RSA Conference 2016

Abu Dhabi | 15 – 16 November | Emirates Palace

Connect to Protect

PNG-T08

Are We Really Ready for Blockchain?

Harshul Joshi

SVP Governance Risk and Compliance, DarkMatter

#RSAC

Contents

INTRODUCTION TO BLOCKCHAIN

01


I THINK WE SHOULD BUILD AN SQL DATABASE.
UH-OH
S. Adams
E-mail: SCOTTADAMS@AOL.COM
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
© 1995 United Feature Syndicate, Inc.(NYC)
WHAT COLOR DO YOU WANT THAT DATABASE?
I THINK MAUVE HAS THE MOST RAM.

Blockchain Defined

The value of something is the price it brings

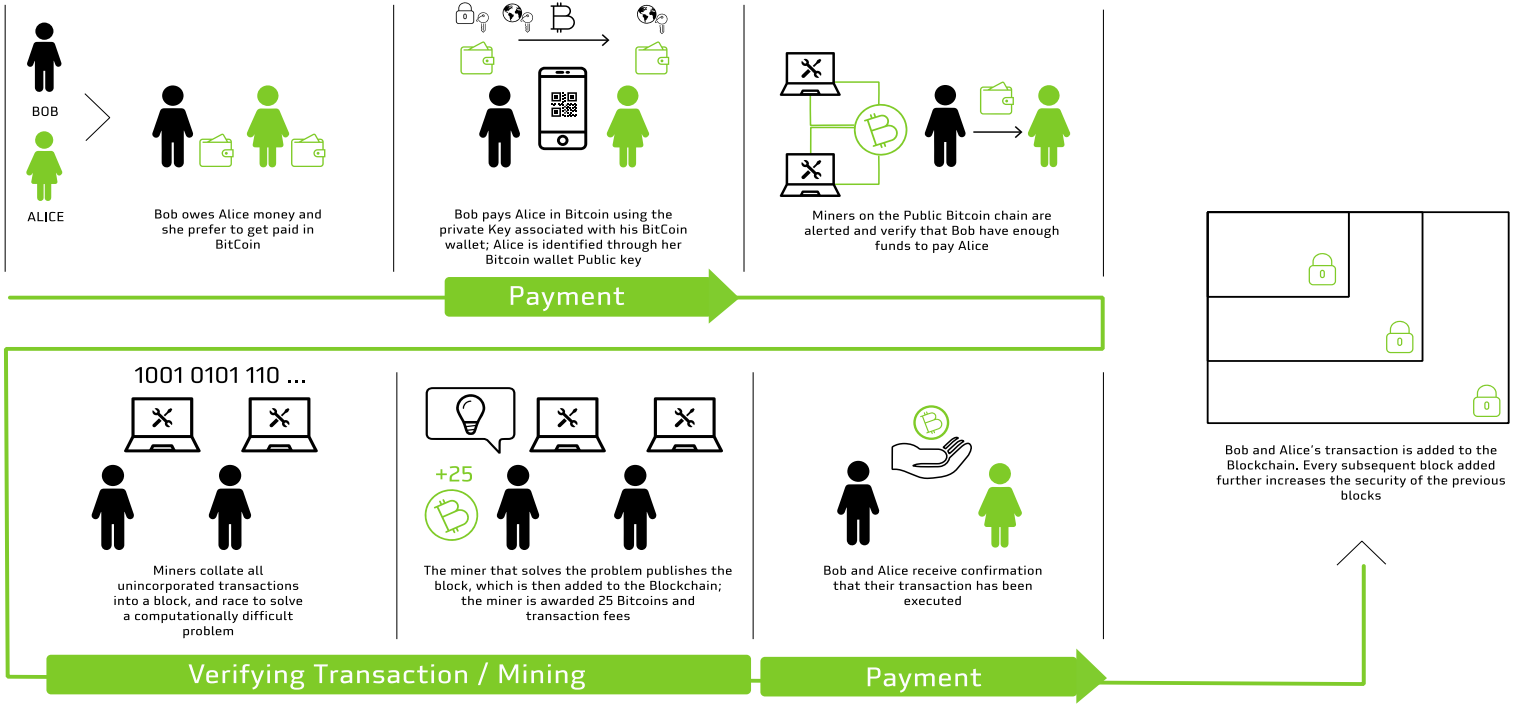
Bitcoin

- A digital currency which was in a lot of ways the first demonstrable use
- A protocol that supports a decentralized, pseudo-anonymous, peer-to-peer digital currency

Blockchain

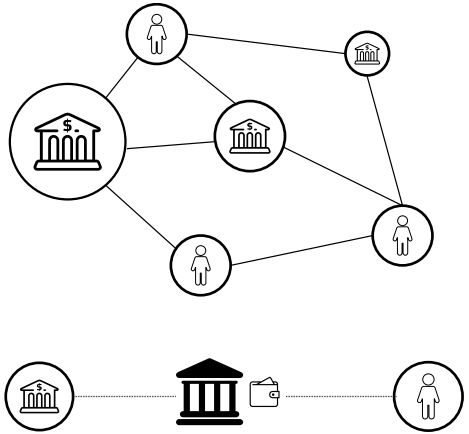
- Distributed
- Secure
- Logfile

Transaction flow for Bitcoin



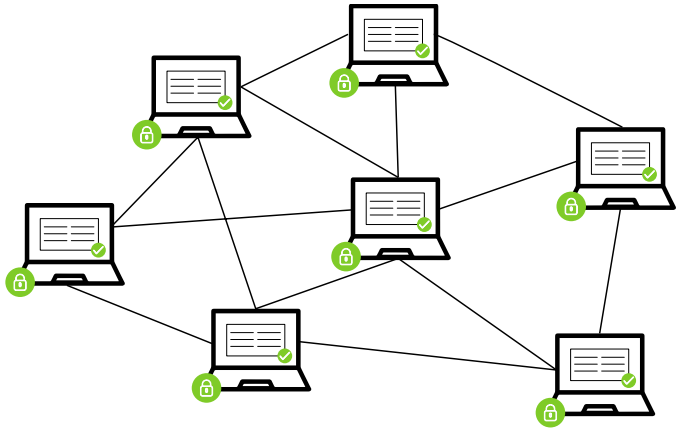
What is blockchain

Current System



- Central authorities (bank, fed, notary, escrow, etc.) transfer actual value between two parties
- Multiple intermediaries and record-keeping are required to facilitate transfer of assets and create trust

Blockchain System



- Distributed network of computers (nodes) that maintain a shared source of information
- Transaction data is immutable
- Peer to Peer transactions using digital tokens to represent assets and value

Introduction to Blockchain

A **shared ledger** technology allowing any participant in the business network to see the **established (via distributed consensus) system of record (ledger)**

Every **viable transaction** is stored in the **shared public ledger**

Transactions are placed in **blocks,** which are linked by **SHA-256 hashes**

Operates in a **peer to peer mode** and is mostly based on DNS and **"seed nodes"**

Each **peer address is anonymous** and **multiple addresses** may map to the same transactor

Blockchain is rapidly gathering momentum globally

Significant levels of venture capital is driving market activity in blockchain – key industry players are exploring new and innovative blockchain applications

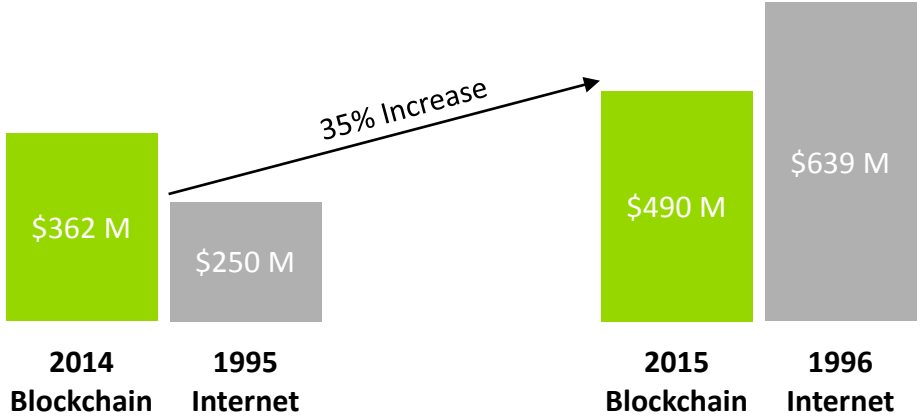
$1.2B
In investments in past 3 years

$14B
Of industry revenue could face downward pressure from Blockchain implementation by 2017

80%
Of the world's largest banks will have initiated Blockchain projects by YE 2016

$20B
In projected annual banking industry saving 2022

Investment activity in blockchain is showing a trend comparable to early stage investment in the internet; Bloackchain investment continues to show strong VC funding despite overall VC funding has been decreasing 9% across industries in 2015



"We can re-implement the entire financial system as a distributed system as opposed to a centralized system. We can reinvent the entire thing."

Marc Andreessen

"The implications of the blockchain for the economy are comparable to those of the Internet for information"

Gartner Research

Over $1 billion has been invested by companies into Blockchain technology

Platforms	Windows Azure, ethereum, factom, Digital Asset Holdings, eris INDUSTRIES, rhain, Blockstream, bloq, CREDITS, Blockstack.io, Counterparty, BLOCKCYPHER, symbiont, consensys
Wallets	xapo, trucoin, coinbase, BitGo, Gem, ARMORY, BLOCKCHAIN, CIRCLE
Identity	onename, Serica, Voatz, clearmatics, everledger
Exchanges	CIRCLE, coinsetter, BITSTAMP, coinx, itBit, kraken
Payment Processors	Bitnet, bitpay, GOCOIN, coinbase
Loyality & Gift cards	loyyal, gyft, BitFury, KnCMiner, Storj.io
Payments & Remittances	ripple, CIRCLE, REBIT, stellar, Bitspark, ABRA
Consortia, VCs & Organizations	R, HYPERLEDGER PROJECT, coala, DIGITAL CURRENCY GROUP

Blockchain benefits overview

Keeping secure records

- Records and validates each and every transaction made in a cryptographic manner
  - Multi-Signatures [public key cryptography, specifically ECC due to key-strength and shorter keys]
  - Encrypted Communication [in particular for generalized B2B transactions]
  - True Non-Repudiation: Transaction unlinkability while incorporating identity management and auditability

Efficient value transfer

- **Blockchain mining discards the need of any third-party or central authority for P2P transactions needed to transfer value between two parties:** *Process and Cost Efficiency; Reduced internal risks; Mitigate Man in the Middle*

Smart contracts

- Decentralization of the technology and distributed Ledger for smart contracts development, exchange and signature
- Transfer over Internet by anyone with computer or smart phone

CHALLENGES?

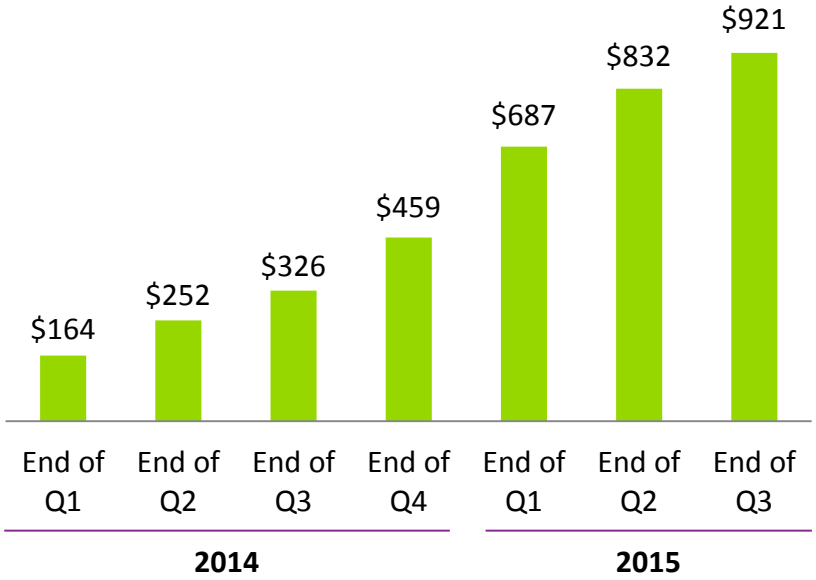
Blockchain challenges

Challenges

- Blockchain significantly alters the need for trusted third-party authentication through a financial institution
  - Challenges of legacy infrastructure
- Challenges in understanding the technology
  - Complex cryptosystems
  - Decentralized cryptosystems
- Attacks on Cryptosystems
- Government backing and standards are currently in exploratory phase only
- Can facilitate money laundering, crime
- Currently cannot support a large number of transactions and is not fast enough

Increased Investment

Cumulative VC Investment in Virtual Currency & Blockchain Tech (USD millions)



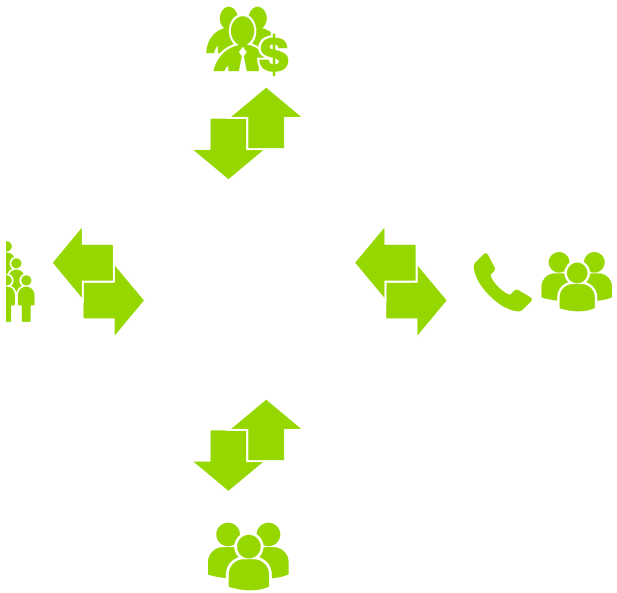
Blockchain challenges – Regulatory

- KYC – Know Your Customer?
- Central Regulation – There is some good to it?
- Judicial System?
- Interoperability
- Legacy process and regulations

USE CASES

03

Smart cities



- *Smart Sovereignty and Provenance*
- *Smart Healthcare*
- *Productivity & Environment Sustainability*
- *Smart Contracts*
- *Critical Infrastructure Supply Chain Traceability*
- *Smart Real Estate*

Smart Sovereignty and Provenance

Counterfeit Product Detection

= 79054025
255fb1a2
6e4bc422
aef54eb4

- Decentralized detection and control of the counterfeit drugs problem
- Smart tracking of quality of product and manufacturing
- Tagging enables physical objects to be represented virtually; tags (e.g., QR codes) can be securely hashed onto a blockchain
- Tags/codes used for counterfeit product detection today
- Blockchain as: world-wide tracking with auditability and without undue infringement of privacy

Reduced Criminal Activity

- Code hidden at point of sale
- Revealed code checked for legitimacy & “freshness*”
- Alteration of code destroys value
- Protect against code reuse

Electronic medical records and health insurance – Making systems Interoperability a Reality

Problems with handling medical records today

Lack of interoperability:

- Current systems generally disconnected from one another – resulting in significant cost and delay (e.g., due to inefficient manual processes) when patients change healthcare providers
- Payer and provider systems are disconnected from one another as well

Attack Surface:

- Centralized healthcare data (maintained in on-site repositories powered by physical servers or on an IT cloud) and heightened vulnerability to security breaches (theft as well as potentially undetected modification/falsification)

Role of block chain

Enablers

- Hospital and Med. Centers Visit-Management
- Peer to Peer Insurance System Mgmt.
- Medical Data Collection and Quantification
- Peer-based Mediation and Legal System
- Paying Ransom when Access is denied

Linkages

Productivity and environmental benefits – Sharing resources

Ride-Sharing

- Fair real-time pricing/rewards:
  - Eliminate middle-man; e.g., just drivers and passengers

Traditional contracts	Smart contracts
1-3 Days	Minutes
Manual remittance	Automatic Remittance
Escrow necessary	Escrow may not be necessary
Expensive	Fraction of the cost
Physical presence	Virtual presence
Lawyers necessary	Lawyers may no be necessary

Smart contracts

Sign lease and insurance contracts:

DocuSign → Pay DocuSign With DocuSign Block chain Cryptocurrency DocuSign

Smart contracts – Simple to complex

Digital value exchange	Smart right and obligation	Basic smart contract	Multiparty smart contract	Distributed autonomous business unit	Distributed autonomous organization	Distributed autonomous government	Distributed autonomous society
A family member sends some bitcoin to another family	Consumer buys a digital content stream	Landlord remotely locks nonpaying tenant out of apartment	Seller lends buyer funds to buy house	Unit of a corporation issues its own bonds, and buyers monitor payments via a shared ledger	Self-driving trucks make P2P deliveries, pay local toll road fees, and buy local electricity	Settlers of a previously uninhabited area code their own self-enforcing government services	Groups of settlers from different areas establish self-enforcing trade agreements

Simple → Complex

Real estate transactions example

Alice

1) **Real estate agent** Alice enrolls and receives **transaction certificates:** *embedded identity, real estate license, and current rating*

3) Alice submits a **transaction** that includes a **link to listing data, hash(listing data),** and **minimum buyer criteria;** this transaction or follow-up transactions can include available/ unavailable date-time appointment slots

Bob

2) **Potential buyer** Bob enrolls and receives **transaction certificates:** *pre-qualification/pre-approval plus price level, and photo ID*

4) **If** Bob **is interested** in Alice**'s listing,** he submits a transaction to set up an appointment to review the property; his photo and appointment request are selectively released to Alice within the transaction –if Bob's transaction is accepted for inclusion in the blockchain

At the appointment date-time: if Bob**'s photo on the blockchain matches the image from the property's camera,** Alice **remotely activates the door unlock and video-calls** Bob **to begin the property tour**

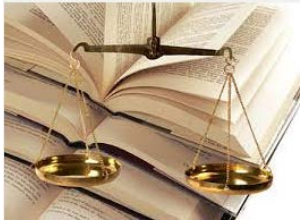
SURMOUNTING BARRIERS AGAINST BLOCKCHAIN

Healthcare BARRIERS – Managing contractual corrections

HIPAA
Health Insurance Portability and Accountability Act

HEALTHCARE BARRIERS	
Barrier Root Cause	"Many hospitals are unwilling to digitally sign some documents because the codes that HIPAA mandates may need to be manually corrected, and those corrections will break a digital signature."
Surmounting the Barrier	■ Instead, such modifications can (and should) be captured in additional digital signatures/follow-on transactions

Juridical BARRIERS – Managing jurisdiction-specific privacy laws



BARRIERS	
Barrier Root Cause	Recording certain types of transactions in a public ledger may be disallowed in a given country because of privacy laws
Surmounting the Barrier	■ Access to confidential data may be restricted within a permissioned blockchain ■ A public blockchain may include one-way hashes of confidential data, where access to that data is controlled; the database(s) containing such data can be (partially or totally) purged, if necessary

Financial transaction BARRIERS – Managing transactional recourse

BARRIERS	
Barrier Root Cause	"It's possible to undo lots of transactions in our current legal environment. Reversing charges on credit cards is possible, for example, and is a desirable feature of our current system."
Surmounting the Barrier	■ Immutability does not imply inability to reverse a transaction via a follow-on linked transaction ■ Blockchains can be made interoperable with legacy systems such as credit card processing

Final Takeaways

Final Takeaways

- Understand your use case
- Understand local and global regulatory impact
- Perform a detail Current Vs New process analysis
- Don’t overlook the anomalies
- What’s the trend in your organization? - Are you an early adaptor?

Thank you