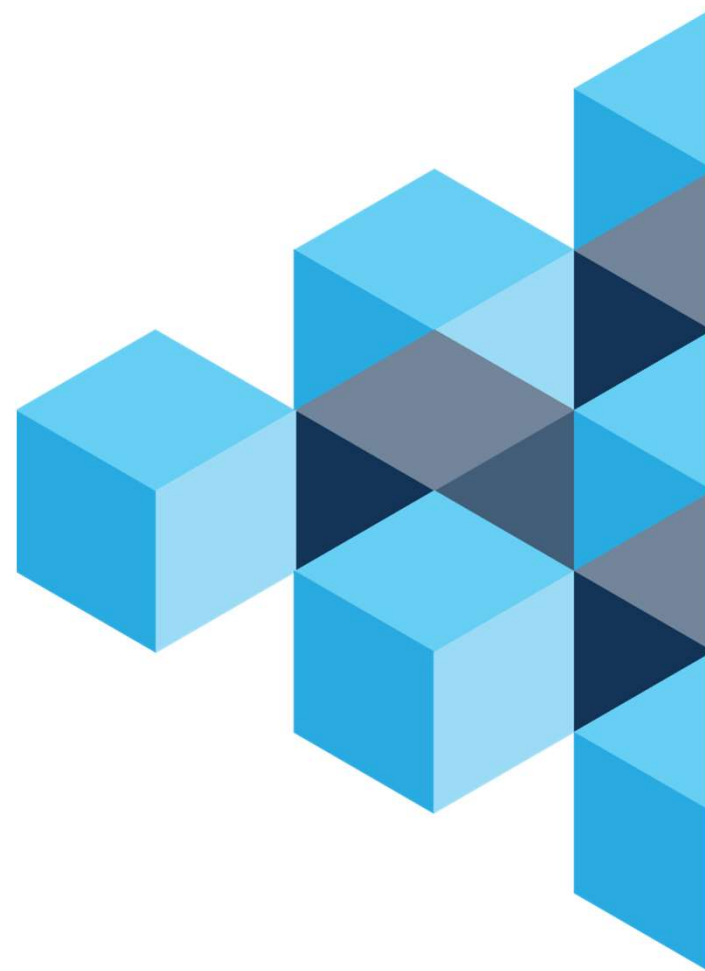




Bridging the Gap Between Blockchain and Business

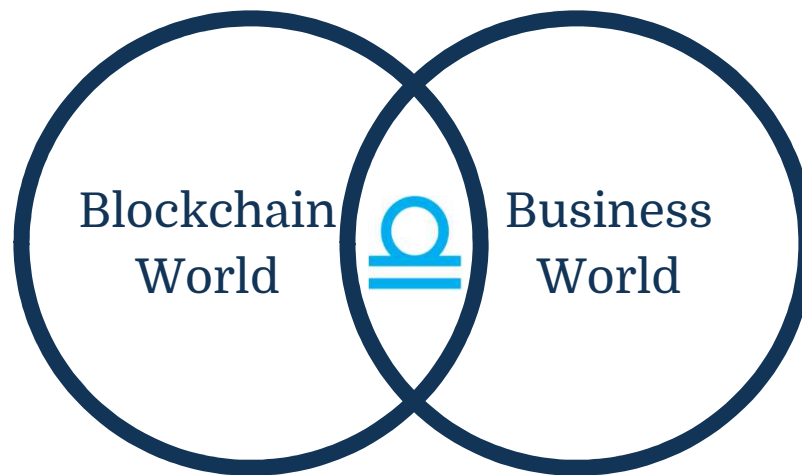
Auditing Blockchains!
WCARS Rutgers Univ Nov 2-3 2018

Gerard (Rod) Brennan CFE, PhD



What we do

Libra aggregates, normalizes and processes data to generate comprehensive audit-ready financial and operational information from the blockchain/DLT ecosystem.



Leadership team



**ROD
BRENNAN**
Audit Tech
Director



**VADIM
SHTEYNBERG**
VP of
Engineering



**NICK
OGURTSOV**
Chief Operating
Officer & Chief
Risk Officer



**EMIL
WOODS**
President



**JAKE
BENSON**
Founder & CEO



**JEREMY
DRANE**
Chief
Commercial
Officer



**GARY
REIFMAN**
VP of Product



Audit Advisory Committee



**MICHAEL
CANGEMI**

Michael currently serves as President of Cangemi Company LLC, through which he serves on Boards and as Senior Advisor to various companies. He ran regional IT Audit at EY and then nationally at BDO. After public practice he was CFO, CEO & Director at Etienne Aigner and CEO and Director of FEI. In addition to the Libra AAB, he currently serves as a Senior Fellow at the Rutgers Continuous Auditing and Reporting Laboratory; Senior Advisor to CaseWare Analytics, Oversight Systems and is an investor in and periodic advisor to Solink Corp. He serves on FEI's Committee on Finance & Technology (CFIT); the EDPACS Editorial Advisory Board; and the ISACA Governance Committee. He has served as a COSO Board Member, on the Financial Accounting Standards Advisory Council (FASAC) and on the International Accounting Council in London and was Editor-in-Chief of the ISACA Journal. He is the author of *Managing the Audit Function*, Third Edition.



**MIKLOS
VASARHELYI**

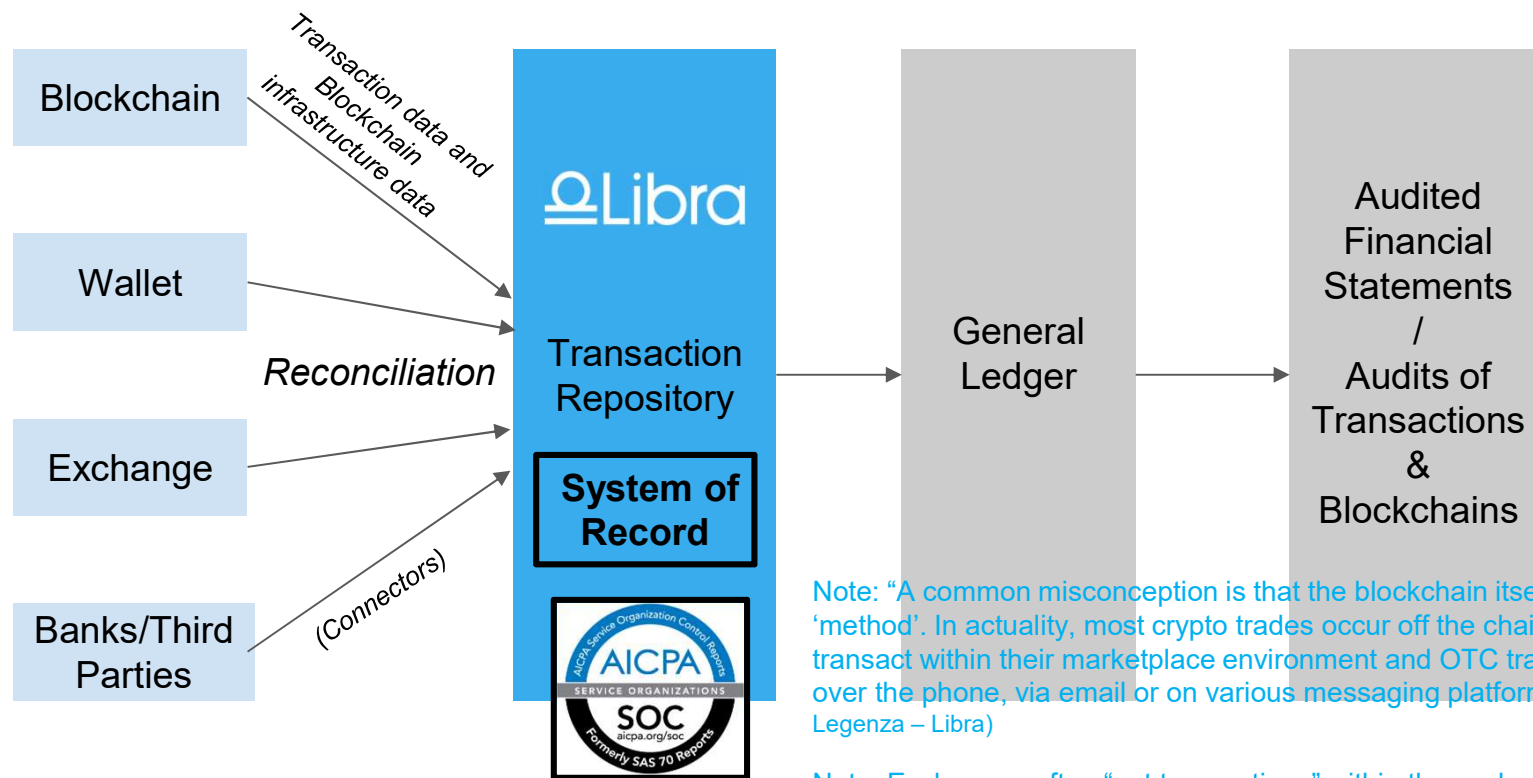
Professor Vasarhelyi is credited with developing the original continuous audit application and is considered by many as the leading researcher in this field. At Rutgers Business School, he heads the Continuous Auditing and Reporting Laboratory, which works on projects for such leading companies as Siemens, Procter & Gamble, AICPA, CA Technologies, and Brazil's Itau-Unibanco. Professor Vasarhelyi also leads the RADAR (Rutgers AICPA Data Analytics Research Initiative) project which is supported by the eight leading CPA firms, AICPA, and CPA Canada.



**ROBERT
(BOB) HERZ**

Bob served as one of the original members of the International Accounting Standards Board which was set up to develop International Financial Reporting Standards (IFRS) and was Chairman of the Financial Accounting Standards Board (FASB) from 2002 to 2010. More recently he began a three-year term on the Sustainability Accounting Standards Board (SASB) which develops sustainability accounting standards for publicly-listed US companies.

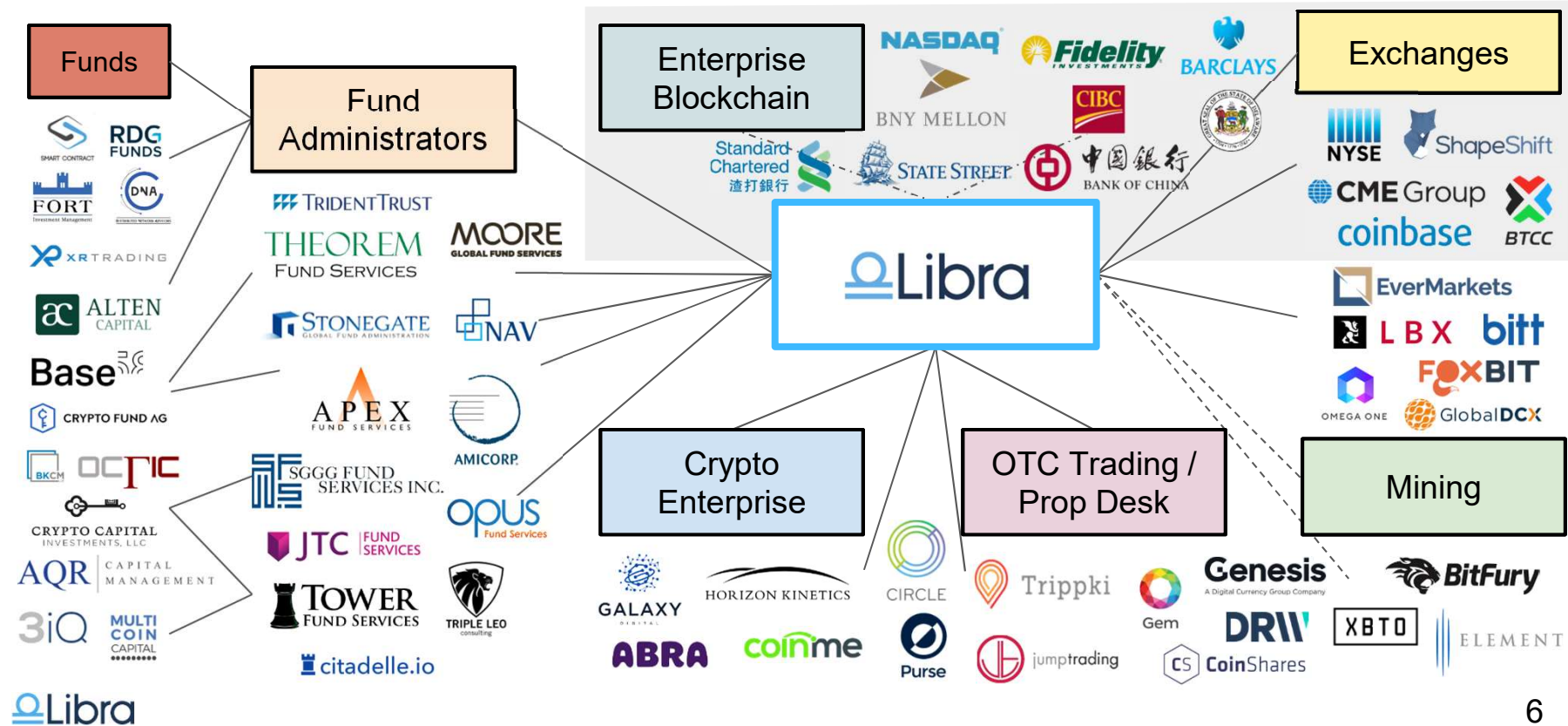
What We Do - Libra is a “System of Record”



Note: “A common misconception is that the blockchain itself is the ‘method’. In actuality, most crypto trades occur off the chain - exchanges transact within their marketplace environment and OTC trades often occur over the phone, via email or on various messaging platforms.” (Sarah Legenza – Libra)

Note: Exchanges often “net transactions” within the exchange so they do not always get on the blockchain right away

Today's Ecosystem: Customers/Potential Customers



Auditing Blockchains



What Does This Mean for Auditors?

....Is this the end of Audit?

.....Am I going to be out of a job?

Auditing Blockchain/DLT Networks

Pros:

- Much higher level of control precision & formalization
- Security / Sustainability via distributed ledgers → no single point of failure
- Fully automated / integrated ecosystem secured by cryptography
- Consensus prevents collusion → instead of “4 eyes” - 8, 100, 1000 eyes!

Cons:

- Blockchain is new/suspect first implementation less than a decade ago
- Objectives, risks, and controls are different for single database processes
- Limited technical expertise / experience in audit and IT around blockchains

With Blockchain, auditing is just plain different

Assertions are much more robust

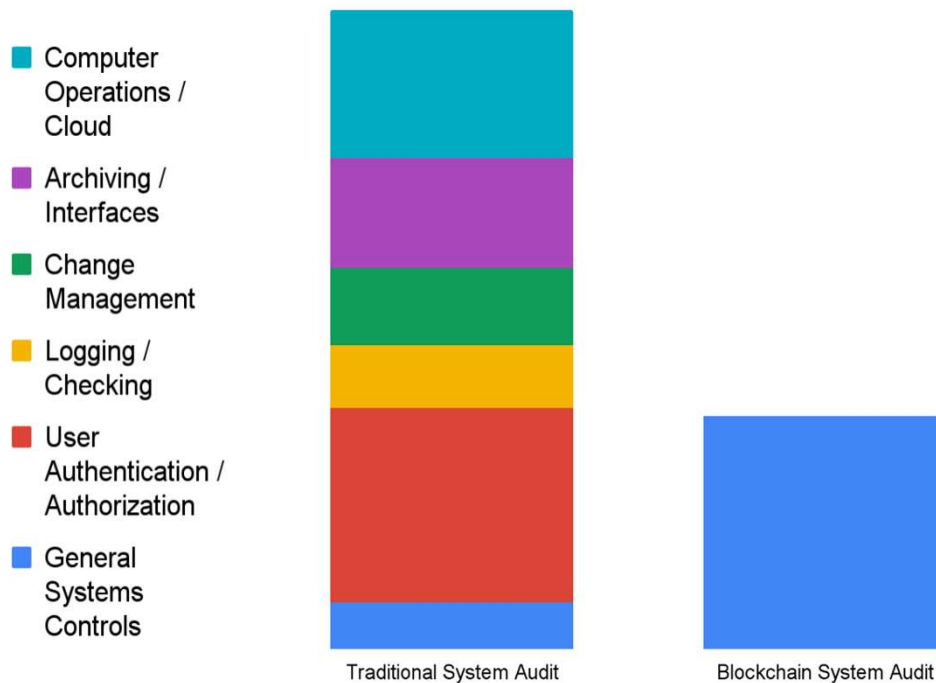
Table 3.1: Using distributed ledgers to test audit assertions

	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	√√√

* More √ indicates greater potential for direct benefit. Excludes indirect benefit where DL might improve data quality in general terms which creates knock-on benefits

Summary of Learning from PoC

Reduces risk and activities



- Blockchain protocol code is open source and secured by the consensus mechanism - mostly self audited. Blockchain transaction controls include ubiquitous cross protocol controls which help address risks with smart contracts
- No passwords, permission is by the consensus or all participants, no SOD, super users, etc..
- The blockchain is an immutable log
- All transactions & change management is controlled by the consensus mechanism
- The blockchain is an immutable archive
- Blockchain has no need of a data center


Blockchain Audit Framework

Protocol Accreditation	CM Monitoring	Transaction Assurance
Verify for participating nodes & regulators the sound design of the protocol against industry standards & best practice respected frameworks / standards (NIST, Cobit, ISO 27001, IIA, etc.) assuring key controls and are not missing.	Verify the sound design of consensus mechanism consistent with requirements of respective protocols and the baseline design approved by the participating nodes.	Assure the security, availability, immutability, processing integrity, confidentiality, validity, scalability, etc. of all transactions on the blockchain/DLT network.
Verify via automated analytics that ubiquitous, “best practice” protocol rules / controls are in place for any public or private blockchain.	Validate node rights / participation, quorum, voting participation, etc. to ensure the protocol required and user defined baseline consensus mechanism is operating effectively.	The Libra Audit Engine will provide assurance on ubiquitous controls related to any smart contract and will allow user configuration of additional controls as defined by the needs of the specific use case.

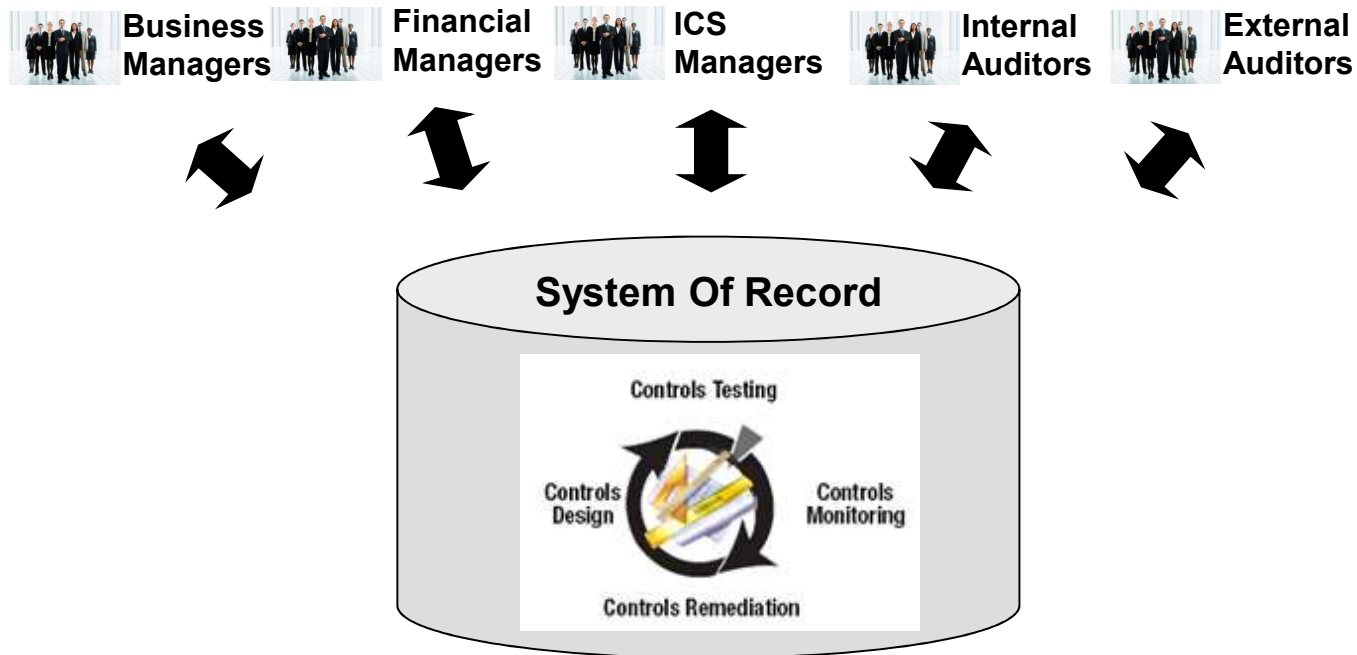
Sample Controls Inventory

Type of Control	Analytic	Detail: Objectives /Risks / Assertions	Impact on Blockchain	Analytic - IF/Then	Alerting Workflow: (i.e. Failure = send closed loop escalating alert to the	Framework Alignment (i.e. COSO, COBIT,
Protocol Control	Inactive nodes	<p>OBJECTIVE: Determine if nodes with no or little activity for a specified period of time should be reviewed or removed from the network to reduce risk of non-compliance.</p> <p>RISK: Inactivity may be an indicator of an operator who should not have or no longer have opportunity to compromise the system</p> <p>ASSERTIONS: Occurance / Rights & Obligations</p>	Inactivity on a PrivBC may be an indicator of a risky node that no longer belongs on the BC	If period of inactivity is reached (i.e. "X" days) Then send an alert, require permissioning / "re-admission into the network"	System Admin-->CIO (after 1 week)-->CEO(after two weeks)	NIST 3.1.10, 3.1.11, COBIT 5.1 ITIL 7.5
Transaction Control	Run Limits	<p>OBJECTIVE: Determine if any program (i.e. SC) on a network ever exceeds it's established "Run Limit or "gas" consumption assuring that a program does not run too fast or too long indicating a risk of non-compliance.</p> <p>RISK: A program exceeding established "Run Limits or "gas" consumption may indicated a compromise or fraud against the system</p> <p>ASSERTIONS: Occurance / Rights & Obligations</p>	The CVM's instruction set is Turing complete. To prevent unbounded use of computational resources, the protocol allows networks to set a run limit that a program is not allowed to exceed. Each instruction consumes some of the limit as it runs, according to its run cost. Chain's run limit mechanism is similar to Ethereum's "gas," except that there is no on-chain accounting for the execution cost of a transaction.	If a programs run limit / gas is exceeded o.i.e. "X" days) Then send alert regarding potential compromise of the program / network	System Admin-->CIO (after 1 week)-->CEO(after two weeks)	NIST 3.1.10, 3.1.11, COBIT 5.1 ITIL 7.5
Consensus Control	Signing multiple blocks at the same height	<p>OBJECTIVE: Assure block signers do not signs multiple blocks at the same height resulting in potential frauds in the consensus</p> <p>RISK: A block signer allowed to sign multiple blocks at the same height may be able to perpetrate or conceal a fraud in the consensus.</p> <p>ASSERTIONS: Occurance / Rights & Obligations</p>	If a block signer signs multiple blocks at the same height, participants can use the inconsistent signatures to construct fraud proofs to warn other nodes or provide evidence for enforcement out-of-band.	If an authorized block signer (or any network participant) signs multiple blocks at the same height, Then send an alter of a potential compromise of the consensus / network	System Admin-->CIO (after 1 week)-->CEO(after two weeks)	NIST 3.1.10, 3.1.11, COBIT 5.1 ITIL 7.5

Controls Inventory Examples – Public/Permissioned BC’s

Protocol Accreditation	CM Monitoring	Transaction Assurance
<ul style="list-style-type: none"> Assure transaction size does not exceed block size Assure transaction min. are not exceeded Assure only permissioned nodes are on the network (no rogue or unregistered nodes) Assure all dependent input transactions have a corresponding output transaction. Assure all nodes are using current network version/ Assure node count does not exceed allowed nodes Etc.. <p>Note: Specific protocol controls will apply to specific use cases and blockchains</p> 	<ul style="list-style-type: none"> Assure the agreed number of dynamic voting nodes are present/vote to submit transactions to the network Assure block signers sign only eligible blocks within the allowed signature timeframe Assure voting nodes do not exceed permissioned nodes (i.e. double voting) Assure no “Frontrunning” by voting nodes by limiting transactions in which validators can participate. Assure no inappropriate concentration of miners/voting nodes (via. Related nodes, Geography, Pools, etc.) Etc.. 	<ul style="list-style-type: none"> Assure compliance with Multisig transactions Assure transactions with location stamps are not coming from sanctioned countries Assure transaction volume does not exceed a quantity/value limits (manipulation, wash trading, etc.) <p>Ubiquitous Smart Contract Controls:</p> <ul style="list-style-type: none"> Assure no “reentrancy” by limiting smart contract execution Assure no “race conditions” by limiting multi smart contract execution where there is risk Assure “DOS GAS Limits” do not exceed established threshold by an node (identifying potential hacks early) Etc..

Audit & Operational Rules based engine runs on the same platform!



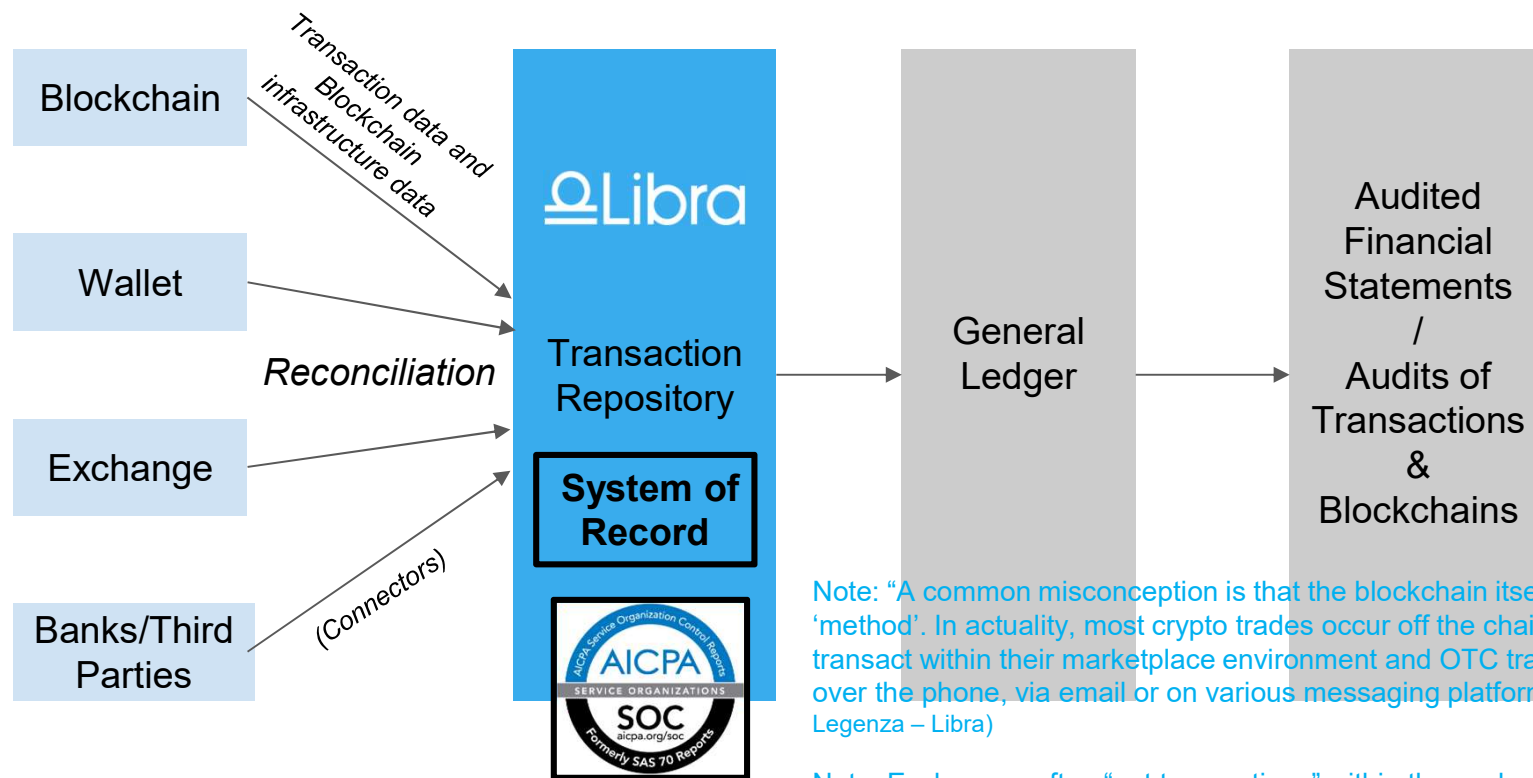
Operational Rules based engine runs on the same platform

Rules based engine allows clients to develop compliance checks throughout the investment lifecycle. If a rule is triggered, the Libra alerting system will notify the necessary parties (compliance officers, PMs, traders, etc.)

Sample Operational rules

- Portfolio checks - tracking index weightings, price floors/ceilings, etc.
- Monitoring exposures by reference data (market cap, sector, etc.) or tag
- Restricted stock lists
- REGULATION
- Etc..

What We Do - Libra is a “System of Record”



Note: “A common misconception is that the blockchain itself is the ‘method’. In actuality, most crypto trades occur off the chain - exchanges transact within their marketplace environment and OTC trades often occur over the phone, via email or on various messaging platforms.” (Sarah Legenza – Libra)

Note: Exchanges often “net transactions” within the exchange so they do not always get on the blockchain right away

Crypto Pricing Project Rutgers & Libra

Note: Token trading needs an accredited automated pricing methodology which mitigates manipulation and volatility

Key Agreement/Actions

- Agreed the IRS/Practice classification of crypto tokens as assets/property (subclass: “Indefinite-lived Intangibles”) is appropriate and that fair value guidance from ASC 350 and 820, IAS 36 and 38, IFRS 13, etc., while not providing specific guidance for crypto assets, support the established concepts of “Mark to Market” valuation for actively traded assets and “Mark to Model” for assets with low or erratic trading volumes.
- Appropriate threshold (i.e. measurable activity level) for “actively traded” token Assets” – for Mark to Market valuations which can be calculated via analytics.
- Propose/define “Prime Exchange” for any actively traded crypto token.
- Define “Fixing Price” methodology for actively traded tokens – assure this mitigates manipulation and can be determined via an analytic.
- Propose an appropriate model for pricing low activity/illiquid crypto assets for “Mark to Model” Note: this may be an analysis based on “Ask & Bid and will need to be proofed with actual data.

Note: All of the above will be simulated/modeled with actual data.

Discussion / Questions:

