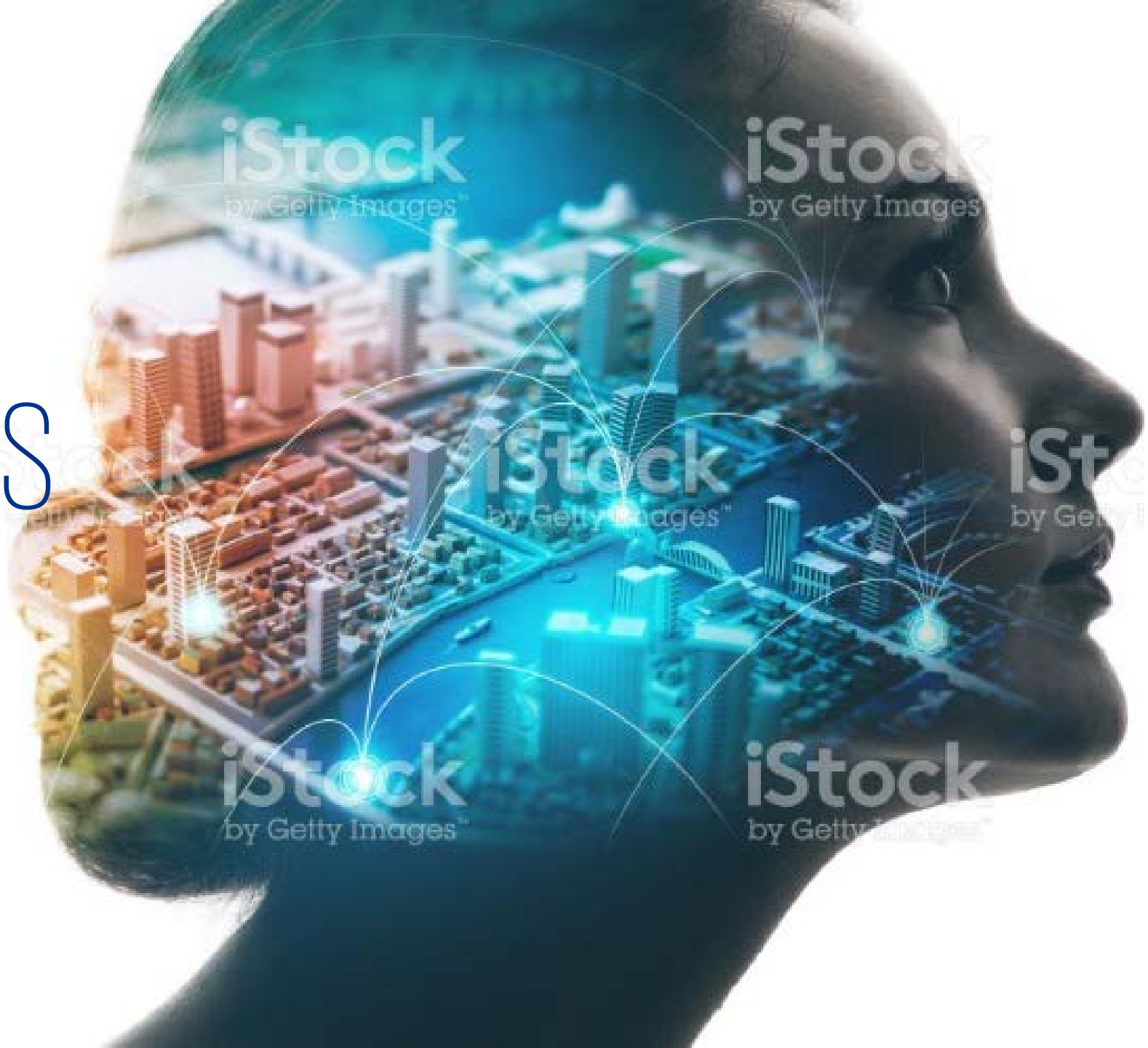
KPMG

Disruptive Technologies



Presented by

Muhanna Almarahleh

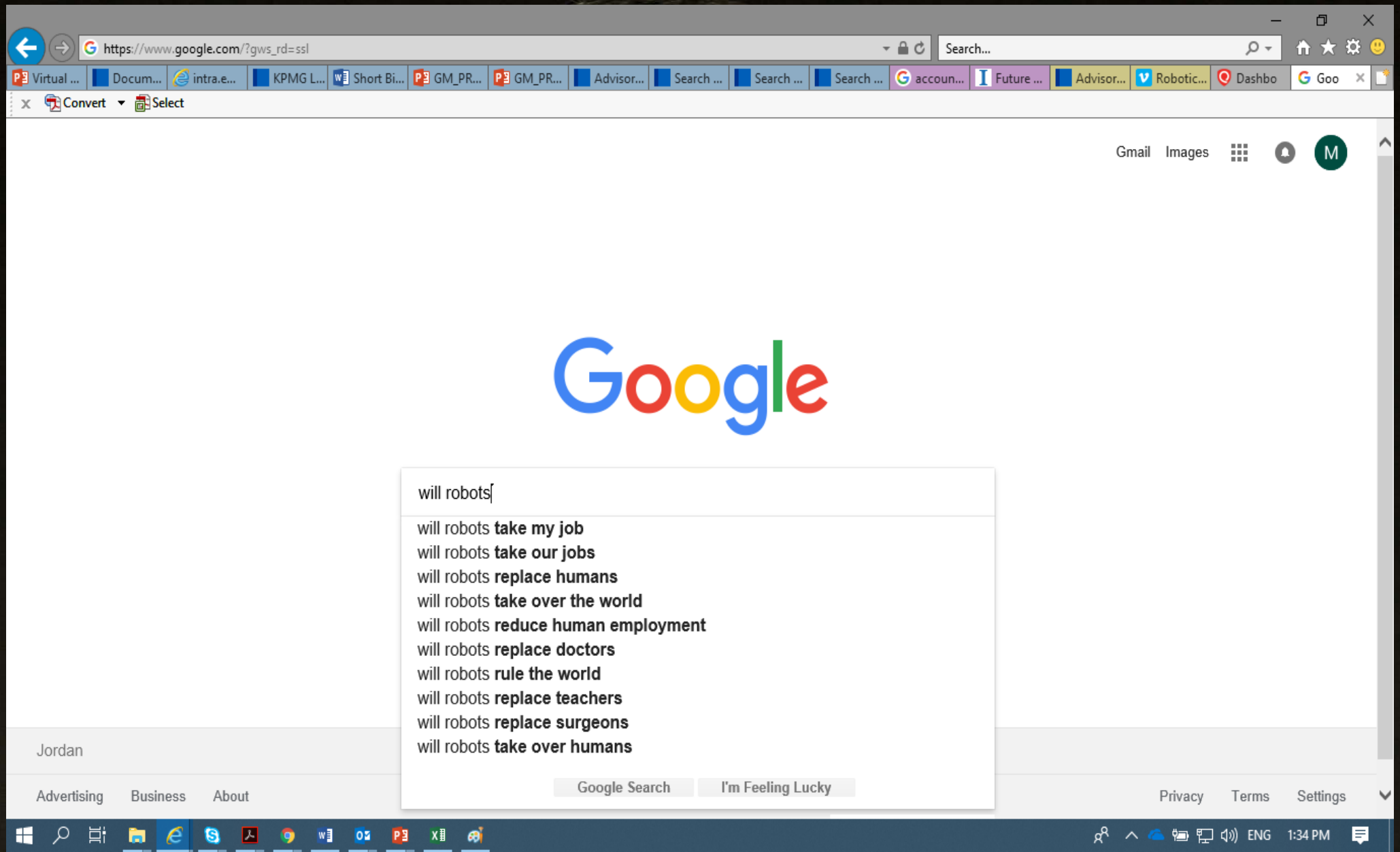
Robotics

"AI is one of the most important things humanity is working on. It's more profound than electricity or fire.

—

Sundar Pichai

Will Robots?

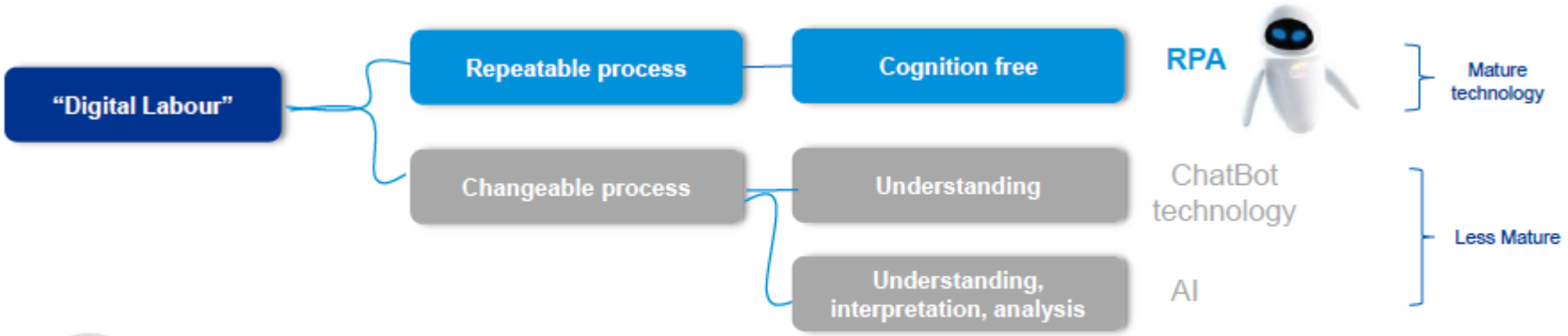

https://www.google.com/?gws_rd=ssl
Search...
Convert
Select
Gmail
Images
Google
will robots
will robots take my job
will robots take our jobs
will robots replace humans
will robots take over the world
will robots reduce human employment
will robots replace doctors
will robots rule the world
will robots replace teachers
will robots replace surgeons
will robots take over humans
Google Search
I'm Feeling Lucky
Jordan
Advertising
Business
About
Privacy
Terms
Settings
ENG
1:34 PM

By 2030 Robot automation will 'take 800 million jobs - BBC report

Report finds 38% of US jobs will be automated by 2030


"
With Artificial Intelligence we are summoning the demon.
—
Elon Musk

Robotic Process Automation (RPA)

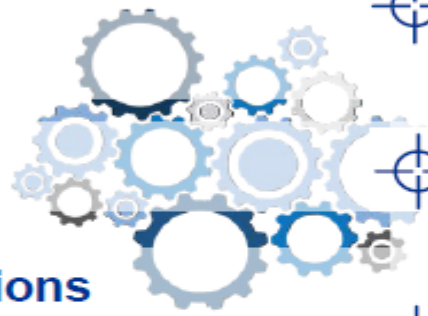


- **RPA is about basic task automation**
- **It is one technology of many that enable what we now call 'Digital Labour"**
- **Driven and used by process analysts, not "techies"**
- **Integrated into workflows; automates stages and facilitates handoffs**

© 2018 KPMG, an Irish partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

Where RPA thrives & expected outcomes

- Stable process
- Repetitive
- High volume
- Multiple staff
- Pre-determined decisions



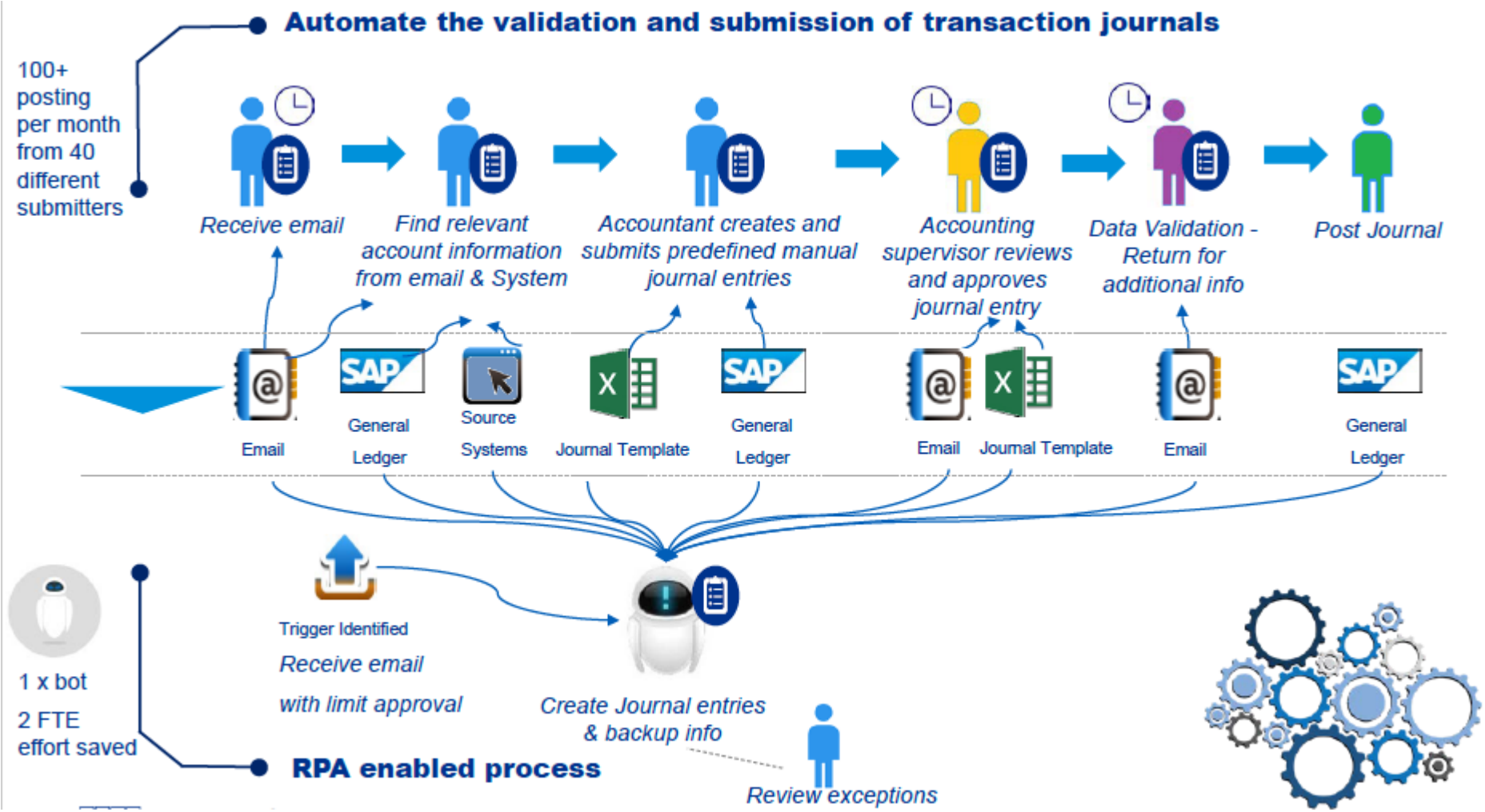
- Improved error rates, scalability, throughput, security, compliance
- 30% to 70% process improvement
- Released human labour for higher value activity
- Savings of 3 to 5 FTE per bot

"Potential economic impact of nearly $6.7 trillion by 2025"

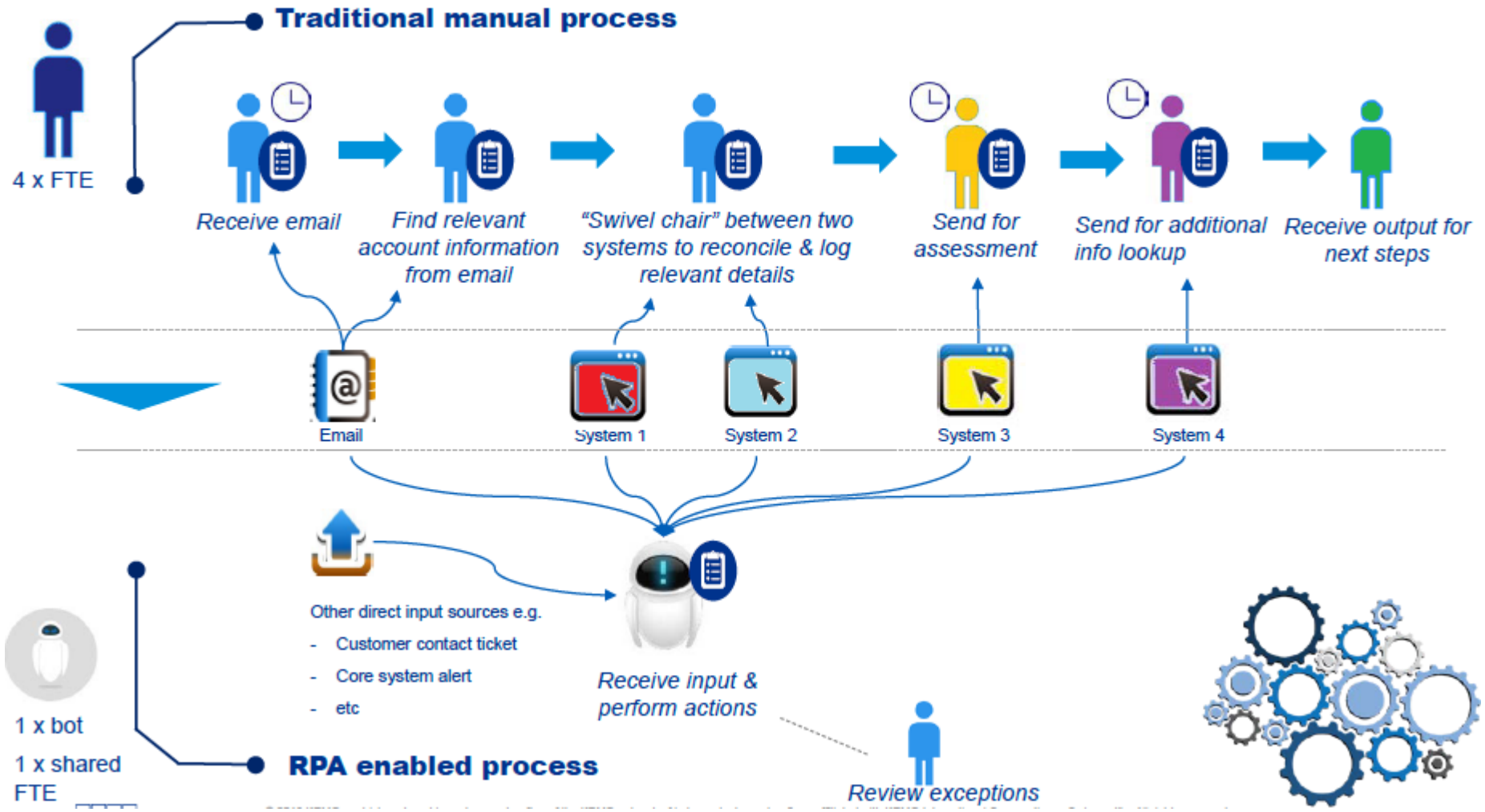
"Second largest economic impact behind mobile Internet"

RPA Opportunities in Finance

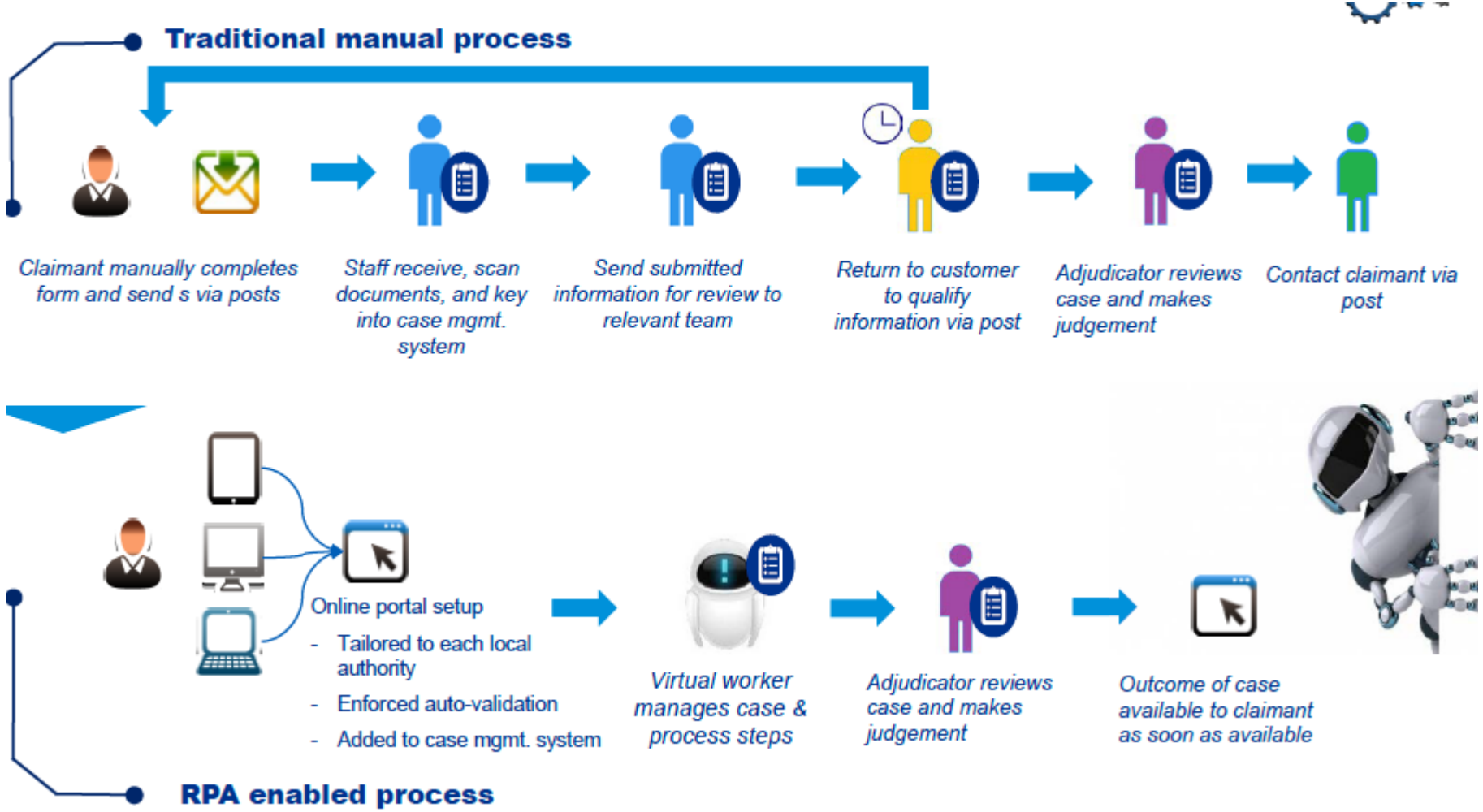
Use Case: Journal Entry -Professional Services Client



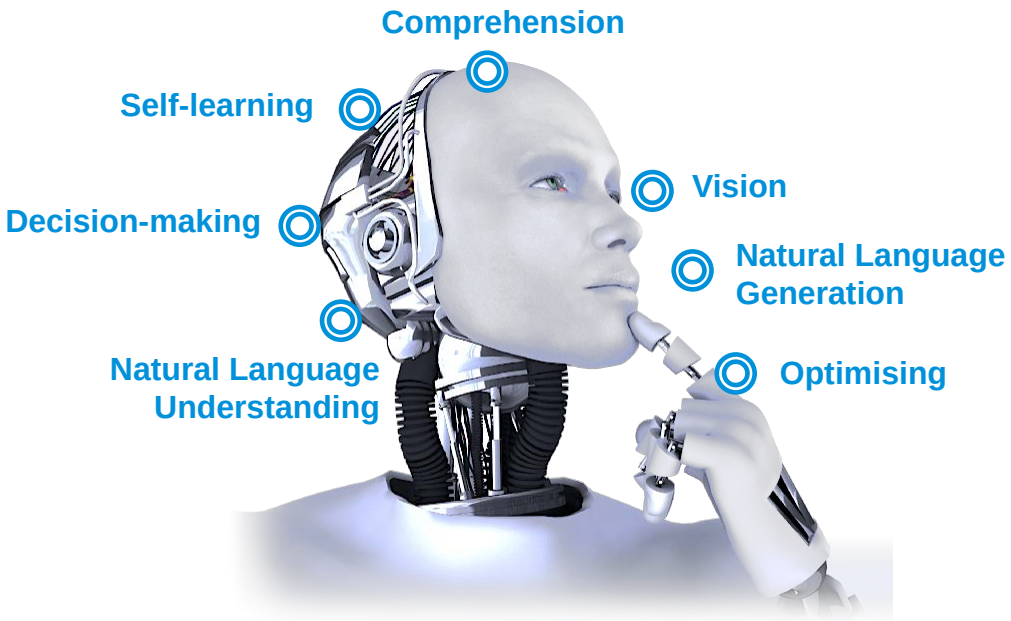
Use Case: Accounting Reports -Professional Services Client



Non-FS Example -Parking Ticket Appeals



Artificial intelligence expands the spectrum of human cognitive capabilities



Traditional Systems

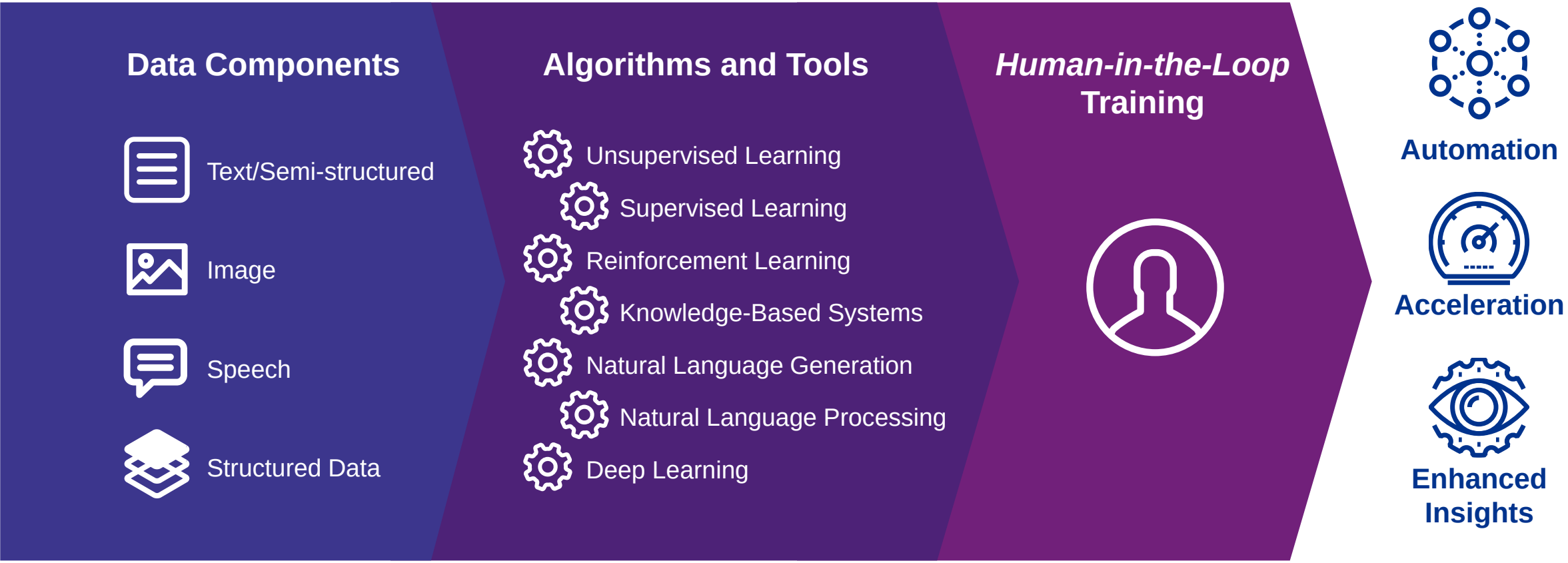
- Programmed with rules
- Structured data
- Binary logic

AI Systems

- Trained with examples
- Non-traditional data
- Natural Interaction
- Probabilistic

Building blocks of AI Systems

Artificial intelligence is the practice of employing advanced analytical techniques and algorithms to train computers how to use data from a wide variety of sources and formats to enhance, accelerate, and automate decisions that drive growth and profitability.



...and value is only realised with the 'human in the loop'

This vision of AI expanding the spectrum of human cognition and capabilities can only be realised when the technology is paired with the ability to develop and train the algorithms to address specific problems.

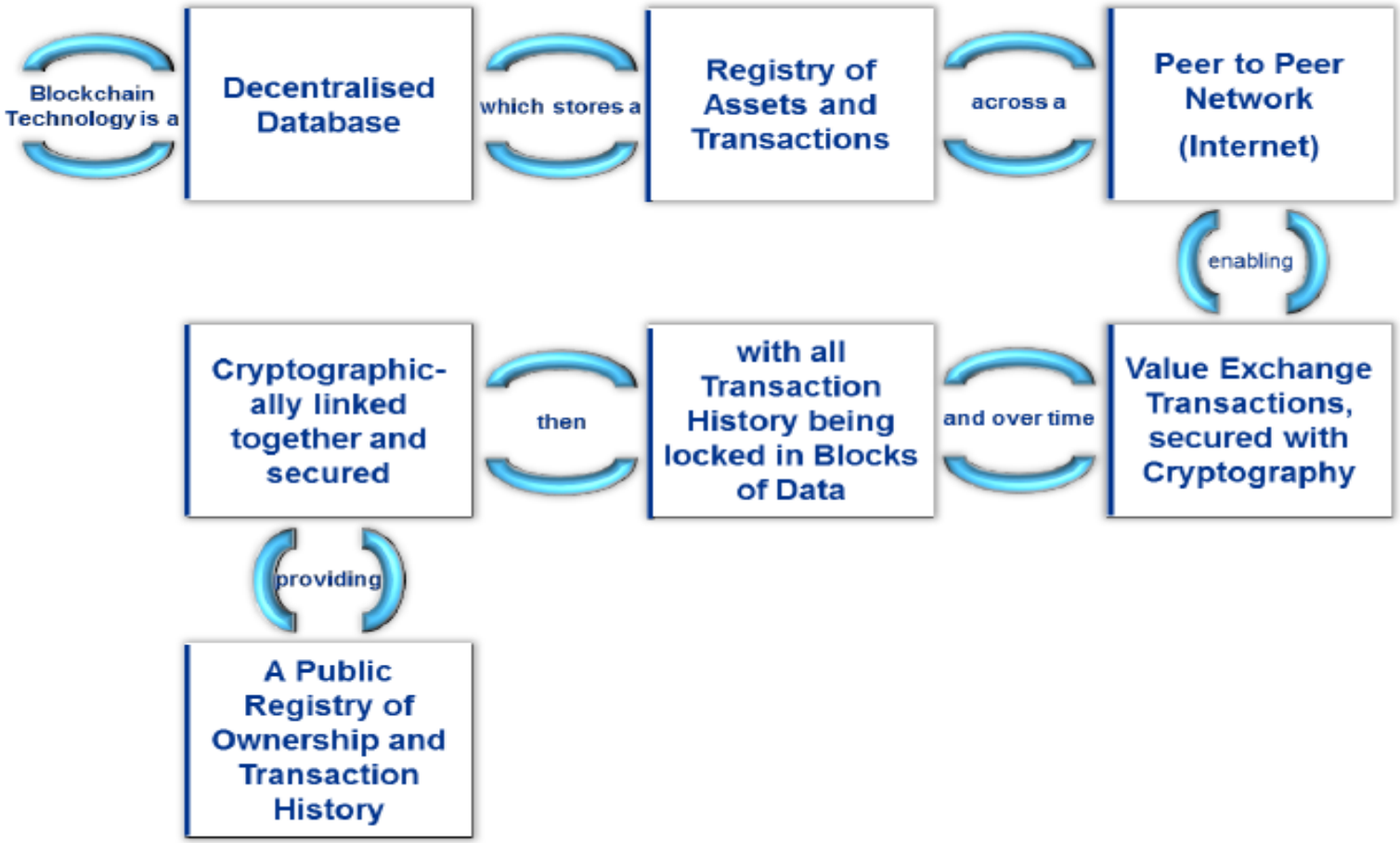
Blockchain

WARNING: Blockchain is slightly more complicated than your typical disruptive technology. May contain traces of cryptography and other concepts that challenge the status quo. Not suitable for all use cases.

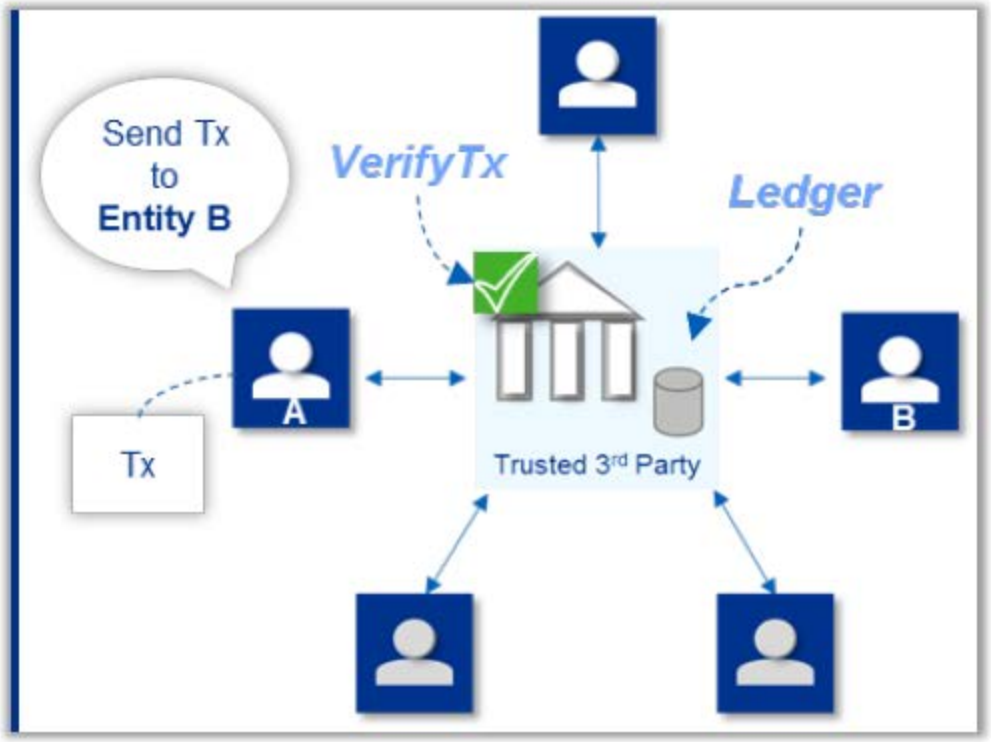
Blockchain *a.k.a.* Distributed Ledger Technology (DLT)

- A **potentially game changing** technology
- Early adopters are **crypto-currencies** such as **Bitcoin**
- However, it is likely that DLT will have greater adoption, acceptance and impact in other areas such as **Supply Chain, Digital Identity, Provenance** and **Asset Tracking, Voting** and **User Experience in Digital Channels**

The Blockchain

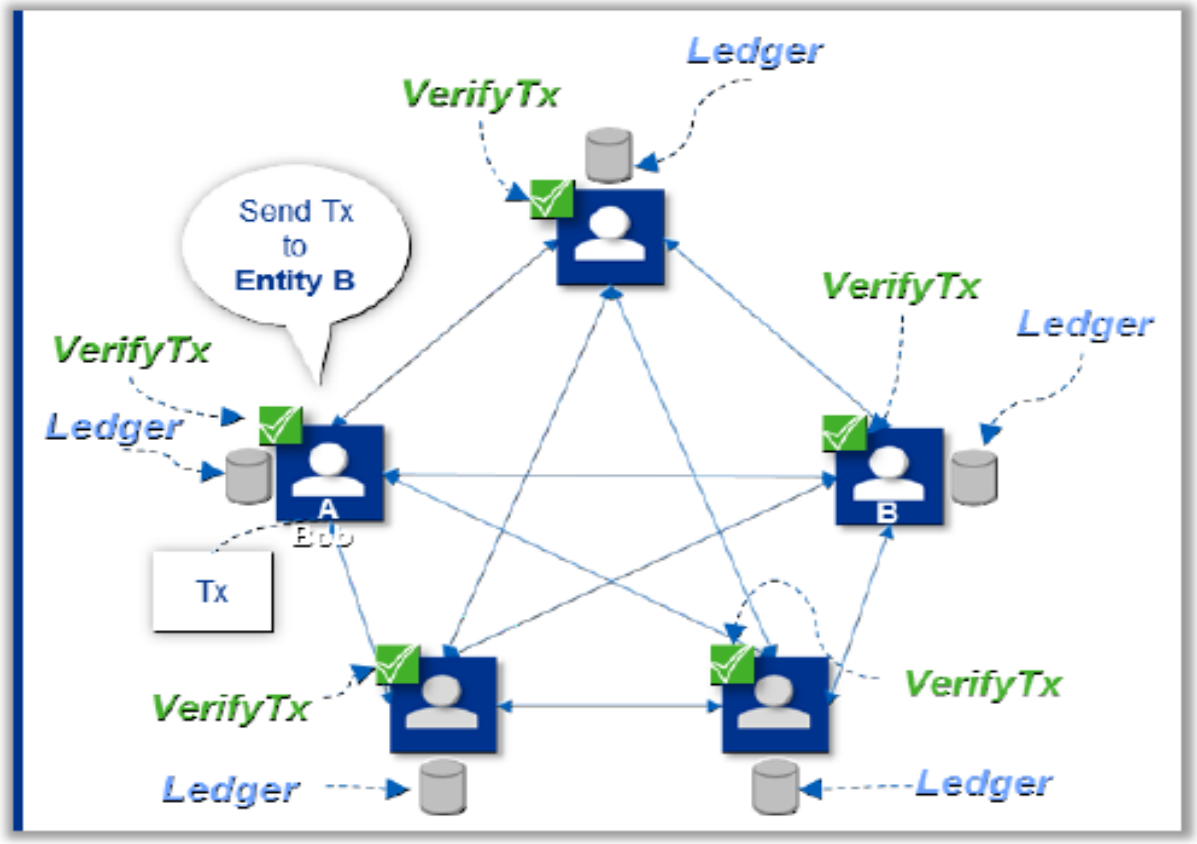


Existing Model of Trust -Centralized



- The exchange of digital value today relies on **trusted 3rd parties** such as Regulators, Banks and Corporations
- These 3rd Parties act is **intermediaries** to establish trust between un-trusted parties, e.g. entity A to entity B
- **Time (delay) and cost** are introduced to the transaction, i.e. processing times and transactions charges.
- They manage and protect a **central ledger** and all transaction history
- For the most part these ledgers and transaction histories are kept private

A New Model of Trust -Decentralised



- All users on the network are **connected to each other**, each having a full copy of the ledger
- All new **transactions are visible** on the network
- The **network verifies** all transactions (Consensus)
- Verified transactions are combined **and new blocks of data are created** for the ledger
- As new blocks are created they are simultaneously **replicated across the network**
- Transactions can support many use cases where **sharing information, exchanging value or changing asset** ownership is important. The blockchain proposition is that the transaction, for whatever reason, can be **trusted.**

A New Model of Trust -Decentralised

A **Blockchain** allows **untrusted parties** to reach **consensus** on a shared digital history, **without a middleman**

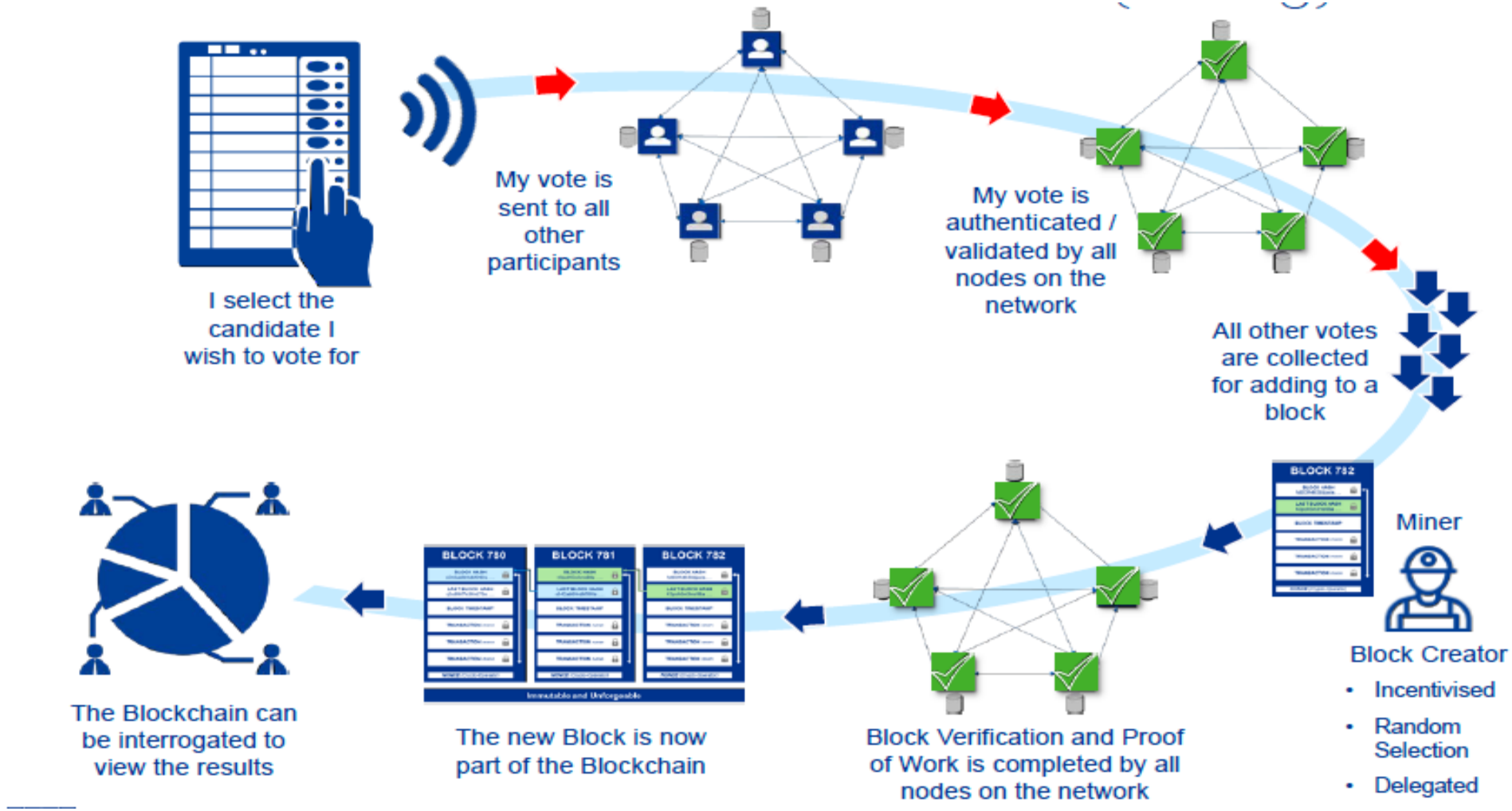
- **Peer to Peer**

- **Decentralised**
- **No central authority or oversight**
- **Everyone holds a copy, no SPOF**

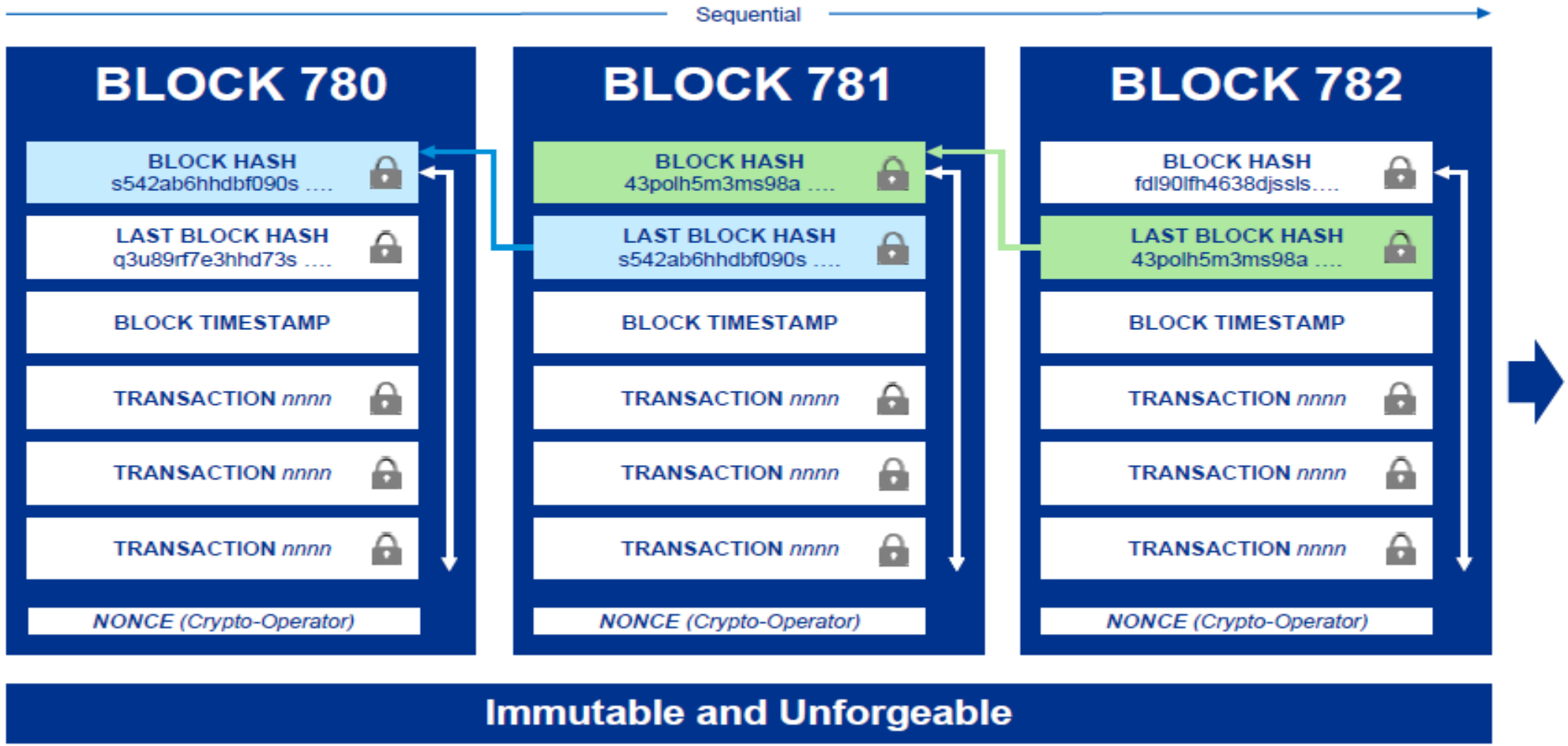
- **Records are added, never changed**
- **Entire history contained on the chain**

- **Use of cryptography**
- **Immutable**

Blockchain Transaction -How it Works (Voting)

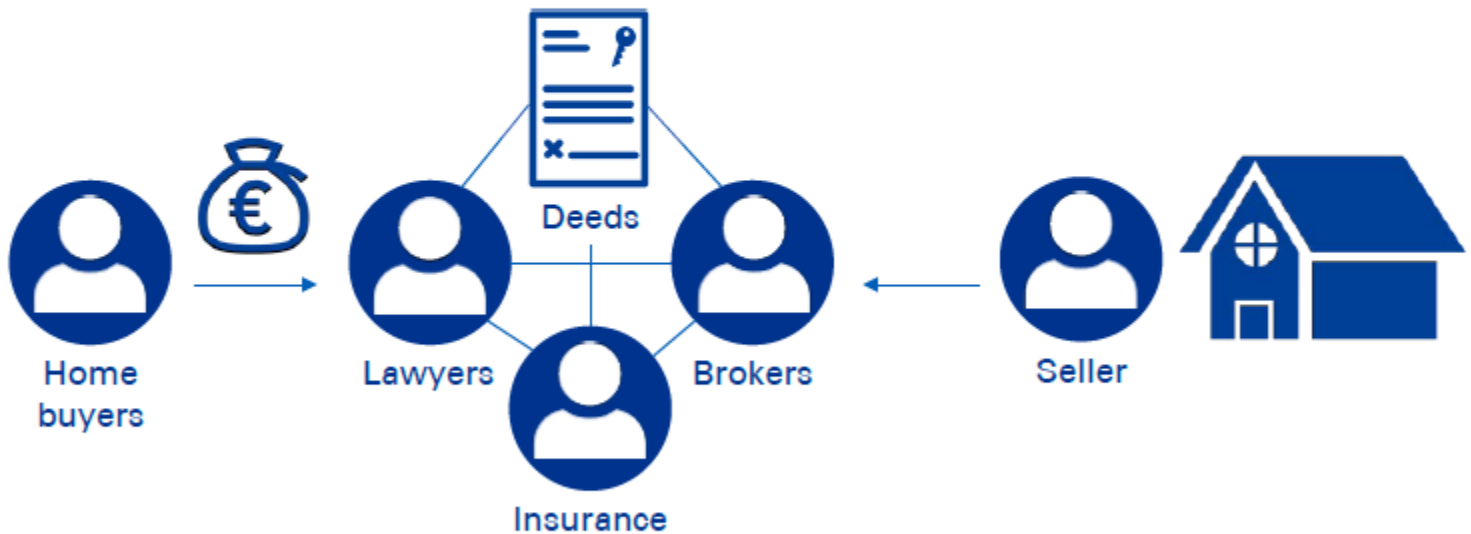


The Block in the Blockchain



Use Case: Land (Asset) Registry

Current State

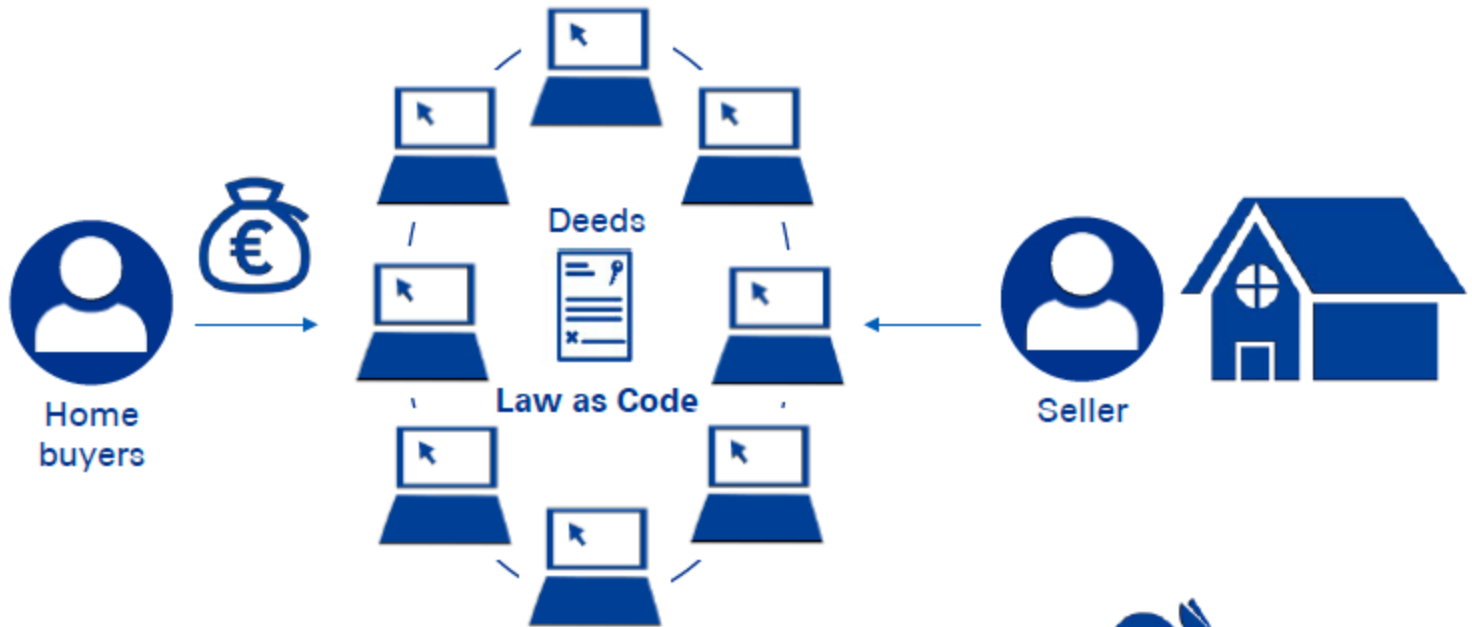


Weeks / Months / Years

Complex | Handoffs | Lengthy Duration | Transparency Issues | Costly | Ownership Issues

Use Case: Land (Asset) Registry

Block-chain enabled Digital Asset Registry – Real Estate tied to a digital token



Simplified | No Handoffs | Rapid Execution | Transparent | Reduced Cost | Immutable Record

Challenges

Scalability ?
Theoretical maximum of seven transactions per second for the entire system, plus the need to replicate the entire ledger in every node in the network

A Fundamental Shift ?
An architectural foundation that is diametrically opposed to the current mechanism of commercial facilitation that is more than 300 years old.

Value ?
Gaining acceptance that a 'Digital Token' has any value in the first instance

Heritage ?
Unclear heritage, Satoshi Nakamoto?

Association with ?..
Illegal activities, e.g. Dark Net

Volatility ?
Volatility in value against traditional FIAT currencies

Regulation ?
ICOs / Securities ??

Security ?
Hackers have created malware to mine currencies including Bitcoin

Consensus ?
It is the majority of "hashpower" (the computational resources used in data mining), not the number of distinct nodes on the network that informs consensus.

This means that a single sufficiently powerful entity on the network can "outvote" the rest of the nodes

Speed ?
A minimum delay of 10 minutes in confirming transactions

Governance ?
Open-source code maintained by a small group, with many fragmented allegiances, divergent ideologies and motives

Contradiction ?
with respect to existing legal, regulatory, accounting and taxation frameworks and rules

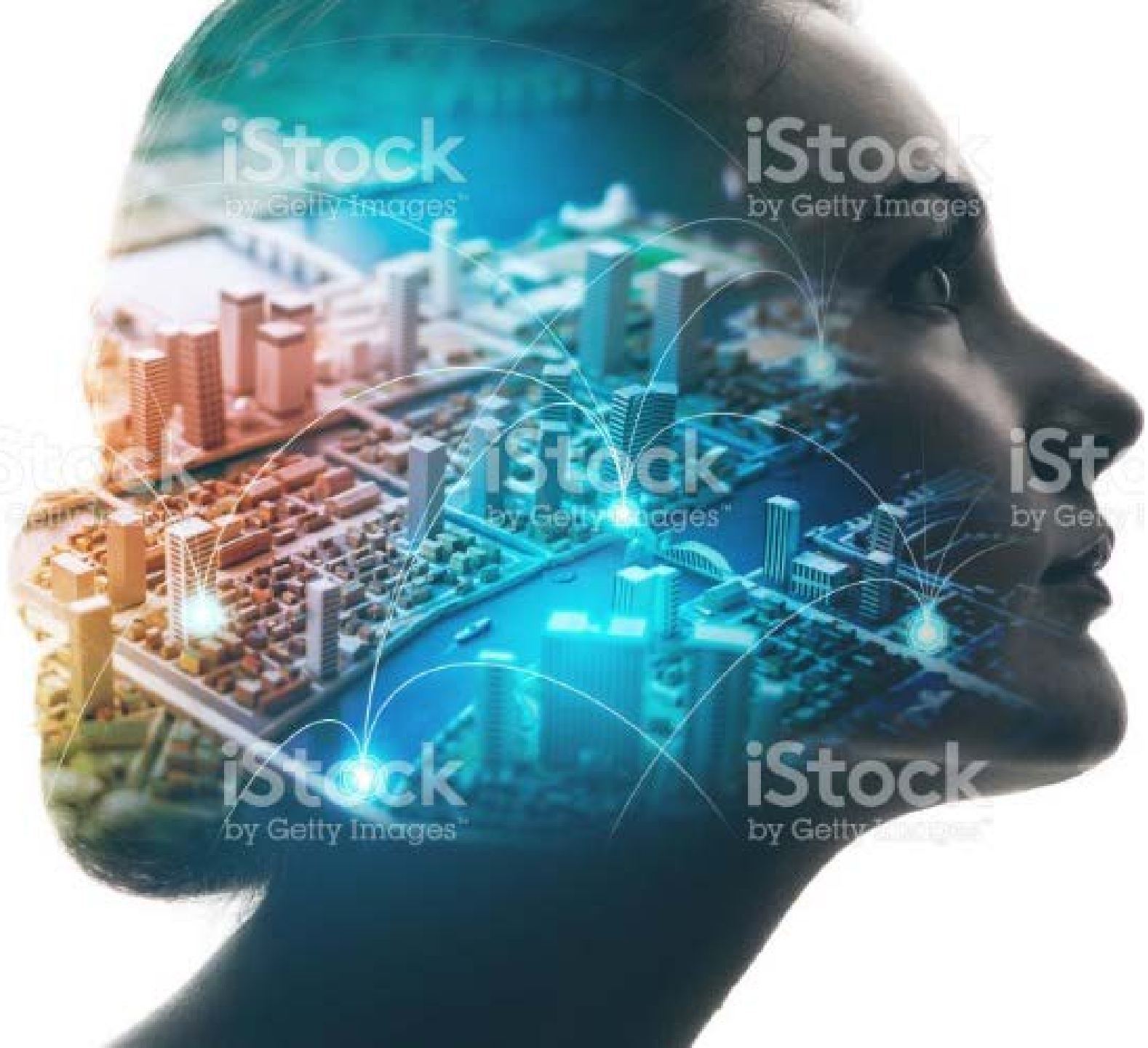
User Experience ?
Wallets and exchanges can be confusing and hard to use, often leading to very poor user experiences

Centralisation ?
Lack of resistance to the effective centralisation of mining power, i.e. 80% of 'haspower' is controlled by just 4 entities in Chins

What is an Initial Coin Offering (ICO)?

- An ICO is a means of raising money from the public, using “coins” or “tokens”. These transferable coins or tokens are issued in exchange for traditional currencies, such as the euro, or more often, virtual currencies.
- Tokens may be used to buy future services from the issuer or may be sold.
- ICOs are not standardised, and their legal and regulatory status is dependent on the circumstances of the issuer ICO.
- The likelihood of regulation will depend on whether the token is deemed a transferable security, a method of raising capital for an investment fund or a cryptocurrency.

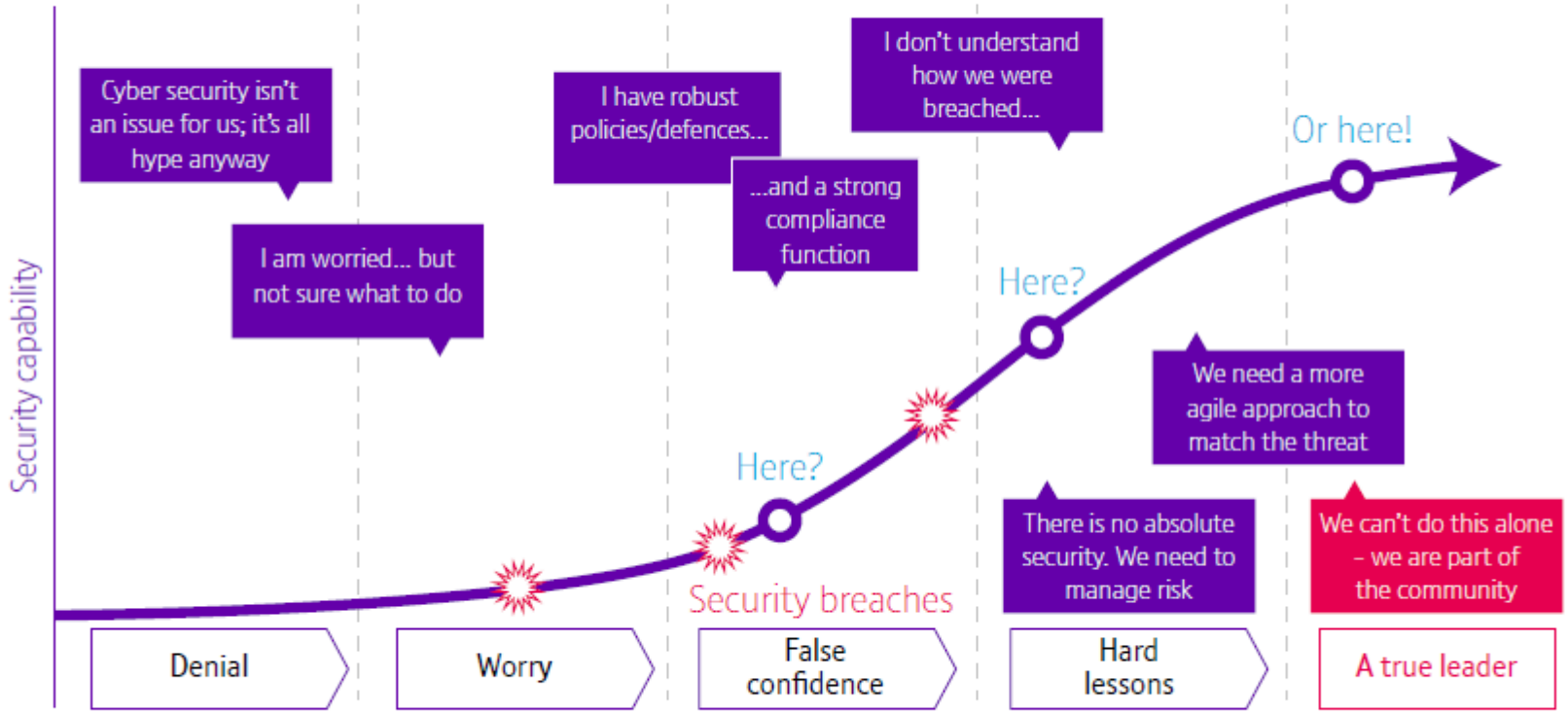
Cyber Security and Data Privacy



Starting Point

> “By 2020, 60% of Digital Businesses will suffer major service failures due to the inability of the IT Security team to manage the digital risk
> - GARTNER ”

Where are you from this Journey?



New "vectors" of threats are accelerating the concern

YESTERDAY…

Bad "actors"
- Isolated criminals
- "Script kiddies"

Targets
- Identity theft
- Self-promotion opportunities
- Theft of services

"Target of opportunity"

TODAY…

Bad "actors"
- Organized criminals
- Nation states
- Hactivists
- Insiders

Targets
- Intellectual property
- Financial information
- Strategic access

"Target of choice"

Common Cyber Security Mistakes!

1. We have to achieve 100 percent security

Mistake

We have to achieve 100 percent security.

Reality

100 percent security is neither feasible nor the appropriate goal.

2. Invest in best-in-class technical tools

Mistake

When we invest in best-in-class technical tools, we are safe.

Reality

Effective cyber security is less dependent on technology than you think.

3. We need better weapons

Mistake

Our weapons have to be better than those of our attackers.

Reality

The security policy should primarily be determined by your goals, not those of your attackers.

4. Cyber security compliance is all about effective monitoring

Mistake

Cyber security compliance is all about effective monitoring.

Reality

The ability to learn is just as important as the ability to monitor.

5. We need the best professionals

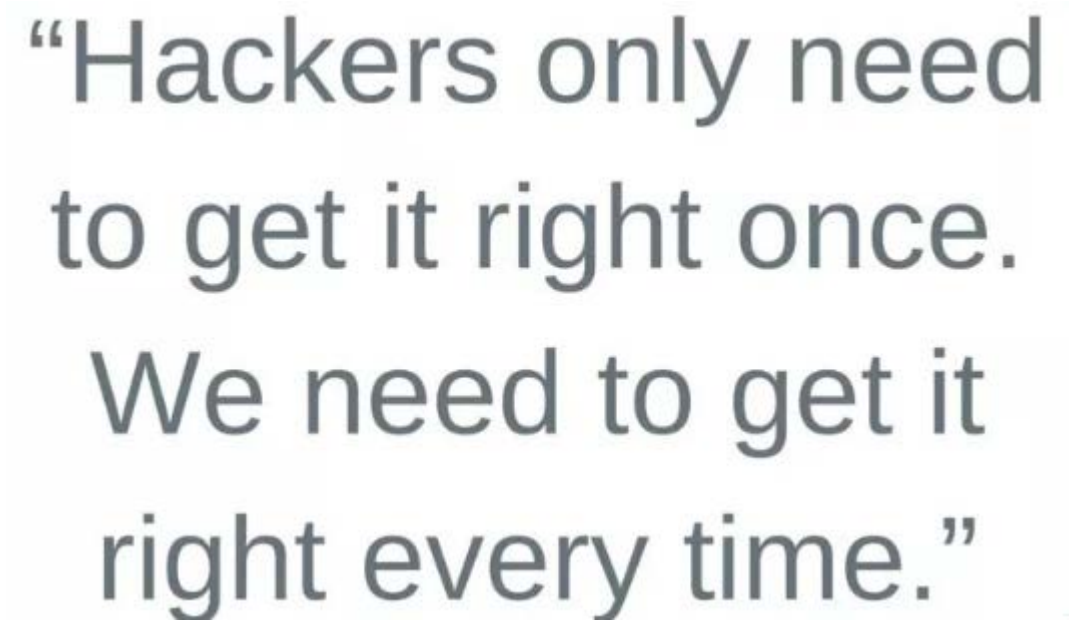
Mistake

We need to recruit the best professionals to defend ourselves against cybercrime.

Reality

Cyber security is not a department, but an attitude.

Hackers against Security Professionals!



Data Privacy

Understanding Key Terminology

Personal Data

Any information relating to an identified or identifiable living individual (also known as the 'data subject'). Examples include name, address, date of birth, telephone number, email address, bank account details, IP address, biometric data. For further information please see slide 8.

Processing

Any operation or set of operations performed on personal data, whether by automated or non-automated means including collection, recording, storage, alteration, retrieval, use, disclosure, dissemination, erasure or destruction.

Controller

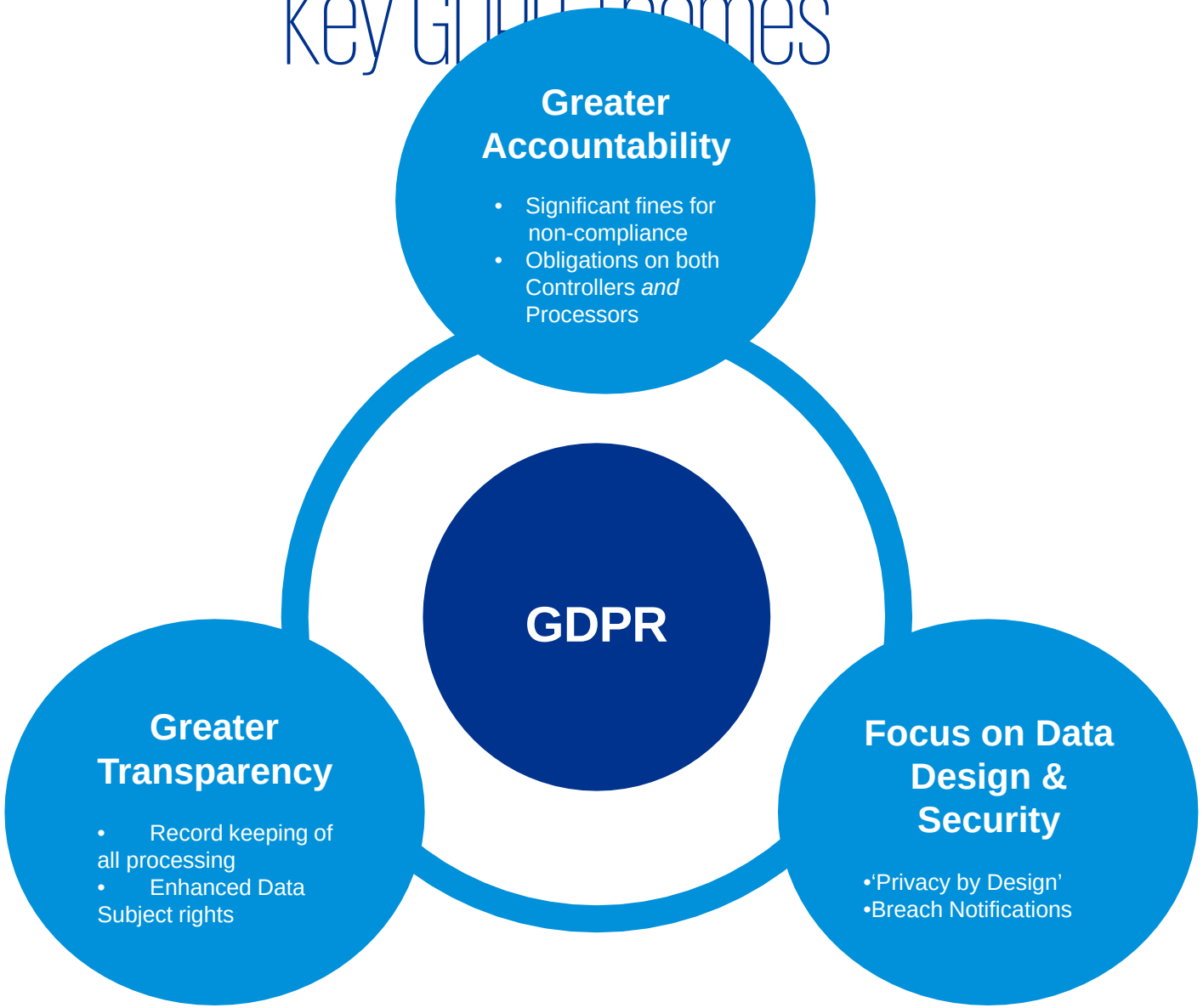
An organisation which, either alone or jointly with others, determines the purpose and means of processing of personal data.

Processor

An organisation that processes personal data on behalf of and instructed by the Controller.

© 2017 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affilia ted with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Key GDPR Themes



© 2017 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affilia ted with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Key Features of the GDPR

Data Incident Reporting

The GDPR introduces new breach reporting obligations for both Controllers and Processors. Controllers must notify the DP regulator of breaches within 72 hours. Processors must notify Controllers without undue delay.

Fines for Non-Compliance

Maximum fines for infringement of data subjects' rights, rules on international transfers and basic principles of processing can be up to EUR 20M or 4% of global turnover, whichever is higher.

Obligations on Controllers and Processors

Both Controllers and Processors must:

i) Implement appropriate technical and organisational measures to protect personal data;

ii) Keep records relating to their processing activities; and

iii) Comply with new data breach reporting obligations.

Extra-Territorial Scope

Controllers / Processors not established in the EU but who process personal data of individuals in the EU need to comply with the GDPR.

International Data Transfers

Can be made with an adequacy decision or through appropriate safeguards (consent, Inter Firm Agreement model clauses) or Binding Corporate Rules (BCRs).

Data Minimisation

Personal data processed must be adequate, relevant and limited to what is necessary. There must be a 'lawful basis' for processing personal data and it must be processed only for the purpose specified at the time of collection.

Explicit Consent

Where consent is the lawful basis for processing personal data, consent must be informed, freely given and unambiguous.

New Rights for Individuals

Individuals have the right to ask Controllers to erase their data in certain circumstances. They also have the right of access, rectification and portability as well as the right to object to processing and to profiling.

Privacy by Design

There is a requirement to build data protection safeguards into new products, services or technologies. This includes the requirement for a privacy impact assessment to be carried out by Controllers prior to using new technologies.

Data Protection Officer

A Data Protection Officer must be appointed where required under GDPR.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Definition of Personal Data

The GDPR defines **Personal Data** as:

- any information relating to an identified or identifiable natural person ('data subject');
- an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The Regulation makes a distinction between Sensitive Personal Data and Personal Data

Personal Data

- Name or User ID
- Address
- Telephone numbers
- Email
- Place of birth
- Date of birth
- Employment history
- Salary
- Dependents
- Next of kin
- Passwords
- Location data
- IP address
- Holiday records
- Online profile
- Tweets / Online messages

Sensitive Personal Data

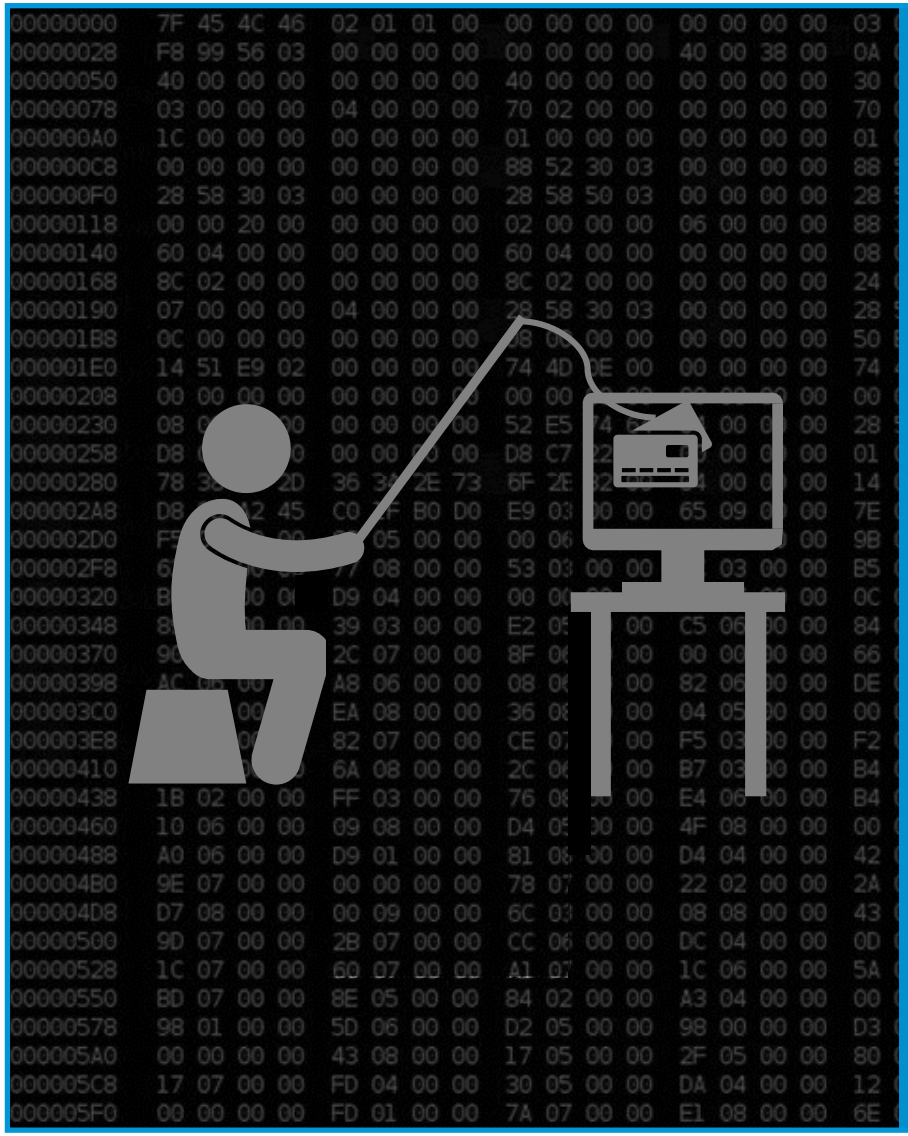
The GDPR's definition of '**Sensitive Personal Data**' relates to specific categories of Personal Data which require extra consideration because of the higher risk to rights and freedoms of an individual. They are:

- An individual's racial or ethnic origin
- Their political opinions
- Their religious or philosophical beliefs
- Their trade union membership
- Their genetic or biometric data
- Any data concerning the health of an individual
- Their sex life or sexual orientation

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Content

Example of Current threats: Phishing and Rogue phone calls



Phishing

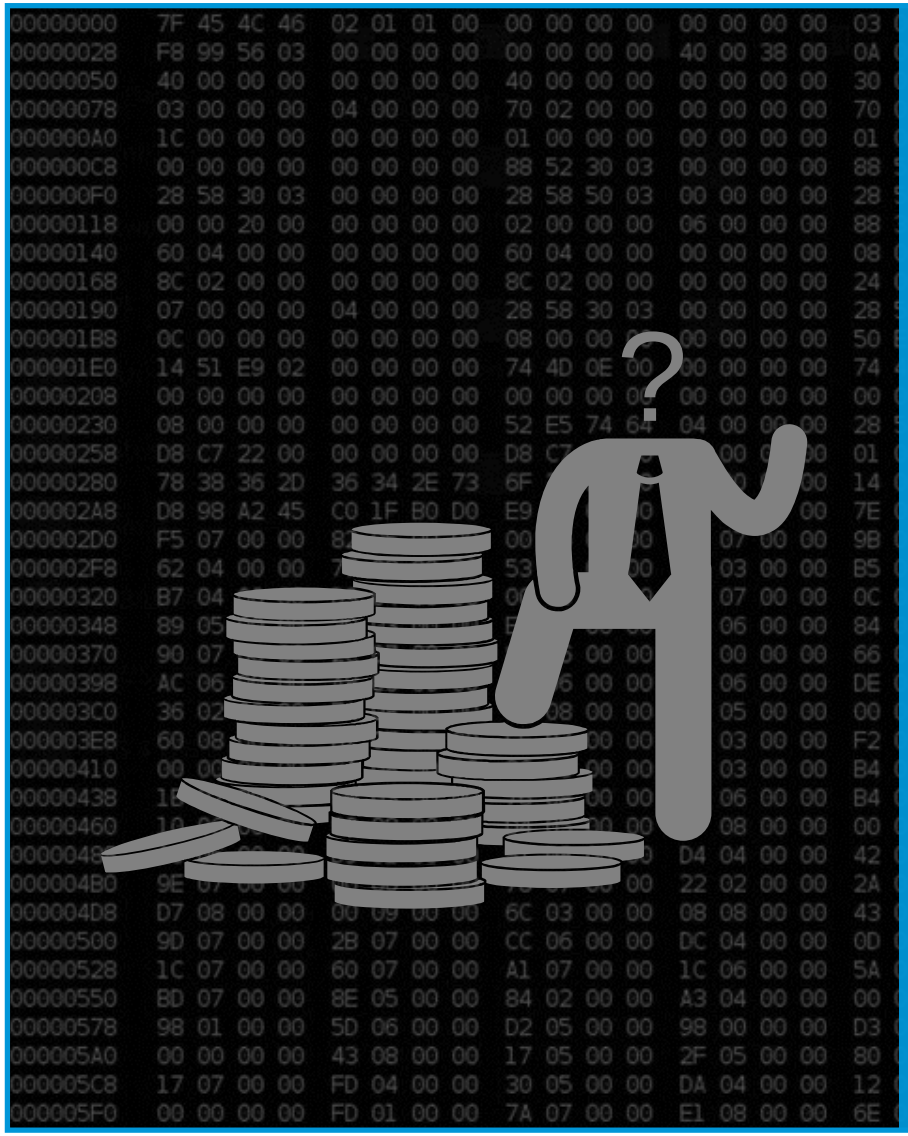
- The practice of **Phishing** (or Spear Phishing) is employed by cyber criminals **to obtain account credentials or trusted access** from employees.
- Obtained account credentials and trusted access can then be used in other cyber attacks
- Increasingly, cyber criminals are targeting highly privileged employees - this practice is called Whaling.
- Also, fraudster are imitating a hotline, asking to ‘confirm’ confidential information.

Example of Current threats: Ransomware

Ransomware

- Ransomware enters an organization either when an employee runs an email attachment or when attackers use previously obtained (→Phishing) credentials to place the software.
- Ransomware is distributed in the form of Cryptolockers. These relatively simple programs encrypt file systems with strong encryption algorithms.
- The victim is then displayed a message to pay ransom and receive the decryption key or loose access to the files forever.
- Many individuals and companies would rather pay high sums than loose their data.

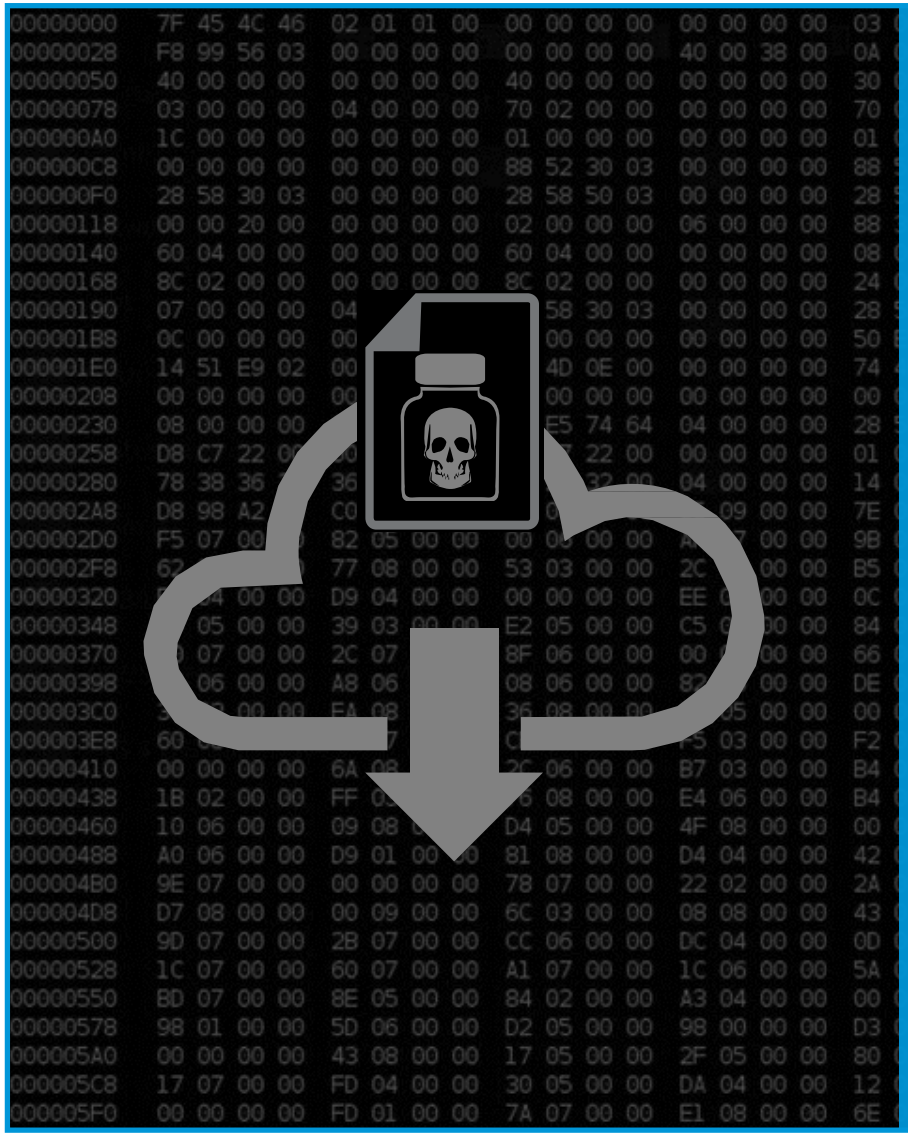
Example of Current threats: Payment Diversion & Fake President



Payment Diversion & Fake President

- As part of the scam Payment Diversion, criminals assume a false identity and try to coerce employees into acting on their behalf.
- In most cases, they want money transferred to a bank account they control.
- Some scams even employ fake companies, including fake, fully functional websites.
- Recent months have seen an increase in cases where attackers first gained extensive internal knowledge from an organization (by exploiting employees or even hacking company IT systems) before commencing with the actual scam.

Current threats: Bogus Invoice



Bogus Invoice

- Fraudster email your business from a source purporting to be a real supplier. The email contains an invoice as attachment.
- Once you open the attachment, your computer gets infected by a malware.
- The malware logs what's happening on the machine and also the company's online banking credentials.
- The attacker uses this information for his own illegal purposes.

Current threats: Ransomware

Ransomware

- Ransomware enters an organization either when an employee runs an email attachment or when attackers use previously obtained (→Phishing) credentials to place the software.
- Ransomware is distributed in the form of Cryptolockers. These relatively simple programs encrypt file systems with strong encryption algorithms.
- The victim is then displayed a message to pay ransom and receive the decryption key or loose access to the files forever.
- Many individuals and companies would rather pay high sums than loose their data.

Anatomy of a Fake President email

From: [CEO of a subsidiary in another country]
To: [Manager in middle management position]

Message:

... we are planning a confidential takeover of the the company Pretense Corp. in India via our local office ...

... Please support us in this matter. All details must remain confidential ...

[... often continued for several messages]

... for confirmation and details on the confidentiality please contact our attorney Mr. Strawman, (+49 1805 764 367) ...

... please wire the sum of EUR 1.341.200 to the account 23432509 at the International Bank of Fraud (BIC INFBCNSJ) ...

The email-address of the fraudster is made to look authentic.

A common tactic is to create a fake domain name that looks like the original: name@com**q**any.com

The company's own email-system may also have been compromised.
The mail „is coming from within the house".

Content

The four golden rules of cyber security

Get the basics right.

Over 75 percent of attacks exploit failures to put in place basic controls.

Look after your critical assets.

You have to prioritize where you spend your money to defend yourself, so build a fortress around your most critical assets.

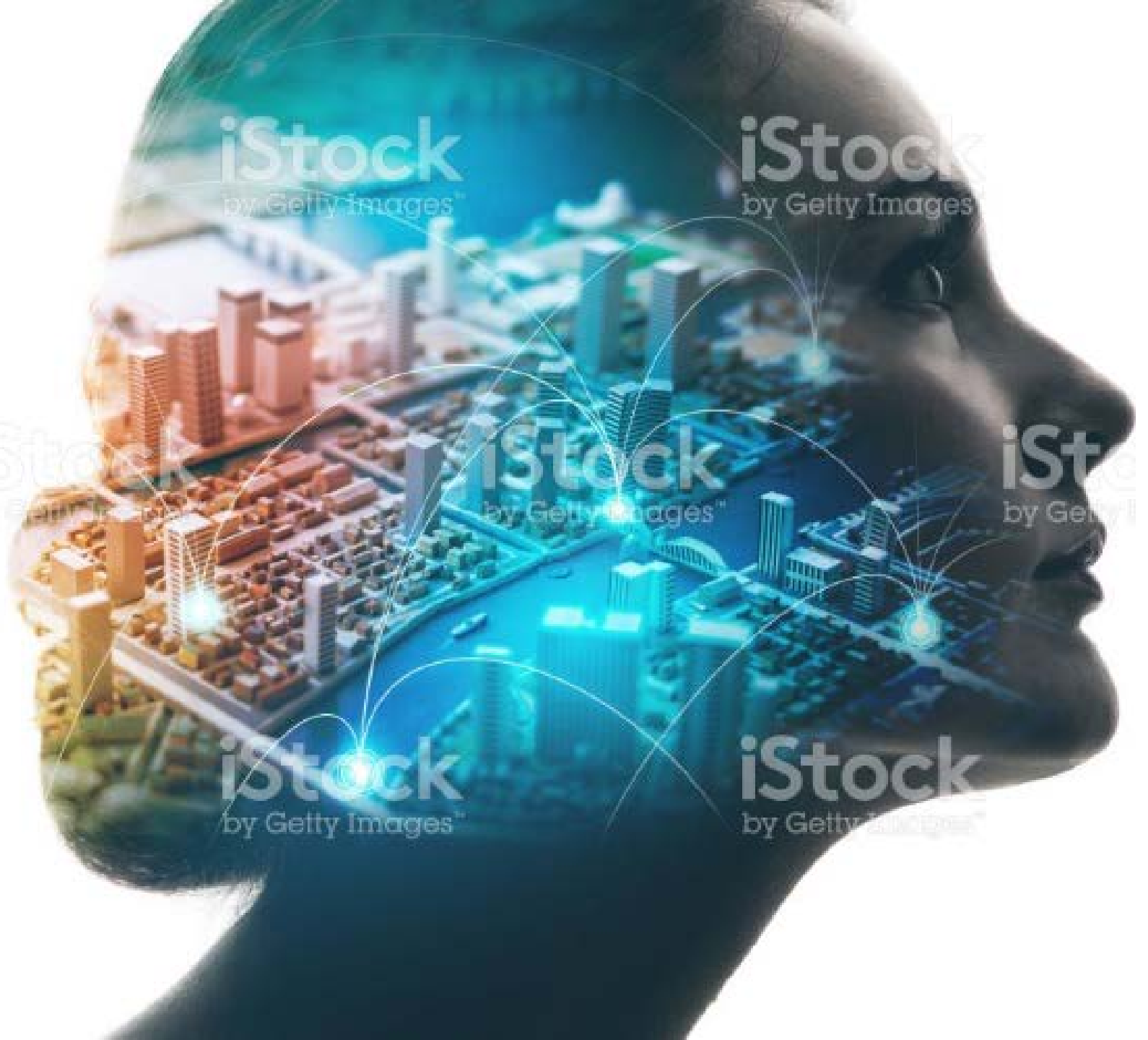
Do your homework on your enemies.

Invest in understanding who might attack you, why and how so that you can anticipate the most likely scenarios and you defend those assets that are most likely to get attacked.

Treat cyber risk as an opportunity to look closely at your business.

Security and resilience can affect nearly every part of an organization. Strategies to protect IT security and business resiliency should align with an organization's broader goals — from protecting intellectual property to maximizing productivity to finding new ways to delight customers.

The Future of Audit and Accounting



A call for Action!

What does this mean for the profession?!

A call for Action!

Thank you