



Blockchain and the possible impact on testing. New technology needs new testing?

Jeroen Rosink

TestCon Vilnius

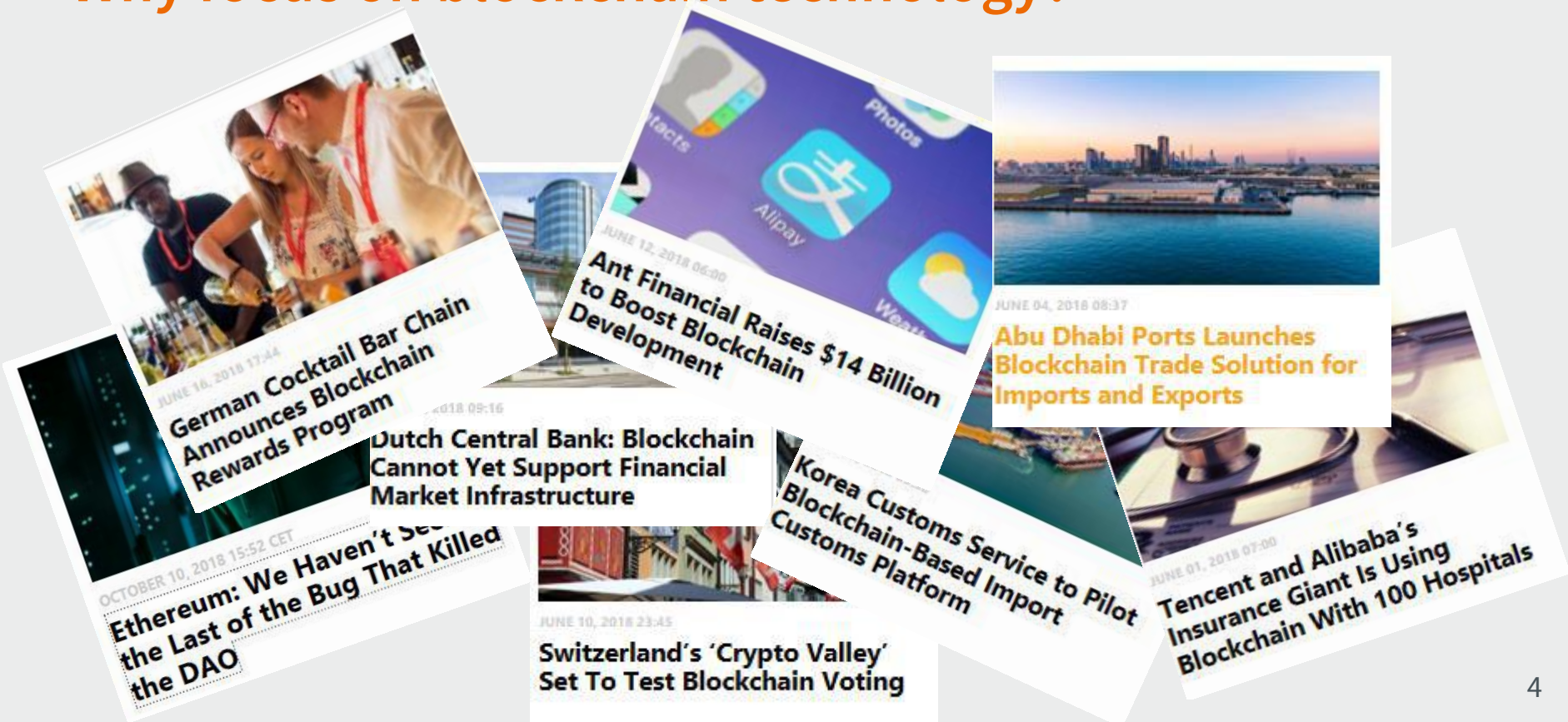
October 18th 2018

Agenda

















- What is Blockchain and are Smart Contracts
- Where to find it?
- Types of blockchains
- Impact on testing
- Impact on tools



Why focus on blockchain technology?



Why focus on blockchain technology?

Cryptocurrencies ▾		Exchanges ▾		Watchlist		USD ▾		← Back to Top 100	
#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	 Bitcoin	BTC	\$109,530,941,343	\$6324.72	17,317,912	\$4,328,706,696	0.29%	0.70%	-3.78%
2	 Ethereum	ETH	\$19,951,383,184	\$194.61	102,520,048	\$1,824,298,912	0.39%	-3.01%	-12.34%
3	 XRP	XRP	\$17,163,616,682	\$0.429116	39,997,634,397 *	\$812,235,180	-0.17%	4.67%	-17.55%
4	 Bitcoin Cash	BCH	\$7,825,800,786	\$449.81	17,397,875	\$345,964,978	0.22%	0.02%	-12.40%
5	 EOS	EOS	\$4,726,999,424	\$5.22	906,245,118 *	\$561,121,418	-0.16%	-2.06%	-8.89%
6	 Stellar	XLM	\$4,063,146,554	\$0.215088	18,890,617,142 *	\$62,016,220	0.07%	0.44%	-11.61%
7	 Litecoin	LTC	\$3,112,687,061	\$53.04	58,687,377	\$322,252,945	0.12%	2.00%	-8.65%
8	 Tether	USDT	\$2,677,096,558	\$0.989165	2,706,421,736 *	\$2,938,168,630	0.15%	-0.69%	-0.88%
9	 Cardano	ADA	\$1,943,129,778	\$0.074946	25,927,070,538 *	\$51,981,415	0.42%	-0.04%	-7.62%
10	 Monero	XMR	\$1,699,641,490	\$103.12	16,481,758	\$16,328,210	0.31%	0.00%	-9.58%
11	 TRON	TRX	\$1,465,525,374	\$0.022290	65,748,111,645 *	\$153,763,732	0.25%	0.71%	-1.96%
12	 IOTA	MIOTA	\$1,390,757,426	\$0.500357	2,779,530,283 *	\$27,806,401	-0.32%	-1.51%	-10.68%
13	 Dash	DASH	\$1,353,668,554	\$161.60	8,376,700	\$171,696,198	0.66%	-1.54%	-10.37%
14	 Binance Coin	BNB	\$1,115,964,191	\$9.50	117,443,301 *	\$17,921,308	0.31%	-0.82%	-8.65%
15	 NEO	NEO	\$1,038,565,327	\$15.98	65,000,000 *	\$215,315,733	0.21%	-0.59%	-10.78%
16	 Ethereum Classic	ETC	\$1,004,295,220	\$9.55	105,213,521	\$226,490,473	-0.06%	-3.86%	-13.47%

What is a blockchain?

A **blockchain**, originally block chain, is a continuously **growing list of records**, called blocks, which are linked and secured using cryptography. Each block typically **contains a cryptographic hash** of the previous block, a **timestamp**, and **transaction data**. By design, a blockchain is resistant to modification of the data. It is "an open, **distributed ledger** that can record transactions between two parties efficiently and in a verifiable and permanent way".

<https://en.wikipedia.org/wiki/Blockchain>

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 proof-of-work chain as proof of what happened while they were gone.

1. Introduction

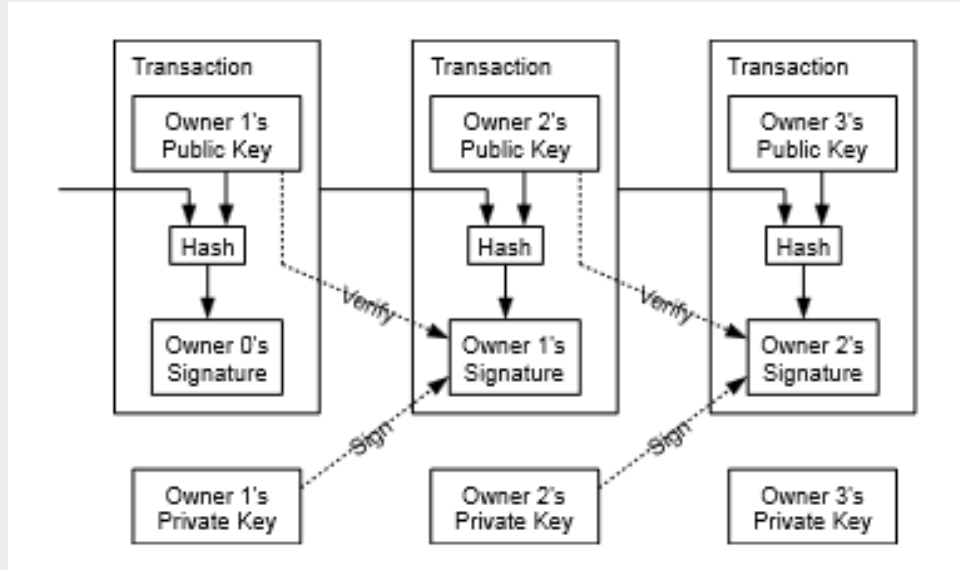
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot

Only 9 pages!!!

How it works - simplified

- A database like Excel
- Shared over the network over 50 PC's (we call them nodes)
- Node makes an update, and the change is distributed over the network
- When another node makes an update, and saved, a notification is shown. (check to remain validity)

How it works



Proof of Work

Under a Proof of Work system, miners compete to verify that all the transactions within the candidate block (the block currently being built) are legitimate. PoW is dictated by competition and computational output.

Proof of Stake

Proof of Stake differs entirely from Proof of Work. Instead of building blocks through work output, the creator of a block is determined by their share, or stake, in a currency.

Types of blockchains

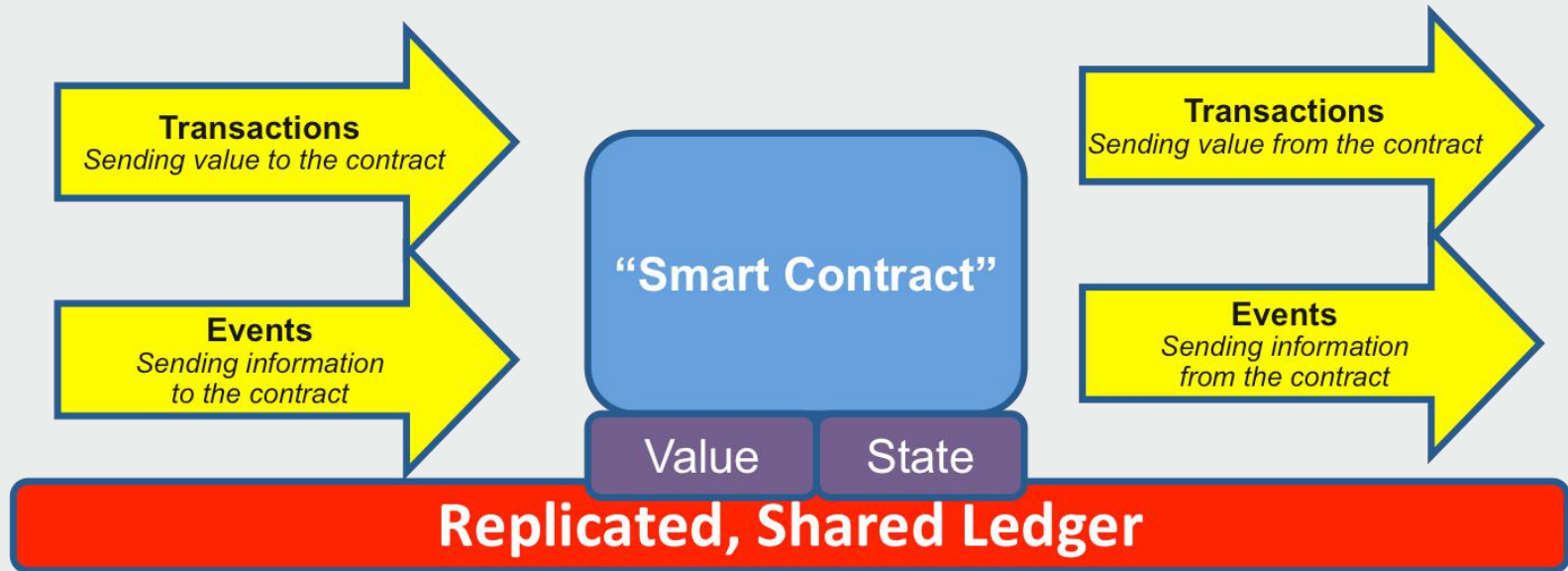
- Public Blockchains
- Federated/Consortium Blockchains
- Private Blockchains

	Public	Private
Access	Open read/write access to DB	Permissioned read/write to DB
Speed	Slower	Faster
Security	PoW/PoS	pre-approved participants
Identity	Anonymous	Known identities
Costs	Expensive	Cheaper

What are smart contracts?

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

Smart contract: the concept



What are smart contracts?

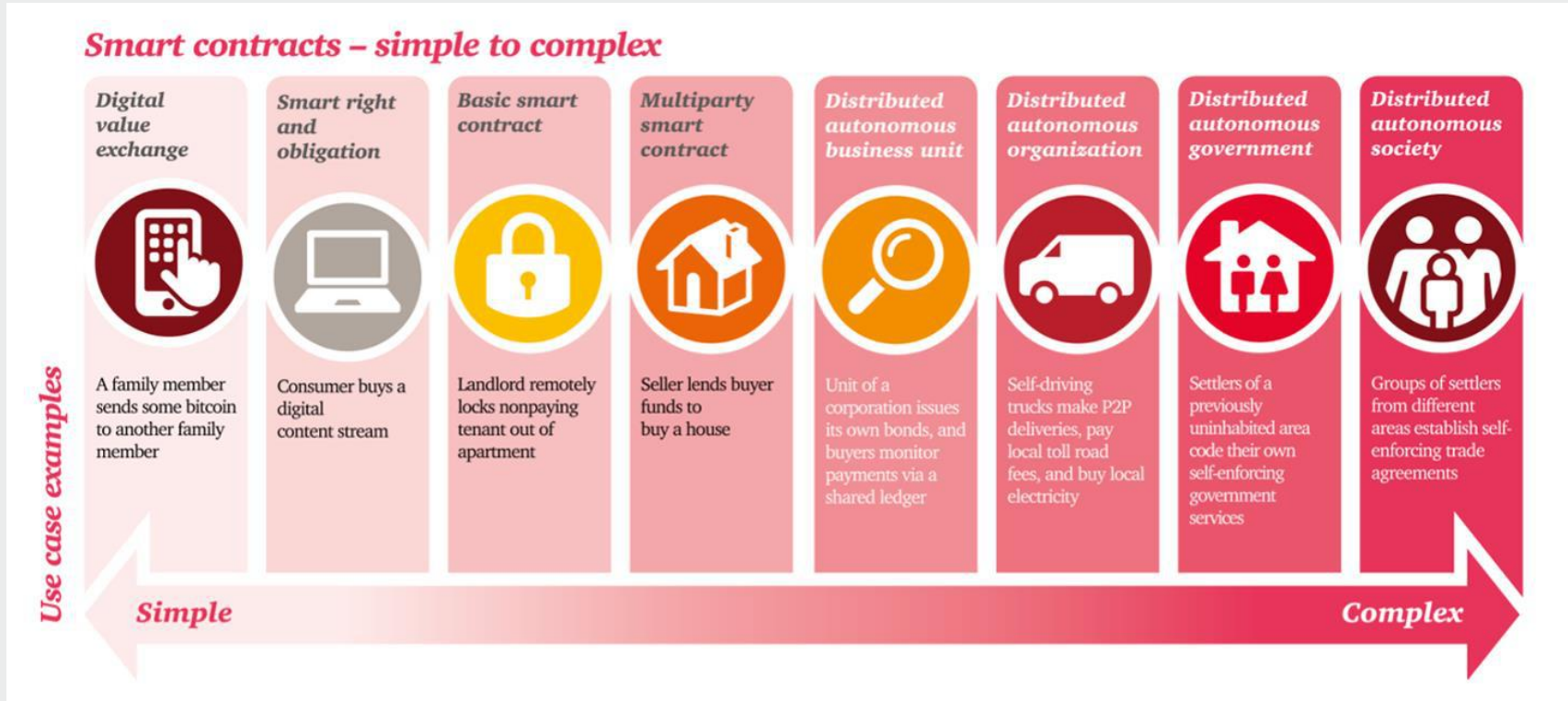
```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then communicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw; // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw; // Check allowance
    balanceOf[_from] -= _value; // Subtract from the sender
    balanceOf[_to] += _value; // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw; // Prevents accidental sending of ether
}
```

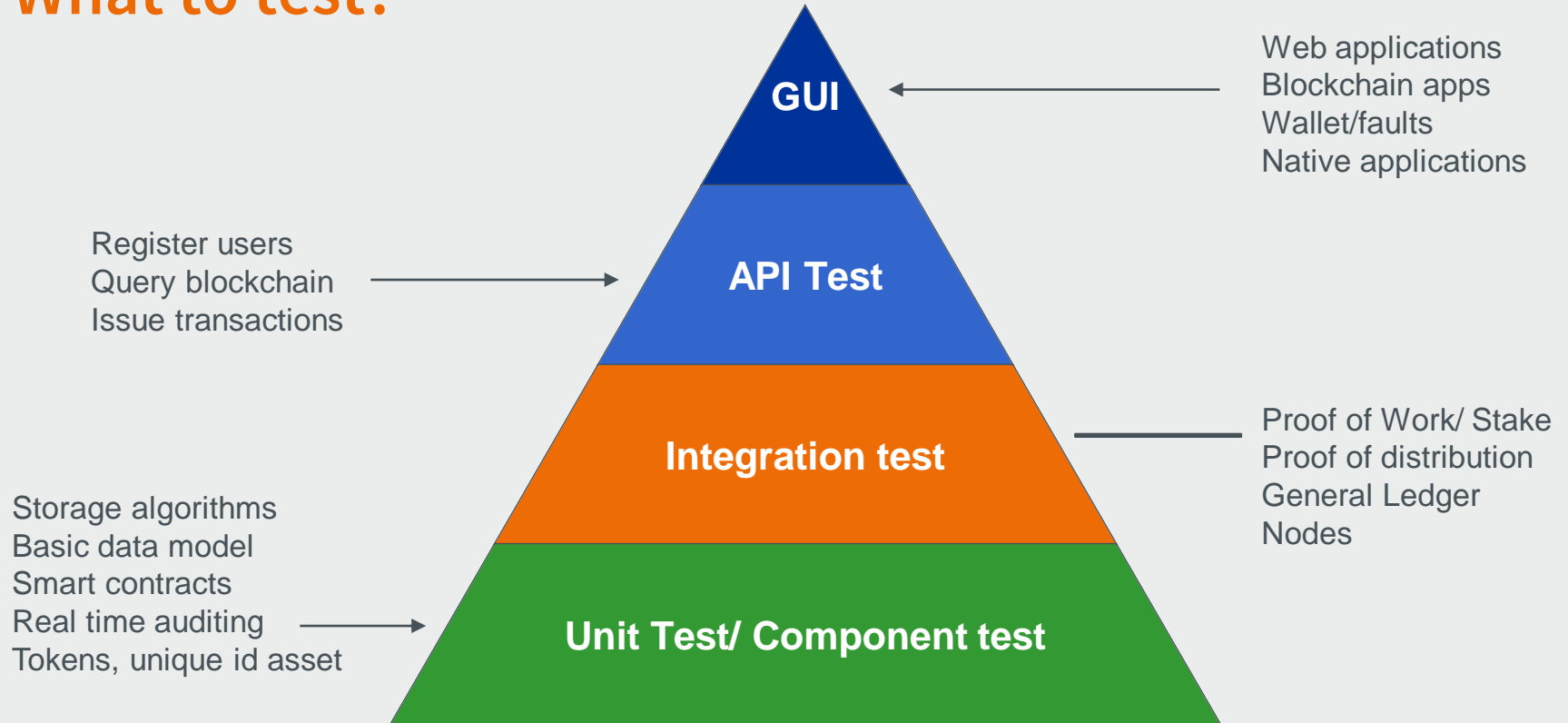
Where to find blockchains and smart contracts?



Impact on testing

- › Fast pace of blockchain technology
- › Adoption and Trust between organizations
 - › Fast moving to be mainstream technology
 - › Volatile transaction fees
- › Replacement of persons and processes
- › Unicity of data/ information
- › Security and authentication
- › Performance
 - › Network latency
- › Test environment
 - › Lack of good practices, tools, models
- › Black swans
- › Lack of Blockchain testing experience and good practices

What to test?



Test Types

Security Testing

Blockchain Acces Testing
Hash algorithm Testing
Signature Testing

Functional Testing

Smart Contract Testing
Database Ledger testing
Node testing
AML/KYC business rules

Non Functional Testing

Platform Performance
Scalability
Stability
Performance
Load
Network Latency

Other Testing

Cloud Testing
SOA/API Testing
GUI & Mobile Apps
Regression Testing

New Skills?

- > Same skills applicable
 - > Transaction process verification
 - > Payment components
 - > Addition requirements (e.g. Terms of smart contract)
 - > No double spending
 - > Boundary testing and Performance

- > Although:
 - > Knowledge of the concept
 - > Cryptographic skills
 - > Ledgers
 - > Getting common with new tools
 - > Compliance & Security (like AML/KYC)

Impact on Test environment

- Miners' resources needed ->also to test load/performance and network latency
- Blockchain test environment ->testing in real environment you pay per transaction in cryptocurrency
- Test data -> transactions are irreversible
- Dynamic environment->
 - private vs public
 - Fork management?!

Blockchain Test Tools

- Ethereum Tester : Ethereum based applications
- Truffle: ability to automate test for your contracts
- Hyperledger Composer: development tool that supports interactive testing, automated unit testing and automated system testing
- Ganache: for testing Ethereum contracts locally
- Corda Testing Tools: Writing contract tests, Integration testing, Writing flow tests, Load testing
- BitcoinJ: library for working with the Bitcoin protocol.



Questions?



Jeroen Rosink

j.rosink@squerist.nl

<https://www.linkedin.com/in/jeroenrosink/>

<https://twitter.com/JeroenRo>