QA AND TESTING IN A BLOCKCHAIN WORLD

October 30th 2018

TASSQ Toronto Association of Systems & Software Quality

Our Proud Sponsors

NVP Software Solutions
We Support the Future

Direct IT Recruiting Inc.

Askida™

STAR CANADA
A TECHWELL EVENT

TASSQ Toronto Association of Systems & Software Quality

Our Board










TASSQ Toronto Association of Systems & Software Quality

QA in a Blockchain World

Oct 2018

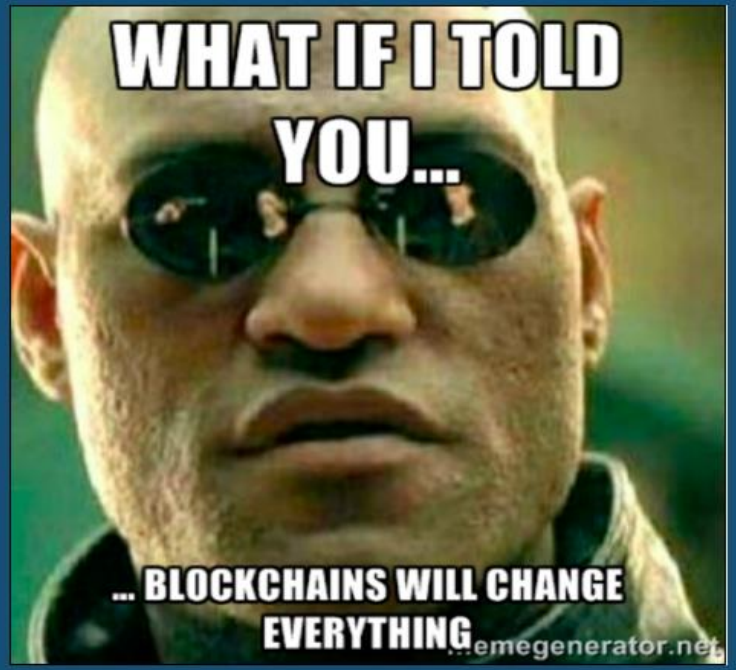
Kiran Vaidya

BLOCKCHAIN CONSULTANT/ MANAGER

Web: kiranvaidya.xyz/bio
Blog: kiranvaidya.xyz/blog
Linkedin: linkedin.com/in/kiranvaidya/
Twitter: twitter.com/kiranvaidya
Whatsapp Group: kiranvaidya.xyz/whatsapp
Email: kiran.vaidya@gmail.com

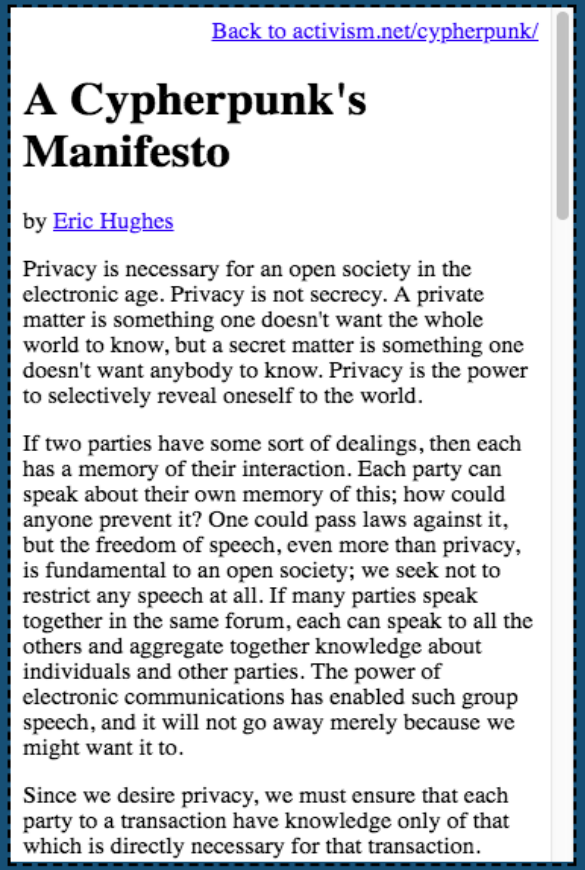
AGENDA

- Origins & Disruption
- What is Blockchain?
- Why the Hype?
- Types of Blockchain
- Blockchain ecosystem
- Considerations before Blockchain Implementation
- Practical Challenges
- QA/ Testing in a blockchain world
- Questions



THE ORIGINS

- Cypherpunk's Manifesto
- HashCash Algorithm
- Nick Szabo's Contributions prominently on Smart Contracts and History of Money
- Satoshi Nakamoto's Whitepaper on Bitcoin
- Recession 2008- The perfect Storm



Back to activism.net/cypherpunk/

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction.

DISRUPTIVE DIGITAL TRANSFORMATION - FROM BITCOIN TO BLOCKCHAIN

- Growth of Sharing Economy and P2P models
- Trust at an all time low
- Ethereum
- Permissioned Ledgers

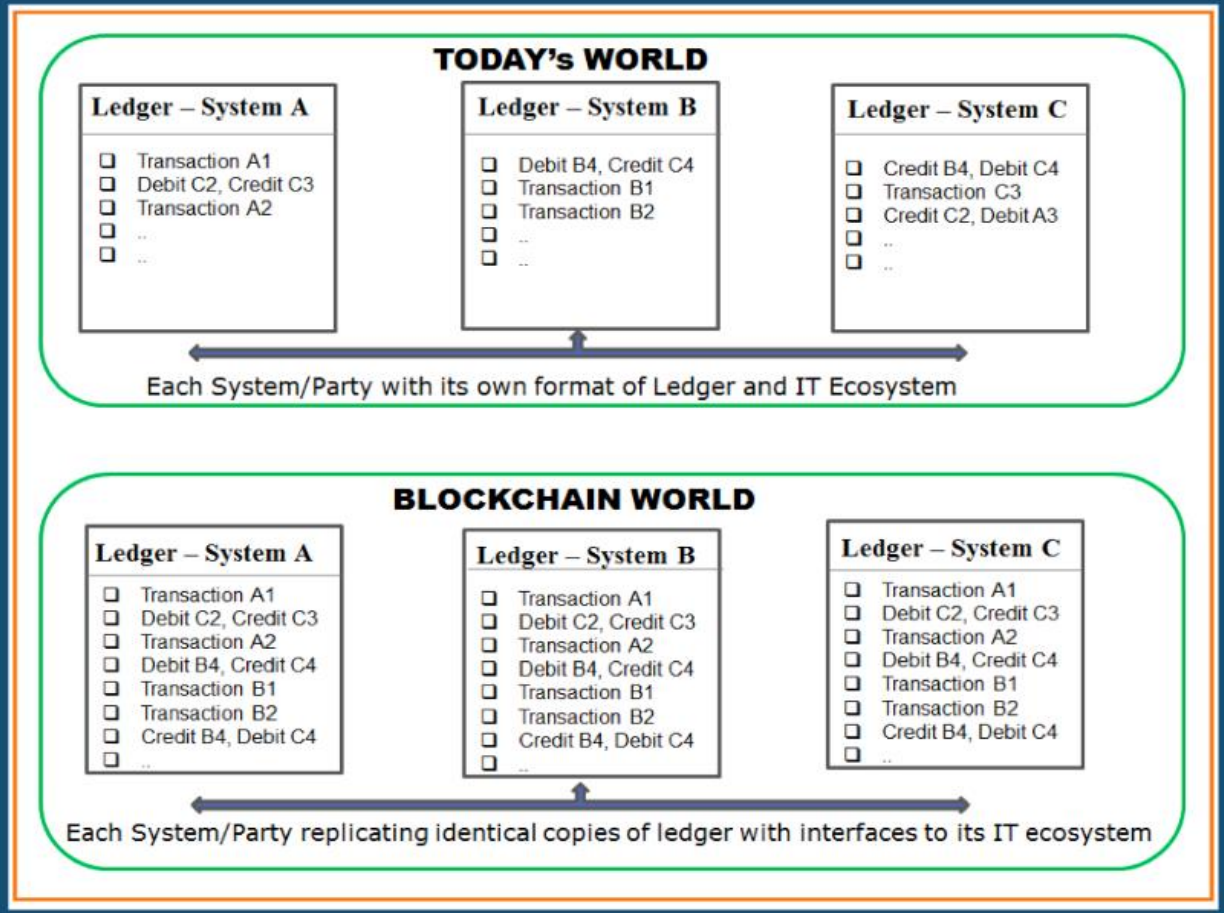
B FOR ~~BITCOIN~~ BLOCKCHAIN

Transfer any **VALUABLE digital asset** in a **TRUSTFUL** manner over a network **WITHOUT** any **INTERMEDIARY**

13 COMPONENTS OF A BLOCKCHAIN NETWORK

DECENTRALIZATION		
LEDGER	NODES/ PEERS/ CLIENT	MINING
CONSENSUS	CRYPTOCURRENCY	BLOCK
KEYS	CRYPTOGRAPHY	WALLET
ECONOMICS	HUMAN BEHAVIOUR	GAME THEORY

TODAY'S WORLD VS BLOCKCHAIN WORLD



BLOCKCHAIN = NETWORK + LEDGER + PROTOCOL

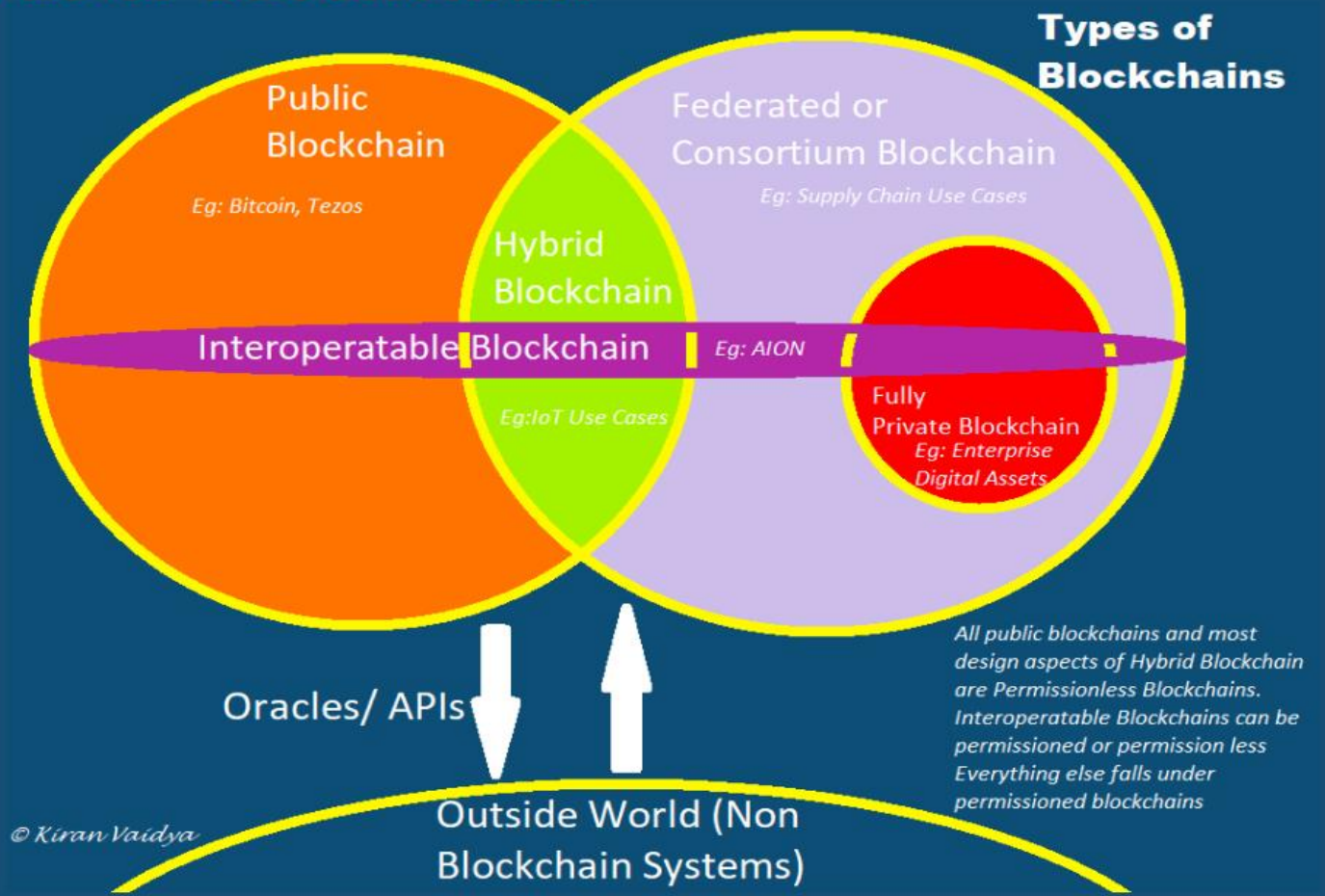
WHY THE HYPE?

- 2 pillars of every society, system, network are **MONEY** and **TRUST**. Blockchain redefines both
- We are surrounded by **LEDGERS** and **CONTRACTS**.
- Applicable to **EVERY** geography, industry and profession
- **DIGITIZATION** of everything
- **EARLY STAGE**
- Fast paced **ADOPTION**

SMART CONTRACTS

- Code is Law
- Self executing
- Define rules and penalties
- Autonomous enforcement
- Transparent

TYPES OF BLOCKCHAIN



FUNDAMENTAL DIFFERENCES IN BLOCKCHAINS

- Definition of Trust
- Native Token & role of miners
- Transaction and Owner visibility
- Node authority
- Who can join the network and how
- Access point for nodes - within the same network?
- Consensus mechanisms

WHATSAPP ANALOGY

1. Ledger
2. Security
3. Immutability
4. Transparency
5. Decentralization
6. Config Parameters
7. Client
8. Full Audit Trail
9. Disagreements/ Forks
10. Identity
11. Transaction Visibility

BLOCKCHAIN ECO-SYSTEM : PARTICIPANTS

. Developers
. Miners
. Wallets
. Exchanges
. Users
. Merchants
. Regulators
. Nodes
. Certifying Authority
. Consortium members
. Users as per the Governance policy
. Traditional data systems and processing platforms

BLOCKCHAIN ECO-SYSTEM: PLATFORMS

Public Permissionless Blockchains
Bitcoin
Ethereum
Tezos
Stellar.. hundreds more

Hyperledger
Fabric
Indy
Sawtooth
Iroha
Burrow

Permissioned Blockchains
Corda
Quorum

BLOCKCHAIN USE CASE CONSIDERATIONS

Mandatory parameters
Immutability
Multiple Parties writing to ledger
Full Audit Trail
Multiple intermediaries
Digital Assets

Blockchain Design Considerations
Settlement & Clearance
Time & Money overheads
Transparency
More trust
Better security
Privacy and anonymity
Size of data on ledger
Participant Interaction
Semi to full decentralization

Other Considerations
Skillset
Budget
Risks
Smart Contract Prog Language
Performance

PRACTICAL CHALLENGES

. **Governance - Node and Repository**
. **Public perception**
. Evolving Technology
. Tools not mature
. Technical Skillset
. Code is Law
. Autonomous execution
. Regulatory
. Immutability
. Scalability
. Energy Consumption

TESTING SPECIFIC TO BLOCKCHAIN

Distributed Systems Testing
All Data is in sync on all ledgers
Double Spend
Block Size is as per spec
Double Spend
Avg time taken for Block creation
Data privacy testing
Tx sequence
Access/ Authorization as per spec
Concurrent Txs from different nodes
Node Integrity

Node Testing
Deploy own test node & connect to blockchain
Uptime of nodes
Purposely shut down node and observe network
Time taken to sync

Smart Contract Testing
Business Logic
Infinite loops
Run out of Gas

BLOCKCHAIN TESTING CONTINUED

API/ Webservices
Blockchain Wallets
Blockchain Explorers (UI Component)
Identity Testing
NFT
Security Testing
Smart Contracts Audit
Boundary Testing

Blockchain Testing Tools
Hyperledger Composer
Ethereum Tools (Next slide)

ETHEREUM TESTING TOOLS

- Solidity code coverage - Solidity code coverage tool
- Solidity coverage - Alternative code coverage for Solidity smart-contracts
- Solidity function profiler - Solidity contract function profiler
- Espresso - Speedy, parallelised, hot-reloading solidity test framework
- Eth tester - Tool suite for testing Ethereum applications
- Cliquebait - Simplifies integration and accepting testing of smart contract applications with docker instances that closely resembles a real blockchain network
- Hevm - The hevm project is an implementation of the Ethereum virtual machine (EVM) made specifically for unit testing and debugging smart contracts
- Ethereum graph debugger - Solidity graphical debugger
- Solhint - Solidity linter that provides security, style guide and best practice rules for smart contract validation
- Solium - Linter to identify and fix style & security issues in Solidity
- Decode - npm package which parses tx's submitted to a local testrpc node to make them more readable and easier to understand
- truffle-assertions - An npm package with additional assertions and utilities used in testing Solidity smart contracts with truffle. Most importantly, it adds the ability to assert whether specific events have (not) been emitted.
- Psol - Solidity lexical preprocessor with mustache.js-style syntax, macros, conditional compilation and automatic remote dependency inclusion.

HYPERLEDGER FABRIC COMPOSER DEMO

https://composer-playground.mybluemix.net/editor

QUESTIONS & ANSWERS