ALTOROS™

Blockchain for Insurance:

From Preventing Fraud to Automating Claims

Insurance is exposed to a variety of fraud schemes: from sharing an insurance plan after divorce to concealing medical diagnoses. This 20-page paper explores how blockchain can help.

Q1 2018

Table of Contents

Featured figures:

1. Executive summary

Globally, both life and non-life insurance premiums for 2015 amounted to about $2.5 trillion and $2 trillion, respectively. Being a trillion-dollar business, insurance stays vulnerable to fraudulent activities. The Coalition Against Insurance Fraud estimates that over $80 billion a year is lost to fraud.

According to IBM, this happens because the current methods of storing and reconciling financial data are too complex and fragmented. There are certain gaps in visibility that cheaters are well aware of and so, as IBM wisely remarks, “the bad guys know more than the good guys.” The examples include sharing the same device to create multiple policies, faking death, misreporting medical diagnoses, filing more than one claim for a single injury, etc.

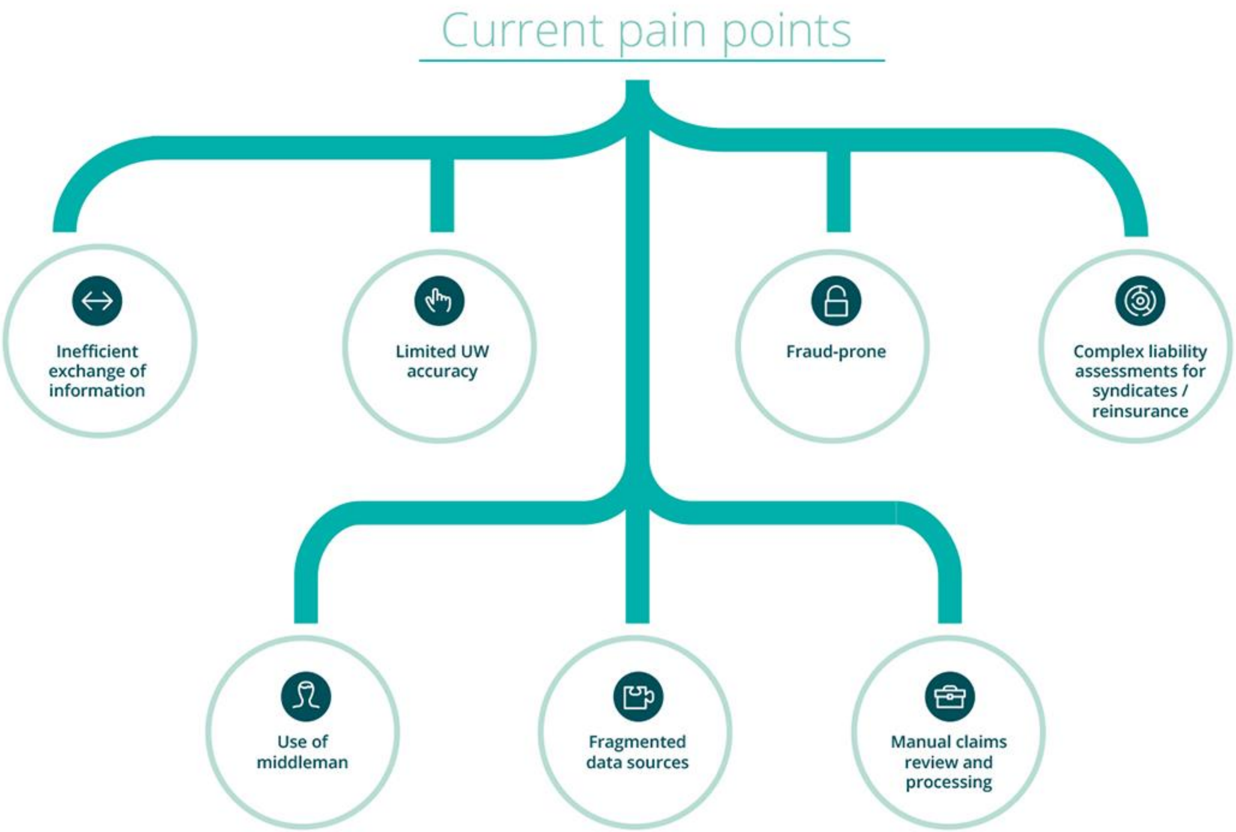

Current pain points
Inefficient exchange of information
Limited UW accuracy
Fraud-prone
Complex liability assessments for syndicates / reinsurance
Use of middleman
Fragmented data sources
Manual claims review and processing

Figure 1.1 Current issues in the insurance industry (Source: Deloitte)

Why does this happen? Organizations involved in insurance are reluctant to share their data due to the following concerns:

- Disclosing personally identifiable information puts privacy at risk.
- Sharing data with organizations in other countries means having to comply with different laws and regulations.
- Organizations are unwilling to share sensitive information, such as profits and losses, to competitors.
- Some insurers may want a central authority to manage the shared data.

- The free-rider problem occurs, implying that larger organizations contribute more and get less value compared to smaller ones.

As a result, criminals use the reluctance of organizations to share data for the advantage of their own. Though such policies as *the Medicare Access and CHIP Reauthorization Act* (MACRA) were introduced by governmental institutions to enable interoperability, insurance providers still experience certain difficulties. The burdens are mostly imposed by workflow issues and vendor costs/capabilities when sharing data. In some cases, sharing *electronic health record* (EHR) can cost from $5,000 to $50,000.

For healthcare insurance, the resistance to share information between organizations becomes an even bigger problem. Hospitals and insurers would rather keep their own data to easily comply with *the Health Insurance Portability and Accountability Act* (HIPAA).

Hampered by “fragmentation” and manual processes, a typical insurance/reinsurance cycle, as a result, would take up to 45 days on average to complete (see the source). It can take even longer, depending on the level of automation involved. Inefficient information validation is yet another weak point that exposes insurance to fraud.

Written for both enterprise readers and startups, this paper explores how blockchain can address the pain points of the insurance industry. In the study, we explain how the decentralized nature of the technology and its immutability improve security of data. Finally, we cover some technical aspects of implementation and provide scenarios where blockchain fits best.

2. Why blockchain?

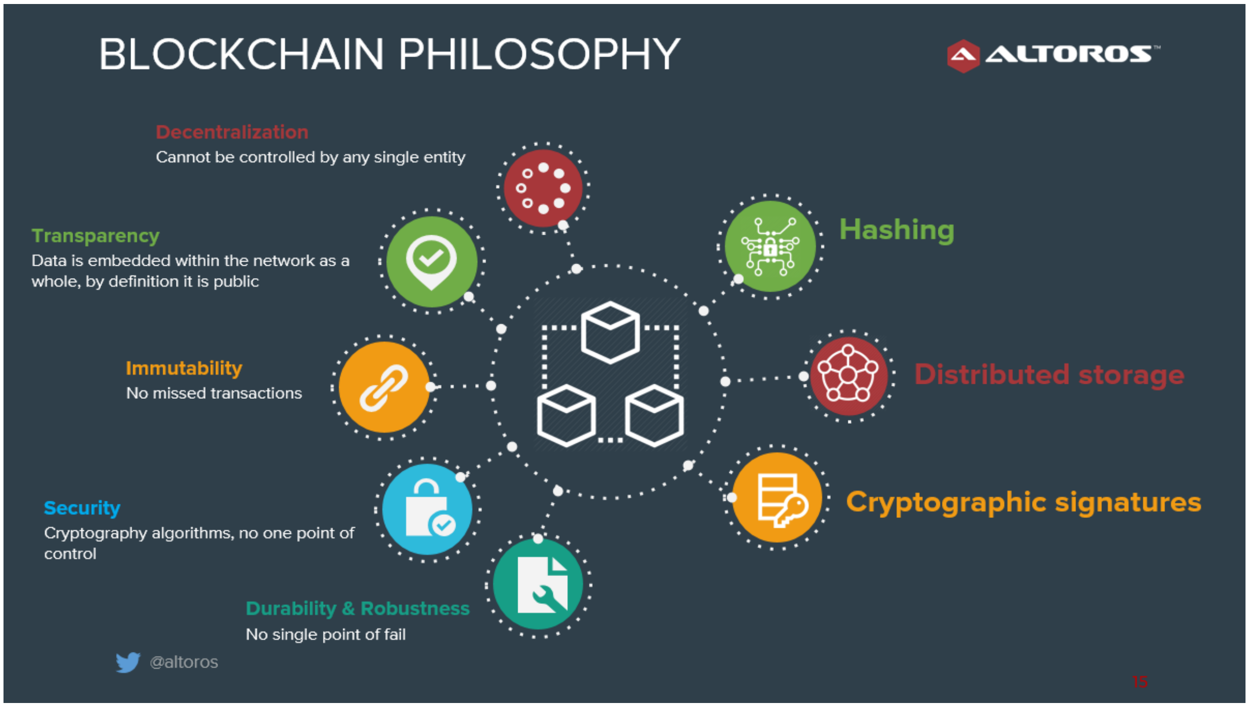
2.1 Blockchain overview

In a nutshell, blockchain is a decentralized ledger that contains data and performs transactions involving multiple parties. A ledger is based upon the following postulates:

- **Decentralization.** There is no single node that has authority over the blockchain network.
- **Transparency.** By design, transactions are public and viewable to all the nodes in the network.
- **Immutability.** Data written in a blockchain is final and cannot be modified or deleted.
- **Security.** The ledger is innately secure due to decentralization and immutability. Security is taken a step further with the use of cryptographic algorithms.
- **Durability and robustness.** Due to the decentralized nature, there is no single point of failure. So, the chances of data loss—e.g., if all the nodes go offline—are really low.

These principles are enabled by three core technical features:

- **Hashing.** Data is encoded and connected through hashing.
- **Distributed storage.** Each node in the network has a copy of all the data.
- **Cryptographic signatures.** Transactions are verified using the sender’s private key and the receiver’s public key.



BLOCKCHAIN PHILOSOPHY

Decentralization
Cannot be controlled by any single entity

Transparency
Data is embedded within the network as a whole, by definition it is public

Immutability
No missed transactions

Security
Cryptography algorithms, no one point of control

Durability & Robustness
No single point of fail

Hashing

Distributed storage

Cryptographic signatures

@altoros

15

Figure 2.1 Blockchain as a decentralized, immutable ledger of records

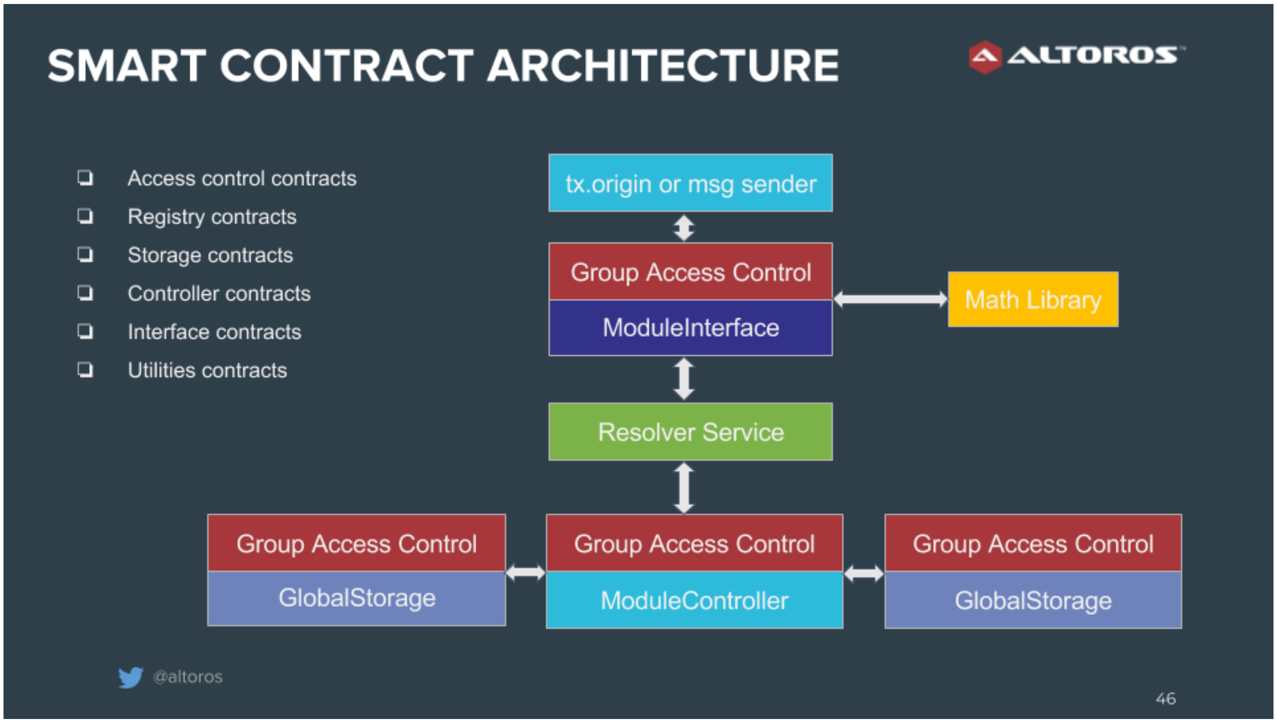
2.2 Smart contracts and ledgers

One of the key building blocks of a decentralized ledger is a **smart contract**—a protocol that contains business logic and conditions for transferring assets between accounts. The contract is executed by the network of computers, and results are stored in a ledger. Based on the principles of modularity, security, and integrity, smart contracts are self-verifying, self-executing, and tamper-resistant.

Below, you can see a sample architecture of the group access control contracts responsible for permissioned access. It is quite a basic one, and it can change to address the needs of a particular case.

This very architecture comprises six components:

- *Access control contracts* define access to the resources.
- *Registry contracts* (name => address) represent a key-value store and permit *interface* and *controller contracts* to resolve the addresses of other contracts.
- *Storage contracts*, naturally, store data. By design, their logic is limited to checking the access level and enabling data getters/setters. Storage contracts are invoked by controller contracts.
- *Controller contracts* manage storage contracts and are invoked by either other controller contracts or interface contracts.
- *Interface contracts* enable interaction between end users and contracts.
- *Utilities contracts* provide additional libraries.



SMART CONTRACT ARCHITECTURE

- ❏ Access control contracts
- ❏ Registry contracts
- ❏ Storage contracts
- ❏ Controller contracts
- ❏ Interface contracts
- ❏ Utilities contracts

tx.origin or msg sender

Group Access Control

ModuleInterface

Math Library

Resolver Service

Group Access Control

GlobalStorage

Group Access Control

ModuleController

Group Access Control

GlobalStorage

@altoros

46

Figure 2.2 A sample architecture of a smart contract

There are two types of ledgers that store blockchain data:

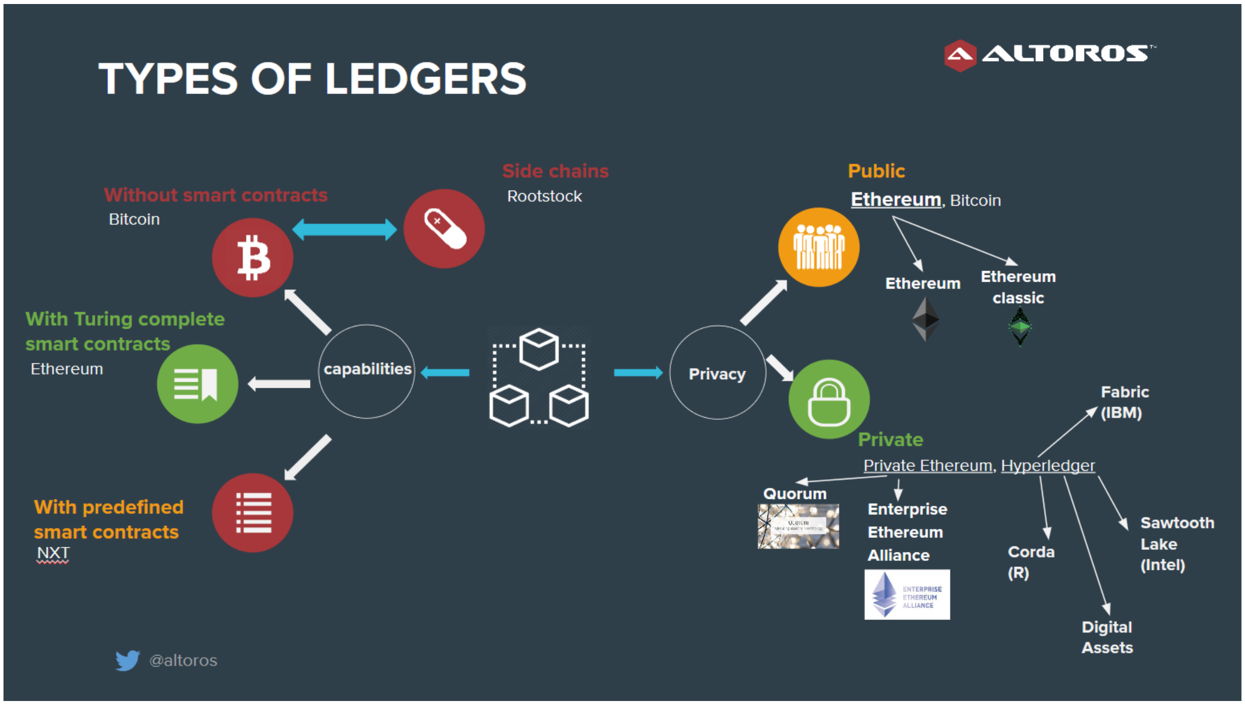
- **Public.** The information about transactions is available to everyone. It makes data anonymous, so you do not see the names, but you can see how many assets are transferred between the accounts.

  Ethereum is one of the popular *public blockchains* that do not focus on cryptocurrency cases only. Though public ledger grants transparency, the security question is still open. So, the Ethereum Foundation is also moving towards creating an enterprise-grade private blockchain. For the purpose, the Enterprise Ethereum Alliance has been founded to connect Fortune 500 members, startups, and academics.

- **Private.** Includes a comprehensive system of permissions and can guarantee any level of privacy. In the private ledgers, transaction content is encrypted, so only authorized participants may see it, protecting the confidentiality of business transactions.

  Driven by the Linux Foundation, the Hyperledger Project is a major option in the domain of *private ledgers*. Now, Hyperledger has five frameworks—Fabric, Iroha, Burrow, Sawtooth, and Indy—each serving particular use cases.

  A federated blockchain has all the distinguishing characteristic of a private ledger. However, it operates under the leadership of a group of companies, or a consortium. An example of such a consortium are the members of the Blockchain Insurance Industry Initiative B3i.



TYPES OF LEDGERS

ALTOROS™

Without smart contracts
Bitcoin

Side chains
Rootstock

With Turing complete smart contracts
Ethereum

capabilities

Privacy

With predefined smart contracts
NXT

Public
Ethereum, Bitcoin

Ethereum

Ethereum classic

Private
Private Ethereum, Hyperledger

Fabric (IBM)

Quorum

Enterprise Ethereum Alliance

Corda (R)

Sawtooth Lake (Intel)

Digital Assets

@altoros

Figure 2.3 Types of a distributed ledger

3. How blockchain can help insurance companies

3.1 Mitigating fraud and sharing records

In insurance, fraud mostly happens due to the inefficient methods of managing information across participants in the network. A study by Deloitte lists common reasons behind fraudulent activities:

- Providers falsify service claims to receive higher payments.
- Plan owners attempt to file claims for ineligible dependents.
- Applicants withhold adding major diseases in their medical history.

Due to its decentralized nature, blockchain grants immutability and transparency with a view to **mitigate fraud**. The technology can help to minimize counterfeiting, double booking, and document or contract alterations. The insurers are able to create receipts at any stage of the claims process, while ensuring an auditable record of all the claims activities. As IBM puts it, all the participants can get a “distributed, single view of the entire exposure data chain.”

Recognizing the potential of blockchain in ensuring secure workflows for insurance, IBM contemplated how a counter-fraud solution would look like.

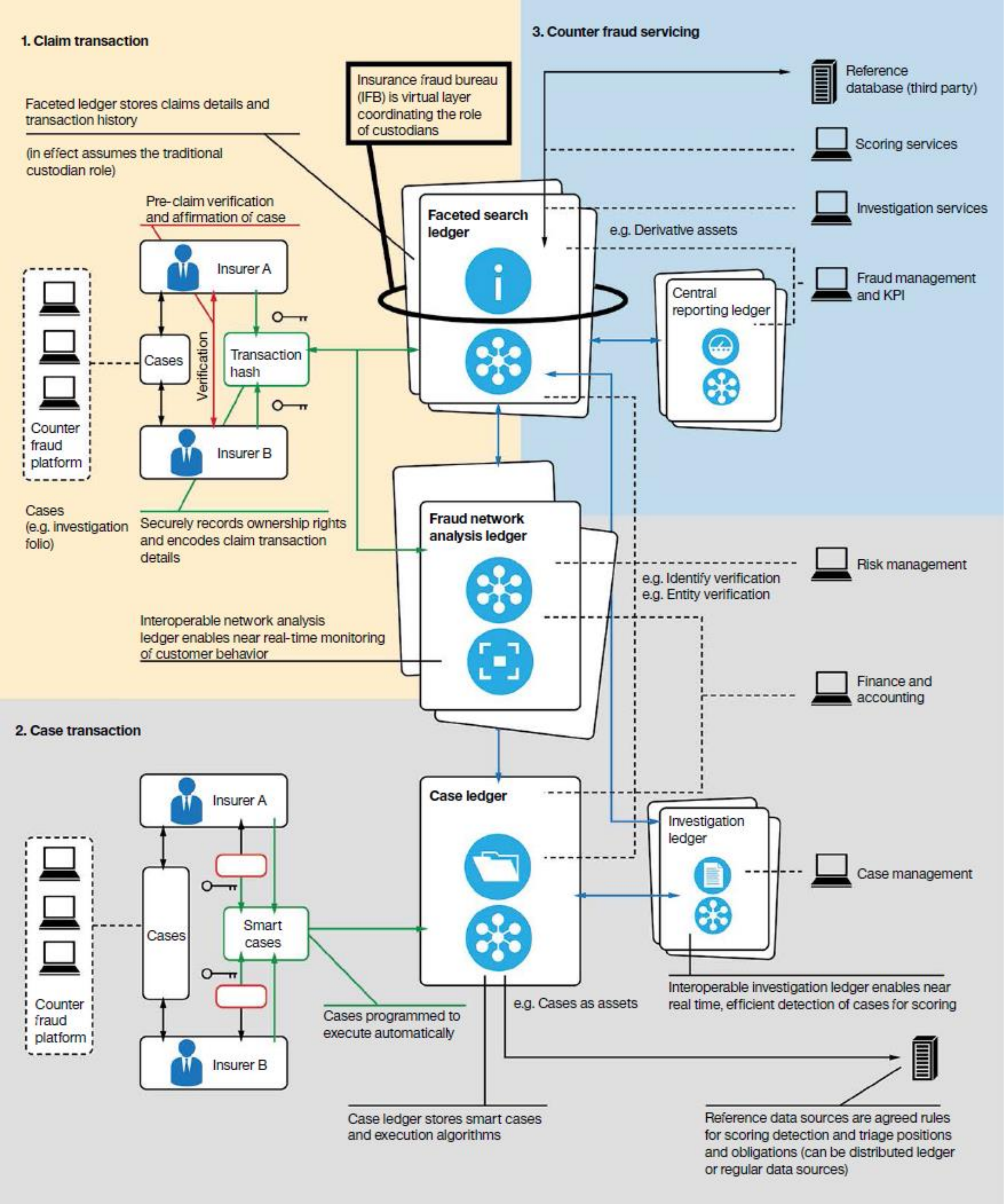
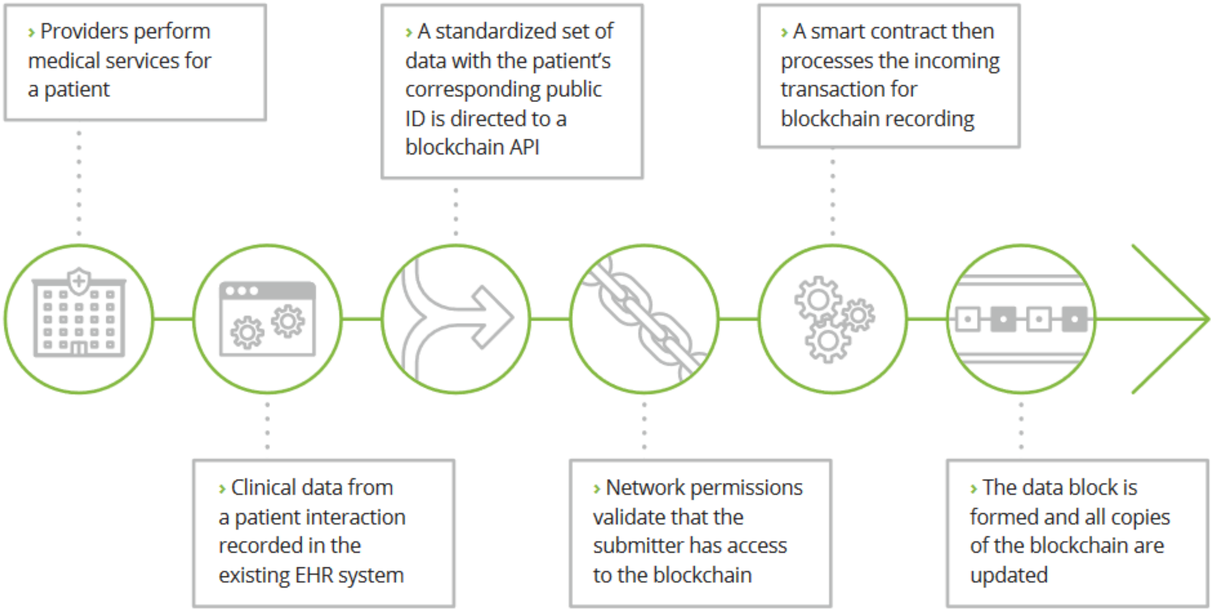

1. Claim transaction
Faceted ledger stores claims details and transaction history
(in effect assumes the traditional custodian role)
Pre-claim verification and affirmation of case
Insurer A
Cases
Verification
Transaction hash
Insurer B
Counter fraud platform
Cases (e.g. investigation folio)
Securely records ownership rights and encodes claim transaction details
Interoperable network analysis ledger enables near real-time monitoring of customer behavior
Insurance fraud bureau (IFB) is virtual layer coordinating the role of custodians
Faceted search ledger
Fraud network analysis ledger
3. Counter fraud servicing
Reference database (third party)
Scoring services
Investigation services
e.g. Derivative assets
Central reporting ledger
Fraud management and KPI
Risk management
e.g. Identify verification
e.g. Entity verification
Finance and accounting
2. Case transaction
Insurer A
Cases
Smart cases
Insurer B
Counter fraud platform
Case ledger
Cases programmed to execute automatically
e.g. Cases as assets
Investigation ledger
Case management
Interoperable investigation ledger enables near real time, efficient detection of cases for scoring
Case ledger stores smart cases and execution algorithms
Reference data sources are agreed rules for scoring detection and triage positions and obligations (can be distributed ledger or regular data sources)

Figure 3.1 A sample counter-fraud architecture with blockchain suggested by IBM (Source)

Using blockchain, healthcare organizations can **safely share data** to create a comprehensive electronic healthcare record for all patients. Patients and other authorized users can then provide private keys to give access to physicians and insurers to improve data security.



› Providers perform medical services for a patient

› Clinical data from a patient interaction recorded in the existing EHR system

› A standardized set of data with the patient's corresponding public ID is directed to a blockchain API

› Network permissions validate that the submitter has access to the blockchain

› A smart contract then processes the incoming transaction for blockchain recording

› The data block is formed and all copies of the blockchain are updated

Figure 3.2 A potential roadmap for writing medical data on blockchain (Source: Deloitte)

With a decentralized database storing shared data, insurers can be certain that the information they see is accurate and up-to-date.

Being one of the fastest adopters and developers, Estonia's government has already put its healthcare system on blockchain. Different healthcare providers across the country come together on the blockchain network to provide a common record for each individual patient.

3.2 Automating data gathering and transaction processing

Deloitte attributes long application/claiming cycles to inefficient information acquisition, processing, and sharing. Their report mentions that slow propagation of information happens because "many insurers are using claims systems that were originally built more than 30 years ago." This issue also makes it hard for insurers to maintain their systems and adopt new strategies.

In addition to improving security while data sharing, blockchain can play its role in automating and streamlining insurance processes. In this scenario, blockchain can enable insurers to:

- Automate information collection and processing through smart contracts
- Improve data access and visibility
- Lower overall cost due to faster transactions and processes automated by smart contracts

IBM has a similar vision on the process automation imposed by blockchain.

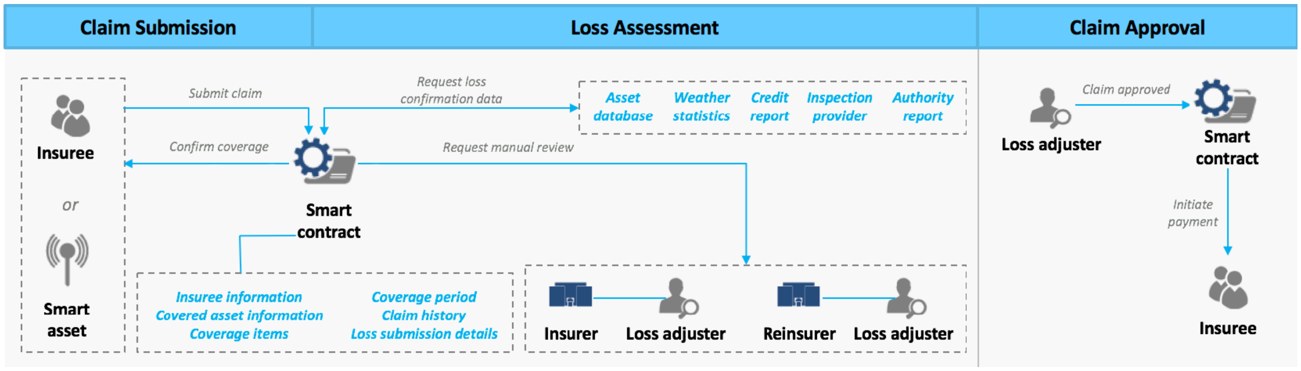
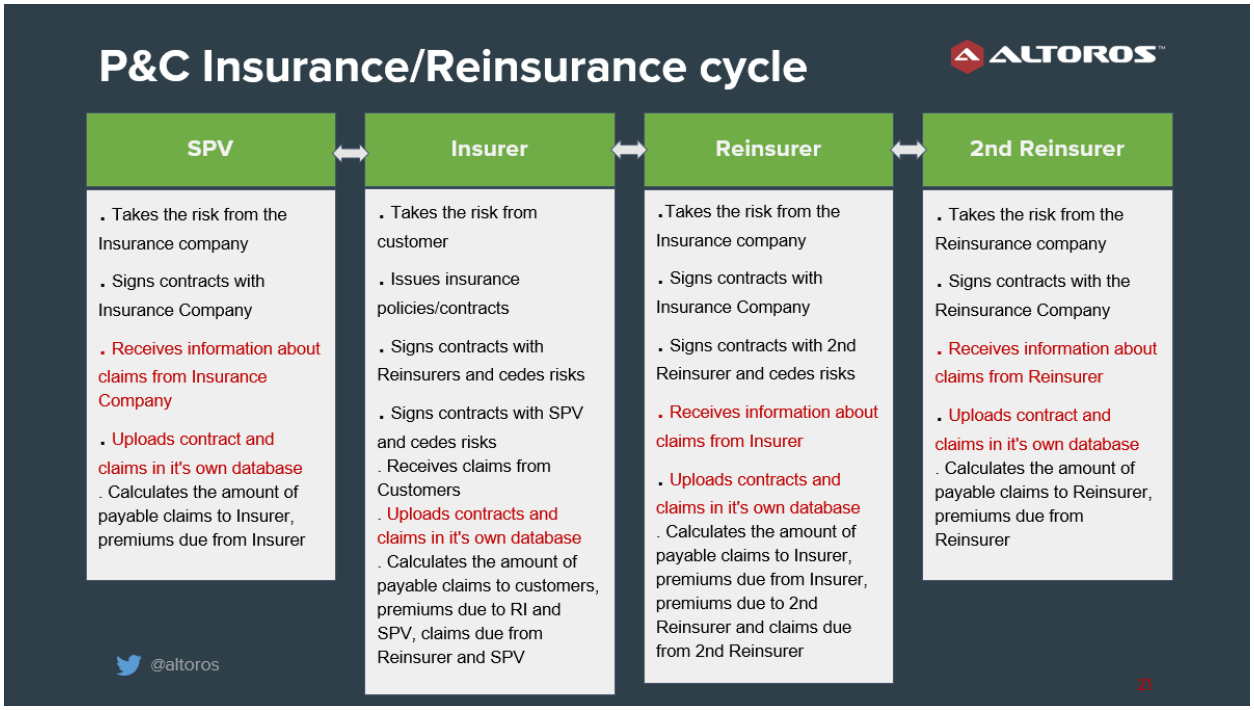


Figure 3.3 The claiming process automated by smart contracts (Source: IBM)

In healthcare insurance, any reduction to overhead costs can help insurers reach a required medical loss ratio as mandated in the Affordable Care Act. Making use of smart contracts to automate information collection also removes any delays, ensuring shared healthcare records are kept up-to-date.

In addition, Deloitte mentions in their report that "with the entirety of a consumer's medical and wellness records consolidated in a series of blockchains, the life insurance underwriting and application process could be whittled down *from an average 45 days to near real time*." By storing healthcare records on blockchain, much of the tedium involved with applying for life insurance can be avoided. Data on blockchain can simply be verified by insurers to approve applications in real time. This removes the trouble applicants usually go through with gathering and submitting current information.

Not only insurance processes, but the reinsurance cycle can be enhanced, as well. Some of the operations that can be improved with blockchain are shown below—exemplified on the property and casualty (P&C) insurance.



P&C Insurance/Reinsurance cycle

SPV	Insurer	Reinsurer	2nd Reinsurer
. Takes the risk from the Insurance company . Signs contracts with Insurance Company . Receives information about claims from Insurance Company . Uploads contract and claims in it's own database . Calculates the amount of payable claims to Insurer, premiums due from Insurer	. Takes the risk from customer . Issues insurance policies/contracts . Signs contracts with Reinsurers and cedes risks . Signs contracts with SPV and cedes risks . Receives claims from Customers . Uploads contracts and claims in it's own database . Calculates the amount of payable claims to customers, premiums due to RI and SPV, claims due from Reinsurer and SPV	.Takes the risk from the Insurance company . Signs contracts with Insurance Company . Signs contracts with 2nd Reinsurer and cedes risks . Receives information about claims from Insurer . Uploads contracts and claims in it's own database . Calculates the amount of payable claims to Insurer, premiums due from Insurer, premiums due to 2nd Reinsurer and claims due from 2nd Reinsurer	. Takes the risk from the Reinsurance company . Signs contracts with the Reinsurance Company . Receives information about claims from Reinsurer . Uploads contract and claims in it's own database . Calculates the amount of payable claims to Reinsurer, premiums due from Reinsurer

@altoros

21

Figure 3.4 Processes involved in the insurance/reinsurance cycle

Blockchain also opens the opportunity for dynamic insurance pricing. As car insurers can make use of a driver's age or a number of accidents, health insurarers may employ a set of similar criteria. With automated blockchain, it becomes much harder to provide false information.

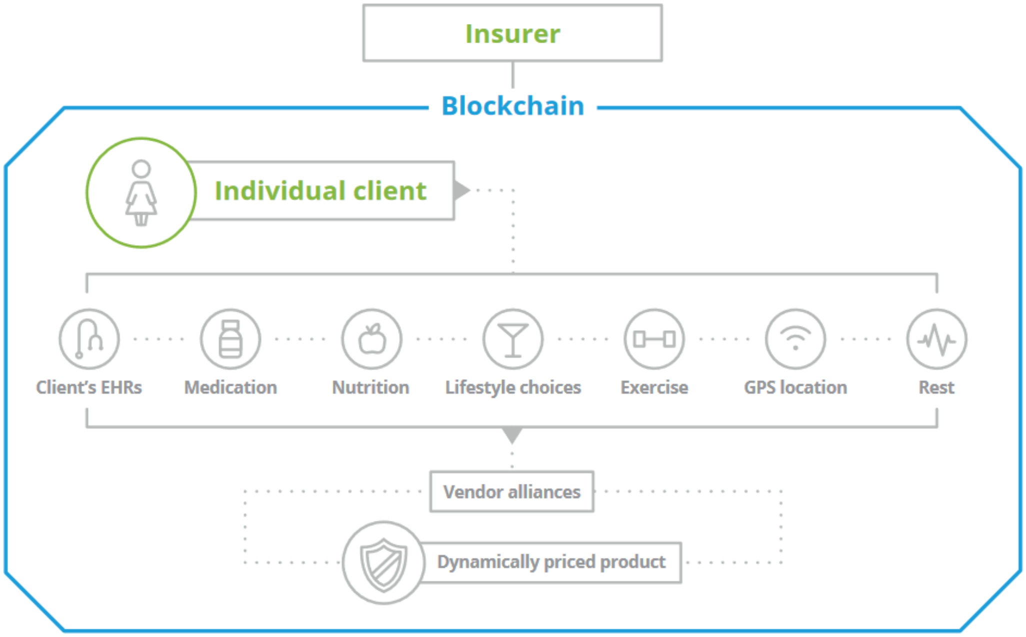


Figure 3.5 Dynamic pricing powered by blockchain (Source: Deloitte)

With a decentralized ledger, insurers are able to aggregate all health-lifestyle data coming from multiple sources in a single place continually updated in almost real time. This allows for more frequent risk reassessments and customized pricing.

3.3 Insurance across borders

When it comes to insurance, there are not so many multinational providers. Typically, insurers operate within a single territory. This is because of the complexity involved in having to comply with the laws and regulations of multiple countries.

By capitalizing on smart contracts, insurers can develop multinational policies using blockchain. American International Group, Standard Chartered Bank, and IBM are looking into multinational insurance policies using Hyperledger Fabric. The collaboration involved converting a controlled master policy written in the UK along with three local policies from the US, Singapore, and Kenya. The three jurisdictions were chosen for their market growth and complex regulatory requirements.

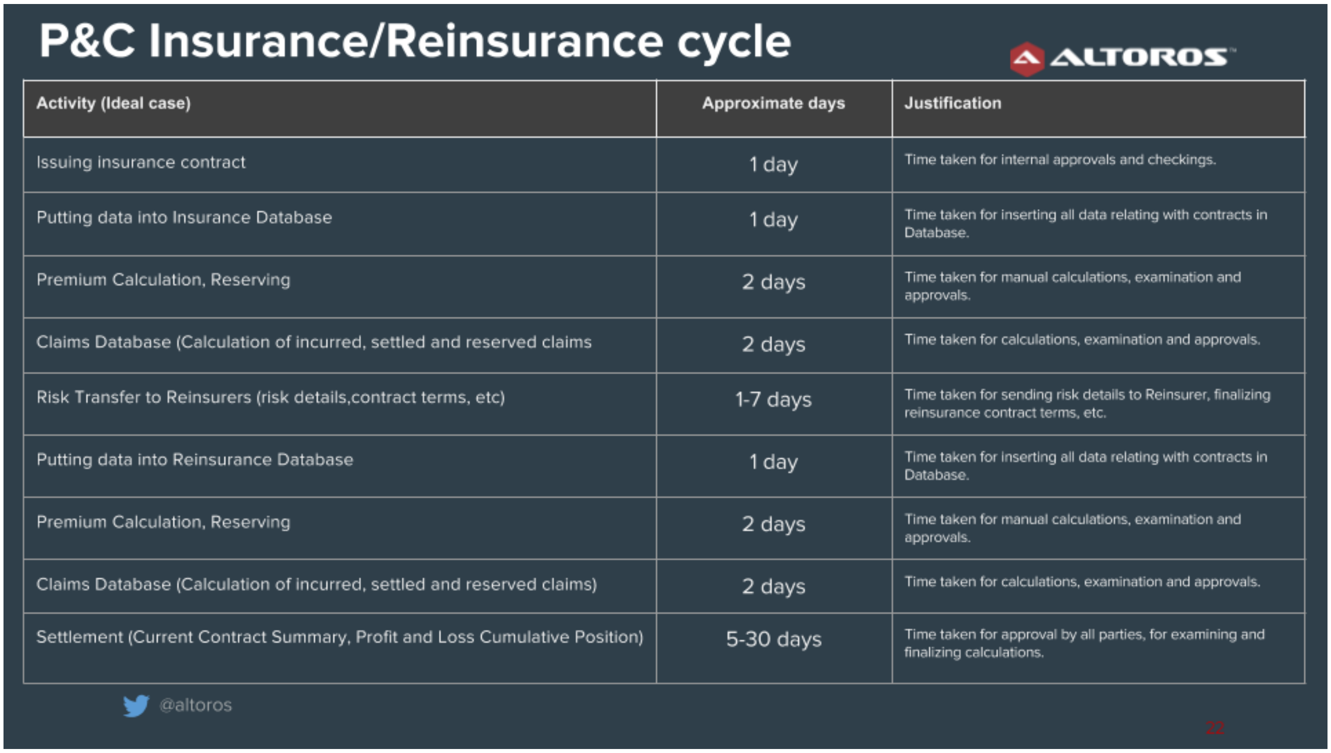
Another global cooperation in this area is the Blockchain Insurance Industry Initiative B3i. In October 2016, Swiss Re, Liberty Mutual, and other major insurance companies joined forces to explore the potential of blockchain. Since then, the initiative has expanded to 15 members.

There also emerge new types of blockchain-based products for insurance across the borders. For instance, an InsurTech startup Etherisc has recently launched a travel insurance app that allows for getting an instant, automated payout in case your flight was delayed or canceled.

4. Cost and time savings driven by blockchain

4.1 Processes automation

Blockchain allows for automating each step of the insurance/reinsurance cycle, removing manual routine from the process. Such steps as issuing contracts or putting data to a database take up to 1–2 days. Some of steps (e.g., a settlement or transferring a risk) can take from 5 to 30 days. If you sum up all the steps, the whole cycle may last from 17 to 48 days on average. The duration depends on the complexity of a particular case and a level of automation. Below, you can see the detailed description of these steps and their time equivalent in days, when done manually.



P&C Insurance/Reinsurance cycle

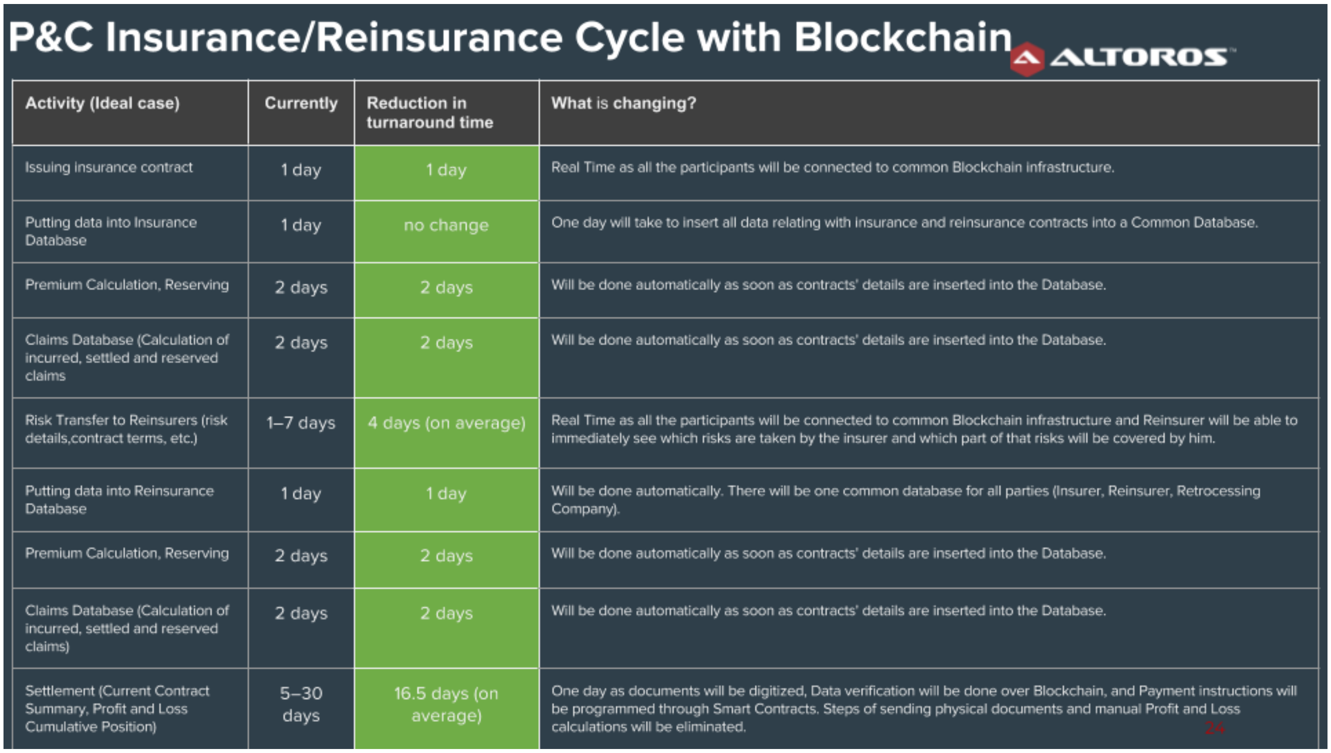
Activity (Ideal case)	Approximate days	Justification
Issuing insurance contract	1 day	Time taken for internal approvals and checkings.
Putting data into Insurance Database	1 day	Time taken for inserting all data relating with contracts in Database.
Premium Calculation, Reserving	2 days	Time taken for manual calculations, examination and approvals.
Claims Database (Calculation of incurred, settled and reserved claims	2 days	Time taken for calculations, examination and approvals.
Risk Transfer to Reinsurers (risk details,contract terms, etc)	1-7 days	Time taken for sending risk details to Reinsurer, finalizing reinsurance contract terms, etc.
Putting data into Reinsurance Database	1 day	Time taken for inserting all data relating with contracts in Database.
Premium Calculation, Reserving	2 days	Time taken for manual calculations, examination and approvals.
Claims Database (Calculation of incurred, settled and reserved claims)	2 days	Time taken for calculations, examination and approvals.
Settlement (Current Contract Summary, Profit and Loss Cumulative Position)	5-30 days	Time taken for approval by all parties, for examining and finalizing calculations.

@altoros

22

Figure 4.1 Manual process of the insurance/reinsurance cycles

So, how does it change with blockchain? The activities that do not need human approval, such as issuing a contract or updating data and storing it in a database, can now be performed in real time. In total, as much as 30.5 days can be removed from the entire process using blockchain.



P&C Insurance/Reinsurance Cycle with Blockchain

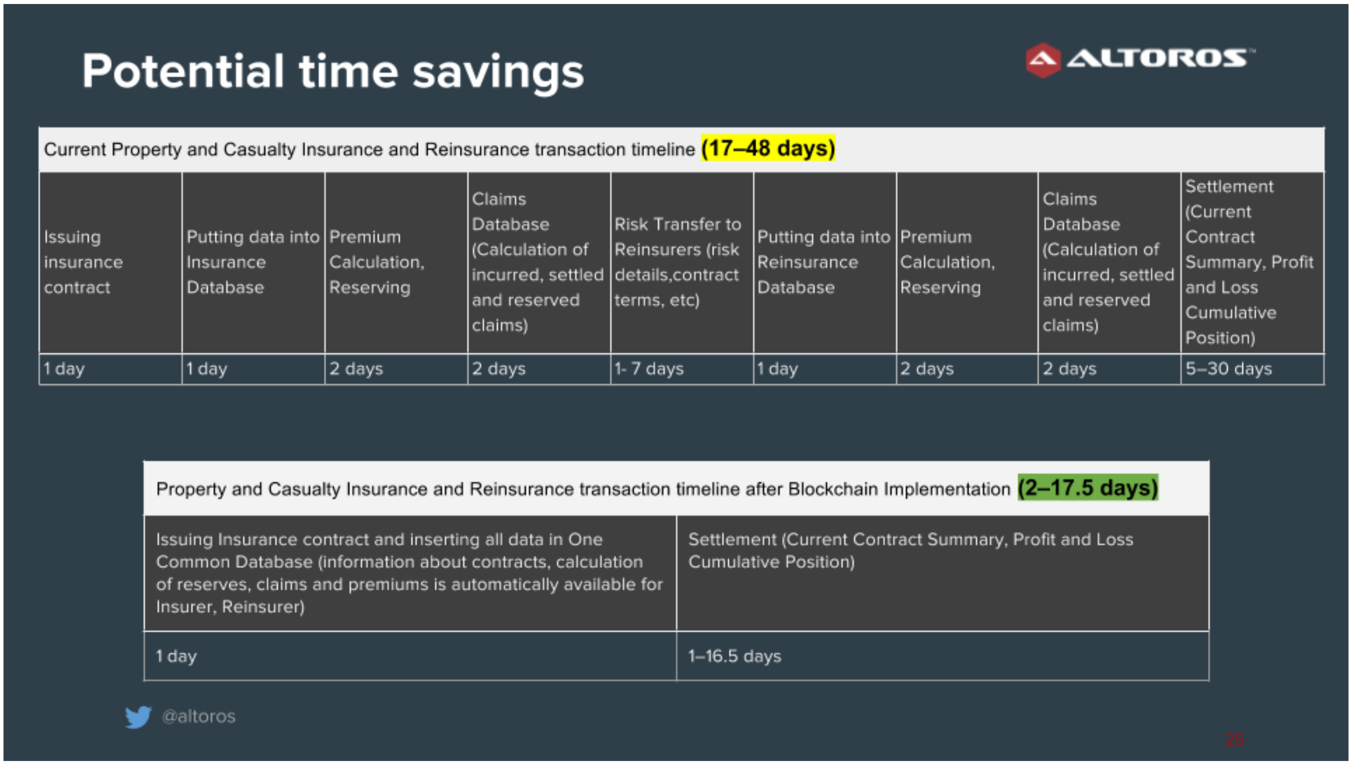
ALTOROS

Activity (Ideal case)	Currently	Reduction in turnaround time	What is changing?
Issuing insurance contract	1 day	1 day	Real Time as all the participants will be connected to common Blockchain infrastructure.
Putting data into Insurance Database	1 day	no change	One day will take to insert all data relating with insurance and reinsurance contracts into a Common Database.
Premium Calculation, Reserving	2 days	2 days	Will be done automatically as soon as contracts' details are inserted into the Database.
Claims Database (Calculation of incurred, settled and reserved claims	2 days	2 days	Will be done automatically as soon as contracts' details are inserted into the Database.
Risk Transfer to Reinsurers (risk details,contract terms, etc.)	1–7 days	4 days (on average)	Real Time as all the participants will be connected to common Blockchain infrastructure and Reinsurer will be able to immediately see which risks are taken by the insurer and which part of that risks will be covered by him.
Putting data into Reinsurance Database	1 day	1 day	Will be done automatically. There will be one common database for all parties (Insurer, Reinsurer, Retrocessing Company).
Premium Calculation, Reserving	2 days	2 days	Will be done automatically as soon as contracts' details are inserted into the Database.
Claims Database (Calculation of incurred, settled and reserved claims)	2 days	2 days	Will be done automatically as soon as contracts' details are inserted into the Database.
Settlement (Current Contract Summary, Profit and Loss Cumulative Position)	5–30 days	16.5 days (on average)	One day as documents will be digitized, Data verification will be done over Blockchain, and Payment instructions will be programmed through Smart Contracts. Steps of sending physical documents and manual Profit and Loss calculations will be eliminated.

24

Figure 4.2 The automated insurance/reinsurance cycle with blockchain

The following table demonstrates how blockchain implementation can help to complete the whole cycle in 2–17.5 days.



Potential time savings

ALTOROS

Current Property and Casualty Insurance and Reinsurance transaction timeline **(17–48 days)**

Issuing insurance contract	Putting data into Insurance Database	Premium Calculation, Reserving	Claims Database (Calculation of incurred, settled and reserved claims)	Risk Transfer to Reinsurers (risk details,contract terms, etc)	Putting data into Reinsurance Database	Premium Calculation, Reserving	Claims Database (Calculation of incurred, settled and reserved claims)	Settlement (Current Contract Summary, Profit and Loss Cumulative Position)
1 day	1 day	2 days	2 days	1- 7 days	1 day	2 days	2 days	5–30 days

Property and Casualty Insurance and Reinsurance transaction timeline after Blockchain Implementation **(2–17.5 days)**

Issuing Insurance contract and inserting all data in One Common Database (information about contracts, calculation of reserves, claims and premiums is automatically available for Insurer, Reinsurer)	Settlement (Current Contract Summary, Profit and Loss Cumulative Position)
1 day	1–16.5 days

@altoros

25

Figure 4.3 Time savings for the insurance/reinsurance after blockchain implementation

4.2 Savings calculation

With smart contracts, insurance and reinsurance can cut down the cost involved in settling claims by 15–25%. This automation of processes can enable cost savings of about $5–10 billion a year worldwide.

Using the insurance/reinsurance cycle described above, it is possible to estimate the potential savings by the example of Germany—based on data from the country's Statistical Yearbook (2016).

According to the study, annual gross operating expenses were €5.6 billion for 205 insurers. The total P&C insurance life cycle was 32.5 days on average. To get the *operating expenses per day*, the gross operating expenses can be divided by the average life cycle duration:

€5.6 billion / 32.5 days = €171.3 million

Using this value, it is possible to estimate the savings gained if blockchain is implemented on all phases of the process. With blockchain reducing turnaround time to 2 days, the total time savings are:

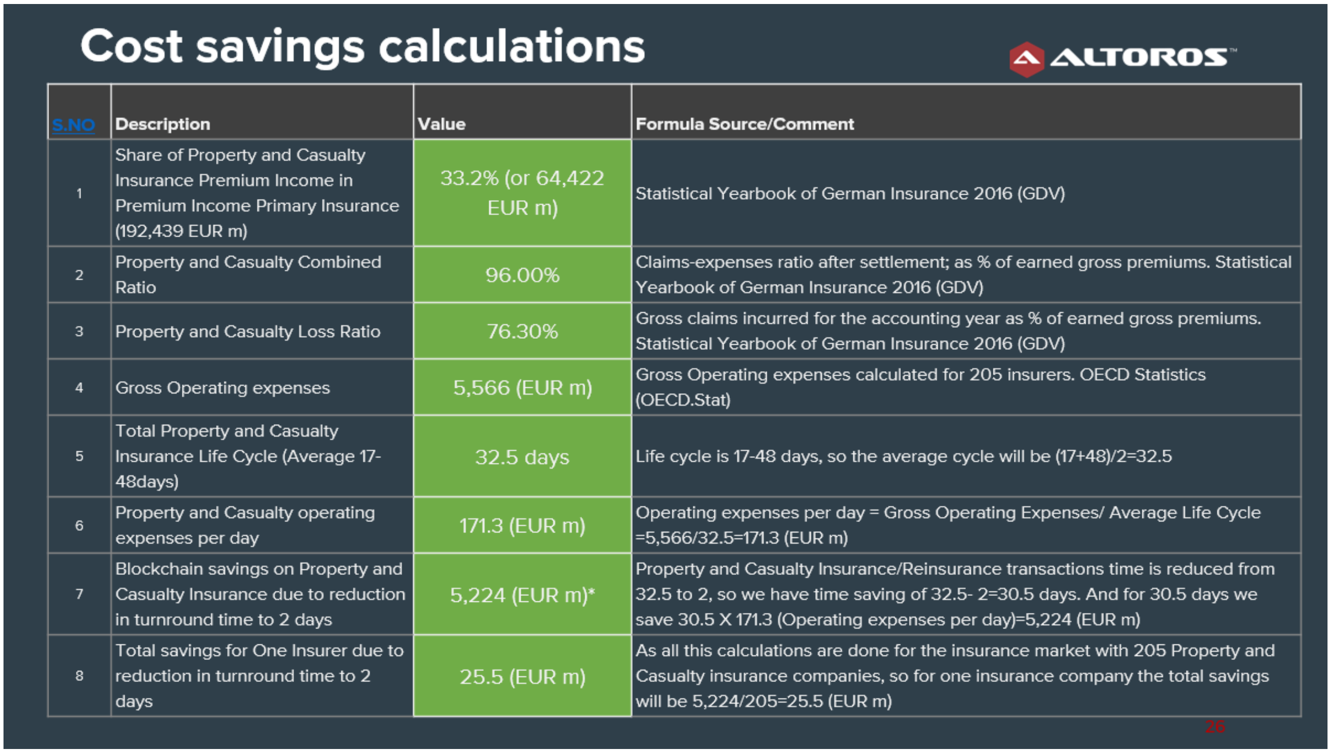
32.5 days – 2 days = 30.5 days

Now, we can calculate the total cost savings across 205 insurers by multiplying operating expenses per day by the amount of the days saved:

€171.3 million × 30.5 days = €5.2 billion

For each insurer, this amounts to:

€5.2 billion / 205 insurers = €25.5 million

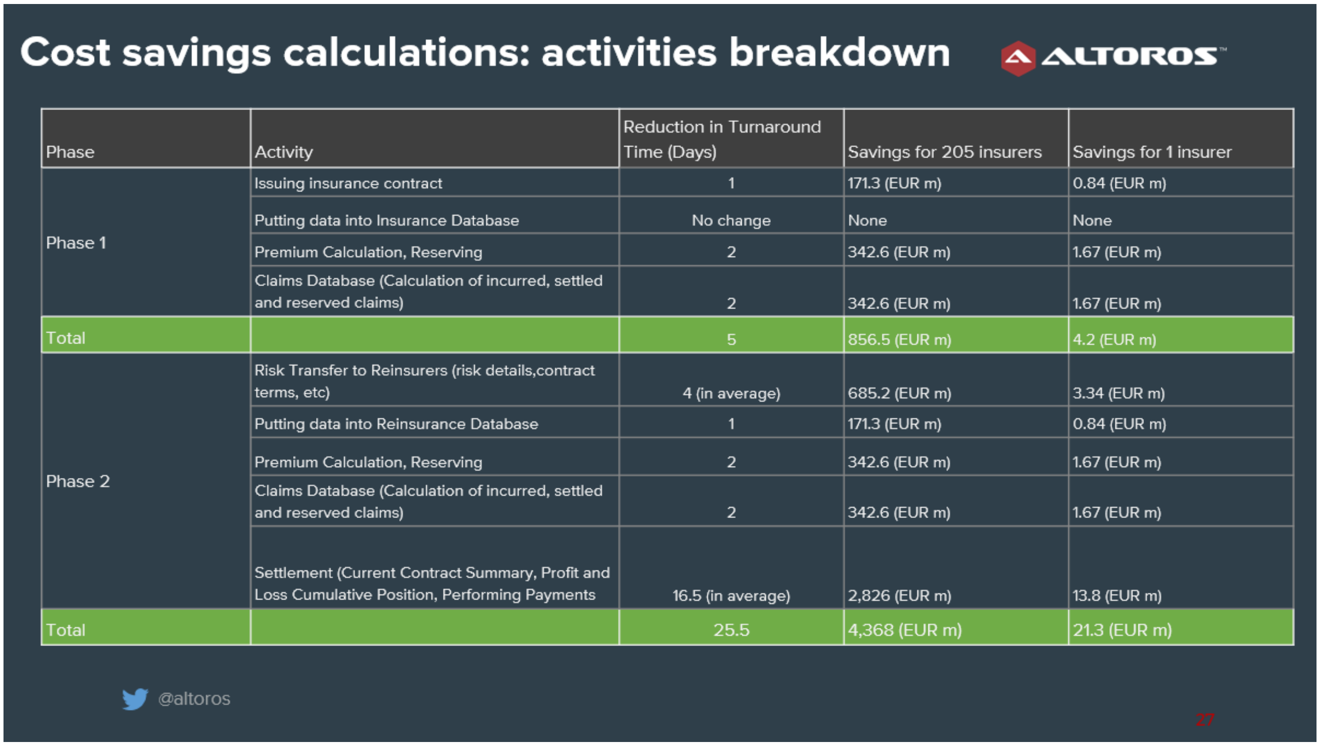


Cost savings calculations

S.NO	Description	Value	Formula Source/Comment
1	Share of Property and Casualty Insurance Premium Income in Premium Income Primary Insurance (192,439 EUR m)	33.2% (or 64,422 EUR m)	Statistical Yearbook of German Insurance 2016 (GDV)
2	Property and Casualty Combined Ratio	96.00%	Claims-expenses ratio after settlement; as % of earned gross premiums. Statistical Yearbook of German Insurance 2016 (GDV)
3	Property and Casualty Loss Ratio	76.30%	Gross claims incurred for the accounting year as % of earned gross premiums. Statistical Yearbook of German Insurance 2016 (GDV)
4	Gross Operating expenses	5,566 (EUR m)	Gross Operating expenses calculated for 205 insurers. OECD Statistics (OECD.Stat)
5	Total Property and Casualty Insurance Life Cycle (Average 17-48days)	32.5 days	Life cycle is 17-48 days, so the average cycle will be (17+48)/2=32.5
6	Property and Casualty operating expenses per day	171.3 (EUR m)	Operating expenses per day = Gross Operating Expenses/ Average Life Cycle =5,566/32.5=171.3 (EUR m)
7	Blockchain savings on Property and Casualty Insurance due to reduction in turnround time to 2 days	5,224 (EUR m)*	Property and Casualty Insurance/Reinsurance transactions time is reduced from 32.5 to 2, so we have time saving of 32.5- 2=30.5 days. And for 30.5 days we save 30.5 X 171.3 (Operating expenses per day)=5,224 (EUR m)
8	Total savings for One Insurer due to reduction in turnround time to 2 days	25.5 (EUR m)	As all this calculations are done for the insurance market with 205 Property and Casualty insurance companies, so for one insurance company the total savings will be 5,224/205=25.5 (EUR m)

Figure 4.4 Cost savings broken down per day of operation

The insurance/reinsurance cycle can be divided into two phases. The first phase involves an insurance company only, while the second implies a reinsurer enters the process. At Phase 1, the total savings for 205 insurers may amount to €856.5 million (€4.2 million for each individual company). At Phase 2, the total savings can equal to €4 billion for 205 insurers (€21.3 million for each insurer).



Cost savings calculations: activities breakdown

Phase	Activity	Reduction in Turnaround Time (Days)	Savings for 205 insurers	Savings for 1 insurer
Phase 1	Issuing insurance contract	1	171.3 (EUR m)	0.84 (EUR m)
	Putting data into Insurance Database	No change	None	None
	Premium Calculation, Reserving	2	342.6 (EUR m)	1.67 (EUR m)
	Claims Database (Calculation of incurred, settled and reserved claims)	2	342.6 (EUR m)	1.67 (EUR m)
Total		5	856.5 (EUR m)	4.2 (EUR m)
Phase 2	Risk Transfer to Reinsurers (risk details,contract terms, etc)	4 (in average)	685.2 (EUR m)	3.34 (EUR m)
	Putting data into Reinsurance Database	1	171.3 (EUR m)	0.84 (EUR m)
	Premium Calculation, Reserving	2	342.6 (EUR m)	1.67 (EUR m)
	Claims Database (Calculation of incurred, settled and reserved claims)	2	342.6 (EUR m)	1.67 (EUR m)
	Settlement (Current Contract Summary, Profit and Loss Cumulative Position, Performing Payments	16.5 (in average)	2,826 (EUR m)	13.8 (EUR m)
Total		25.5	4,368 (EUR m)	21.3 (EUR m)

@altoros

27

Figure 4.5 Cost savings broken down per process

For insurers that offer their services across a few types of insurance, cost savings multiply across each type of the service. In case a company offers P&C, life, and health insurance, there is a potential to save €25.5 million × 3 insurance types = €76.5 million a year.

5. Implementation considerations and limitations

As we can see, blockchain allows for executing transaction in a trusted network and preventing records from being altered. So, an insurance company may consider the ledger implementation if the transactions currently involve *multiple parties* and require a precise and *immutable record* of the date and time, and need *no central authority*. Likewise, blockchain is effective when there is a risk of data tampering, as well as when data is accessed or manipulated multiple times.

On the other hand, there may be a case where the decentralized ledger is not an appropriate solution. Insurers may continue to work under their current models if transactions involve a limited number of parties, do not require an intermediary, or if a well-established, trusted intermediary already exists.

There are also some technical limitations to consider:

- **Scalability**. Due to the consensus-based validation mechanisms and the continuous replications, as well as the ever-growing amount of stored immutable data, the scalability of a blockchain system is a challenge yet.

- **Standardization**. A lack of standards among blockchain network participants hampers data sharing between organizations, complicating existing workflows.

Regardless the challenges, both enterprises and startups are already infusing blockchain into their workflows and innovative products. For instance, Allianz has adopted blockchain for its global captive insurance program, which also includes cash transfer between countries.

Meanwhile, startup companies develop complementary products to enable business optimization. A brilliant example is Everledger with its digital ledger that tracks provenance of assets for various stakeholders—including insurance companies, claimants, law enforcement agencies, etc. Over 1.2 million diamonds are digitally stored on the Everledger blockchain, ensuring product identification and transaction verification. Etherisc, another InsurTech startup, is building a platform for creating decentralized insurance apps.

The achievements reached by the adopters of blockchain leave us optimistic about the technology. What we observe now is while key industry players are still evaluating the pros and cons of blockchain, newcomers do not hesitate to give it a go in an attempt to disrupt the market. In the digital age, there are chances that their new business models—based on a blockchain—may significantly change the insurance landscape soon.

6. About the authors

Carlo Gutierrez is a Research Analyst at Altoros with 10+ years of experience in publishing and a background in software technology. As part of the Altoros editorial team, his focus has been on emerging technologies, such as Cloud Foundry, blockchain, and the Internet of Things. Prior to Altoros, Carlo primarily wrote about enterprise and consumer technology. Previously, he has served as an Editor for PC World Philippines and Questex Asia.

Elena Travkina is Director of Digital Transformation, Insurance, at Altoros. She has 10+ years of experience in delivery and support of business-critical software applications, working closely with business owners and providing strategic and organizational leadership for software development. Over the years, Elena has served in different capacities, ranging from Software Engineer to Software Engineering Manager and Head of Altoros Ruby Department. She is also one of the founders of the Belarus Ruby User Group.

Alexis Losik is Head of Business Development Team, Hyperledger Project, at Altoros. She is experienced in assessing marketing opportunities and target markets, intelligence gathering on customers and competitors, generating leads for possible cooperation, follow-up connection activities, formal proposal writing, and business model design. Alexis also specializes in evaluating a business and then realizing its full potential, using such tools as marketing, information management, and customer service.

Sophie Turol is passionate about delivering well-structured articles that cater for picky technical audience. With 3+ years in technical writing and 5+ years in editorship, she enjoys collaboration with developers to create insightful, yet intelligible technical tutorials, overviews, and case studies. Sophie is enthusiastic about deep learning solutions—TensorFlow in particular—and PaaS systems, such as Cloud Foundry.

Alex Khizhniak is Director of Technical Evangelism at Altoros and a co-founder of Belarus Java User Group. Since 1998, he has gained experience as a journalist, an editor, an IT blogger, a tech writer, and a meetup organizer. Alex is digging into IoT, Industry 4.0, data science, and distributed systems. The articles he had created (or helped to publish) reached out to nearly one million tech-savvy readers. Some of the pieces were covered at TechRepublic, ebizQ, NetworkWorld, DZone, etc. Find him on Twitter at @alxkh.

***Altoros** is a 300+ people strong consultancy that helps Global 2000 organizations with a methodology, training, technology building blocks, and end-to-end solution development. The company turns cloud-native app development, customer analytics, blockchain, and AI into products with a sustainable competitive advantage. Altoros is a member of the Hyperledger Foundation since 2015. For more, visit www.altoros.com.*

To download more research papers and articles on blockchain:

- *check out our resources page,*
- *subscribe to the blog,*
- *or follow @altoros for daily updates.*

Appendix. Technical aspects of implementation

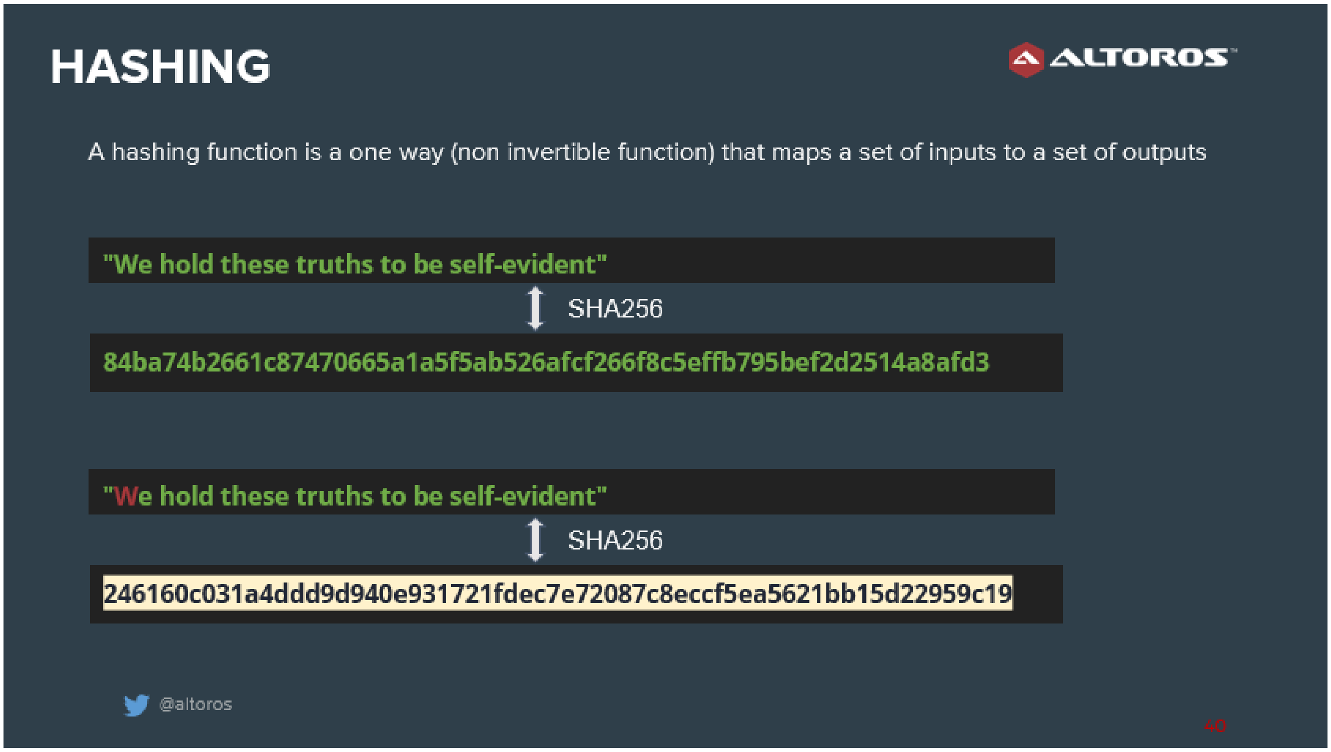
In this section, we highlight the things to know when it comes to the technical side of blockchain adoption from choosing a ledger type to executing smart contracts.

The first priority when implementing a blockchain network is figuring out what kind of a ledger is required. In the world of insurance, private blockchains with Turing-complete smart contracts is advised. This model is preferred due to security concerns and regulations in insurance, as well as the complexity of processes to be automated.

To ensure privacy and security, blockchain makes use of hashing, as well as of private and public keys. Hashing is a cryptographic function that converts any input of data into output depending on the type of algorithm used. The algorithms have to meet two requirements:

- *Preimage resistance.* The complexity involved in decoding the input using the output.
- *Collision resistance.* The chance of getting the same output with two or more different inputs.

In blockchain, hashing is used to store blocks and to generate public keys using private keys.



HASHING

A hashing function is a one way (non invertible function) that maps a set of inputs to a set of outputs

"We hold these truths to be self-evident"

↕ SHA256

84ba74b2661c87470665a1a5f5ab526afcf266f8c5effb795bef2d2514a8afd3

"We hold these truths to be self-evident"

↕ SHA256

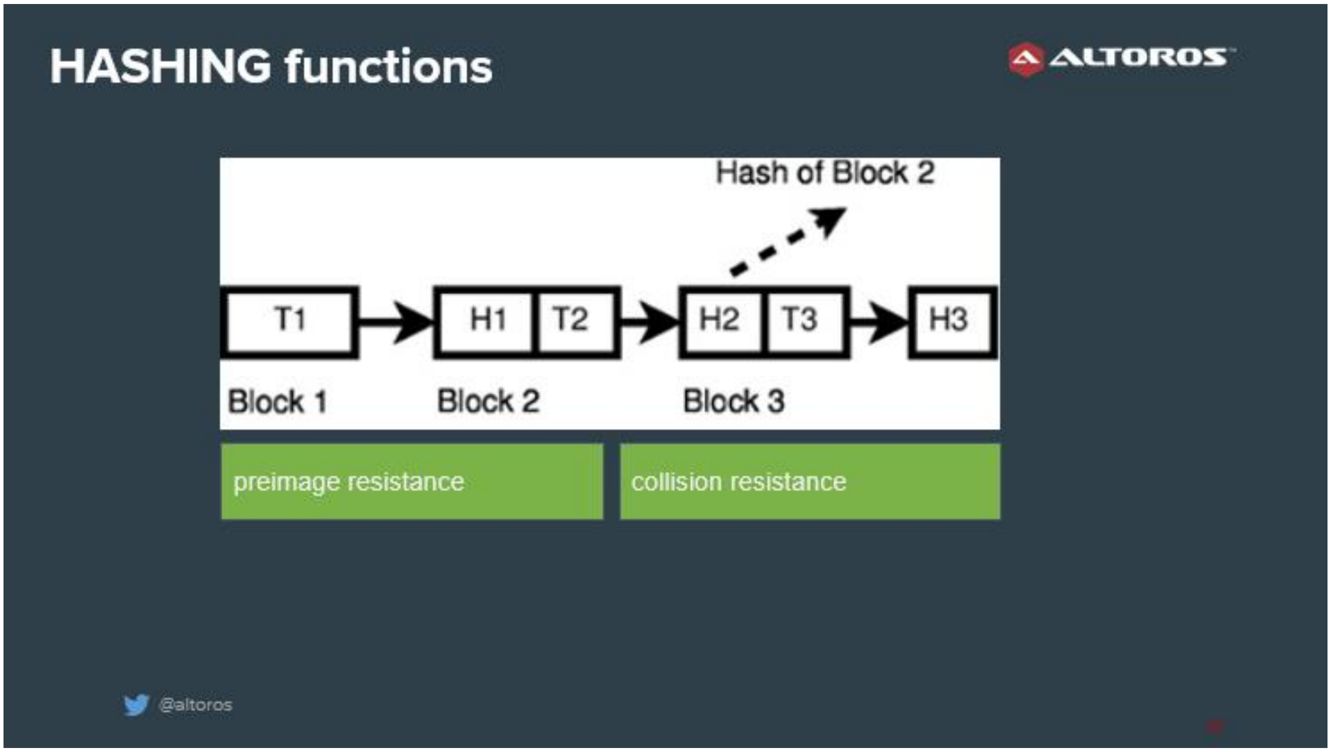
246160c031a4ddd9d940e931721fdec7e72087c8eccf5ea5621bb15d22959c19

@altoros

40

Figure A.1 Hashing with the SHA 256 algorithm

As visualized below, each block contains its own list of transactions, as well as the previous block's hash.



HASHING functions

ALTOROS™

Hash of Block 2

T1

H1 T2

H2 T3

H3

Block 1

Block 2

Block 3

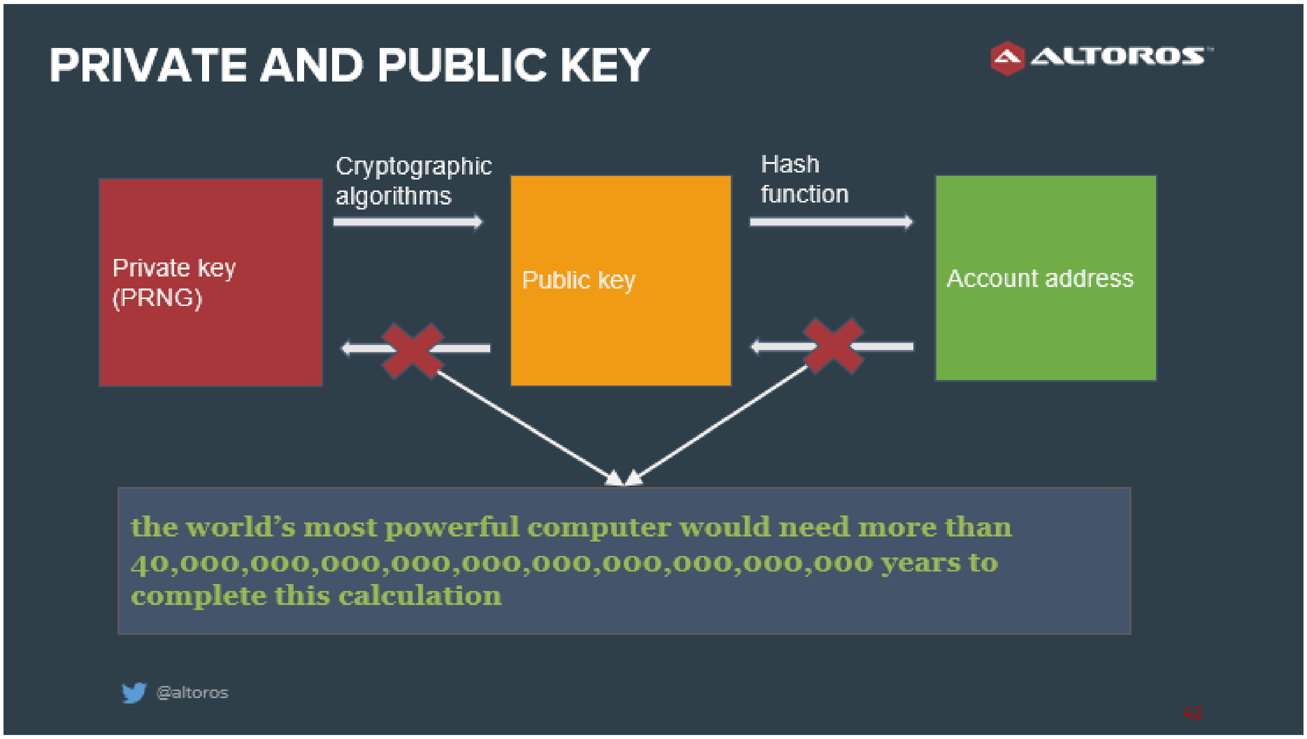
preimage resistance

collision resistance

@altoros

Figure A.2 A sample simplified blockchain using a single transaction

Private keys are created by a pseudorandom number generator. These are then put through a hashing function to generate public keys.



PRIVATE AND PUBLIC KEY

ALTOROS™

Private key (PRNG)

Cryptographic algorithms

Public key

Hash function

Account address

the world's most powerful computer would need more than 40,000,000,000,000,000,000,000,000,000,000 years to complete this calculation

@altoros

42

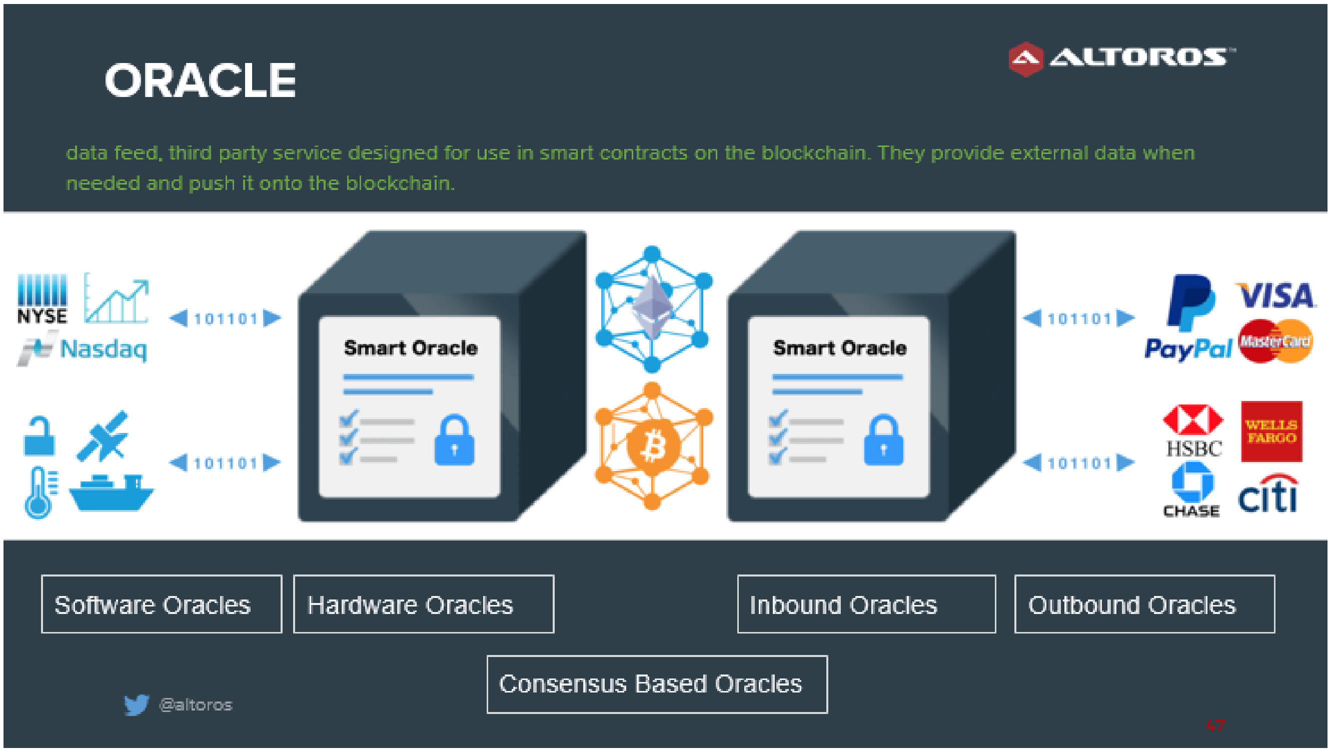
Figure A.3 Practically impossible to reverse engineer keys

Next, smart contracts are executed by events triggered by information collection outside the blockchain.

Finally, blockchains cannot access data outside its own network. To trigger smart contracts, oracles—known as data feeds—provide external data, when certain conditions are met, such as weather temperature, successful payment, price fluctuations, etc.

There are different types of oracles based on usage:

- *Software oracles* extract information from sources available online like temperature and the price of goods.
- *Hardware oracles* extract information from the physical world, such as motion and RFID sensors.
- *Inbound oracles* provide smart contracts with data from the external world, such as an automatic buy order if USD hits a certain price.
- *Outbound oracles* provide smart contracts with the ability to send data to the outside world.
- *Consensus-based oracles,* as a collection of oracles, are used by prediction markets to forecast future outcomes.



ORACLE

data feed, third party service designed for use in smart contracts on the blockchain. They provide external data when needed and push it onto the blockchain.

Software Oracles

Hardware Oracles

Inbound Oracles

Outbound Oracles

Consensus Based Oracles

Figure A.4 Oracles feeding external data to blockchain
(Image credit for the graphic illustrating the process)

Using a single oracle type as a source of information can be risky and unreliable. To avoid any data manipulations, it is better to implement a rating system for oracles or a combination of different oracles.