Block Chains and Applications

Daniel J. Mashao, PhD

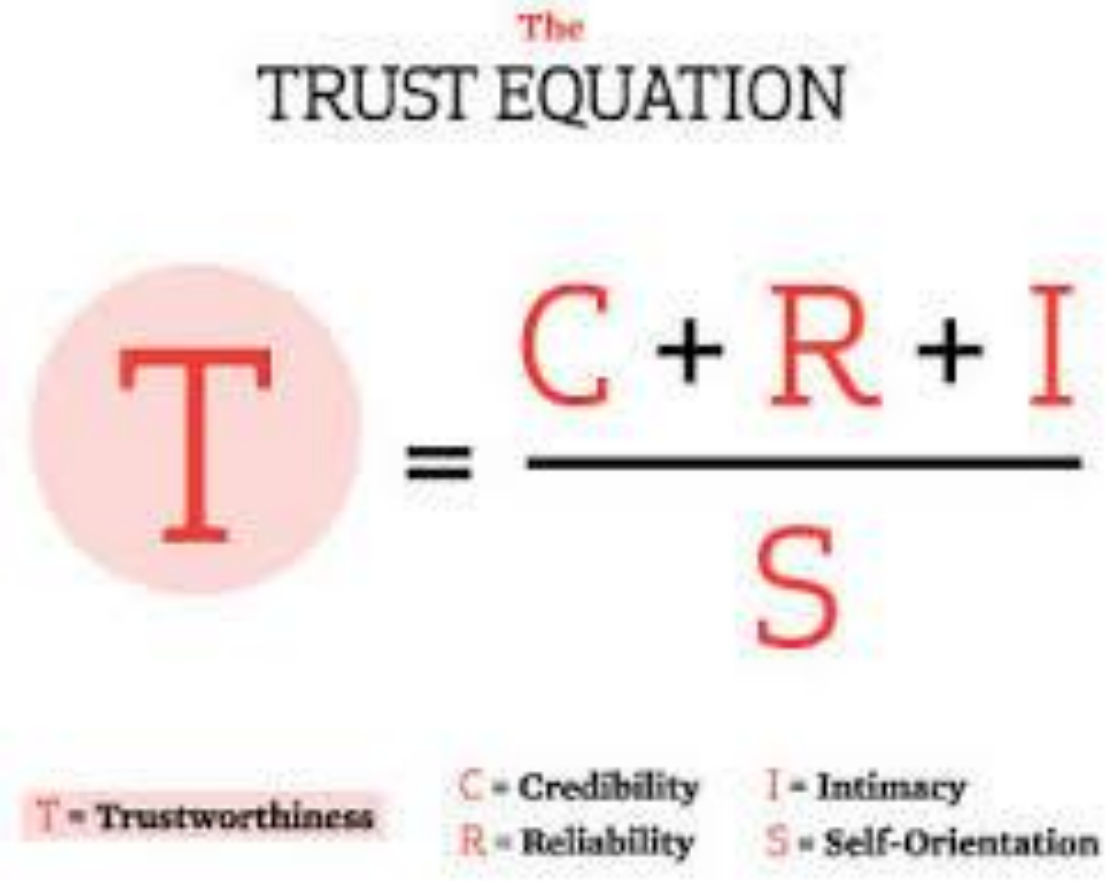
State Information Technology Agency (SITA), reporting to the Ministry of Telecommunications and Postal Services

16 October 2016

SITA

stateinformationtechnologyagency

Alternative Title of This will



SITA
stateinformationtechnologyagency

What is Trust?

Trust is CRII over ME

Trust = Credibility*Reliability*Integrity*Intimacy/ME

If ME is too high, that reduces Trust; If I get the sense that you are interacting with me with only yourself in mind, then that lessens trust

Higher the credibility, the reliability and the Integrity the higher the trust.

SITA
stateinformationtechnologyagency

TRUST

There are many things you will not be able to do without Trust

You cannot leave your home, unless you have faith that you will come back safely,

Lack of trust may allow you to engage in small things, but not big things

SITA
stateinformationtechnologyagency

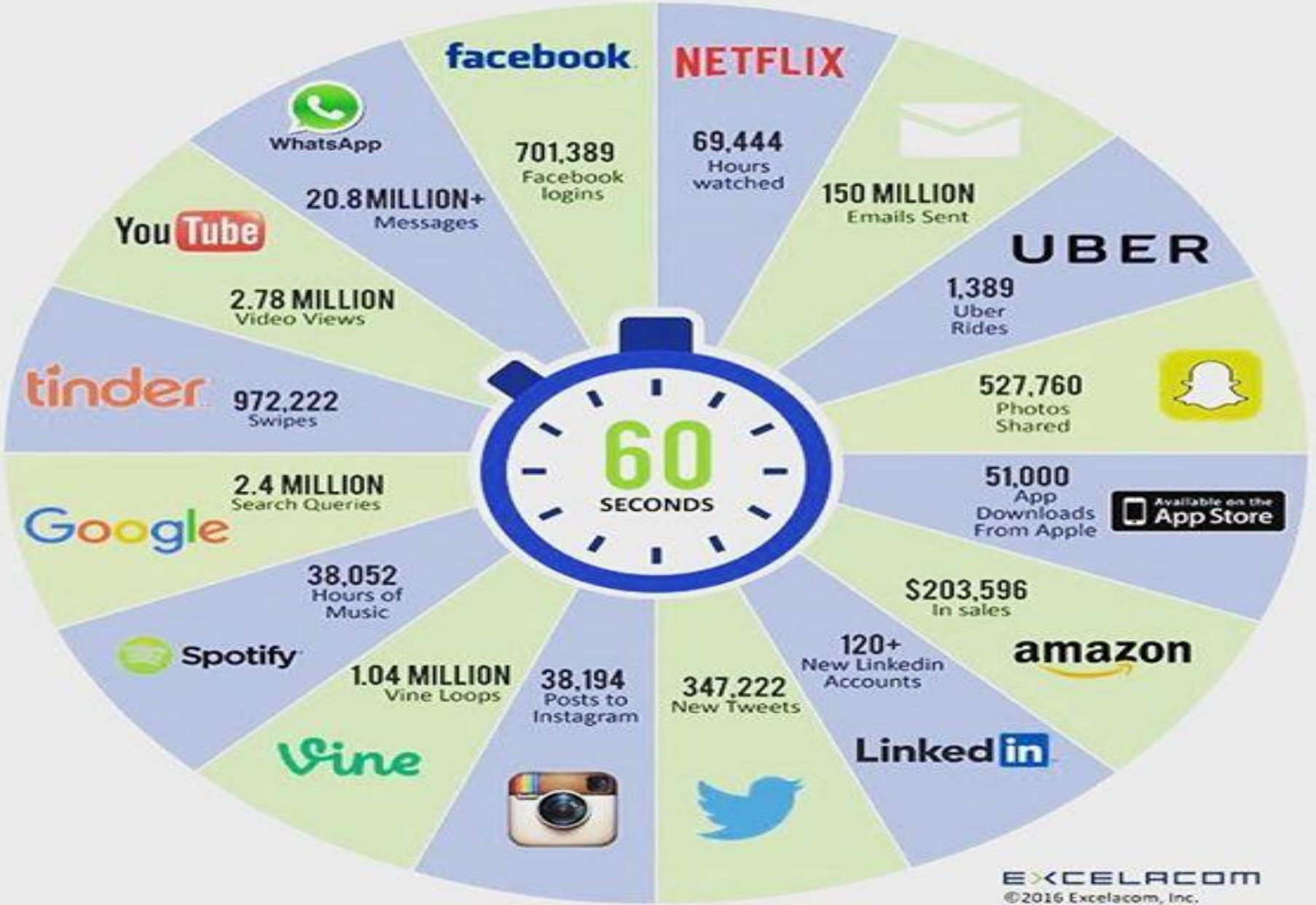
INTERNET as we Have it Currently

Internet is about connectivity, you do not know who is connecting with you and you may not know their intentions

To connect you do not need to trust, but to transact you will need to have trust

SITA
stateinformationtechnologyagency

2016 What happens in an INTERNET MINUTE?



EXCELACOM

©2016 Excelacom, Inc.

Trust is now in Fashion

Applications that are trending and actually uses Trust

1. Uber

   Get into a taxi; you can trust that in addition to convenience
   Someone is monitoring the taxi driver, someone knows that they are genuine
   There are other people reviews of the taxi driver, etc

2. Airbnb

   Sleep in strangers home;
   You can get reviews about other people previous experience

The role of trust is critical and there is a level of comfort that is being introduced

SITA
stateinformationtechnologyagency

Examples of Trust

Uber

Software company

UBER

uber.com

Uber Technologies Inc. is an American worldwide online transportation network company headquartered in San Francisco, California. Wikipedia

Headquarters: San Francisco, California, United States

Founded: March 2009, San Francisco, California, United States

CEO: Travis Kalanick (2011–)

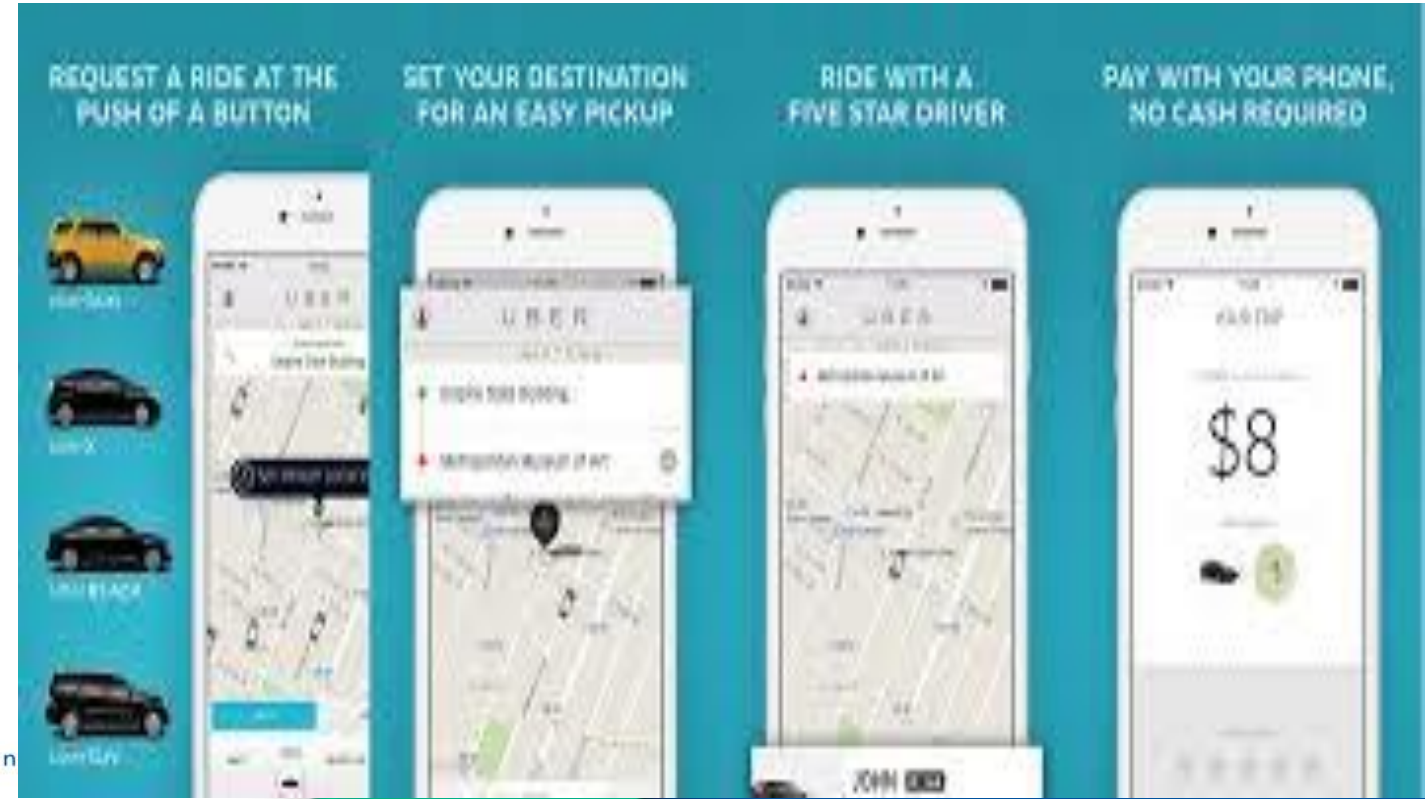
Revenue: 1.5 billion USD (2015)

Founders: Travis Kalanick, Garrett Camp

SITA
stateinformationtechnologyagency

Five star driving rating

- ★ I wouldn't want to be a passenger in your car!
- ★★ There's room for improvement. Quite a lot of room, in fact
- ★★★ You're mid-table, which is fine, but who really wants to be average?
- ★★★★ Almost perfect, safety could almost be your middle name
- ★★★★★ Perfection to a tee, great acceleration, cornering and braking



SITA
stateinformationtechnologyagen

Example of Trust

Airbnb, Inc.

Company

Airbnb is a peer-to-peer online marketplace and homestay network that enables people to list or rent short-term lodging in residential properties, with the cost of such accommodation set by the property owner. Wikipedia

Headquarters: San Francisco, California, United States

Founded: August 2008, San Francisco, California, United States

SITA
stateinformationtechnologyagency

Model of Trust Currently

The current model of trust is based on having some sole authority; a central server or system that can give authority

Single point of failure is introduced

SWIFT System used by Banks

The **Society for Worldwide Interbank Financial Telecommunication** (**SWIFT**) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment

SITA
stateinformationtechnologyagency

SWIFT as an Example of a Single Authority

Society for Worldwide Interbank Financial Telecommunication

Type	Cooperative
Industry	Telecommunications
Founded	1973; 43 years ago
Headquarters	La Hulpe, Belgium
Key people	Yawar Shah (Chairman); Gottfried Leibbrandt (CEO)
Products	Financial Telecommunication
Number of employees	>2000
Website	www.swift.com

TECH › CYBER SECURITY

Standard Bank computer was hacked in R300m ATM fraud hit - report

2016-06-30 11:03 - Gareth van Zyl, Fin24

POST A COMMENT 0

SHARE:

Johannesburg - Investigators have reportedly discovered that a Standard Bank South Africa computer system was hacked in a R300m ATM fraud hit in Japan.

This is according to a report by the Japan News, which was carried by the Chicago Tribune this week.

SITA
stateinformationtechnologyagency

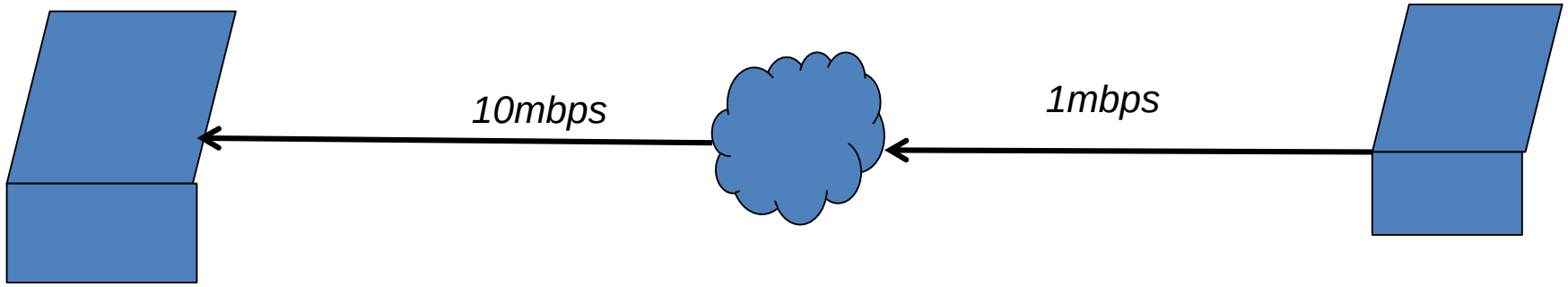
What is Special About Block Chains and Bitcoins

1. Trust built from common internet technologies
2. Decentralized authorization
3. Provable confidence

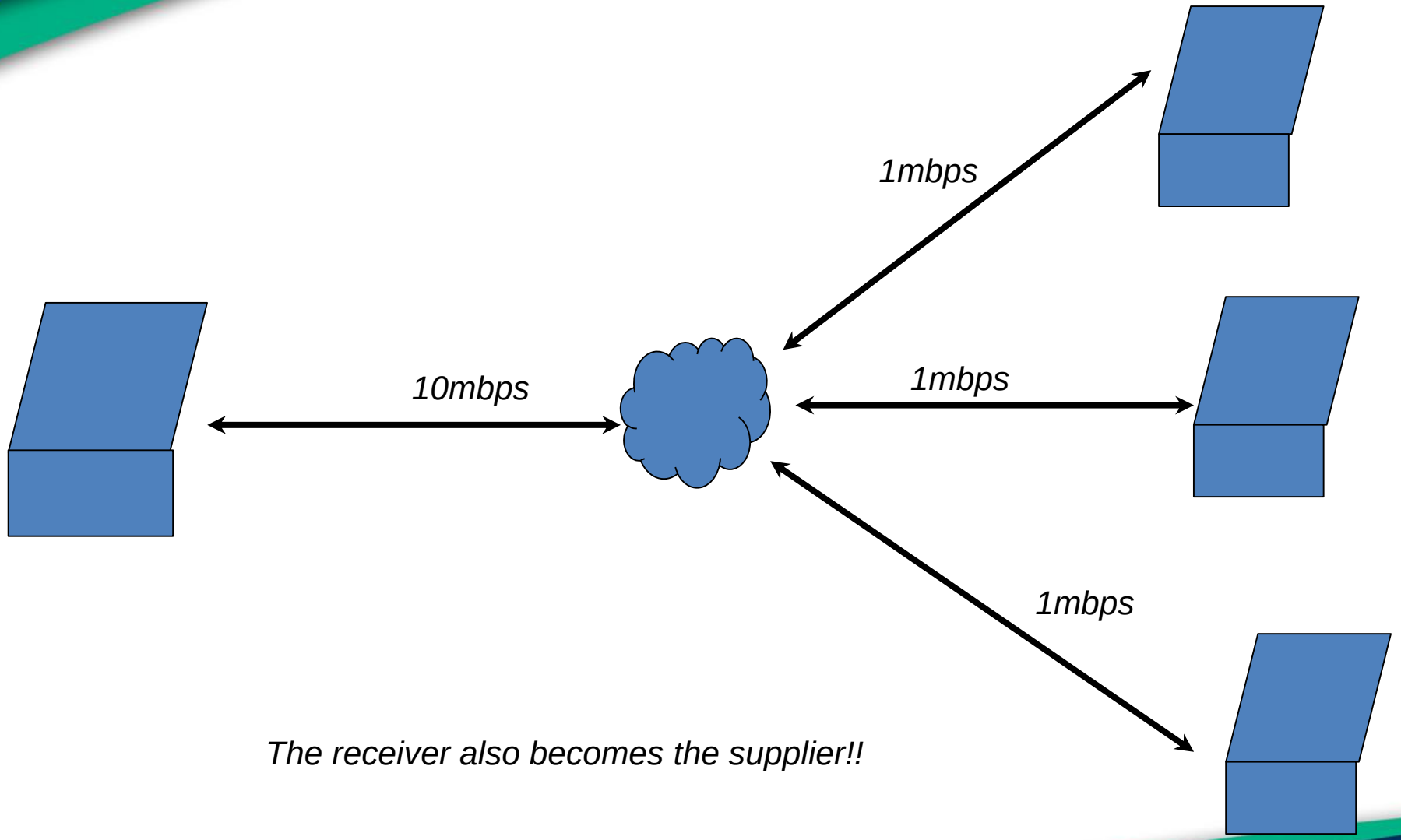
SITA
stateinformationtechnologyagency

Bittorent: A communications protocol for peer-to-peer file sharing

Typically used to download large files



With BitTorrent

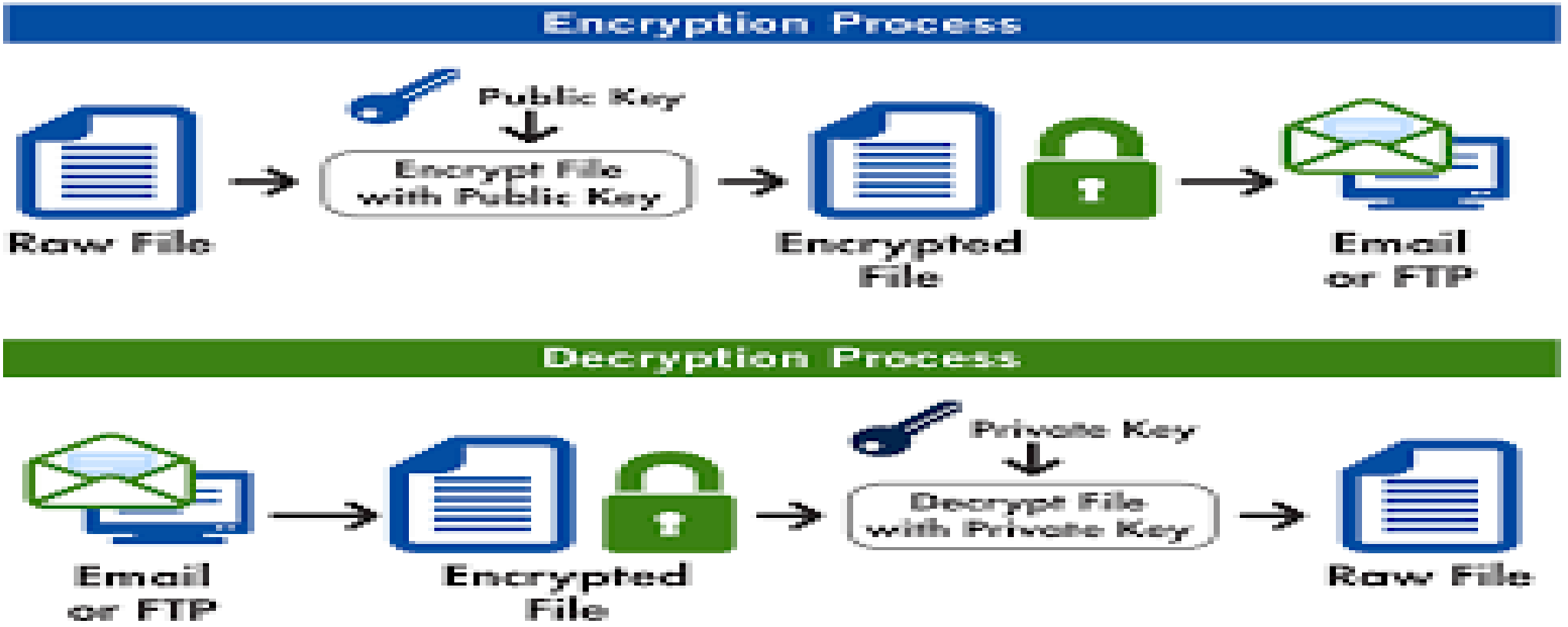


The receiver also becomes the supplier!!

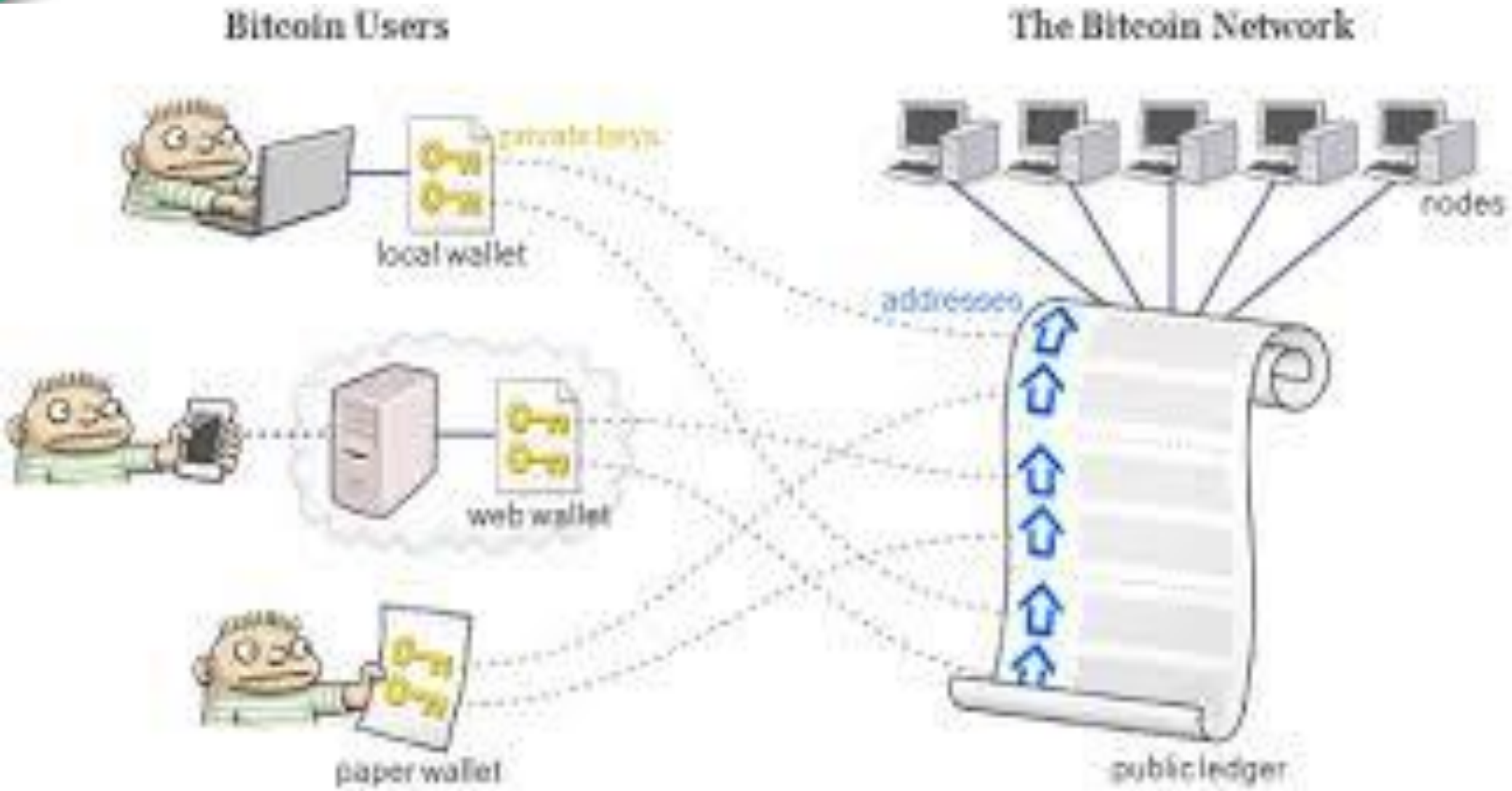
SITA
stateinformationtechnologyagency

Pretty Good Privacy: Private-Public Key Infrastructure

Allows you to send information/messages that can be read by only the intended recipient and no one else who does not have the recipient private key.



Public Ledger



Block Chains System

Now a transaction has to be provided to several servers to check for accuracy and to check that the Bitcoin is valid.

This check is done by bit-miners;

The first bit-miner is rewarded for discovering that the transaction is valid.

SITA
stateinformationtechnologyagency

BITCOIN BASICS: HOW IT WORKS

BOB

ALICE

Bob owes Alice money for lunch, so he picks up his smartphone and opens his Bitcoin smartphone app.

To pay her, he needs two pieces of information: his private key, and her public key.

Bob gets Alice's public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.

Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.

The app alerts Bitcoin "miners" around the world of the impending transaction.

The miners verify that Bob has enough bitcoin to make the payment.

Miners race to bundle data from the pending transaction with other unrecorded transactions, plus the last block of transactions recorded in the public ledger, as well as a random number known as a nonce.

Then the miner applies a mathematical function known as a hash, which produces a unique cryptographic "fingerprint" that makes transactions verifiable.

The hashed block must have a certain, but arbitrary, number of zeroes at the beginning. It's unpredictable which nonce will produce a hash with the correct number of zeroes, so the miner has to keep trying different nonces to find the right value.

When a miner finds a hash with the correct number of zeroes, the discovery is announced to the rest of the network. Other miners communicate their acceptance when they turn their attention to finding the next block, with the newly made block as a component.

The algorithm rewards the winning miner with 25 newly created bitcoins, and the hashed block is published in the public ledger.

Within 10 minutes of Bob initiating the transaction, he and Alice each receives the first confirmation that the bitcoin was signed over to her.

The parties receive several more confirmations as th block that recorde their transaction is embedded into subsequent blocks

POTENTIAL USES OF BLOCK CHAINS

Financial	Public Records	Private Records	Semi-Public Records	Physical Assets Keys
Currency	Land titles	Contracts	Degrees	Home Keys
Private Equities	Vehicle Registries	Signatures	Learning Outcomes	Vacation Home
Public Equities	Business Licence	Wills	Medical Records	Hotel Rooms
Bonds	Criminal Records	Trusts	Genome Data	
Spending Records	Passports	Escrows		
Trading Records	Certificates	GPS trails		
Crowd Funding	Permits			

List from http://www.the-blockchain.com/potential-uses-of-blockchain/

SITA
stateinformationtechnologyagency

Applications in Government

1. Declaration of Interests [Government] – SITA has developed an app that allows civil servants to declare their interests online. Block chains can add the signature of the manager to confirm that the supervisor has reviewed block chains
2. SASSA Grants [Government]– these are meant to assist children; parents could be using them for other things. The grants can be provided in the form of block chains so that they can be traced for what they were used for. Nearly like DOA
3. Company rewards [SITA]; to ensure that rewards can only be used in the company
4. US Food Stamps

Some of the Benefits of Block Chains

1. Trust less lending
    1. Strangers can lend you money over the internet; they do not have to trust you.
2. Reduction in Litigations
    1. 57% of litigations (44% in US) in UK is about contract disputes; smart contracts done with block chains can provide irrefutable evidences e.g. when was contract changed and what was the change [reference 54 in Blockchains]
3. Title deeds for Houses and Motor Vehicles
    1. Ideally suited to Block chains. – enable speedy transactions

SITA
stateinformationtechnologyagency

THANK YOU

SITA

stateinformationtechnologyagency