Acronis

Solving “SAPAS“ challenges with innovative Cyber Protection strategies

Markus Bauer

Technology Evangelist EMEA

Dual headquarters
in Switzerland and Singapore

Agenda

Chapter 1: Cyber Attacks and Prevention methods

Chapter 2: Secure Content for the mobile Enterprise

Chapter 3: How Blockchain Technologies can help to ensure the integrity of business-critical data

Acronis

Chapter 1:

Cyber Attacks and Prevention methods

Data Volume is Growing

63% say the frequency of endpoint attacks has increased in 2018

The average time to patch is 102 days

Antiviruses miss 57% of attacks

Data is growing 33 times faster than IT staff

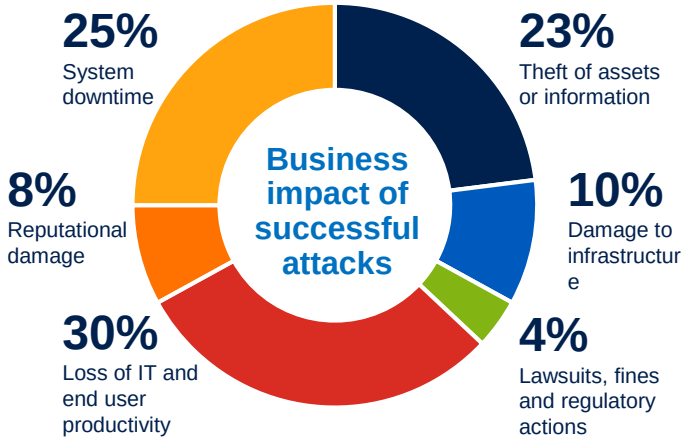
50% of hard drives die within 5 years

60% of enterprises have been hit by ransomware

64% has experienced successful endpoint attacks in 2018 vs 54% in 2017

Endpoints

- Remote Offices
- Cloud Servers
- Hosted Servers
- Desktops
- Mobile



Each successful attack costs $7.1 million for a large organization or an average of $301 per employee or $440 per endpoint

Sources: "Trends in SaaS Data Protection", Spanning, 2016; "Understanding the Depth of the Global Ransomware Problem", Osterman Research, 2016; "Hosting and Cloud Study 2017", 451 Research, 2017, The 2018 State of Endpoint Security Risk, Emerson Network Power-sponsored study by the Ponemon Institute (2016), PWC 2016 US CEO Survey

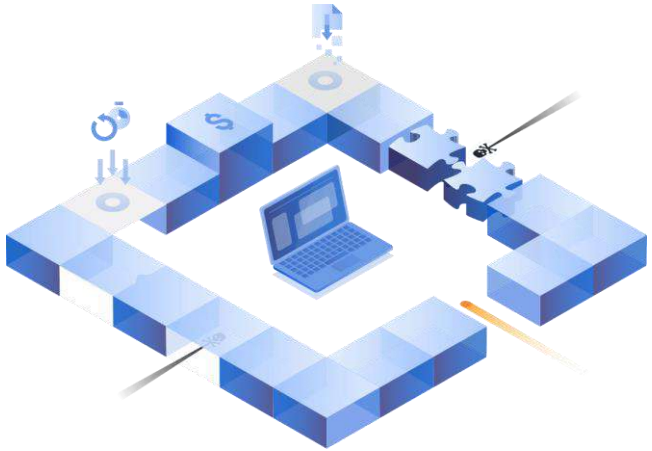
Traditional Approach to Endpoint Protection

Traditional AVs do not protect data

- No data recovery capabilities
- May not protect from advanced 0-day attacks and sophisticated threats
- Do not protect from known vulnerabilities

Non-integrated bundle of traditional backup and AV

- Expensive and complex to manage
- Heavily impacts performance, incompatibilities
- Needs additional tools for management and recovery
- Still prone to infected backups



Traditional backups are not secure

- Backups are vulnerable to attacks, breaches and modifications
- Can backup infected non-restorable machines
- No self-protection, do not help investigations

Multiple IT tools add complexity

- Multiple agents, backends, licensing policies, UIs => conflicts
- Supported by different IT persons, longer learning
- No single, unified view – less visibility and control

Complex **Expensive** **Not Secure**

Samples: Cyberattacks and business impacts

Company	Product	Date	Type	Impact	Losses
Norsk Hydro	Aluminum parts	March 2019	Ransomware	Halted production in metal extrusion plants, forced manual-mode operation in aluminum processing plants, reduced output by at least 50% for weeks	**$70M**
Hoya	Eyeglass lenses	February 2019	Credential stealing / cryptojacking	Shut down Thailand plant for three days, shrank total output by 60% for a month	**Unknown**
TSMC	Semiconductors	August 2018	Ransomware	Halted production of main processor for iPhones at three plants in Taiwan for three days	**$250M**
Boeing	Airplanes	March 2018	Ransomware	Halted production of automated spars for 777 passenger jets in North Carolina plant for one day	**Undisclosed**
Merck	Drugs and vaccines	June 2017	Ransomware	Halted or reduced production of some drugs	**$870M**
Mondelez	Snack foods	June 2017	Ransomware	Halted production, delivery and invoicing systems for several days. Cyber insurance claim for losses later denied	**$188M**
Reckitt Benckiser	Consumer health products	June 2017	Ransomware	Halted production, delivery and invoicing systems for several days	**$129M**
Nissan / Renault	Autos	May 2017	Ransomware	Halted production at plants in Japan, UK, India, France and Romania	**Unknown**
Honda	Autos	May 2017	Ransomware	Brought down older production line computers, resulting in one-day halt at Sayama plant and loss of output of 1,000 vehicles	**Unknown**
AW North Carolina	Automatic transmissions	August 2016	Unknown malware	Halted production of transmissions for Toyota vehicles for four hours	**$1.08M**

Proactive prevention

The best protection is prevention. Take these steps to keep ransomware from harming your business

Patch your system

Keep browsersm, OSes, and other software applications up-to-date.

Educate users

One pf the moste common ways that computers are infected with ransomware is through social engineering. Educate users on how to detect phishing campaings, suspicious websites, and other scams.

Back up files

Make secure copies of your data on a regular basis and store them offsite.

- Be sure backup files are not stored on a mapped drive. Some strains of ransomware can even encrypt files over unmapped network shares.
- If backing up onto a USB or external hard drive, be sure thr devices are physicsally disconnected from the computer.
- We recommend storage on a secure cloud server with high-level encryption and multiple-factor authentication.

Invest in layered security

Installing multiple layers of cybersecurity protection can detect and block ransomware attacks before they happen. For the best protection, we recommend these layers:

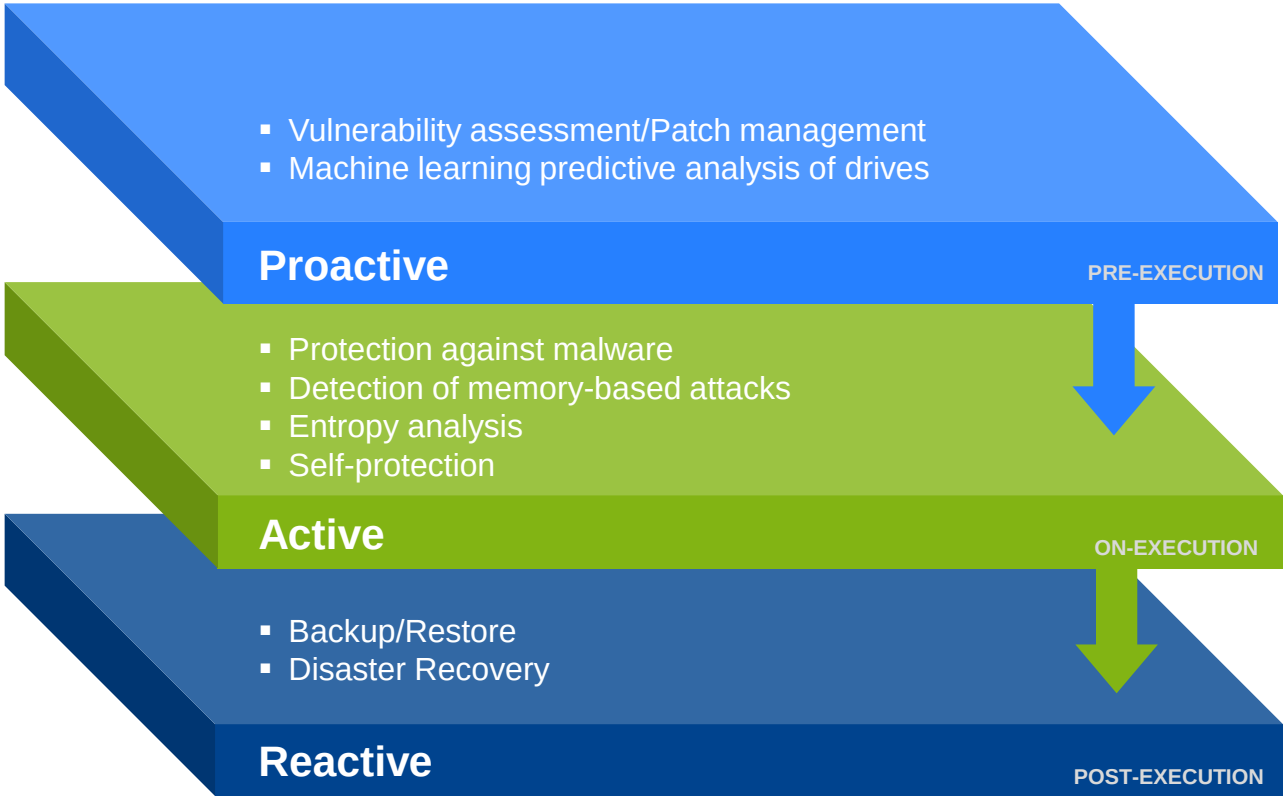
- Firewall
- Antiexploit
- Antivirus with active monitoring
- Antimalware
- Antiransomware

3 Backup copies

2 Media types

1 Copy offsite

Multi Layered Protection Approach



Prevent

Detect

Response

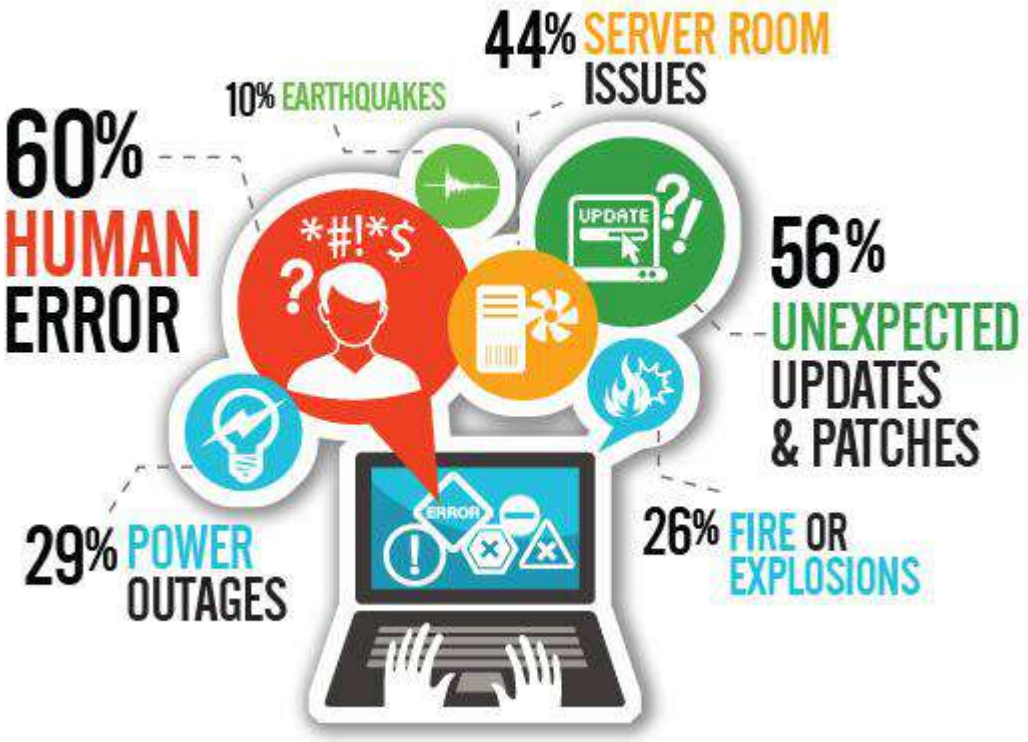
What is Disaster Recovery?

Disaster Recovery involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events.

Disaster recovery can therefore be considered as a subset of business continuity.

Causes of Outages



Source: http://www.abacustechnologies.com

Downtime Costs Are Very High (Per Hour)

Average cost of downtime
(across all businesses)

$4,333

Data centers
(unplanned outages)

$8,851

Auto industry
(unplanned outages)

$22,000

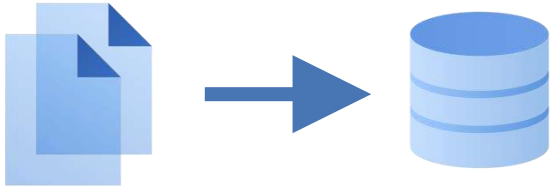
Online business
(unplanned outages)

$500,000

Source: Aberdeen Group report, “Maintaining Infrastructure Uptime in Today’s Transforming IT Infrastructure”

Backup Is Not a Disaster Recovery

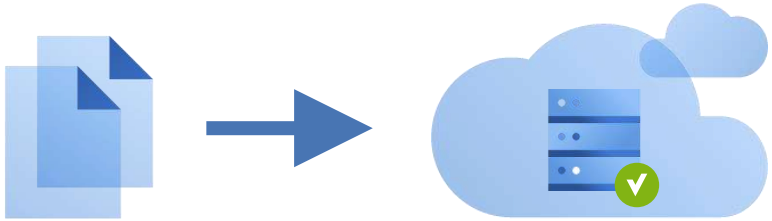
- Backup is a copy of your data/apps that keeps your data safe and enables you to **bring a failed system back online**
- Backup **does not include the infrastructure to immediately restore your workload**



Customer's data

Backed up data

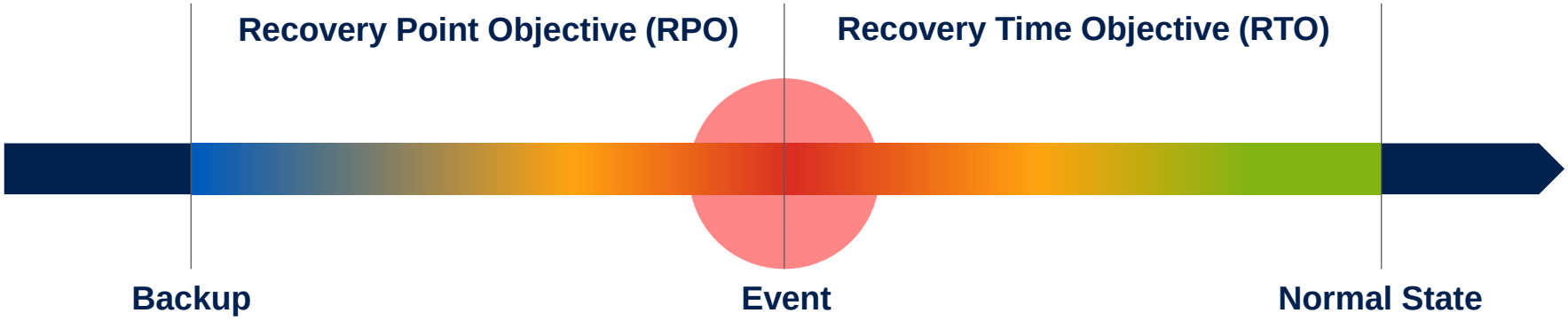
- Disaster recovery solutions include a most recent copy of your data and **processing capabilities – infrastructure**
- Disaster recovery cloud platforms **guarantee near-instant, automatic availability of your data/apps, enabling you to keep running**



Customer's data

Backed up data, plus cloud infrastructure to run them

Key differentiator: Guaranteed data recovery with minimal RTO and RPO



Things to consider:

- Many solutions can’t restore the data
- Often this is a semi-manual process from local or cloud backup. This takes a lot of time.
- With Instant Recovery functionality any files are restored immediately

Disaster Recovery Checklist

Here are a few simple questions to help evaluate the business and plan needed to recover.

- Do you have a plan to account for all potential business-impacting events such as natural disasters, human error, IT failures, and cyber attacks? Is the plan current?
- Does your plan include all critical systems (accounting, operations, IT, HR) and prioritize recovery tasks?
- Do you have redundancies in place for critical systems data, such as redundant power supplies, replication of software, and backups stored in multiple locations?
- Does your plan include a clear timeline for all objectives?
- Do all employees have a copy of the plan that is accessible to them in the midst of a disaster? Do they know their roles?

Acronis

Chapter 2:

Secure Content for the mobile Enterprise

Employee Needs

- Access to their files and content anywhere
- Access from any device
- Securely share files
  and collaborate with others

Business Needs

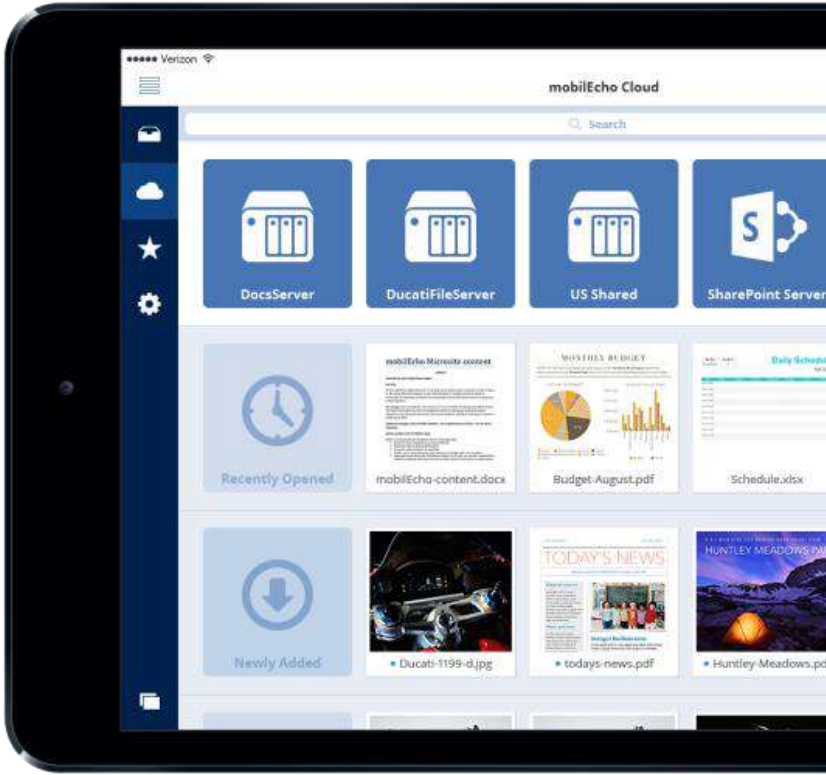
- Support BYOD and company devices
- Provide safe access to files and documents
- Support sharing and sync across multiple devices
- Include desktops, laptops, mobile devices, and web browsers as part of the solution

IT Needs

- Control data, users, and devices with flexible, granular policies
- Protect and safeguard the company's critical data assets with advanced authentication, encryption, secure in-app editing, and remote wipe features
- Easily integrate into existing infrastructure and operations (Active Directory, MDM, etc.)

Solving Employee, Business and IT Needs

- Access to on-premises file servers, SharePoint and other data sources
- Syncing of file shares and SharePoint files to Macs and PCs via “desktop sync client”
- Safe sharing of files on any platform
- Secure editing of sensitive documents
- Centralized management and an advanced policy engine
- Intuitive, natural, and consistent user experience



Benefits of Enterprise File Sync and Share

Secure file sharing

- Granular access control, secure authentication protocols, and authorization policies
- Remote wipe, device lock, passcode protection, white/black listings, and data expiration policies
- Real-time tracking and auditing of user activity
- Integration with enterprise directory services to simplify authentication and user provisioning
- Upload and download restrictions, file expiration dates, and restricted access based on network location

Anywhere access

- People are no longer limited to a single corporate-owned device or office location to get work done. Today's increasingly mobile workforce expects to be able to access what they need, from any device or location, with a consumer-like experience
- File sharing services enable mobile work styles by allowing users to sync files across all their devices and easily access what they need from anywhere

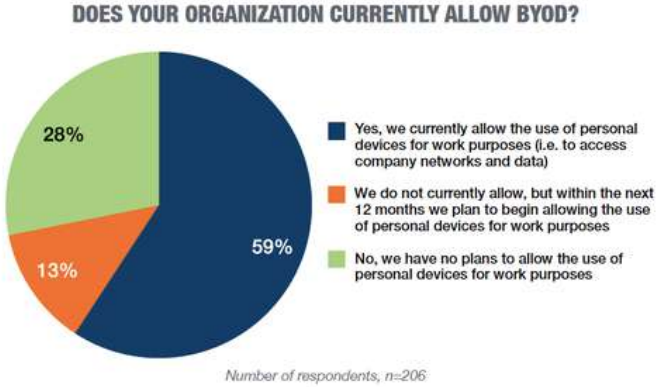
Data loss prevention and disaster recovery

- When data is centrally stored and managed with an file sharing service, your data is better protected from data leakage, whether from a cyberattack, a lost or stolen device, or employee error. File sharing services make it easy to keep data backed up and secure

Some facts about BYOD

- **67%** of employees use personal devices at work
- **BYOD annually generates $350** of value per employee
- A BYOD-carrying employee works an **extra two hours**
- **87%** of businesses are dependent on their employee's ability to access mobile business apps from their smartphone
- **69%** of IT decision-makers in the U.S. say BYOD is a good thing
- BYOD market size is expected to reach **$366.95 billion by 2022**
- **59%** of organisations adopt BYOD

Source: Tech Jury



Source: Tech Pro Research

	Overall
To protect secure information and reduce future risk	44%
We wanted to boost productivity	43%
To save money	38%
To conform with legal requirements to reimburse employees for their mobile usage	31%
To better understand how smartphones and applications are used within the company	29%
Our employees demanded clarification	24%
We experienced a security breach	17%

Source: Syntonic

Acronis

Chapter 3:

How Blockchain Technologies can help to ensure the integrity of business-critical data

What is Blockchain?

A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp and transaction data.

Secure

Blockchain uses strong cryptography to create transactions that are impervious to fraud and establishes a shared truth. Also, all the transactions are signed with the digital certificate.

Shared

The real benefits of blockchain, over conventional technology, are achieved when we use it to link organizations to share information on a distributed ledger.

Distributed

A blockchain can be distributed across multiple organizations and becomes more secure as replicas are added.

Ledger

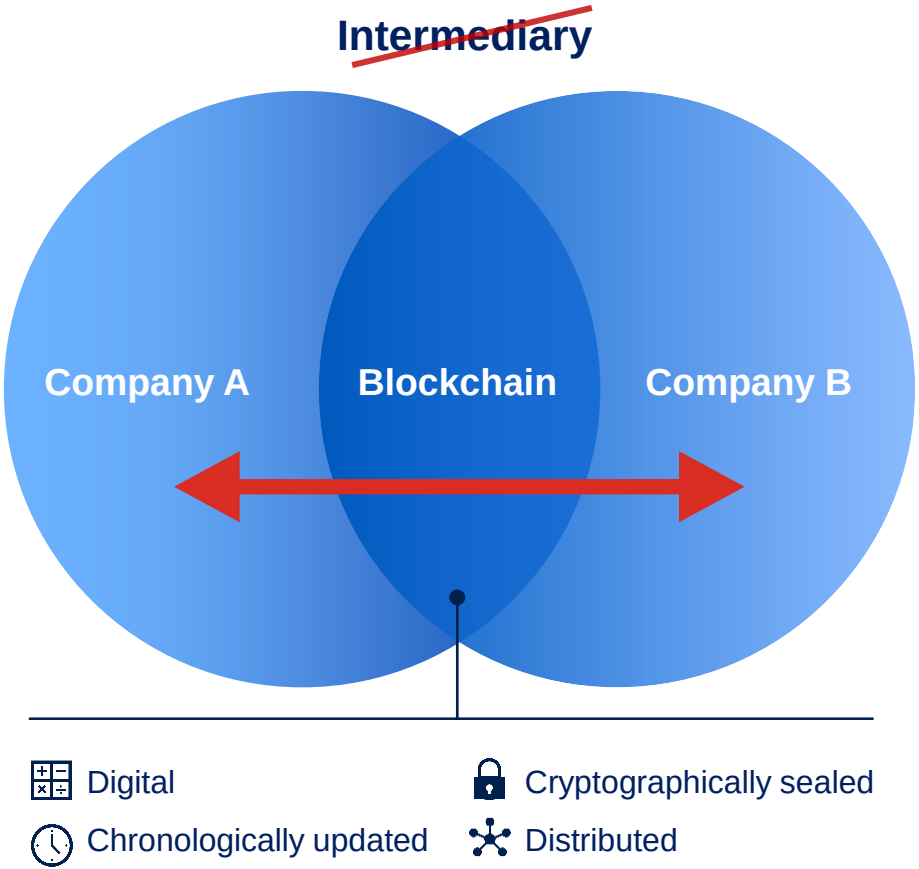
Every transaction is written into the ledger once and cannot be changed after the fact.

Source: Wikipedia, Accelerating the adoption of enterprise blockchain

Conclusive Verification Without a Trusted Party

- The need for a third party is eliminated
- Falsifying or destroying entries to conceal malicious activity is practically impossible
- Rapidly verifiable results
- Complete, automated audit > Reduces the cost and time necessary to conduct an audit

*Every transaction becomes "notarized", similar to the transaction being verified by a **notary** – only in an electronic way*



Source: Deloitte: Blockchain Technology A game-changer?

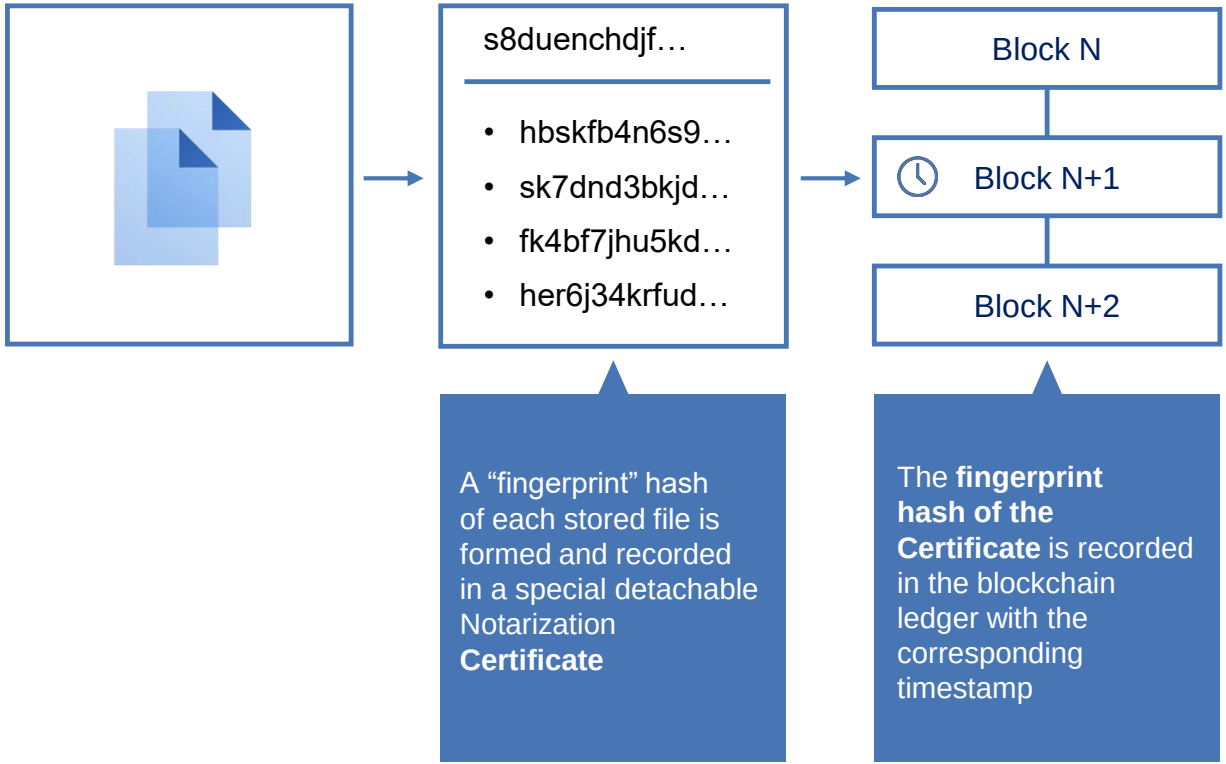
Before Blockchain, Trusted Third Parties Guaranteed the Immutability of Records





~100 BC	~1100 AD	Modern era	Digital era	Blockchain
Ancient Rome ▪ Notarius took dictation of Roman court and Senate proceedings ▪ Scribae acted as court recorders ▪ Tabellio facilitated private contracts and archived documents	**Byzantine and Renaissance Italy** ▪ Notaries created contracts by witnessing signing, dating and reciting in court ▪ Church priests took over some of the functions	**Notaries underpin the modern economy by providing trust in** ▪ Contracts ▪ Land titles ▪ Wills ▪ Power of attorney ▪ etc.	**In the digital era, companies act as sources of trust via** ▪ Electronic signatures ▪ Web of trust ▪ Trusted timestamping ▪ Trusted computing ▪ Remote notaries ▪ Web evidence	**Blockchain provides a distributed source of trust with** ▪ Smart contracts, trusted timestamping, e-signatures, etc. ▪ No need for third-party verification from either private or government agencies

How It Works?



Any record in the blockchain is immutable and independently verifiable.

That is why the Notarization Certificate cannot be manipulated.

The completeness of all records and authenticity of each file can be checked automatically or manually.

Trusted Third Party: Blockchain

Use hashing. “Hashing is the main mechanism to ensure data has not changed,” says Alan Rynarzewski Jr, MIS, a faculty member at Purdue University Global and course lead for IT and cybersecurity. “We currently use hashing when downloading files from the internet. You can download the file and run the hashing algorithm against it. The hexadecimal value you get should match the value of where you downloaded it from. The data has been altered if the values do not match.”

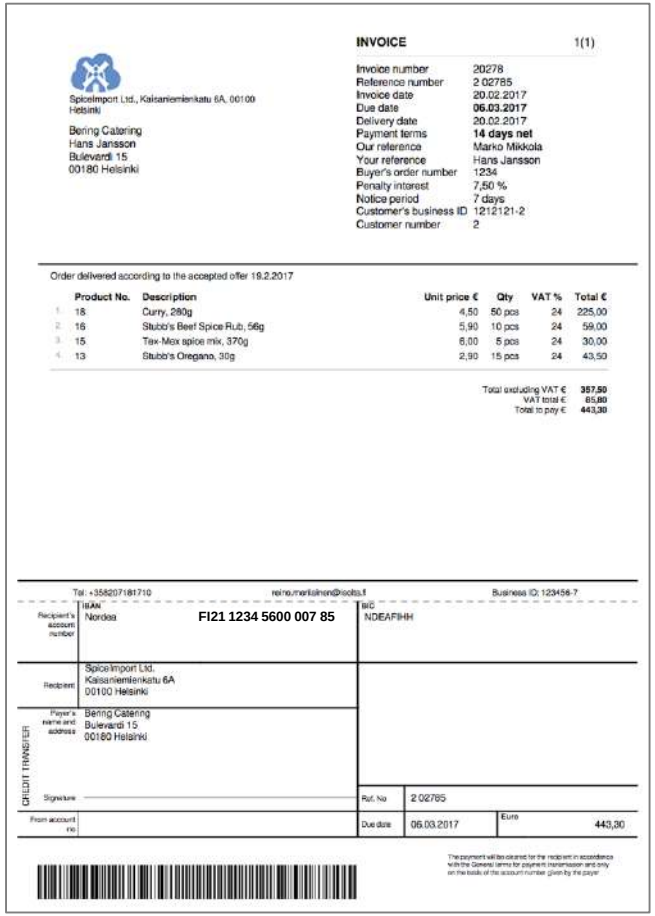
“We can take that same technology and implement it on our files. Encrypt your file and hash it. The hash should not change. If it does, then someone has modified the file.”

Data Manipulation: The Next Level of Cyberattacks

Rather than stealing data, attackers corrupt its integrity to generate revenue or much worse cause chaos and catastrophe

Source: https://www.channelfutures.com/mssp-insider/data-manipulation-the-next-level-of-cyberattacks

If your data were being manipulated, would you notice?



INVOICE 1(1)

SpiceImport Ltd., Kaisaniemenkatu 6A, 00100 Helsinki

Bering Catering
Hans Jansson
Bulevardi 15
00180 Helsinki

Invoice number	20278
Reference number	2 02785
Invoice date	20.02.2017
Due date	**06.03.2017**
Delivery date	20.02.2017
Payment terms	**14 days net**
Our reference	Marko Mikkola
Your reference	Hans Jansson
Buyer's order number	1234
Penalty interest	7,50 %
Notice period	7 days
Customer's business ID	1212121-2
Customer number	2

Order delivered according to the accepted offer 19.2.2017

	Product No.	Description	Unit price €	Qty	VAT %	Total €
1.	18	Curry, 280g	4,50	50 pcs	24	225,00
2.	16	Stubb's Beef Spice Rub, 56g	5,90	10 pcs	24	59,00
3.	15	Tex-Mex spice mix, 370g	6,00	5 pcs	24	30,00
4.	13	Stubb's Oregano, 30g	2,90	15 pcs	24	43,50

Total excluding VAT € **357,50**
VAT total € **85,80**
Total to pay € **443,30**

Tel: +358207181710 reino.merikoinen@isotta.fi Business ID: 123456-7

CREDIT TRANSFER

Recipient's account number — IBAN: Nordea **FI21 1234 5600 007 85** — BIC: NDEAFIHH

Recipient: SpiceImport Ltd. Kaisaniemenkatu 6A 00100 Helsinki

Payer's name and address: Bering Catering Bulevardi 15 00180 Helsinki

Signature

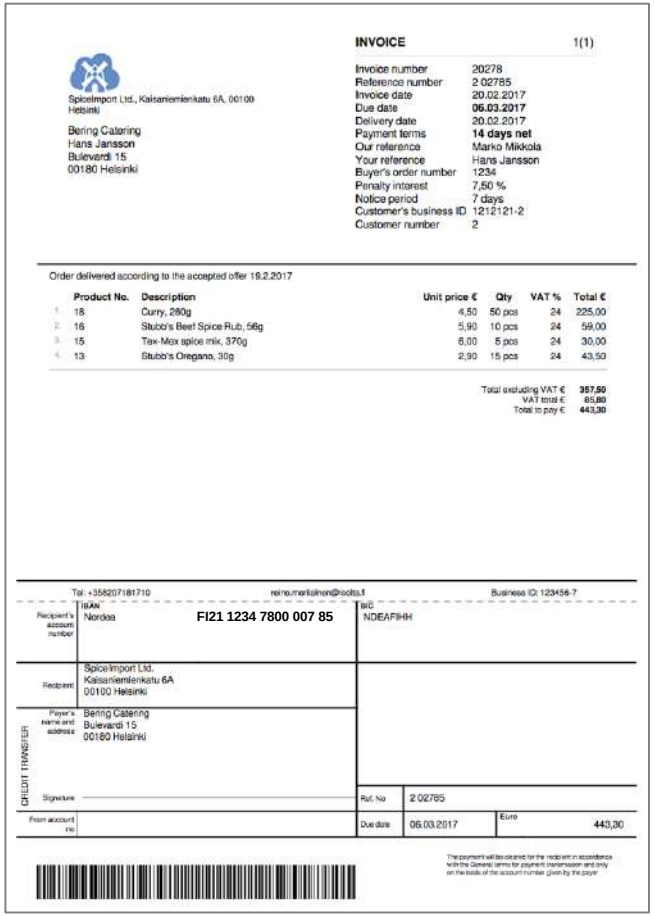
From account no

Ref. No 2 02785

Due date 06.03.2017

Euro 443,30

The payment will be obtained for the recipient in accordance with the General terms for payment transmission and only on the basis of the account number given by the payer



INVOICE 1(1)

SpiceImport Ltd., Kaisaniemenkatu 6A, 00100 Helsinki

Bering Catering
Hans Jansson
Bulevardi 15
00180 Helsinki

Invoice number	20278
Reference number	2 02785
Invoice date	20.02.2017
Due date	**06.03.2017**
Delivery date	20.02.2017
Payment terms	**14 days net**
Our reference	Marko Mikkola
Your reference	Hans Jansson
Buyer's order number	1234
Penalty interest	7,50 %
Notice period	7 days
Customer's business ID	1212121-2
Customer number	2

Order delivered according to the accepted offer 19.2.2017

	Product No.	Description	Unit price €	Qty	VAT %	Total €
1.	18	Curry, 280g	4,50	50 pcs	24	225,00
2.	16	Stubb's Beef Spice Rub, 56g	5,90	10 pcs	24	59,00
3.	15	Tex-Mex spice mix, 370g	6,00	5 pcs	24	30,00
4.	13	Stubb's Oregano, 30g	2,90	15 pcs	24	43,50

Total excluding VAT € **357,50**
VAT total € **85,80**
Total to pay € **443,30**

Tel: +358207181710 reino.merikoinen@isotta.fi Business ID: 123456-7

CREDIT TRANSFER

Recipient's account number — IBAN: Nordea **FI21 1234 7800 007 85** — BIC: NDEAFIHH

Recipient: SpiceImport Ltd. Kaisaniemenkatu 6A 00100 Helsinki

Payer's name and address: Bering Catering Bulevardi 15 00180 Helsinki

Signature

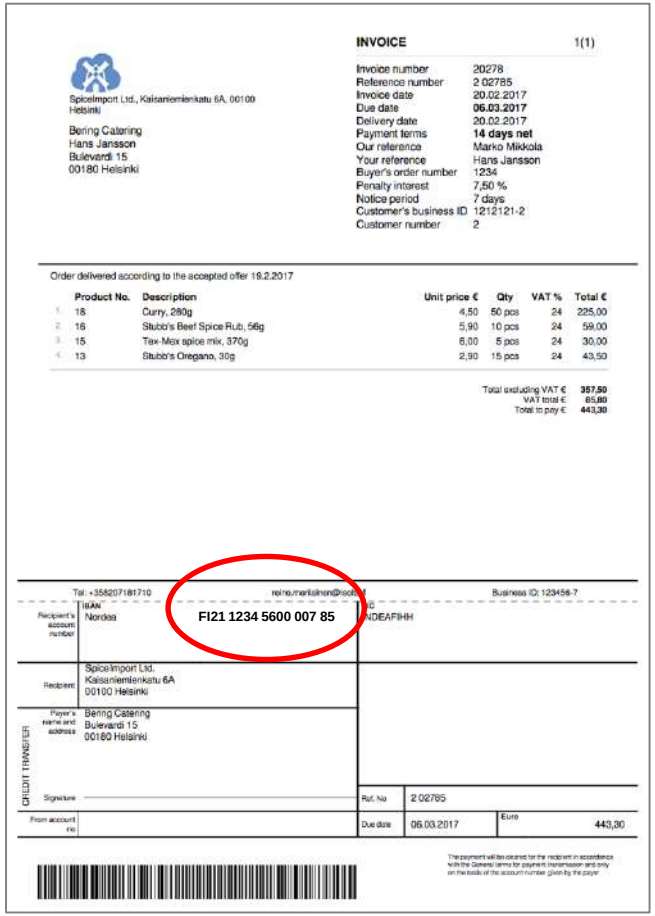
From account no

Ref. No 2 02785

Due date 06.03.2017

Euro 443,30

The payment will be obtained for the recipient in accordance with the General terms for payment transmission and only on the basis of the account number given by the payer



INVOICE 1(1)

SpiceImport Ltd., Kaisaniemenkatu 6A, 00100 Helsinki

Bering Catering
Hans Jansson
Bulevardi 15
00180 Helsinki

Invoice number	20278
Reference number	2 02785
Invoice date	20.02.2017
Due date	**06.03.2017**
Delivery date	20.02.2017
Payment terms	**14 days net**
Our reference	Marko Mikkola
Your reference	Hans Jansson
Buyer's order number	1234
Penalty interest	7,50 %
Notice period	7 days
Customer's business ID	1212121-2
Customer number	2

Order delivered according to the accepted offer 19.2.2017

	Product No.	Description	Unit price €	Qty	VAT %	Total €
1	18	Curry, 280g	4,50	50 pcs	24	225,00
2	16	Stubb's Beef Spice Rub, 56g	5,90	10 pcs	24	59,00
3	15	Tex-Mex spice mix, 370g	6,00	5 pcs	24	30,00
4	13	Stubb's Oregano, 30g	2,90	15 pcs	24	43,50

Total excluding VAT € **357,50**
VAT total € **85,80**
Total to pay € **443,30**

Tel: +358207181710 reino.merikoinen@ice... Business ID: 123456-7

CREDIT TRANSFER

Recipient's account number: IBAN Nordea **FI21 1234 5600 007 85** BIC NDEAFIHH

Recipient: SpiceImport Ltd. Kaisaniemenkatu 6A 00100 Helsinki

Payer's name and address: Bering Catering Bulevardi 15 00180 Helsinki

Signature

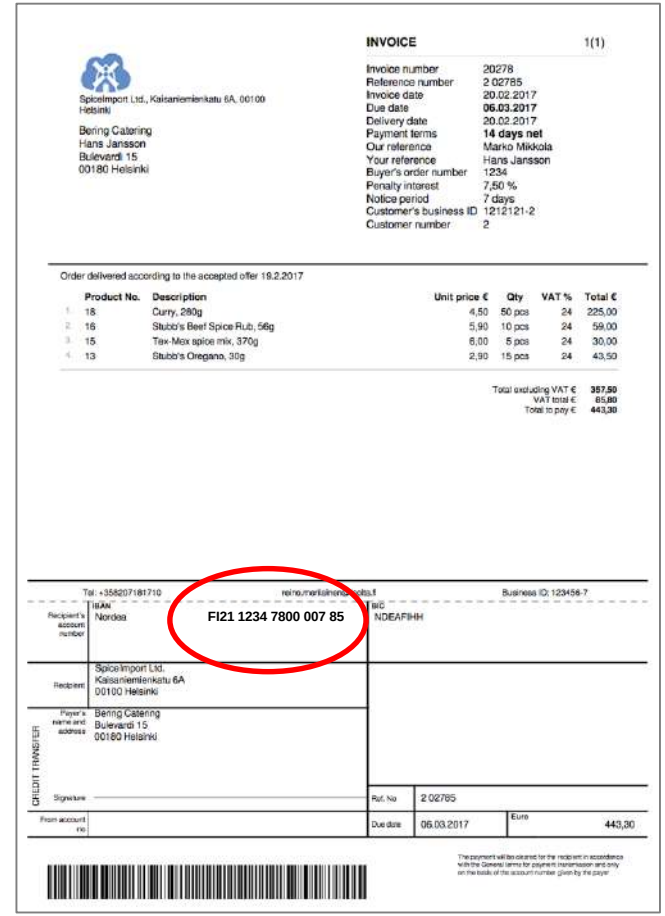
From account no

Ref. No 2 02785

Due date 06.03.2017

Euro 443,30

The payment will be obtained for the recipient in accordance with the General terms for payment transmission and only on the basis of the account number given by the payer



INVOICE 1(1)

SpiceImport Ltd., Kaisaniemenkatu 6A, 00100 Helsinki

Bering Catering
Hans Jansson
Bulevardi 15
00180 Helsinki

Invoice number	20278
Reference number	2 02785
Invoice date	20.02.2017
Due date	**06.03.2017**
Delivery date	20.02.2017
Payment terms	**14 days net**
Our reference	Marko Mikkola
Your reference	Hans Jansson
Buyer's order number	1234
Penalty interest	7,50 %
Notice period	7 days
Customer's business ID	1212121-2
Customer number	2

Order delivered according to the accepted offer 19.2.2017

	Product No.	Description	Unit price €	Qty	VAT %	Total €
1	18	Curry, 280g	4,50	50 pcs	24	225,00
2	16	Stubb's Beef Spice Rub, 56g	5,90	10 pcs	24	59,00
3	15	Tex-Mex spice mix, 370g	6,00	5 pcs	24	30,00
4	13	Stubb's Oregano, 30g	2,90	15 pcs	24	43,50

Total excluding VAT € **357,50**
VAT total € **85,80**
Total to pay € **443,30**

Tel: +358207181710 reino.merikoinen@... Business ID: 123456-7

CREDIT TRANSFER

Recipient's account number: IBAN Nordea **FI21 1234 7800 007 85** BIC NDEAFIHH

Recipient: SpiceImport Ltd. Kaisaniemenkatu 6A 00100 Helsinki

Payer's name and address: Bering Catering Bulevardi 15 00180 Helsinki

Signature

From account no

Ref. No 2 02785

Due date 06.03.2017

Euro 443,30

The payment will be obtained for the recipient in accordance with the General terms for payment transmission and only on the basis of the account number given by the payer


Acronis
Cyber Foundation
www.acronis.org
Building a more knowledgeable future
CREATE, SPREAD
AND PROTECT
KNOWLEDGE WITH US!
Building new schools • Providing educational programs • Publishing books