Research Report

Smart Contracts for the Insurance Market

THE RECENT EVOLUTION OF SMART CONTRACTS AND THEIR FAST ADOPTION ALLOW TO RETHINK PROCESSES AND TO CHALLENGE TRADITIONAL STRUCTURES. THEREFORE, WE INTRODUCE THE UNDERLYING TECHNOLOGY AND RECENT IMPROVEMENTS. FURTHER, WE PROVIDE AN OVERVIEW OF HOW THE INSURANCE SECTOR MAY BE AFFECTED BY BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS. WE SHOW AN EXEMPLARY USE CASE AND EMPHASIZE CURRENT CHALLENGES AND LIMITATIONS IN THIS AREA.

Ronny Hans
Hendrik Zuber
Amr Rizk
Ralf Steinmetz

Introduction

Blockchain provides an open and decentralized platform technology that allows the creation of a transparent, secure, and robust data record. It is designed to be a flexible, transparent, and efficient decentralized database. Thus, it may be employed to replace centralized systems that organize and administrate information (Davidson et al., 2016). Second-generation blockchains, like the Ethereum platform, additionally offer Turing-complete programmability for the integration of smart contracts (Wood, 2014). Thereby, the implementation of terms of an agreement between various parties can be enabled based on predefined, i.e., programmed, rules. These rules can be realized in self-executing code and are triggered automatically. As a consequence, there are many different applications, such as finance, insurance, smart energy systems, governments, and the Internet of Things.

In our work, we show the potential of smart contracts and blockchain technology and how it may fundamentally alter the world-wide insurance sector (Hans et al., 2017).

Blockchain and Smart Contracts

It is worth noting that the main purpose of the first introduced blockchain has been to obtain a system that is publicly governed by participants in their network without depending on any credible parties. The clients within the network use a consensus protocol to protect the information records.

In general, a blockchain is a decentralized and trustful database that contains all records of events or transactions that have been executed and shared between participating parties (Shrier et al., 2016). In addition, the blockchain incorporates a full, unaltered, and verifiable history of every single transaction providing a high level of transparency (Wood, 2014). The blockchains' generic structure consists of a chain of connected blocks including ordered transactions. Each transaction is linked to the previous one to maintain an ordered structure. As a consequence, transactions can be traced back in time. To guarantee security for the information on the blockchain, every transaction must be approved by the network. Here, no external authentication measures are necessary. Instead, different consensus mechanisms can be used to achieve a consistent state at participating parties.

A blockchain can possess different characteristics in terms of accessibility:

- *Public/Private:* Submitting transactions is not limited or limited to a predefined list of entities.
- *Permissionless/Permissioned:* All identities or a predefined list of identities can process transactions.

Note that a permissioned design with known identities makes a consensus model unnecessary but decreases the degree of data transparency.

Consensus protocols are used to protect the system against malicious participants. These protocols achieve a consistent and universal picture of the system state. Contemporarily, the proof-of-work (PoW), proof-of-stake (PoS), and Byzantine fault-tolerant (BFT) protocols are the most widely applied consensus protocols and possess completely different scalability characteristics (Davidson et al., 2016). In brief, a blockchain based on PoW provides favorable node scalability paired with a deficient performance which makes it highly cost-intensive due to considerable energy consumption – whereas PoS exhibits significantly lower costs and also a high scalability. The PoS consensus protocol processes significantly more transactions per second compared to other protocols. In contrast, a blockchain that uses BFT exhibits a good performance and restricted scalability. Here, every node must know all of its peer nodes that are engaged in the network to achieve consensus (Vukolić, 2015). As a consequence, a trusted and centralized administration is needed to emit identities and cryptographic authorization to nodes making this algorithm suitable for permissioned blockchains.

A smart contract can be defined as an event- and state-driven program that may run on a blockchain platform to administer assets that are included in the blockchain (Luu et al., 2016). Further, the scripting attributes of blockchains can be utilized to create cryptographic contracts that execute predefined agreement obligations by using self-enforced scripting languages. This type of contracts needs an unbiased mediator to take decisions and actions on the agreement. Consequently, blockchains are perfectly suitable to run smart contracts as they provide incentives for the mediator to decide honestly. The verification process of such contracts is the same as used for blockchain technology.

A main challenge for smart contracts is to achieve sustainability and to prevent malicious usage. In Ethereum, this is resolved by requiring a "fee" (ether) that is consumed by the nodes to compensate for contract execution. The amount of "ether" for a contract execution depends on its complexity. In addition, smart contracts need external data input for the evaluation process. Oracles, i.e., trusted third parties, deliver validated external data to a smart contract that can be logically evaluated to make a decision. To guarantee that the information has not been manipulated, signature concepts, such as "three out of five", are installed.

Privacy concerns paired with the vast amount of necessary data required for smart contracts lead to new structured approaches for the development of blockchain designs, e.g., creating parallel working blockchains which permit the transfer of assets and data between them. The concept of using various blockchains resulted in a scheme consisting of the following blockchains: identity chains, transaction chains, and content chains (Mainelli and Smith, 2015). First, the identity chains are responsible to grant authorization for participants to a transaction chain. Second, transaction chains keep track of the executed transactions and store solely the corresponding hashes for optimized performance. Third, content chains are decentralized storages that secure the data and guarantee accessibility. This structure allows having a public and permissionless identity chain and private transaction chains.

Blockchain and Smart Contracts in the Insurance Industry

Emerging initiatives and innovation strategies address key challenges of the insurance industry and focus on improvements in more individual pricing schemes, increasing profitability, and retaining clients (Mainelli and Smith, 2015). Major insurance companies started to put effort into evaluating possible ways of adopting blockchain technology to support and enhance their core businesses. Using smart contracts, several processes that are currently spread across numerous systems and databases can be streamlined. They automatize authentication and computation processes or similar tasks which may exhibit a high incidence of errors or abuses. Hence, smart contracts may strongly change the insurance industry as insurance policies can often be translated directly to computer code due to their "if-then" structure.

The blockchain technology has generated promising opportunities for disruption due to the following reasons (Deloitte, 2016):

- decreasing the need for trust and financial exposure in already existing agreements and provide legal clarity,
- facilitating the deployment and maintenance of internal or inter-organizational infrastructures,
- enhancing uptime and overall security, and
- reducing costs of running services, error-proneness, and the organization's reputational risk.

The prevention of fraud continues to be a top priority for the insurance industry. The underlying goal is to apply blockchain technology to streamline the payment and claims handling process to reduce the risk of fraudulent claims. Further, consumer insurance policies are often distributed by brokers that use third-party software platforms. They are regularly implemented in entirely independent and different code schemes due to an individual realization of the insurer's pricing model. As a consequence, several intermediaries might become dispensable by a shift to blockchain technology (Mainelli and Smith, 2015).

Example Use Case: Smart Contracts Based on Trusted Data Feeds

In 2013, the worldwide market for wholesale insurance and reinsurance summed up to a gross written premium of more than USD 520 billion (Hearn and Tischhauser, 2014). Insurance against natural catastrophes plays an important role in this sector. Such catastrophes may cause instantaneous large costs for insurers. Therefore, reinsurers apply various approaches such as prefunding and risk-sharing by selling, e.g., "cat bonds", which can easily be expressed as smart contracts with simple contractually agreed conditions.

A promising proof of concept for such natural catastrophe swaps was recently piloted by Allianz Risk Transfer and Nephila Capital to facilitate and improve their contract management process.

In more detail, the process consisting of four main tasks is presented subsequently and its mode of operation is illustrated in Figure 1 (Alonso et al., 2015).

Contractual agreements: Contract terms are translated to executable code that can be evaluated automatically and independently.

External information: A third party serves as external and trustful data source to provide necessary and secure input information.

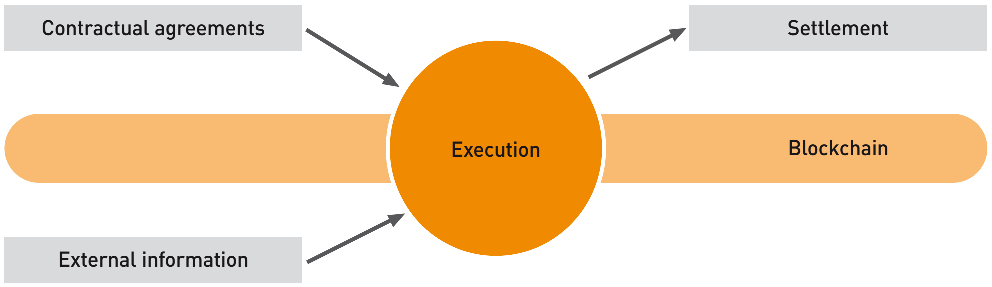

Figure 1: Basic Principle of a Smart Contract (adopted from Alonso et al., 2015)

Execution of smart contract: The receipt of information triggers the validation whether the predefined conditions are met, followed by the execution of the corresponding smart contract.

Settlement: In case that the criteria are met, the value transfer process is automatically initiated as imposed by the contract terms and payouts are determined between the participants. Also off-chain asset settlements can be performed by tracking account modifications on the blockchain to guarantee a creditworthy system.

In this example, the blockchain technology allows improving auditability, reliability, and execution time of the contract management process of both cat swaps and bonds. Particularly, this is achieved because of fewer manual processing as well as less verification and authentication through intermediaries.

Potential, Challenges, Limitations

In the following, we focus on the potential, challenges, and limitations of blockchain technology within the insurance sector.

An important driver of recent developments is the potential application of blockchains in daily activities such as identity authentication and validation, payment operations, as well as data management. Hence, more personalized insurance products can be offered at lower prices by simultaneously increasing transparency, automating processes, and introducing the exchange of individual customer's data (Mainelli and Smith, 2015). Further, new markets can be accessed in regions that lack good data maintenance and exhibit high grades of corruption as blockchain technology provides a more reliable and inalterable alternative to current registries (Shrier et al., 2016). This leads to developing new concepts that face increasing attention, e.g., peer-to-peer and just-in-time insurance.

Rethinking the so far existing concept of centralized insurance models, peer-to-peer models to insure risk may arise as the overhead problem of collecting premiums and processing payouts can be resolved using the concepts of blockchain and smart contracts. Especially, the fast growing sharing community demands different types of insurance and requires a higher degree of flexibility. For example, using car sharing, cars are available instantly and insurance policies may be hired per trip for which smart contracts guarantee a suitable integration. The blockchain approach might become a core technology enabling the development of instant, economical decentralized systems (Mainelli and Smith, 2015). Blockchain and smart contracts may increase the consumer's confidence and diminish identity or claim fraud.

An important challenge is improving the currently applied consensus mechanisms. The choice between the existing approaches is accompanied by a trade-off between scalability and the desired degree of decentralization, security, and performance, as well as energy consumption and costs (Vukolić, 2015). Smart contracts depend heavily on the quality of external resources provided by oracles. As a consequence, it must be ensured that oracles provide trustful data.

Conclusions

The blockchain technology and smart contracts are in an early stage. To realize their full potential, these technologies still must overcome several challenges, such as scalability, incorporation of external information, underlying real assets, flexibility, privacy, as well as permissioning schemes. We expect that blockchain solutions will be heavily cost-efficient compared to centralized approaches as these technologies offer extraordinary potential in all areas where trustful transaction records are needed.

References

Alonso, J.; Cámara, N.; Sebastián, J.; Tuesta, D.; Urbiola, P.; Vegas, I.:
Digital Economy Outlook.
In: Digital Economy Outlook, October 2015.

Davidson, S.; De Filippi, P.; Potts, J.:
Economics of Blockchain.
In: Proceedings of the Public Choice Conference, Fort Lauderdale, US, 2016.

Deloitte:
CFO Insights – Getting Smart About Smart Contracts.
Press Release, 2016.

Hans, R.; Zuber, H.; Rizk, A.; Steinmetz, R.:
Blockchain and Smart Contracts: Disruptive Technologies for the Insurance Market.
In: Proceedings of the Americas Conference on Information Systems (AMCIS), Boston, US, 2017.

Hearn, S.; Tischhauser, P.:
London Matters: The Competitive Position of the London Insurance Market, 2014.

Luu, L.; Chu, D.-H.; Olickel, H.; Saxena, P.; Hobor, A.:
Making Smart Contracts Smarter.
In: Proceedings of the ACM SIGSAC Conference, Vienna, Austria, 2016.

Mainelli, M.; Smith, M.:
Sharing Ledgers for Sharing Economies: An Exploration of Mutual Distributed Ledgers (aka Blockchain Technology).
In: The Journal of Financial Perspectives, 3 (2015) 3, pp. 38–69.

Shrier, D.; Sharma, D.; Pentland, A.:
Blockchain & Financial Services: The Fifth Horizon of Networked Innovation.
MIT Blockchain Whitepaper, 2016.

Vukolić, M.:
The Quest for Scalable Blockchain Fabric: Proof-of-Work Vs. Bft Replication.
In: Open Problems in Network Security: IFIP International Workshop, 2015, pp. 112–125.

Wood, G.:
Ethereum: A Secure Decentralised Generalised Transaction Ledger, Ethereum Project.
Whitepaper, 2014.