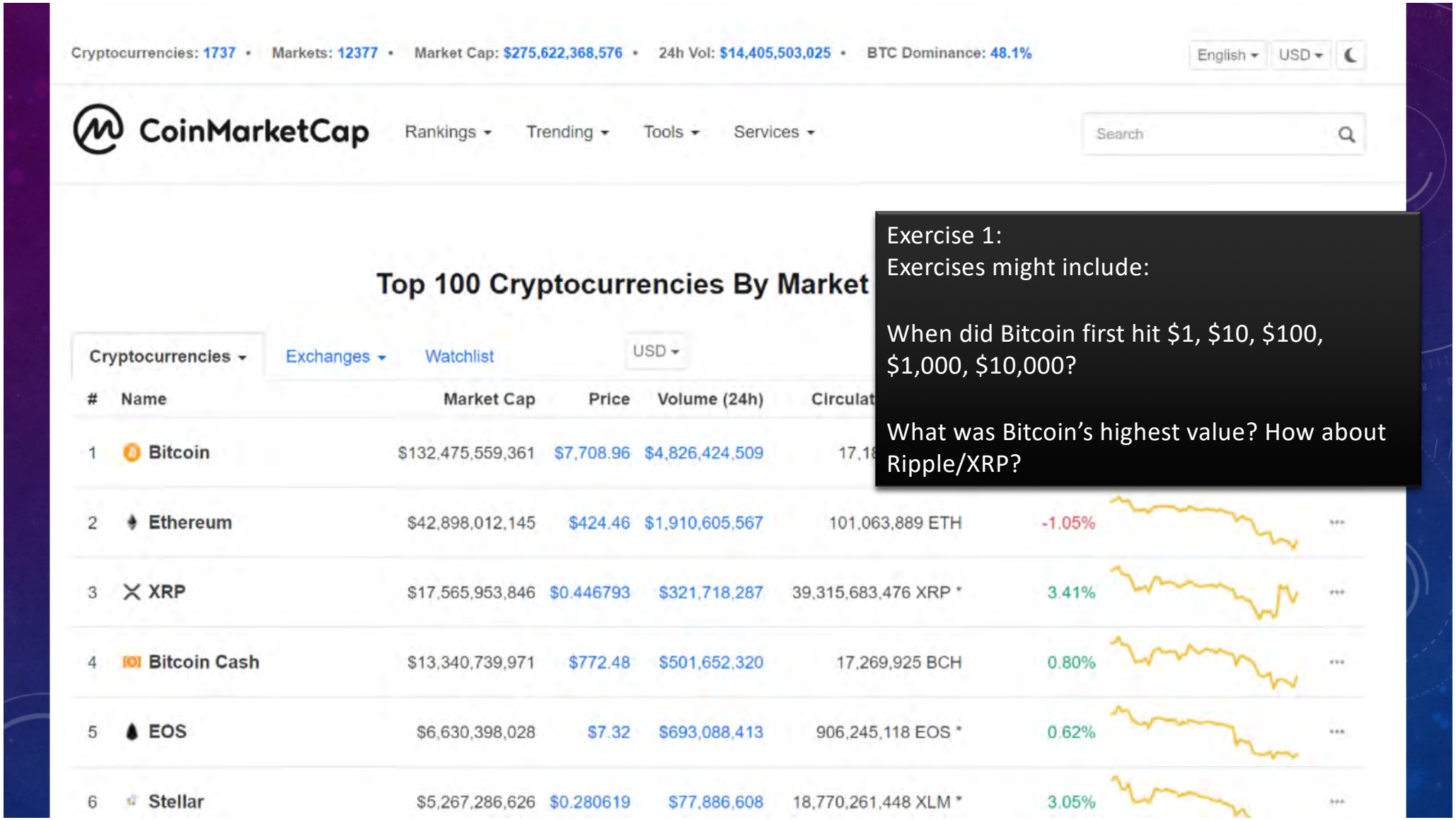
DECENTRALIZED “MONEY”

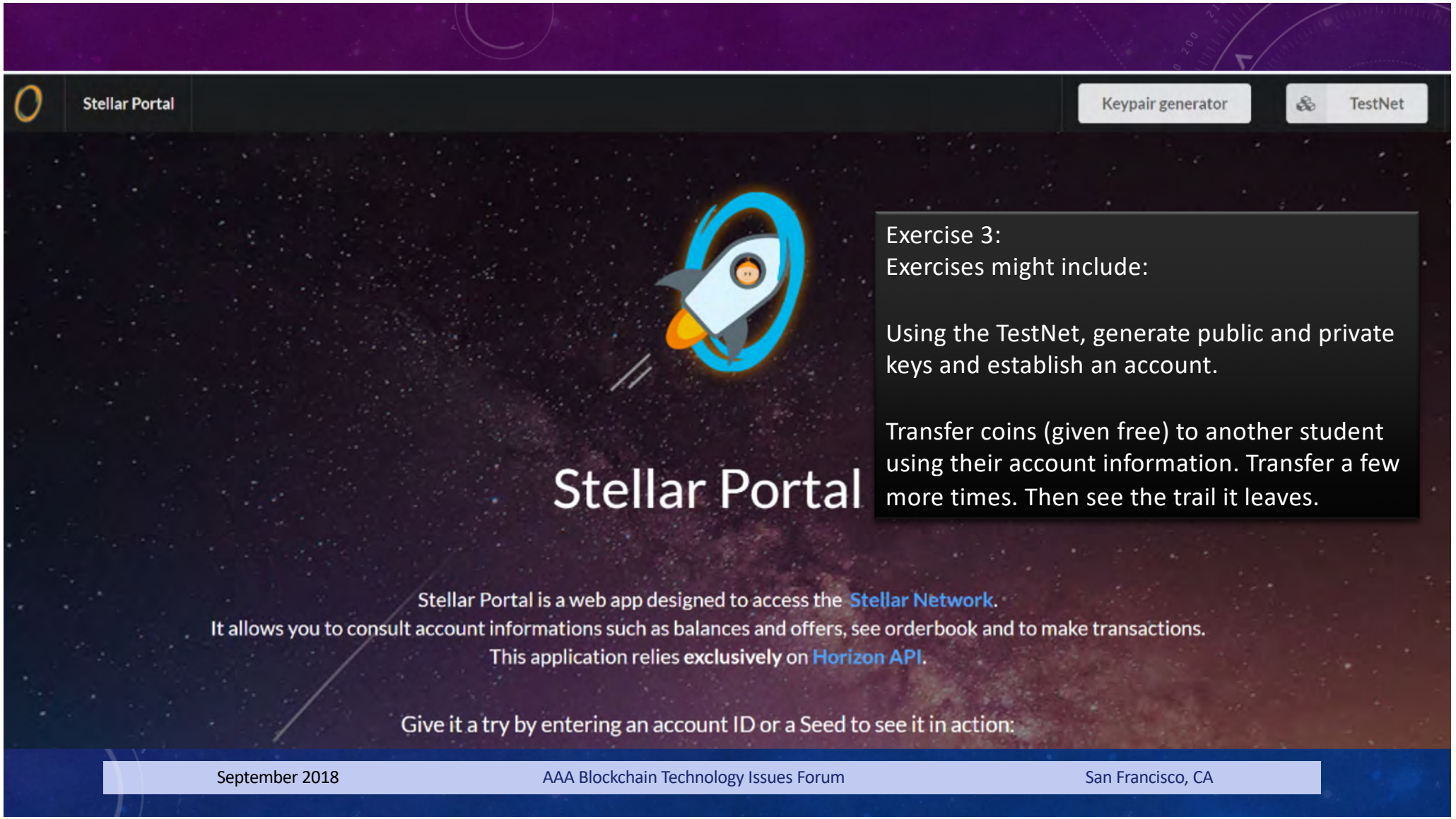
- Kept at third party (e.g., exchange) – easy, but many risks
  - Exchanges and KYC/anonymity
- Kept on your device on a wallet
- If you lose your keys/phrases, you are out of luck
- Will public/private keys become worse than tracking passwords?
- No FDIC guarantee
- No one to get you back in
- Attackers galore


HOWEYCOINS
ABOUT
INVESTMENT LADDER
MEET THE TEAM
TESTIMONIALS
CONTACT
PRE-ICO SALE IS LIVE
15% BONUS ENDS IN
14 : 22 : 26 : 32
Day(s) Hours(s) Minute(s) Second(s)
TOKEN SALE!
Learn More
DON'T MISS THIS EXCLUSIVE OPPORTUNITY TO PARTICIPATE IN

CLASS EXERCISES

- Use of **Coinmarketcap.com** to find coins and transactional/price history
- Use of blockchain explorers like **blockchain.info** to find specific transactions and balances in different chains
  - 10,000 bitcoin for two pizzas transaction
  - Wallets with the most value in them
  - And others
- Use of Stellar testnet (https://portal.willet.io/) to obtain test coins, obtain keys/wallet address, transfer Stellar test coins between wallets and track the activities
- Use of **RoyalFork** to visualize and better understand private and public keys, wallet addresses and why random numbers as input are necessary


Cryptocurrencies: 1737 • Markets: 12377 • Market Cap: $275,622,368,576 • 24h Vol: $14,405,503,025 • BTC Dominance: 48.1%
English
USD
CoinMarketCap
Rankings
Trending
Tools
Services
Search
Top 100 Cryptocurrencies By Market
Cryptocurrencies
Exchanges
Watchlist
USD
Name Market Cap Price Volume (24h) Circulat
1 Bitcoin $132,475,559,361 $7,708.96 $4,826,424,509 17,1
2 Ethereum $42,898,012,145 $424.46 $1,910,605,567 101,063,889 ETH -1.05%
3 XRP $17,565,953,846 $0.446793 $321,718,287 39,315,683,476 XRP * 3.41%
4 Bitcoin Cash $13,340,739,971 $772.48 $501,652,320 17,269,925 BCH 0.80%
5 EOS $6,630,398,028 $7.32 $693,088,413 906,245,118 EOS * 0.62%
6 Stellar $5,267,286,626 $0.280619 $77,886,608 18,770,261,448 XLM * 3.05%
Exercise 1:
Exercises might include:
When did Bitcoin first hit $1, $10, $100, $1,000, $10,000?
What was Bitcoin's highest value? How about Ripple/XRP?


Stellar Portal
Keypair generator
TestNet
Stellar Portal
Exercise 3:
Exercises might include:
Using the TestNet, generate public and private keys and establish an account.
Transfer coins (given free) to another student using their account information. Transfer a few more times. Then see the trail it leaves.
Stellar Portal is a web app designed to access the Stellar Network.
It allows you to consult account informations such as balances and offers, see orderbook and to make transactions.
This application relies exclusively on Horizon API.
Give it a try by entering an account ID or a Seed to see it in action:

BLOCK/TRANSACTION VIEWING TOOLS

- Bitcoin: https://blockchain.info/
  - But see https://cryptograffiti.info/
- Ethereum: https://etherscan.io/ https://etherchain.org/
- Ripple: https://lnkd.in/drqks5n
- Litecoin: https://lnkd.in/der2REx
- Stellar: https://stellarchain.io/

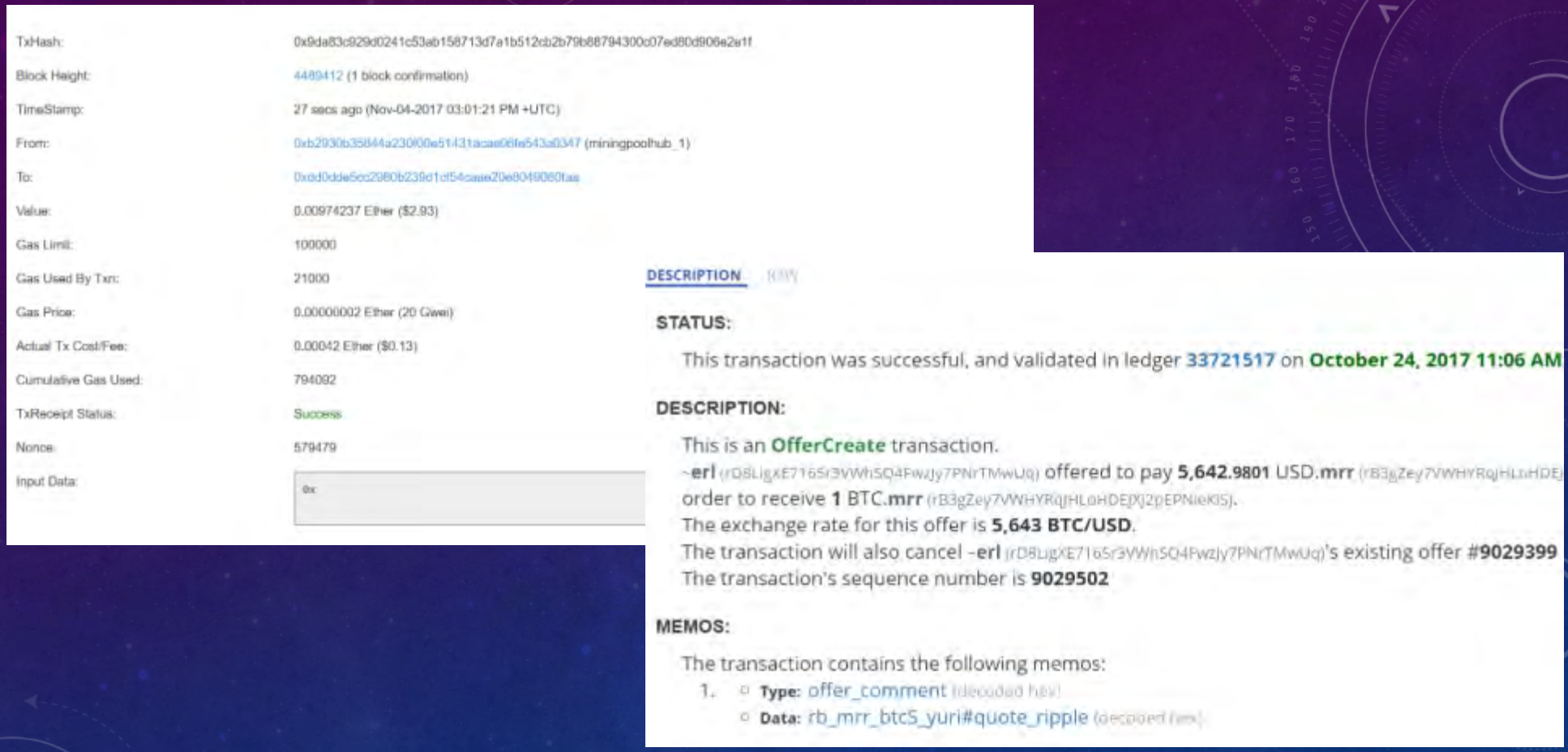
- 16 different chains: https://bchain.info

Exercise 2:
Exercises might include:
Using Blockchain.info, provide a print screen showing the exchange of 10,000 Bitcoin that purchased two pizzas
https://bitcointalk.org/index.php?topic=137.0

Identify the wallet addresses holding the most USD equivalent in Bitcoin, Ether or other cryptocurrencies

See later exercises; use these viewing tools to show transactions that will take place in class

Coinmarketcap accepts donations in crypto – how much has been put into those wallets?


TxHash: 0x9da83c929d0241c53ab158713d7a1b512cb2b79b88794300c07ed80d906e2a1f
Block Height: 4489412 (1 block confirmation)
TimeStamp: 27 secs ago (Nov-04-2017 03:01:21 PM +UTC)
From: 0xb2930b35844a230f00e51431acae96fe543a0347 (miningpoolhub_1)
To: 0xdd0dde5cc2980b239d1cf54caae20e8049060fas
Value: 0.00974237 Ether ($2.93)
Gas Limit: 100000
Gas Used By Txn: 21000
Gas Price: 0.00000002 Ether (20 Gwei)
Actual Tx Cost/Fee: 0.00042 Ether ($0.13)
Cumulative Gas Used: 794092
TxReceipt Status: Success
Nonce: 579479
Input Data: 0x
DESCRIPTION
STATUS:
This transaction was successful, and validated in ledger 33721517 on October 24, 2017 11:06 AM
DESCRIPTION:
This is an OfferCreate transaction.
-erl (rD8LigXE7165r3VWh5Q4PwzJy7PNrTMwUq) offered to pay 5,642.9801 USD.mrr (rB3gZey7VWHYRqJHLoHDEJXJ2pEPNieKiS)
order to receive 1 BTC.mrr (rB3gZey7VWHYRqJHLoHDEJXJ2pEPNieKiS).
The exchange rate for this offer is 5,643 BTC/USD.
The transaction will also cancel -erl (rD8LigXE7165r3VWh5Q4PwzJy7PNrTMwUq)'s existing offer #9029399
The transaction's sequence number is 9029502
MEMOS:
The transaction contains the following memos:
1. Type: offer_comment (decoded hex)
Data: rb_mrr_btcS_yuri#quote_ripple (decoded hex)

Large Prime Number 1

Large Prime Number 2

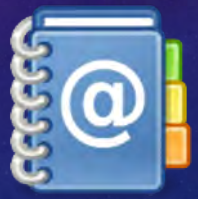
Really Large Number (P1 x P2)

See it in action!

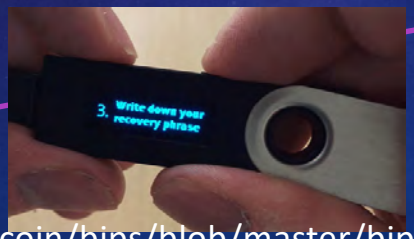
Bitcoin
https://www.royalfork.org/2014/08/11/graphical-address-generator/
Ether
https://www.royalfork.org/2017/12/10/eth-graphical-address/

Private Key (a number derived from the above)

Public Key (a number derived from the private key)



Public Address (a number derived from the public key)
(Bitcoin, Ethereum, etc.)

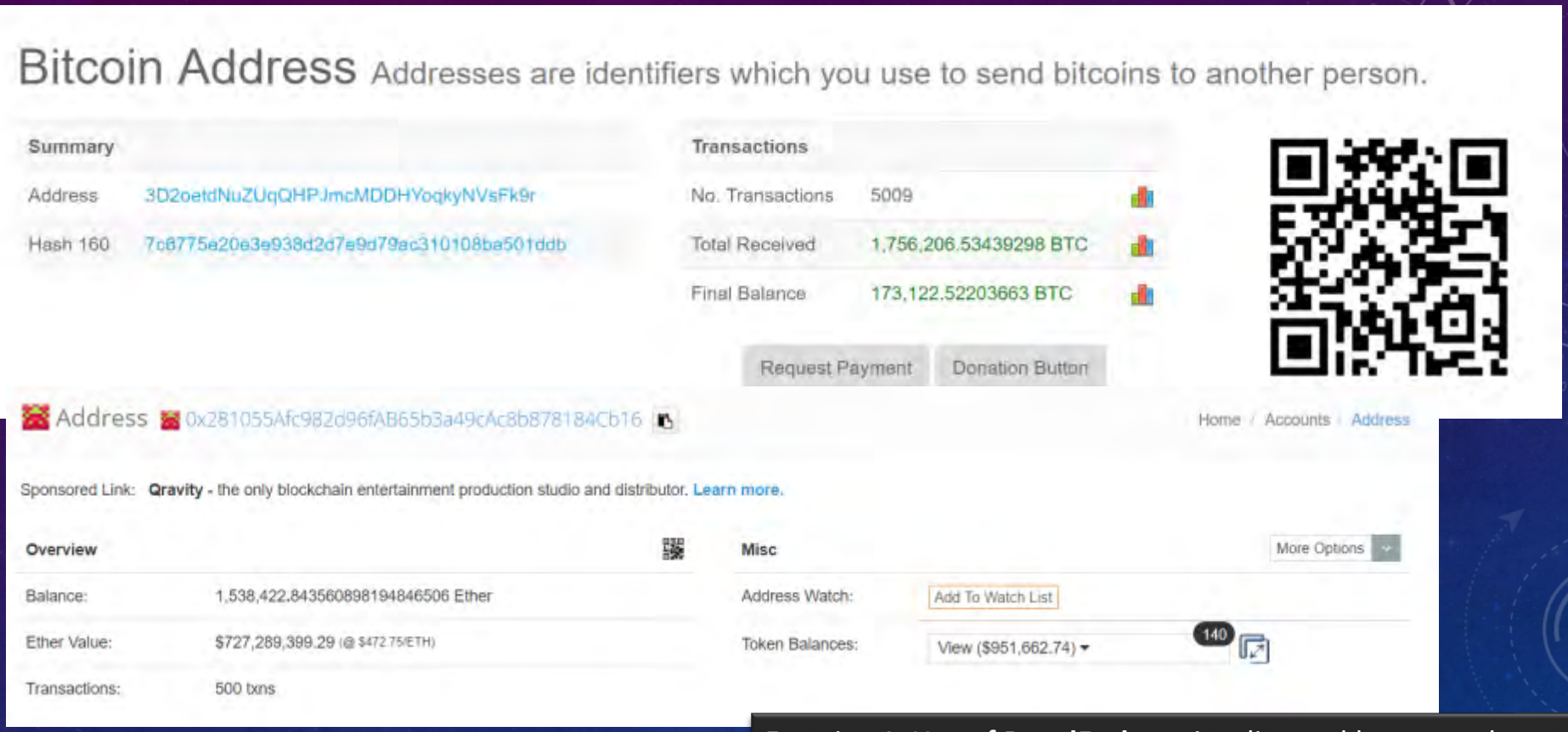


doctor prolapse practice feed shame frail despair banjo road again bridge least

Wallet Specific Recovery Phrase, based on wallet-specific wordlist

https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

Whoever holds the private keys to these two addresses has access to $1B of assets each as of 6/23/2018



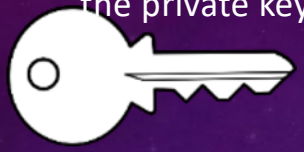
Exercise 4: Use of **RoyalFork** to visualize and better understand private and public keys, wallet addresses and why random numbers as input are necessary

https://bitinfocharts.com/top-100-richest-bitcoin-addresse

https://etherscan.io/accounts

Private Key (a number derived from the above)

Public Key (a number derived from the private key)



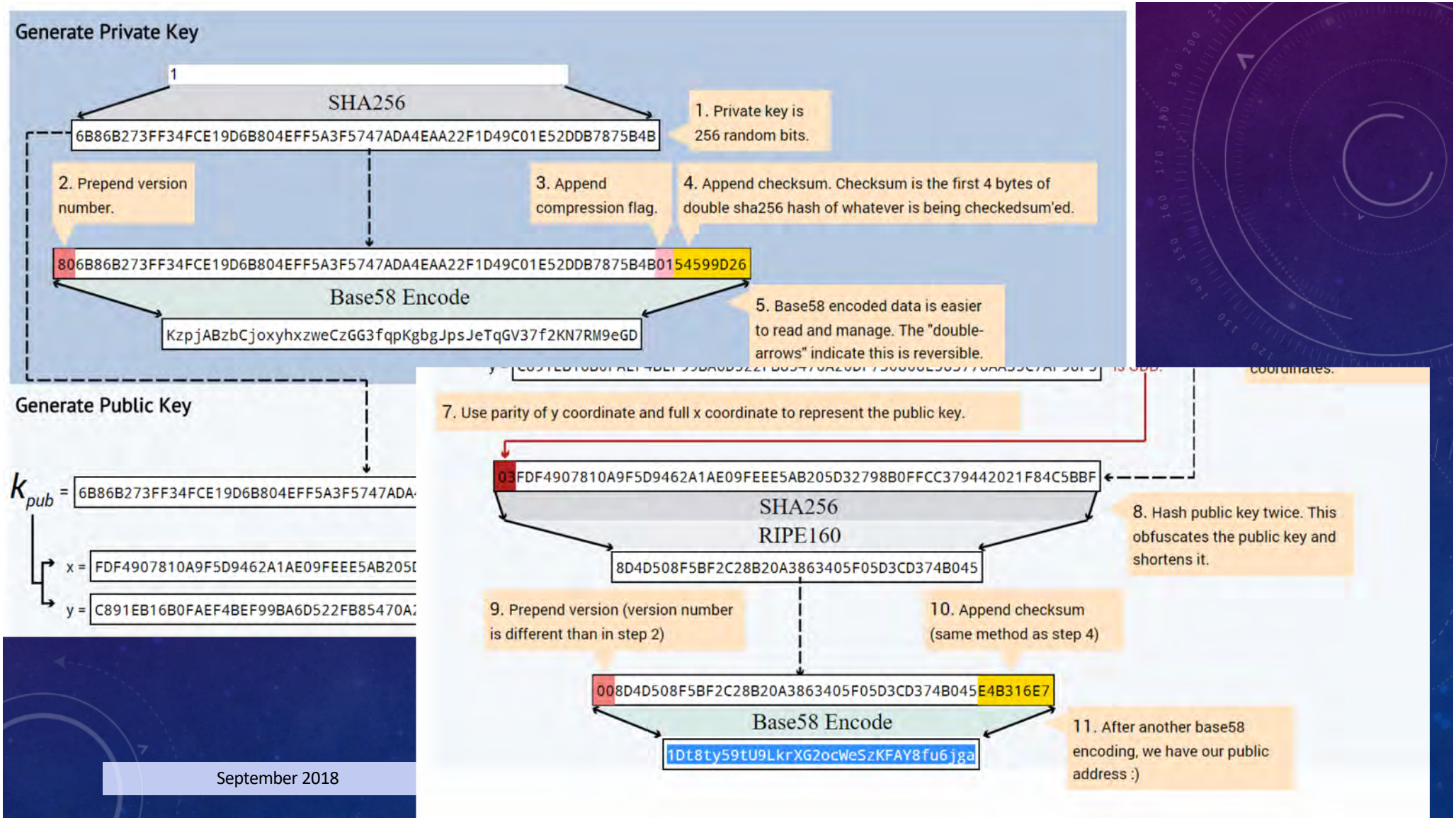
Public Address (a number derived from the public key)

While it is “simple” to move from private key to public key and public addresses (“deterministic”), it is very difficult to go the other way. If someone has your private key, they have access to all related resources.

All **public addresses** are public and viewable on a specific public chain or ledger. They are not associated directly with the owner. Still, it is recommended to only use a public address once.

Public keys can be made public, so third parties can know a specific owner has signed a transaction.

Private keys are used to sign transactions sending cryptocurrency to others. The key should be tightly controlled (be very careful what applications you enter them into). The public key can verify that the private key was used to sign the transaction due to the tight coupling of the two.


Generate Private Key
1
SHA256
6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
1. Private key is 256 random bits.
2. Prepend version number.
3. Append compression flag.
4. Append checksum. Checksum is the first 4 bytes of double sha256 hash of whatever is being checkedsum'ed.
806B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B0154599D26
Base58 Encode
KzpjABzbCjoxyhxzweCzGG3fqpKgbgJpsJeTqGV37f2KN7RM9eGD
5. Base58 encoded data is easier to read and manage. The "double-arrows" indicate this is reversible.
Generate Public Key
k_{pub} = 6B86B273FF34FCE19D6B804EFF5A3F5747ADA
x = FDF4907810A9F5D9462A1AE09FEEE5AB205
y = C891EB16B0FAEF4BEF99BA6D522FB85470A
7. Use parity of y coordinate and full x coordinate to represent the public key.
03FDF4907810A9F5D9462A1AE09FEEE5AB205D32798B0FFCC379442021F84C5BBF
SHA256
RIPE160
8D4D508F5BF2C28B20A3863405F05D3CD374B045
8. Hash public key twice. This obfuscates the public key and shortens it.
9. Prepend version (version number is different than in step 2)
10. Append checksum (same method as step 4)
008D4D508F5BF2C28B20A3863405F05D3CD374B045E4B316E7
Base58 Encode
1Dt8ty59tU9LkrXG2ocWeSzKFAY8fu6jga
11. After another base58 encoding, we have our public address :)
September 2018

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1Dt8ty59tU9LkrXG2ocWeSzKFAY8fu6jga
Hash 160	8d4d508f5bf2c28b20a3863405f05d3cd374b045

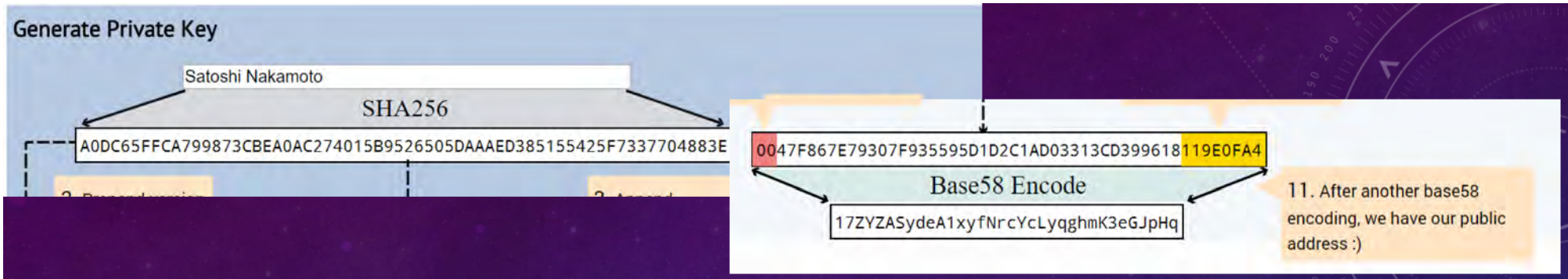
Transactions	
No. Transactions	4
Total Received	0.00316 BTC
Final Balance	0 BTC

Request Payment Donation Button

Transactions (Oldest First)

Filter

150d614ad0a0d70a5e6274fc318e92ad8a2b8ed61f6d1b17316bb8cfa07ee726			2017-10-26 08:24:41
1Dt8ty59tU9LkrXG2ocWeSzKFAY8fu6jga	→	1LcYgQajhpyDd1hm4xAVqreEJ7BE8A6xXd	0.00009661 BTC



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	17ZYZASydeA1xyfNrcYcLyqghmK3eGJpHq
Hash 160	47f867e79307f935595d1d2c1ad03313cd399618

Transactions	
No. Transactions	2
Total Received	0.000254 BTC
Final Balance	0 BTC

Request Payment Donation Button

Transactions (Oldest First)

Filter

eac5f7cba9734250f8477b04087f263c44a59a3f5fde524244d5f9e6828c3047 2014-09-12 20:58:38

A **cryptographic hash** (sometimes called 'digest') is a kind of 'signature' for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. See below for the source code.

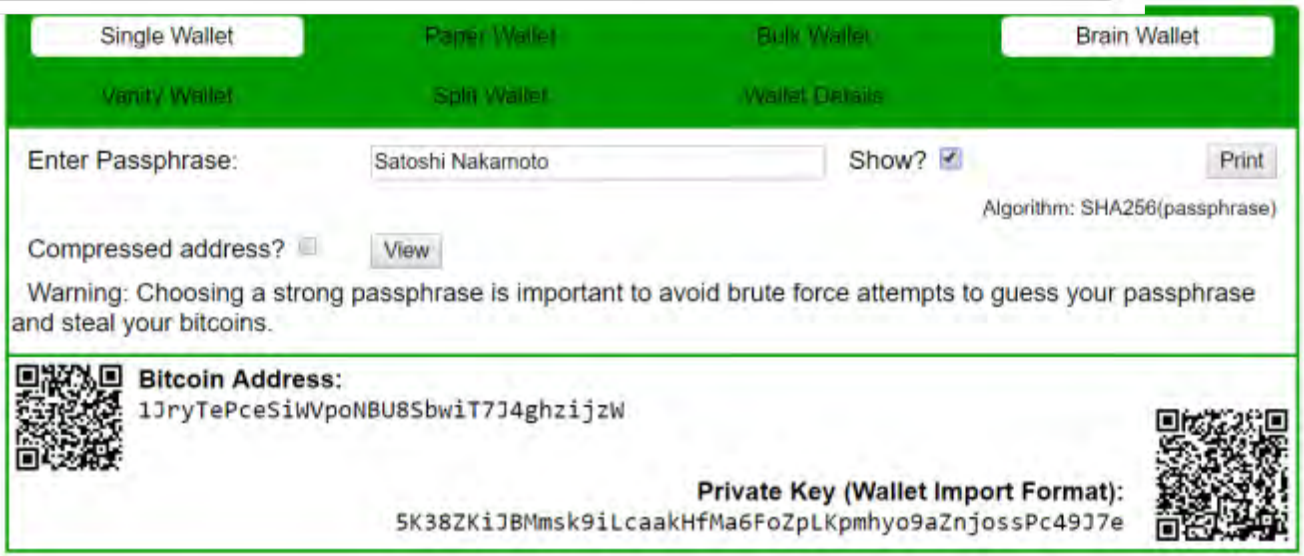
Enter any message to check its SHA-256 hash

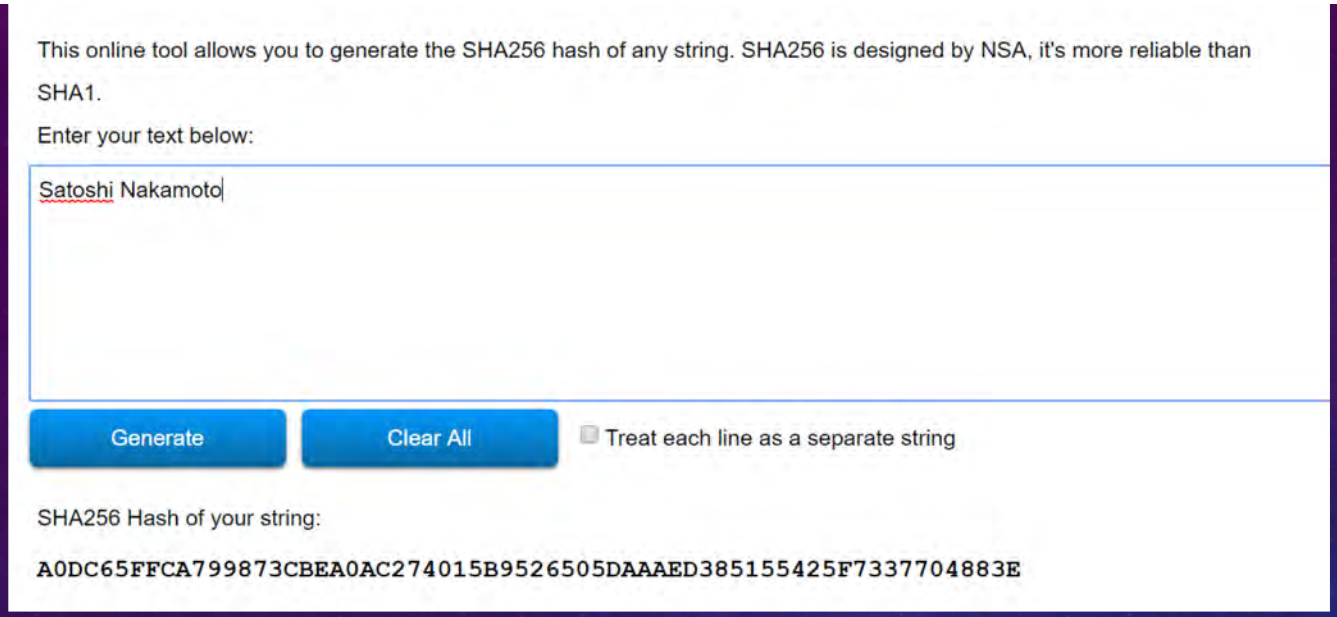
Message Satoshi Nakamoto

Hash a0dc65ffca799873cbea0ac274015b9526505daaaed385155425f7337704883e 0.900ms

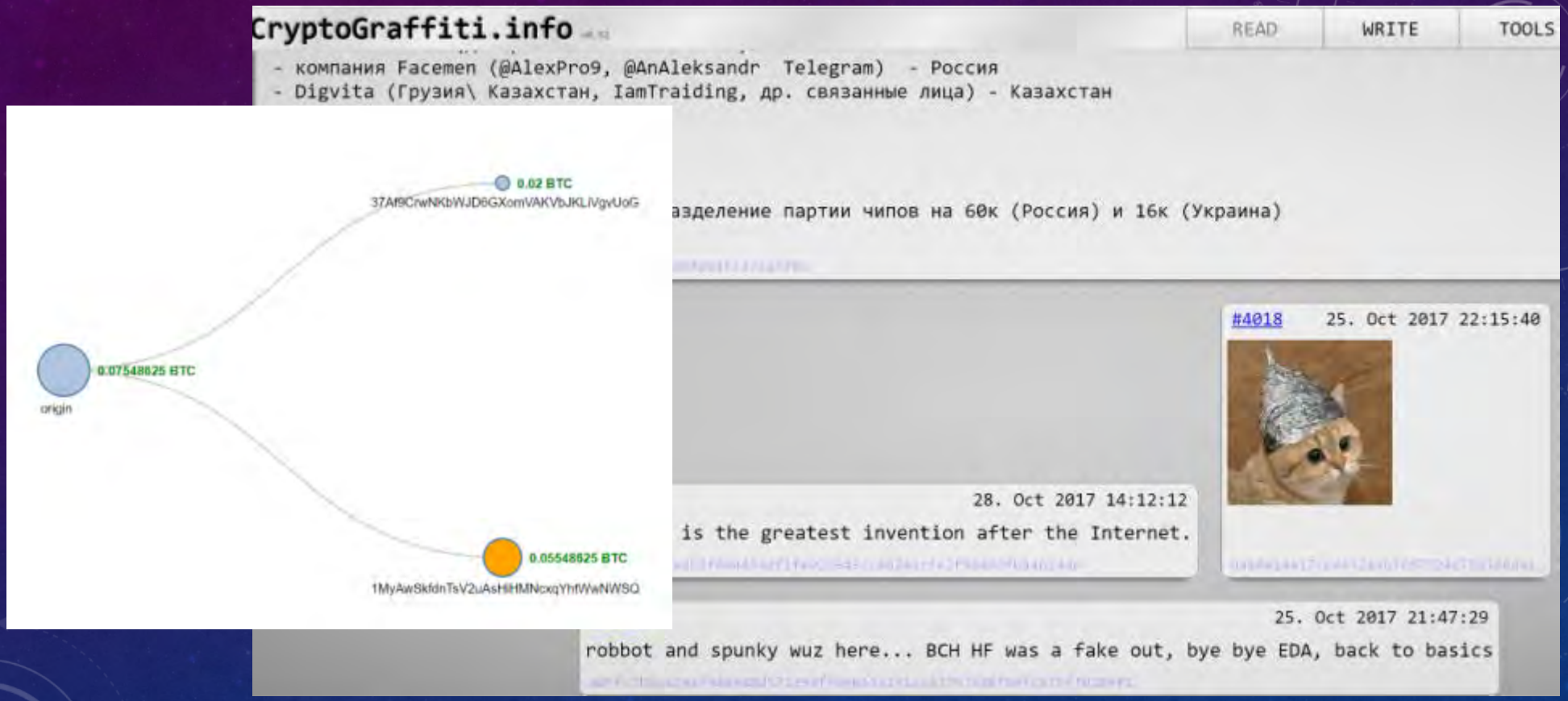
Note SHA-256 hash of 'abc' should be: ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

https://www.movable-type.co.uk/scripts/sha256.html





https://passwordsgenerator.net/sha256-hash-generator/


CryptoGraffiti.info
READ
WRITE
TOOLS
- компания Facemen (@AlexPro9, @AnAleksandr Telegram) - Россия
- Digvita (Грузия\ Казахстан, IamTraiding, др. связанные лица) - Казахстан
0.02 BTC
37Af9CrwNKbWJD6GXomVAKVbJKLiVgvUoG
азделение партии чипов на 60к (Россия) и 16к (Украина)
0.07548625 BTC
origin
0.05548625 BTC
1MyAwSkfdnTsV2uAsHiHtMNcxqYhfWwNWSQ
#4018
25. Oct 2017 22:15:40
28. Oct 2017 14:12:12
is the greatest invention after the Internet.
25. Oct 2017 21:47:29
robbot and spunky wuz here... BCH HF was a fake out, bye bye EDA, back to basics

ISO 3166, 4217, 8601 etc.

WHAT IS ISO/TC 307?

- ISO Technical Committee (many projects underway)
  - Proposal from Australia: ISO/TS/P 258 April 2016
    - *Standardisation of blockchains and distributed ledger technologies to support interoperability and data interchange among users, applications and systems.*
    - ***Very broad in scope**; maturity and readiness for standards questioned*
  - ISO/TC 307 established September 2016
    - https://www.iso.org/committee/6266604.html
  - Mirror committees began to prepare
  - First meeting in Sydney, April 2017
  - Second meeting in Tokyo, November 2017
  - Third meeting in London, May 2018
  - Next meeting – Moscow in October

WHAT WILL IT DO?

- Answer 1: TBD
- Answer 2: Whatever the participants agree it should do, under the rules defined by ISO
- Answer 3: Terms agreed in London last month, to be made more generally public
- *Technical committees are established by the ISO/**T**echnical **M**anagement **B**oard (TMB) on a provisional basis. Within 18 months, provisionally established technical committees are required to prepare a **strategic business plan** for review by the ISO/TMB . The committees are formally established by the ISO/TMB at the time of acceptance of the business plan. This does not preclude the initiation of standardization projects during this 18 month period.*

WHO IS INVOLVED?

Australia (SA)
Austria (ASI)
Brazil (ABNT)
Belgium (NBN)
Brazil (ABNT)
Canada (SCC)
China (SAC)
Croatia (HZN)
Cyprus (CYS)
Denmark (DS)
Finland (SFS)
France (AFNOR)
Germany (DIN)
Hungary (MSZT)
India (BIS)
Ireland (NSAI)
Italy (UNI)
Jamaica (BSJ)
Japan (JISC)
Kazakhstan (KAZMEMST)
Korea, Republic of (KATS)
Luxembourg (ILNAS)
Malaysia (DSM)
Netherlands (NEN)
New Zealand (NZSO)
Portugal (IPQ)
Russian Federation (GOST R)
Singapore (ESG)
Spain (UNE)
Sweden (SIS)
Switzerland (SNV)
Ukraine (DSTIJ)
United Arab Emirates (ESMA)
United Kingdom (BSI)
United States (ANSI)

Ever expanding list of "P" countries provide experts, actively participate, vote

LIAISONS

- Many ISO groups
- SWIFT
- EC
- UNECE
- ITU
- FIG (Surveyors)
- And others …

ISO/TC 307 BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES

Scope: Standardisation of blockchain technologies and distributed ledger technologies

Study Group	Related Working Group
1. Reference Architecture, Taxonomy and Ontology	1. Foundations
2. Use cases	(continues as SG)
3. Security and Privacy	2. Security, Privacy and Identity
4. Identity	(combined with WG 2, above)
5. Smart Contracts	3. Smart Contracts and their applications
	JWG 4 IT Security
6. Governance of B&DLT Systems	(newer SG)
7. Interoperability of B&DLT Systems	(newer SG)

https://www.iso.org/committee/6266604.html

TIMELINE TO DATE

April 2017	November 2017	May 2018
• Sydney, Australia • Establishment of SG 1 - 5	• Tokyo, Japan • Establishment of first WGs and SG 6 - 7	• London, UK • Establishment of new projects and joint WGs

STANDARDS/PROJECTS UNDER DEVELOPMENT

- Reference architecture
- Taxonomy and Ontology
- Terminology and concepts
- **Discovery**
- Security risks and vulnerabilities
- Overview of privacy and personally identifiable information (PII) protection
- Overview of identity
- **Security of digital asset custodians**
- Legally binding smart contracts
- Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems

FOCUS ON HOW BLOCKCHAIN/DLT IS UNIQUE

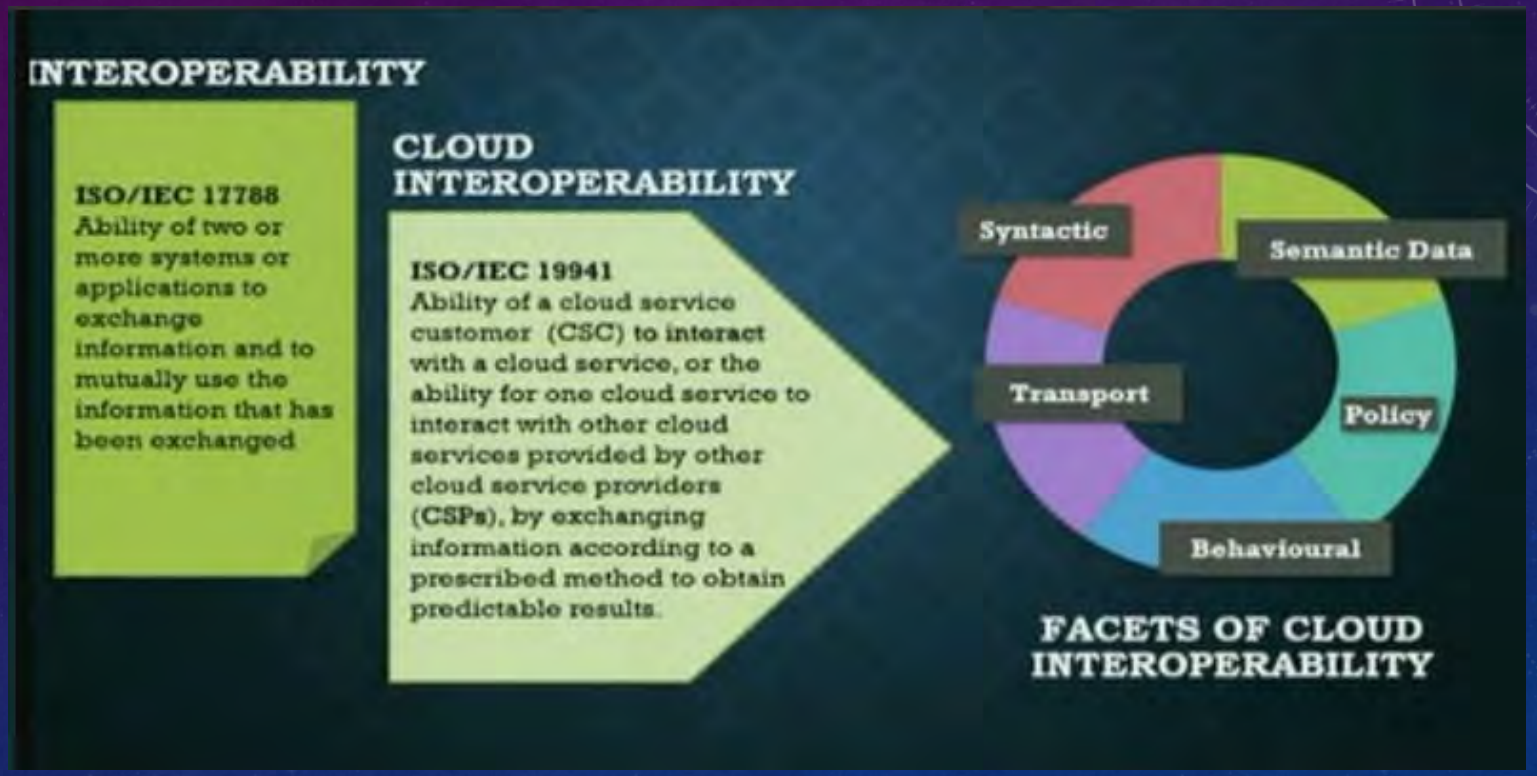
- How different from Cloud Computing, IoT?
  - Cryptoassets/stores of “value”
  - Decentralization and consensus mechanisms
  - Immutability by design
  - Smart Contracts
  - Unique fingerprint of the layers of the Reference Architecture

SG 7: INTEROPERABILITY

- Looking to prior work and finding what is unique for B/DLT
  - CORBA (1995)
  - EDI (1960s) and XML (1990s)
  - Web Services (2004)
  - ISO recent effort
    - Cloud Services Interoperability (ISO/IEC 19941 2017)
    - Internet of Things Interoperability (ISO/IEC AWI 21823-1 2018)

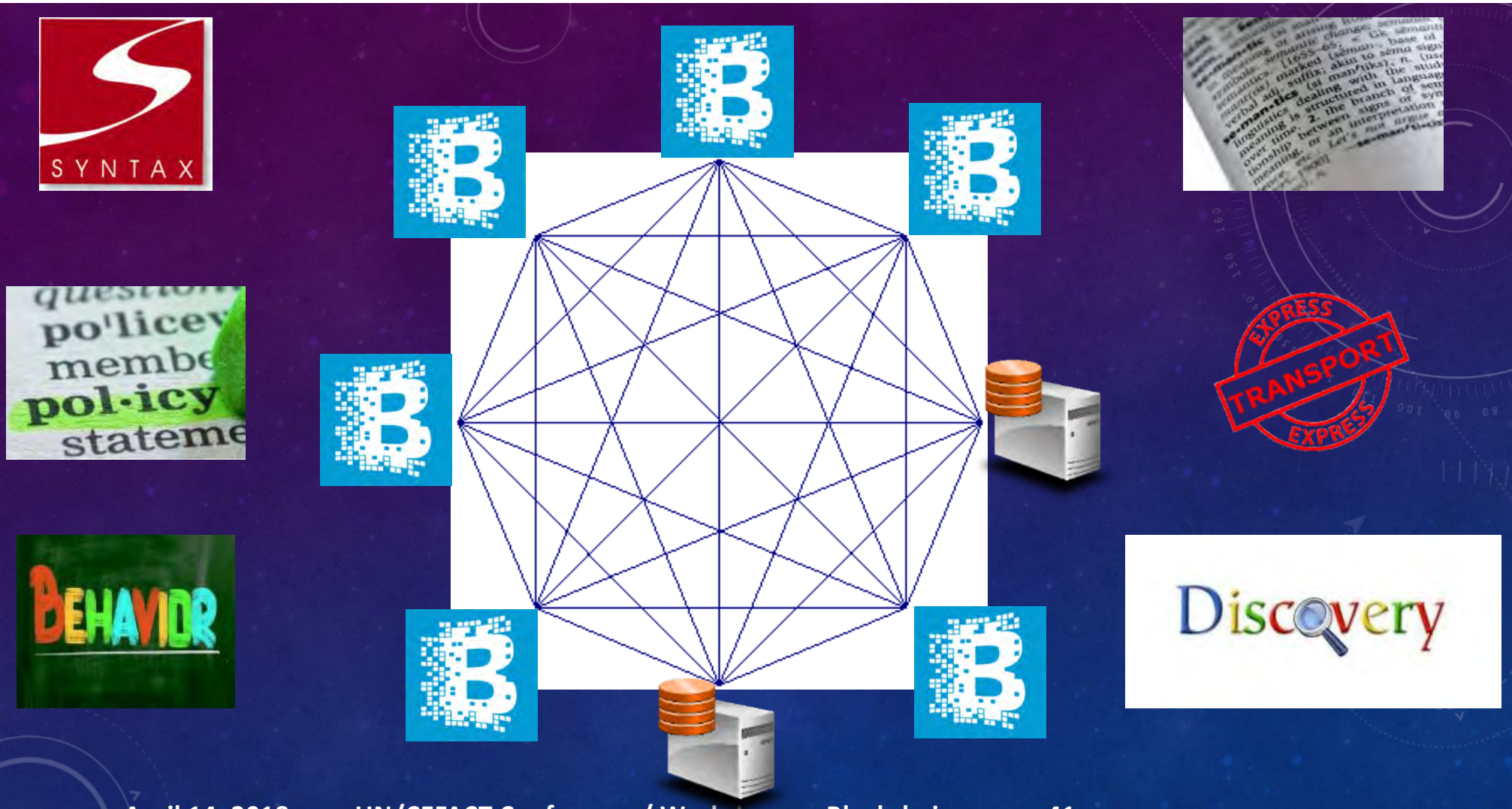
PRIOR ISO WORK: “5 FACETS” MODEL FROM ISO/IEC 19941

Source: NIST tweet: https://twitter.com/usnistgov/status/776122926353362944



SG 7 PROCESS

- Application of “five facets” to/from/between layers of B/DLT
  - Syntax: Format of information
  - Semantics: Meaning of information
  - Behavior: Informational rules behind information and services
  - Policy, Trust, Organization: Legal and organizational rules behind information and services
  - Transport: Method of moving information
- Also considered
  - Discovery: Publishing/responding to inquiries and finding sources for information and services
- And Cryptoassets and interoperability


SYNTAX
police
member
policy
statement
BEHAVIOR
EXPRESS
TRANSPORT
EXPRESS
Discovery

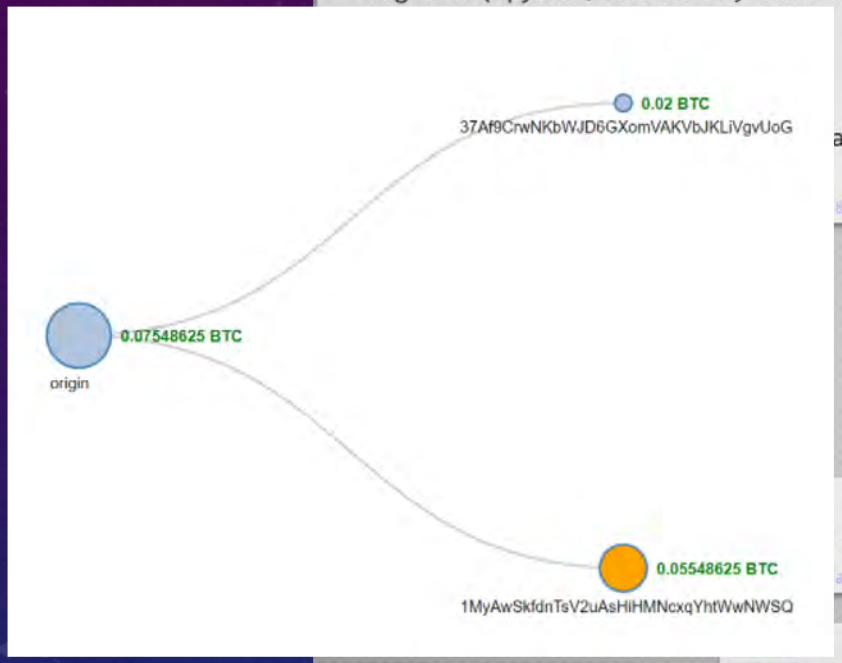
SG 7 PROCESS SINCE NOVEMBER (CONT.)

- Since London, now underway
  - Cryptoassets: Coins, tokens, et al.
- Recommendations made for consideration in London on
  - Which topics should become new projects (TR, TS, IS)
  - Which should be picked up under the work of existing WGs
  - Ongoing work of SG 7
  - Which should be left to the market to develop

ACCOUNTING AND AUDIT

An Internet-facilitated single, global, immutable, public, cryptographically-supported standardized audit trail supporting continuous audit, leveraging digital signatures and hashes

I'VE BEEN DISCUSSING THIS FOR > 15 YEARS



CryptoGraffiti.info

READ | WRITE | TOOLS

- компания Facemen (@AlexPro9, @AnAleksandr Telegram) - Россия
- Digvita (Грузия\ Казахстан, IamTraiding, др. связанные лица) - Казахстан

азделение партии чипов на 60к (Россия) и 16к (Украина)

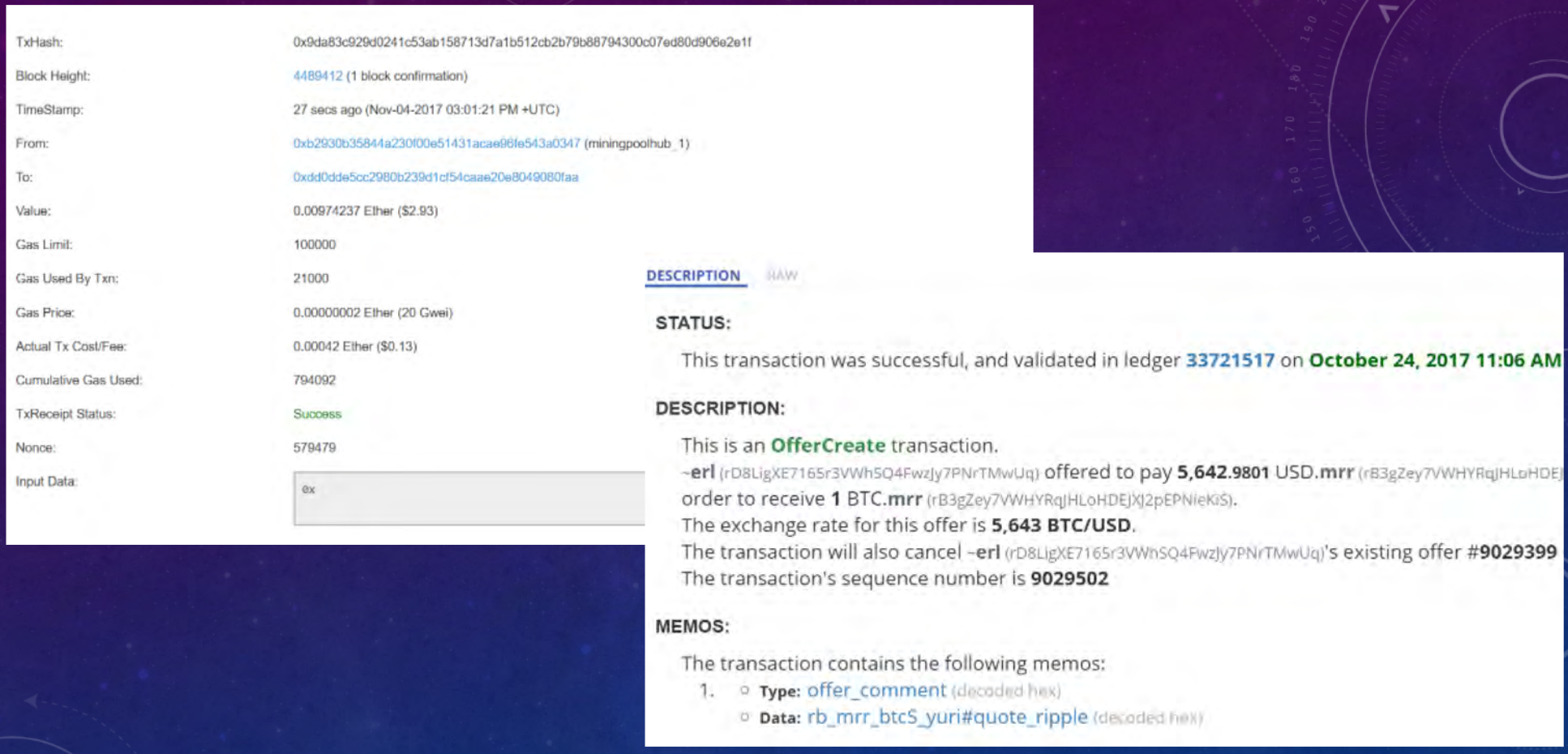
#4018 25. Oct 2017 22:15:40

28. Oct 2017 14:12:12

is the greatest invention after the Internet.

25. Oct 2017 21:47:29

robbot and spunky wuz here... BCH HF was a fake out, bye bye EDA, back to basics


TxHash:
0x9da83c929d0241c53ab158713d7a1b512cb2b79b88794300c07ed80d906e2e1f
Block Height:
4489412 (1 block confirmation)
TimeStamp:
27 secs ago (Nov-04-2017 03:01:21 PM +UTC)
From:
0xb2930b35844a230f00e51431acae96fe543a0347 (miningpoolhub_1)
To:
0xdd0dde5cc2980b239d1cf54caae20e8049080faa
Value:
0.00974237 Ether ($2.93)
Gas Limit:
100000
Gas Used By Txn:
21000
Gas Price:
0.00000002 Ether (20 Gwei)
Actual Tx Cost/Fee:
0.00042 Ether ($0.13)
Cumulative Gas Used:
794092
TxReceipt Status:
Success
Nonce:
579479
Input Data:
0x
DESCRIPTION
RAW
STATUS:
This transaction was successful, and validated in ledger 33721517 on October 24, 2017 11:06 AM
DESCRIPTION:
This is an OfferCreate transaction.
~erl (rD8LigXE7165r3VWhSQ4FwzJy7PNrTMwUq) offered to pay 5,642.9801 USD.mrr (rB3gZey7VWHYRqJHLoHDEJ
order to receive 1 BTC.mrr (rB3gZey7VWHYRqJHLoHDEJXJ2pEPNieKiS).
The exchange rate for this offer is 5,643 BTC/USD.
The transaction will also cancel ~erl (rD8LigXE7165r3VWhSQ4FwzJy7PNrTMwUq)'s existing offer #9029399
The transaction's sequence number is 9029502
MEMOS:
The transaction contains the following memos:
1. Type: offer_comment (decoded hex)
Data: rb_mrr_btcS_yuri#quote_ripple (decoded hex)

“BLOCKCHAIN MAKES AUDITORS OBSOLETE; IT IS SELF-AUDITING”

Valuation
Existence
a**L**location
Occurrence
Completeness
class**I**fication
unde**R**standability
Accuracy
Presentation
cu**T**off
Obligations
Rights

PROVIDE THE DETAIL – THE SUMMARY CAN BE A SIMPLE BY-PRODUCT (50 YEAR OLD IDEA)

To aggregate, or not to aggregate … that is the question:
Whether 'tis more transparent in the mind to provide "Events" of underlying detail for stockholders to make outrageous Fortunes
Or to summarize a Sea of Troubles
And by the "Value" report them.

An "Events" Approach to Basic Accounting Theory

George H. Sorter

In 1966, after two years work, a committee of the American Accounting Association issued *A Statement of Basic Accounting Theory*.[1] Undoubtedly, the most startling recommendations were the sanctioning of current costs and the advocacy of two columns (historical and current) reports. To this member of the committee, however, even more startling was that the near unanimous agreement on the recommendations was arrived at by following two very divergent paths originating from two very dissimilar basic concepts about accounting. This split is not confined to committee members but rather seems representative of a more widespread and pervasive difference in the world outside. The majority view of the committee and the predominant faction outside believes in what I here define as the "value" approach to accounting. The minority view, of which I am sometimes the only member, I describe as the "events" approach. This view although implied by some in the past has never to my knowledge been explicitly stated but might have far-reaching implications. This paper seeks to describe and contrast the two schools, present arguments for and illustrate the consequences of an "events" approach to accounting theory; and examine the logic leading to the conclusions embodied in the *Statement of Basic Accounting Theory*. Hopefully, this will provide not only insights and help for the analysis and evaluation of the committee's monograph but perhaps also stimulate discussion and criticism of a new approach and suggest new avenues of research and experimentation to make accounting more responsive to present day conditions.

Two Views—Value and Events

The Value Theory

The "Value" school within the committee, or as they would probably prefer to be termed the "User need" school, assumed that users' needs are known and sufficiently well specified so that accounting theory can deductively arrive at and produce optimal input values for used and useful decision models. Most of the value theorists visualize accounting's purpose as producing optimum income and capital value or values.[2] This leads to the popular tenet of proper matching of costs and

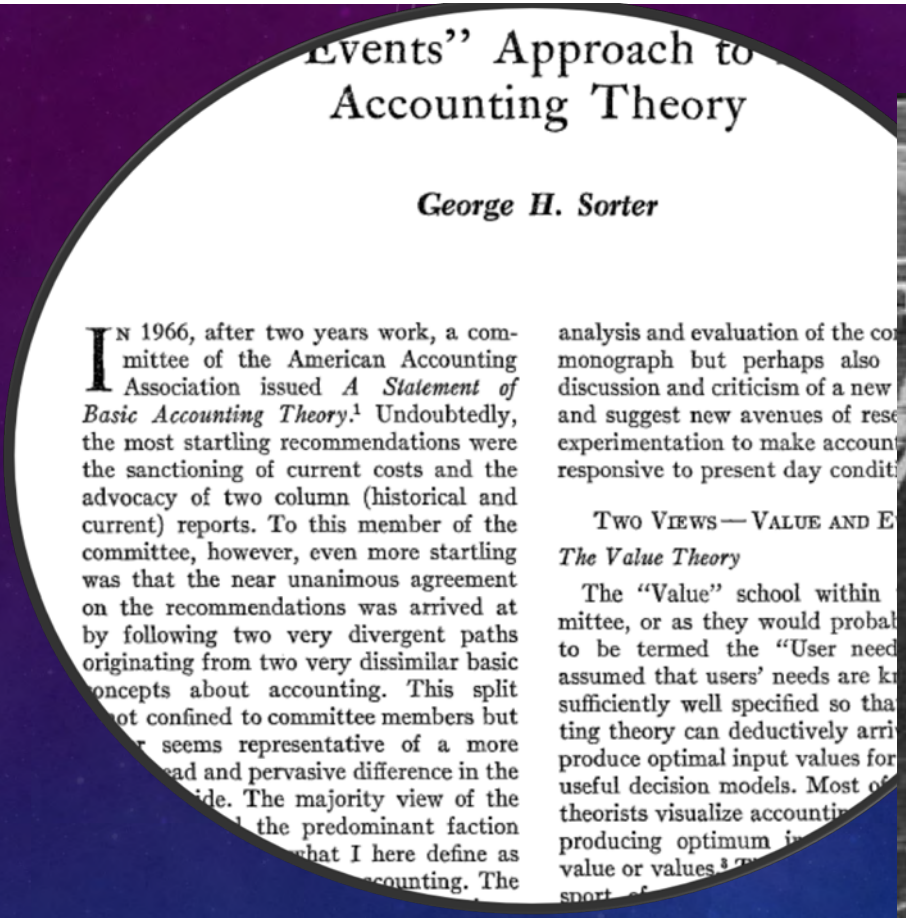
[1] American Accounting Association, *A Statement of Basic Accounting Theory*, A Report Prepared by the Committee on Basic Accounting Theory (American Accounting Association, 1966).

[2] This idea, like so many others had its origin partially in the writings and thought of Professor William J. Vatter who I hasten to absolve from any of its shortcomings.

[3] Not all value theories are 'income' oriented. Chambers for example can be considered a "value" but certainly not an "income" theorist.

George H. Sorter is Arthur Young Visiting Professor of Accounting at the University of Kansas.

The Accounting Review, January 1969



Events" Approach to
Accounting Theory

George H. Sorter

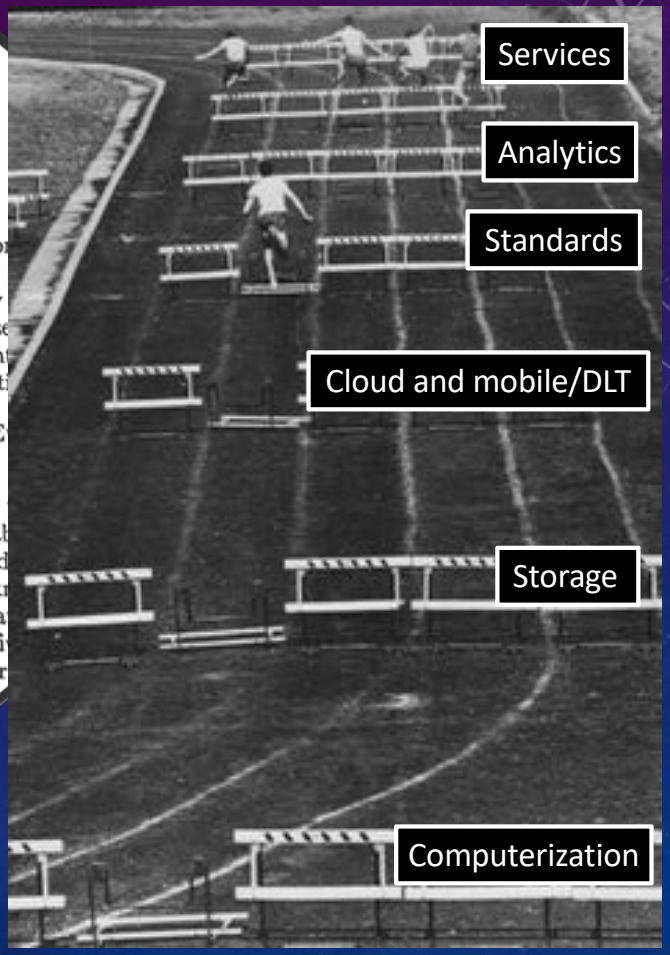
In 1966, after two years work, a committee of the American Accounting Association issued *A Statement of Basic Accounting Theory*.[1] Undoubtedly, the most startling recommendations were the sanctioning of current costs and the advocacy of two column (historical and current) reports. To this member of the committee, however, even more startling was that the near unanimous agreement on the recommendations was arrived at by following two very divergent paths originating from two very dissimilar basic concepts about accounting. This split not confined to committee members but seems representative of a more ad and pervasive difference in the ide. The majority view of the the predominant faction what I here define as counting. The

analysis and evaluation of the co
monograph but perhaps also
discussion and criticism of a new
and suggest new avenues of rese
experimentation to make accoun
responsive to present day conditi

Two Views — Value and E

The Value Theory

The "Value" school within
mittee, or as they would probab
to be termed the "User need
assumed that users' needs are k
sufficiently well specified so tha
ting theory can deductively arri
produce optimal input values for
useful decision models. Most o
theorists visualize accountin
producing optimum i
value or values.[3] T
sport of



Some hurdles to making Events Approach practicable; role of Blockchain and Events recording

POTENTIAL APPROACHES AND THINGS TO CONSIDER

- Partial or total tokenization
  - Digital, physical and intangible assets, including IP and rights
    - Tracking
    - Ownership and obligations
- Removing after-the-fact, untraceable decisions
  - Smart contracts and standard business rules
- Audit
  - Transaction authentication
  - Audit trail
  - Automated audit processes

3EA

- Cryptographic means and mechanisms
- The trade document is the transaction
- Pseudonymity
- Integrated payments

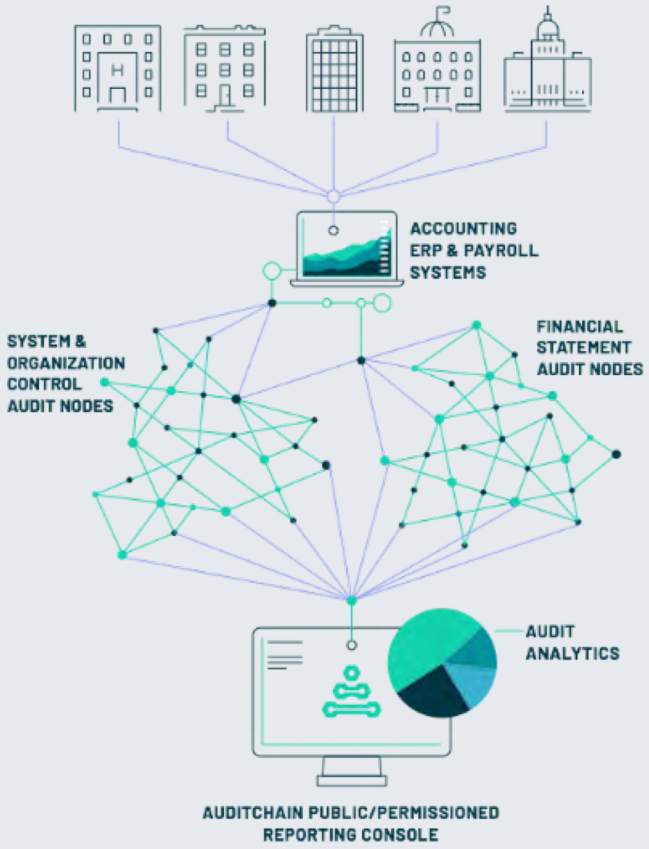
- “One source of the truth”

- Implementations - examples

Moving Accounting & Audit to B/DLT

What if there was an ecosystem that uses distributed ledger technology and an open source library of accounting smart contracts sufficient to capture, process, audit and report enterprise data and performance data on a real time continuous basis under a continuous independent audit exceeding current accounting, audit and control standards?

One with the capacity to meet and exceed the reliability of existing reporting and audit standards but laying down a foundation for the potential token economy?


ACCOUNTING
ERP & PAYROLL
SYSTEMS
SYSTEM &
ORGANIZATION
CONTROL
AUDIT NODES
FINANCIAL
STATEMENT
AUDIT NODES
AUDIT
ANALYTICS
AUDITCHAIN PUBLIC/PERMISSIONED
REPORTING CONSOLE

INPUTS AND OUTPUTS OF AUDIT

The objective of the auditor is to **plan** and **perform** the audit to obtain appropriate **audit evidence** that is sufficient to support the **opinion** expressed in the auditor's report.[1]

IAASB

INTERNATIONAL STANDARD ON AUDITING 500
AUDIT EVIDENCE

(Effective for audits of financial statements for periods beginning on or after December 15, 2009)

PCAOB

AS 1105: Audit Evidence

Effective Date: For audits of fiscal years beginning on or after Dec. 15, 2010
Final Rule: PCAOB Release No. 2010-004
Guidance on AS 1105: Staff Audit Practice Alerts No. 8 and No. 12

AICPA

AU-C Section 500

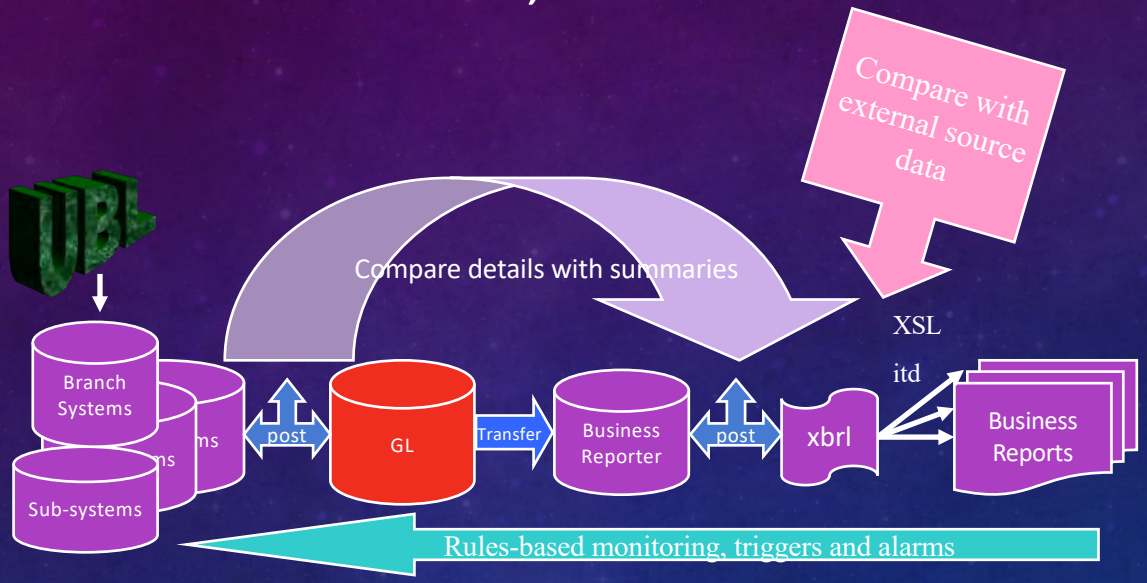
Audit Evidence

Source: SAS No. 122; SAS No. 128.

See section 9500 for interpretations of this section.

Effective for audits of financial statements for periods ending on or after December 15, 2012.

CREATE AN ELECTRONIC STANDARDIZED AUDIT TRAIL – "BLACK BOX AUDIT TRAIL" EEC, 2001-2003



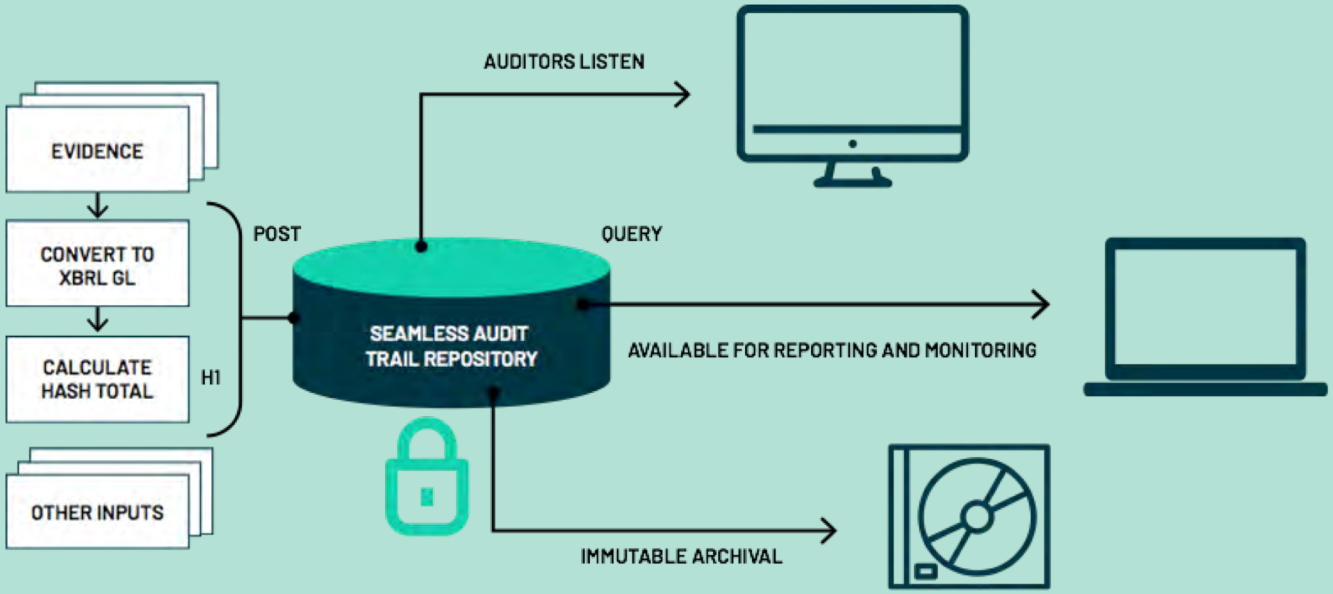
XML-based source documents can be stored in databases and retrieved and reported upon as needed.

XML-based universal audit trail can represent transactions AND processes; archive and query anytime.

XML-based universal audit trail provides drill-down detail from standardized business reports.

XML data can be from a file, a data stream, or a web service.

ERIC'S BLACKBOX AUDIT TRAIL FROM 15 YEARS AGO



WCARS 2005

Smart Contract Platform

- Commitments and contingencies
- Board Resolutions
- Audit Committee Resolutions
- Employment Agreements
- Equity Issuance Agreements
- Debt Issuance
- Equity Based Compensation
- Equipment Purchase
- Purchase Orders

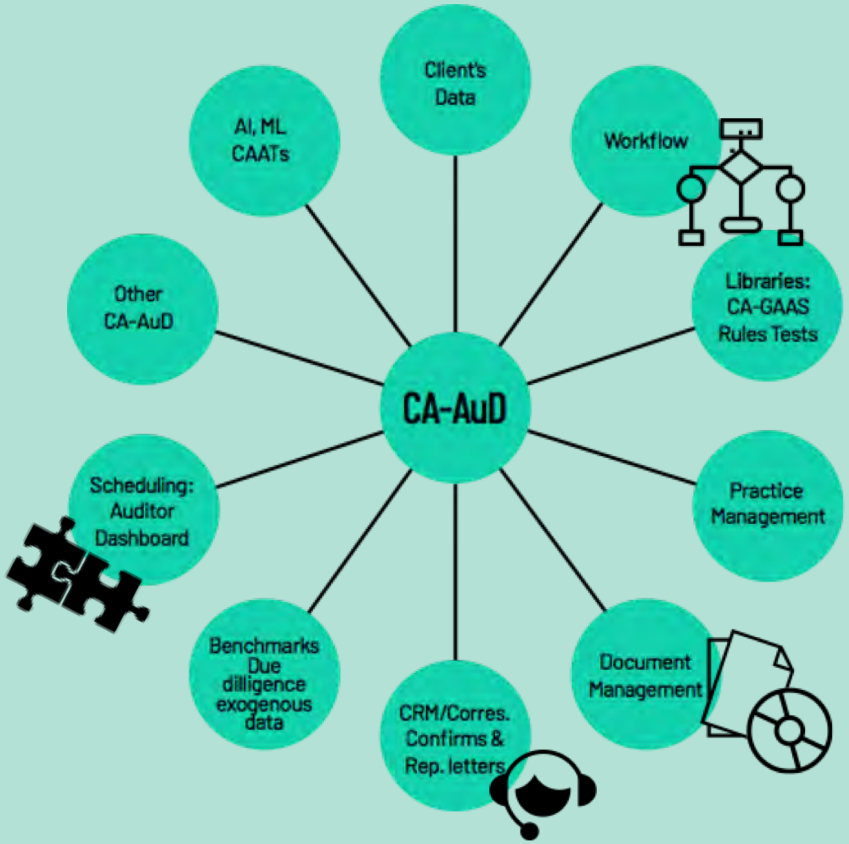
ROLE OF AI AND MACHINE LEARNING

- Supporting automated analytics
- Bridging the gap from periodic to real-time
- Learning and adapting
- Reducing delays from need for manual effort
- Example: Steps related to the work of management's expert

EXAMPLE: ROLE OF AI/ML AND MANAGEMENT'S EXPERT

- Information regarding the competence, capabilities and objectivity of a management's expert may come from a variety of sources, such as:
  - **Personal experience** with previous work of that expert.
  - **Discussions** with that expert.
  - **Discussions** with others who are familiar with that expert's work.
  - Knowledge of that expert's **qualifications**, membership of a professional body or industry association, license to practice, or other forms of external recognition.
  - **Published papers** or books written by that expert.
  - An **auditor's expert**, if any, who assists the auditor in obtaining sufficient appropriate audit evidence with respect to information produced by the management's expert.

FULLY INTEGRATED CONTINUOUS PROCESS



WCARS 2005

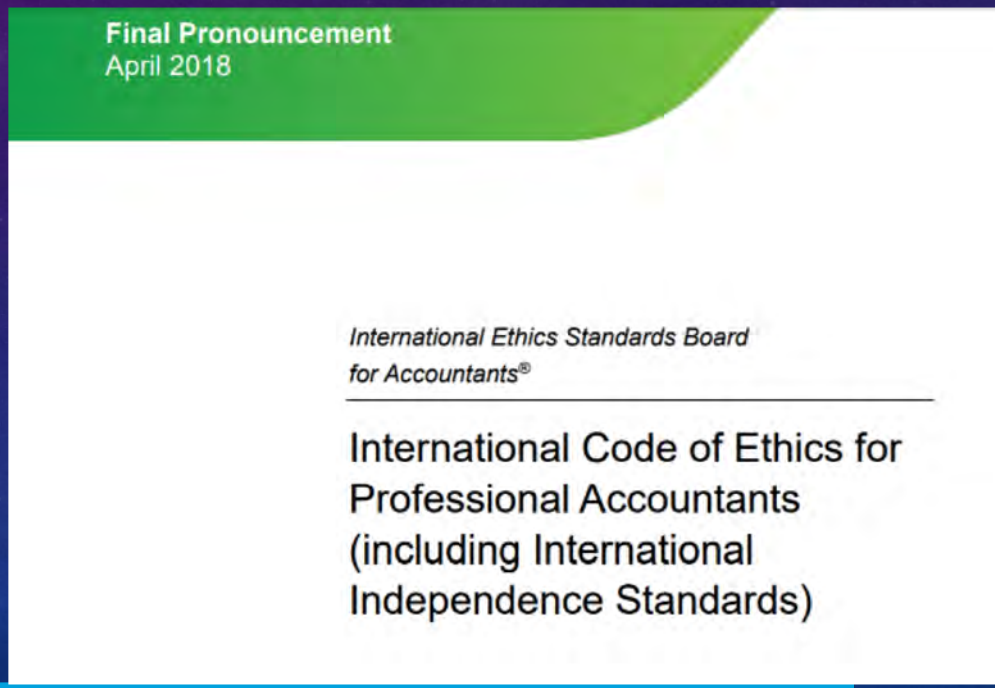
ACCOUNTING AND AUDIT SERVICES, CONSORTIUMS

- Best known “accounting” efforts
  - Balanc3 from Consensys
  - LIBRA
  - Auditchain
  - Many 3EA wannabes
- Accounting oriented consortiums
  - Accounting Blockchain Coalition
    - https://accountingblockchain.net
  - DCARPE Alliance
    - DCARPE.org

ETHICS AND AI

- Training
- Education
- Supervision
- Judgement
  - Artificial intelligence, intuition, gut feel
- Who signs the auditor's report?

https://www.ifac.org/system/files/publications/files/Final-Pronouncement-The-Restructured-Code_0.pdf



AUDIT PROCEDURES AND PHASES

Risk assessment procedure, Test of controls, Substantive procedures

Procedures to obtain audit evidence (ISA 500 .A2, AS 1105 .15-.21, AU-C 500 .A14 - .A26)	**Blockchain/DLT How do you store it**	**XBRL How do you represent it? (Data and Asserted Rules)**	**AI/Machine Learning How do you perform it?**	**IohT How do you enter, monitor, act on its?**
Inspection (documentation, including vouching, tracing, scanning?)				
Observation (processes or procedures)				
(External) Confirmation				
Recalculation				
Reperformance				
Analytical procedures, including scanning (AICPA)				
Inquiry				

WORKING ON THESE AREAS:

What's practical – today

What's practical – tomorrow

What's necessary or no longer necessary tomorrow (e.g., token economy)

INTERNET OF THINGS AND ACCOUNTING

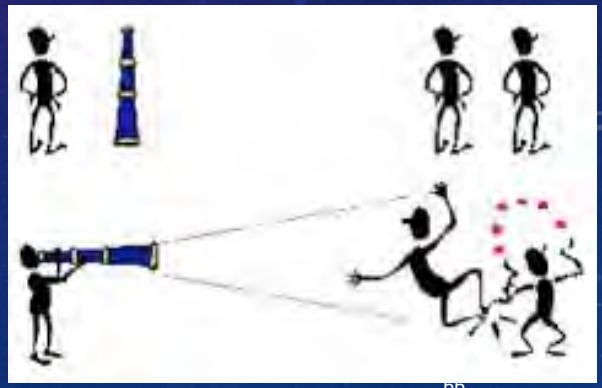
- IoT is happening: *monitoring, recording, acting*
- Benefits and concerns for the business reporting supply chain
  - Automating collection of information necessary for record-keeping and decision making with potential benefit of facilitating the capture of increased amounts of information (*more detail, more often*) with reduced manual errors
  - Reducing time lapse between an event and its recording for more timely decision making
  - Facilitating assessment of process-driven activities
  - Good news/bad news: more data, more action, more observation, reduction of immediate direct human impact

EMERGING TECHNOLOGIES IMPACT ON THE ACCOUNTING PROFESSION

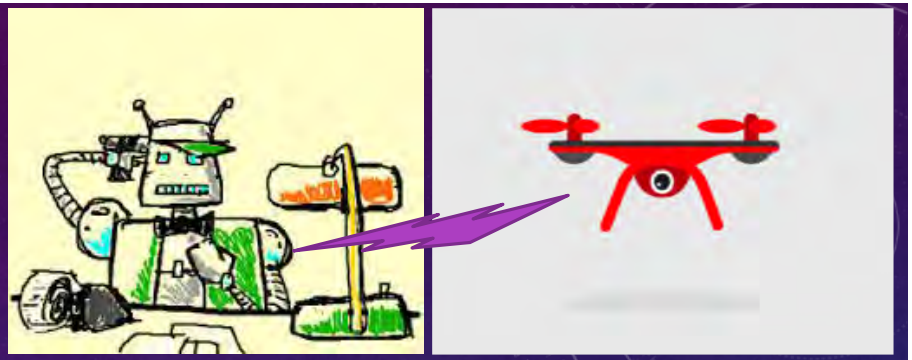
- Accounting and audit profession's history of embracing technology
  - History of my inspiration: NYS CPE circa 1990
  - From Lotus 1-2-3 to PCAOB AI 20.16-.18 (early adopter or white-flag)
  - IFRS updating its principles of disclosure … role of digital reporting?
    - "The [IASB] decided that the staff should perform further analysis about whether and how to consider the effect of technology and digital reporting within the scope of the Principles of Disclosure project for discussion at a future Board meeting."

IOT IN AUDITING; AUDITING IOT

- Nonetheless, technology can be a facilitator
  - Facilitation of human involvement
    - Drones, virtual/augmented reality, virtual presence, wearable tech
  - Facilitation of automated processes to maximize human involvement
    - RF ID, advanced analytics, use of exogenous data, AI, Tokenization, autonomous vehicles
- IOT in auditing
- Auditing IoT



INVOLVE IOT IN AUDITING



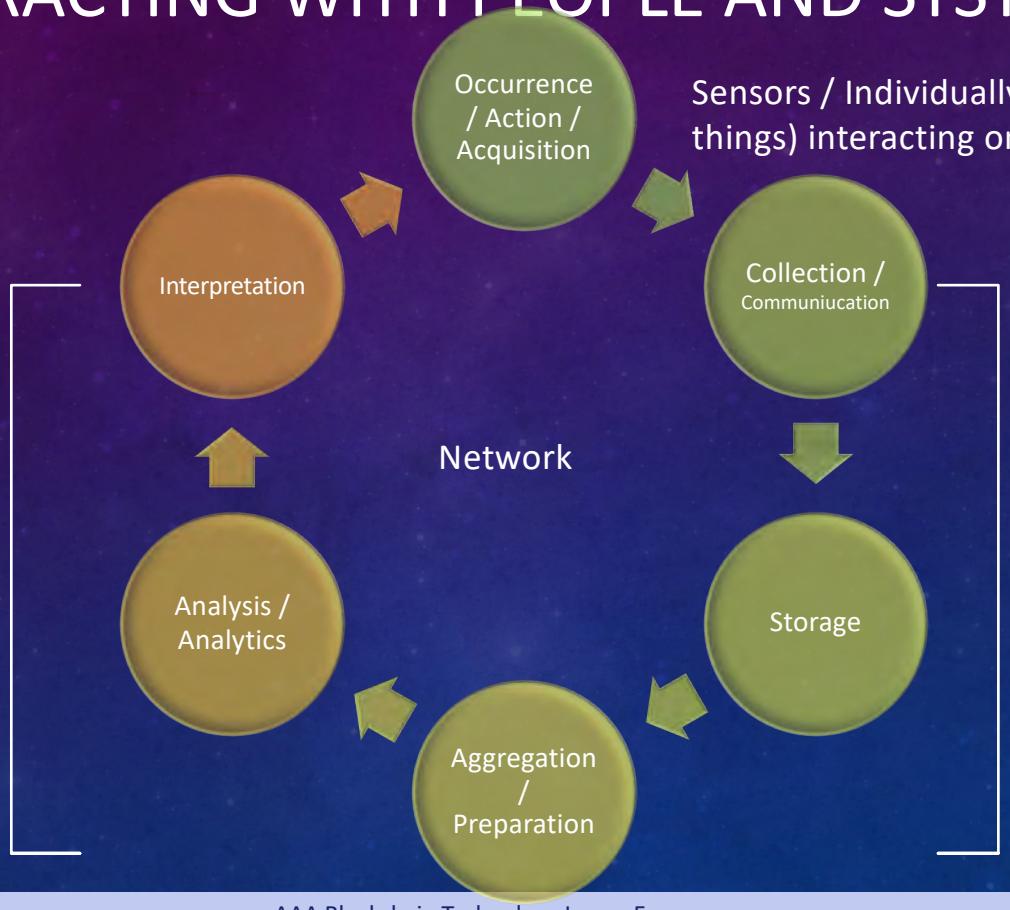
- Auditor's "physical" involvement – but not full-time involvement – is expected in practice
- The *observer effect* (Hawthorne Effect)
  - Theory that observing a process necessarily changes the process
- Insulation: benefits and concerns
  - Greater and lesser exposure at the same time (remote proctoring example)
  - Necessary for dealing with increased technology, need for speed, globalization and automation
  - Gut-feel, whistleblowers, observation of topics other than those under focus

IOT: GATHERING EVIDENCE TO SUPPORT ASSERTIONS

Valuation
Existence
a**L**location
Occurrence
Completeness
class**I**fication
unde**R**standability
Accuracy
Presentation
cu**T**off
Obligations
Rights

OBJECTS INTERACTING WITH PEOPLE AND SYSTEMS

Sensors / Individually identified objects (people and things) interacting on the Network



Standard Rules
Artificial Intelligence
Visualizations

Standards

EXAMPLE: EXPECTATION OF PHYSICAL PRESENCE

- *Attend, observe, inspect … or modify your opinion (ISA 501)*
- *Be "present"*
  - *.01 **Observation of inventories is a generally accepted auditing procedure**. The independent auditor who issues an opinion when he has not employed them must bear in mind that he has the burden of justifying the opinion expressed.*
  - *.09 When inventory quantities are determined solely by means of a physical count, and all counts are made as of the balance-sheet date or as of a single date within a reasonable time before or after the balance-sheet date, **it is ordinarily necessary for the independent auditor to be present at the time of count** and, by suitable observation, tests, and inquiries, satisfy himself respecting the effectiveness of the methods of inventory-taking and the measure of reliance which may be placed upon the client's representations about the quantities and physical condition of the inventories. (PCAOB AS 2510: Auditing Inventories)*

AS 2510 (PCAOB), AU-C Section 501.11 - .15, .A21-.A38 (AICPA); ISA 501.4-.8, .A1-.A16 (IAASB)

- *Has "present" changed in an IoT era?*

AUDIT PROCEDURES AND PHASES

Risk assessment procedure, Test of controls, Substantive procedures

Procedures to obtain audit evidence (ISA 500 .A2, AS 1105 .15-.21, AU-C 500 .A14 - .A26)	**Internet of Things Actors on the Network; sensors and "doers"**	**Blockchain/DLT How do you store it**	**Audit & Accounting Standards How do you represent it? (Data and Asserted Rules)**	**AI/Machine Learning How do you perform it?**
Inspection (documentation, including vouching, tracing, scanning?)				
Observation (processes or procedures)				
(External) Confirmation				
Recalculation				
Reperformance				
Analytical procedures, including scanning (AICPA)				
Inquiry				

WORKING ON THESE AREAS:

What's practical – today

What's practical – tomorrow

What's necessary or no longer necessary tomorrow (e.g., token economy)

Auditing the Internet of Things

- For us to audit with IoT, we need to have comfort in IoT
- For us to have comfort in client's and third party IoT, we need to have ways to assess it

AUDITING THE INTERNET OF THINGS

- Organizational oversight, policies, controls
- Assessing and remediating risks
  - Existence/completeness, tracking, monitoring the pieces in place
  - Configurations, patching (firmware, OS, apps) and maintenance
  - Security of sensors (esp. privacy); security of actors
  - Resiliency, dealing with DoS
  - Safety
  - True to purpose
- Prevention, detection, remediation

“CONFUSED” ABOUT IOT: RISK EVALUATION FRAMEWORK

CONFUSED

- **CONF – Configuration risks**
- **USED – Activity risks**

“CONFUSED”ABOUT IOT: “CONF”

- **CONF - Configuration**
  - **Configuration risks**
    - Is each thing properly (virtually, software configuration) set up, patched and maintained?
  - **Operational limitations**
    - Is each thing properly physically set up in order to achieve its purpose?
  - **iNventory mismanagement**
    - Are all of the things in the network inventoried and working together, as well as physically tracked and maintained?
  - **Flawed design**
    - Is each thing in the network initially (and kept on an ongoing basis, or replaced as necessary) inherently suitable to do the required monitoring, recording or acting task?

“CONFUSED” ABOUT IOT: “USED”

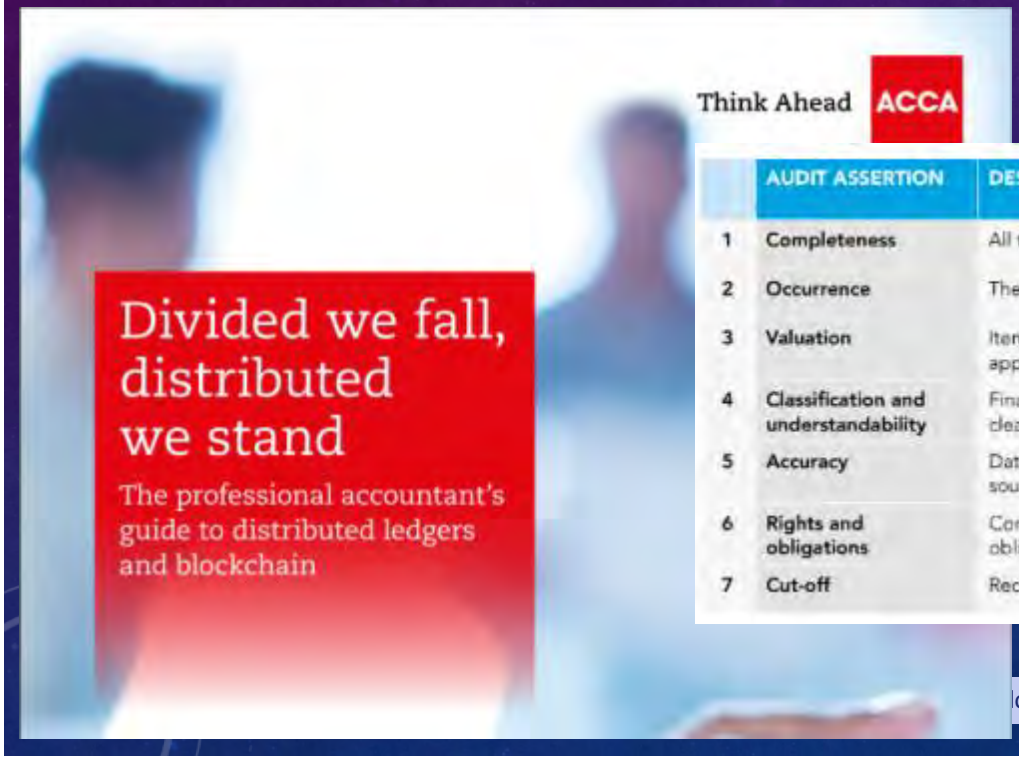
- **USED - Activities**
  - **Use limited**
    - Use limited to and kept accessible to legitimate users: authorized use isn’t blocked, redirected, time shifted or abused (once again, consider every caper film and how they get around cameras and alarm systems)
  - **Surveillance and exposure**
    - Surveillance and exposure by illegitimate users blocked, monitored and assessed
  - **Ease-of-use**
    - Easy-to-use by those who should have access; users are frustrated by trying to use the data or control the "thing".
  - **Difficult of use**
    - Difficult to use by those who shouldn’t have access

SUMMARY RESEARCH IDEAS

- Do audit procedures need to change to fully benefit from IoT in audit?
- Do ethics rules need to change to fully benefit from IoT in audit?
- Is there anything better than being CONFUSED about IoT?

RESOURCES, CALL TO ACTION AND NEXT STEPS FOR ACCOUNTANTS

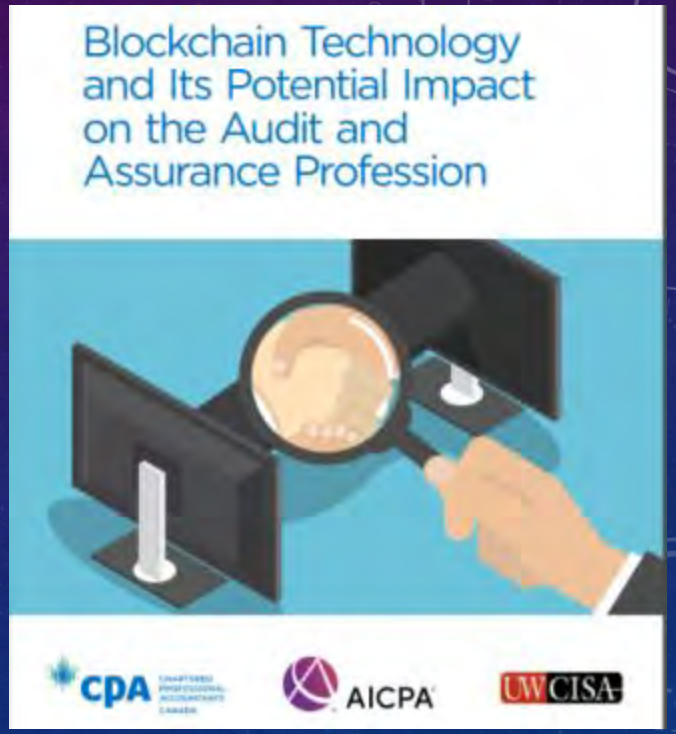
http://www.accaglobal.com/uk/en/technical-activities/technical-resources-search/2017/april/divided-we-fall-distributed-we-stand.html



	AUDIT ASSERTION	DESCRIPTION	POTENTIAL FOR DIRECT BENEFIT FROM DISTRIBUTED LEDGERS (INDICATIVE VIEW)*
1	**Completeness**	All transactions are recorded in the financial statements	√√
2	**Occurrence**	The transactions in the financial statements actually happened	√√√
3	**Valuation**	Items in the financial statements have been included at appropriate amounts	√
4	**Classification and understandability**	Financial information is correctly categorised and disclosures are clearly communicated	√
5	**Accuracy**	Data is recorded at the correct amounts, which are verifiable in source documents	√√
6	**Rights and obligations**	Correctly establishing right to use or dispose of assets as well as obligations to pay off liabilities	√
7	**Cut-off**	Recording of transactions for the correct accounting period	√√√

RESOURCES (CONT.)

https://www.icaew.com/-/media/corporate/files/technical/information-technology/technology/blockchain-and-the-future-of-accountancy.ashx



https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/blockchain-impact-on-auditing.html

RESOURCES

- Handbook of Applied Cryptography
  - http://cacr.uwaterloo.ca/hac/index.html
  - http://math.fau.edu/bkhadka/Syllabi/A%20handbook%20of%20applied%20cryptography.pdf
- Stellar TestNet environment (to work with keys and obtain “free” coins/tokens for class exercises)
  - https://portal.willet.io