Meralli *Financial Innovation* (2020) 6:7
https://doi.org/10.1186/s40854-020-0172-y

Financial Innovation

RESEARCH Open Access

Privacy-preserving analytics for the securitization market: a zero-knowledge distributed ledger technology application

Sophie Meralli

Correspondence:
sophie.meralli@sloan.mit.edu
[1]Massachusetts Institute of Technology (MIT) Digital Currency Initiative, 285 Third Street, Unit 715, 02142 Cambridge, Massachusetts, USA

Abstract

A zero-knowledge proof or protocol is a cryptographic technique for verifying private data without revealing it in its clear form. In this paper, we evaluate the potential for zero-knowledge distributed ledger technology to alleviate asymmetry of information in the asset-backed securitization market. To frame this inquiry, we conducted market data analyses, a review of prior literature, stakeholder interviews with investors, originators and security issuers and collaboration with blockchain engineers and researchers. We introduce a new system which could enable all market participants in the securitization lifecycle (e.g. investors, rating agencies, regulators and security issuers) to interact on a unique decentralized platform while maintaining the privacy of loan-level data, therefore providing the industry with timely analytics and performance data. Our platform is powered by zkLedger (Narula et al. 2018), a zero-knowledge protocol developed by the MIT Media Lab and the first system that enables participants of a distributed ledger to run publicly verifiable analytics on masked data.

Keywords: Structured finance, Securitization, Blockchain, Zero-knowledge proofs, Distributed ledger technology, Privacy, Data analytics

Introduction

The securitization market presents inefficiencies due to the inherent complexity surrounding its structured products. The process of bundling thousands of loans and issuing related securities involves many intermediaries, with diverging incentives and access to information (European Central Bank Publication N. 975 2008; Fligstein and Roehrkasse 2013). Due to information delays, lack of data standardization and limited traceability of collateral flow throughout the securitization chain, there is a lack of transparency about the performance of the many loans backing up these securities (Sindle et al 2017). This lack of transparency prevents investors from making their investment decisions independently and in a timely manner, and has led to significant regulatory reforms (Code of Federal Regulations Title 17 Commodity and Securities Exchanges Chapter II Part 246 Credit Risk Retention 2017) in the past recent years to improve disclosure requirements, network governance and accountability mechanism.

The inherent complexity and lack of transparency involved in the securitization industry makes it a compelling use case for distributed ledger technology (DLT) application. Recently, financial institutions and regulators in the industry have investigated DLT's

potential (Sindle et al 2017; Financial Industry Regulatory Authority (FINRA) 2017). DLT uses independent computers (referred to as nodes) to record, share and synchronize transactions in their respective electronic ledgers (instead of keeping data centralized as in a traditional ledger) (The World Bank 2018). Blockchain is one type of distributed ledger where data is organized into blocks, which are chained together in an append-only mode. In this paper, blockchain and DLT are used interchangeably. Blockchain/DLT enable recording of interactions and transfer ownership of asset (e.g. money, securities, land titles and specific information) peer-to-peer, without a need for a centrally coordinating entity (The World Bank 2018). Applied to the securitization market, DLT may enable market participants to store and update securely the information of thousands of individual loans on a near-real time basis on one unique shared ledger, without the need for reconciliation among each party's database (Sindle et al 2017). It has the potential to bring secure, traceable near-real time performance data to the industry. However, DLT adoption faces a dilemma between data privacy-preserving and public sharing that can be described by two limitations: 1) participants will lose data privacy if they are to share data in the public ledger (such as loan level data); 2) encrypting loan level data will keep privacy but will therefore not support data analytics at the asset pool-level. As security issuers do not have the incentive to reveal sensitive proprietary loan-level data to investors and third-parties[1], current blockchain applications cannot scale at industry level. In order for blockchain applications to scale, there is a need for flexible privacy settings that can reflect the subtleties of current market interactions.

We aim to address this dilemma by introducing a decentralized market platform, zkABS, powered by zero-knowledge proofs and designed for the securitization industry. In cryptography, a zero-knowledge protocol or proof is a method by which one party (the prover) can prove to another party (the verifier) that he knows a secret statement without revealing the secret itself (Goldwasser et al. 1989). Our platform is based on zkLedger (Narula et al. 2018), an experimental system developed by the MIT Media Lab that leverages zero-knowledge proofs to preserve data privacy while providing its users with a suite of publicly verifiable analytics at the aggregate level (e.g. sums, averages and variances).

Applied to the securitization industry, we argue that zkLedger could preserve the confidentiality of individual loan data while providing participants with publicly verifiable near-real time analytics at the asset pool level. It could therefore power a decentralized digital platform where all market participants (e.g. investors, issuers, regulators, rating agencies) could get access to publicly verifiable market analytics in near-real time. We introduce the concept of near-real time frequency to address the security vulnerability and privacy leaks that real-time frequency solutions entail. In the securitization market, near-real time analytics is defined as data analysis based on up-to-date information and can range from bi-weekly updates to daily updates, depending on the types and volume of assets hosted in the system[2].

Our system has applications throughout the value chain: in the security construction and issuance steps, it could enable investors to pick up loans on an aggregate basis, without revealing data on the individual loans. In the trading phase, it could provide anonymity of trading in the primary and secondary issuance side and

[1] Expert interviews of four Investors, four Issuers and one Attorney. See "Introduction" section for more details about expert interviews

[2] See "The inefficiencies of the securitization market" section for more details.

enable investors to get analytics about security ownership concentration. Post-issuance, investors could get anonymized performance analytics and query about trends in the market at any point of time. Overall, our system could reduce asymmetry of information and improve transparency in the securitization market. In summary, the contributions of this paper are:

- Identification of inefficiencies in the securitization market that could benefit from DLT technology, specifically related to information asymmetry between the sell-side and the buy-side of the industry.
- Review of current blockchain initiatives in the industry and their privacy limitations
- Introduction of zkABS, a decentralized platform based on zkLedger that aims to reduce the information asymmetry in the market. In our use case, zkABS is used as a model to share loan electronic records among distrusting participants in a secure and confidential way without compromising the independent verifiability of the data. Due to its selective visibility property, zkABS allows all market participants to interact on the same platform and to benefit from more timely market data.

Research methodology

While there has been an increasing number of companies exploring blockchain-based solutions for their business, reports show that the industry is still nascent (Pemberton and Levy 2018; Pawczuk et al. 2018). A key headwind to blockchain adoption is the fact that organizations focus on the technology with hopes that it can redefine their business, instead of spending time on identifying practical business use cases that could benefit from the technology (Pawczuk et al. 2018). They tend to start by applying the solution first rather than identifying a problem and proving that blockchain is the adequate solution for it, and therefore face challenges in market adoption. In order to capitalize on a blockchain, companies should spend more time identifying frictions and processes that could benefit from the unique characteristics of this technology (Pawczuk et al. 2018). In this paper, we purposely spent "Research methodology" section identifying the key market inefficiencies that could benefit from blockchain technology, before introducing a blockchain solution for the market.

To frame this inquiry, we conducted market data analyses, a review of prior literature, stakeholder interviews with investors, originators and security issuers and collaboration with blockchain engineers and researchers. While our research focused mainly on the US market, we performed an extensive review of the Chinese securitization market and interviewed stakeholders from different countries to contrast perspectives and highlight characteristics of the US and global markets. China was selected for its pioneer application of distributed ledger technology in the securitization market (Jingli 2017). As part of our research, we first conducted market data analyses through tracking historical trends in terms of volume, pricing and liquidity by asset class using databases such as Bloomberg (Bloomberg database 2018), Sifma (SIFMA database 2018) and Wind (Wind database 2018). In addition, we reviewed professional publications to collect information about market trends. We then conducted a review of prior literature with the goal of identifying historical market dynamics and structural challenges that could be potentially addressed by distributed ledger technology. Ten articles were selected due to their special attention to the 2008 financial crisis (European Central Bank Publication N. 975 2008;

Fligstein and Roehrkasse 2013; Wheeler et al 2017; OICV-IOSCO Technical Committee 2012), the evolution of relevant US regulation (U.S. Department of Treasury 2017) and the business application of distributed ledger technology (Sindle et al 2017; U.S. Chamber of Digital Commerce SFIG 2017; Catalini and Tucker 2018; Financial Industry Regulatory Authority (FINRA) 2017; The World Bank 2018). Relevant literature was identified through a systemic backward search of economic papers from professional and government organizations, leading scholarly journals and industry publications. A summary of existing blockchain initiatives in the industry is provided in Appendix I. We then performed expert interviews with stakeholders in the securitization industry. We interviewed 18 experts, including two portfolio managers and two traders in investment and trading operations for large asset management firms ("Investors"), one trader and three managers at large financial institutions issuing securitized assets ("Issuers"), five manager in the asset-backed security origination and servicing department at financial institutions ("Originators and Servicers"), one attorney, two consultants and two auditors specialized in applying distributed ledger technology to the securitization industry. Experts were selected based on their leadership positions and in some cases their deep knowledge of distributed ledger technology. We intentionally interviewed experts from both senior leadership position and junior positions with operating trading experience to gain comprehensive insights on the industry. Twelve interviewees were based in the US, four were based in China and the rest were spread worldwide.

Regarding the technology, we leveraged existing literature review on zero-knowledge proofs described in "ZkLedger, a privacy-preserving protocol section" (Narula et al. 2018) and reviewed relevant articles on Pedersen commitments (Pedersen TP 1992) and sigma protocols (Maurer 2009; Wang and et al 2019; Schnorr 1991; Cramer et al. 1994; Bernhard et al. 2012). We received guidance from the zkLedger developing team to validate our approach for designing a novel system based on zkLedger for the securitization market. We took the example of the investor viewpoint to demonstrate zkLedger's benefits. To build our model, we leveraged anonymized samples of servicer reports and loan tapes obtained during our expert interviews which enabled us to understand existing product for investors.

The inefficiencies of the securitization market

In this section, we provide a brief overview of the market and present the structural problems of today's securitization market. Structuring securities is a complex process involving different participants. The incentives of these participants are not aligned with each other, which becomes the primary attribution of market inefficiencies. Rather than providing an exhaustive list of pain points, this section aims to provide the readers with an overview of the two main problems we collected from our interviews with market participants and that could be alleviated with zkLedger implementation. For a detailed description of the securitization market and the potential of blockchain technology in the industry, we refer to recent industry reports (Sindle et al 2017; U.S. Department of Treasury 2017; Financial Industry Regulatory Authority (FINRA) 2017).

Overview Today, the US securitization market represents $10 trillion (SIFMA database 2018) and comprises a wide variety of securitized products such as mortgage loans, auto-loans, credit card loans and consumer loans. Securitization is the process by which cash

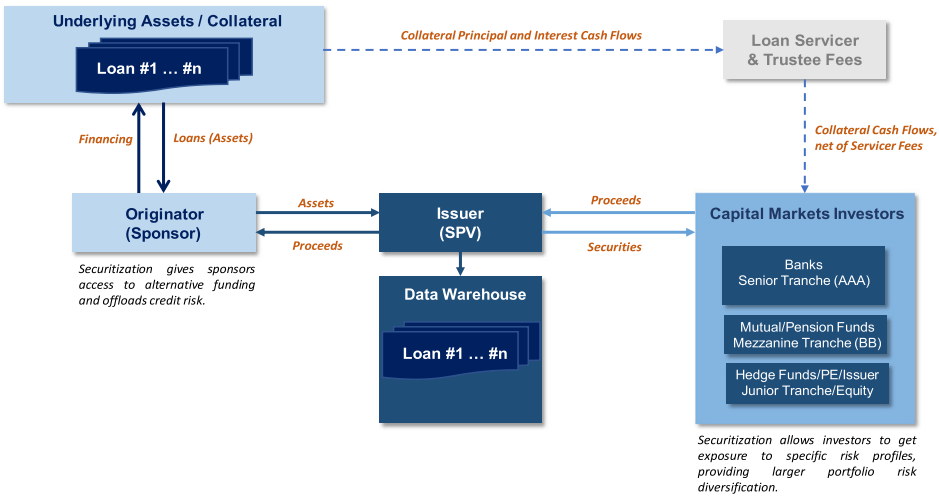

Fig. 1 Overview of the securitization process

flows from thousands of individual assets (e.g. auto loans, mortgages, student loans, etc.) from a loan originator are pooled together and transferred to a newly created remote special-purpose vehicle (SPV) managed by a security issuer, and then sold as financial instruments (commonly referred to as "asset-backed securities"[3]) to investors. By transferring the credit risk of the loans to the SPV in return for cash, the originator is able to recycle capital into the origination of new loans. The SPV finances the purchase of the underlying loans with a mix of equity and debt interests in the pool, structured in tranches[4] with different risk profiles. For instance, the senior tranche of an asset-backed security has the lowest risk since it has priority liquidation preference over junior tranches in case of default. Rating agencies play a significant role in the process by rating these tranches based on the credit quality of the underlying assets and the reputation of the issuer and originator, using their proprietary rating protocols. These asset-backed securities are then sold to different investors depending on their risk tolerance – senior tranches (e.g. Tranche AAA) are typically bought by central banks and traditional banks. Mezzanine tranches have higher yields and tend to be bought by mutual funds, while a large portion of the junior tranche and equity remains with the issuer. Over the life of the security, the cash flows generated by the underlying assets are collected by the loan servicer – sometimes the same entity as the originator – and used to repay investors and equity holders (see Fig. 1). Because there are multiple parties involved, there are time lags before investors get notified about the loan payments or defaults.

Misaligned Incentives The securitization process involves transactions among numerous participants, with diverse incentives. We can distinguish broadly four types of parties: loan originators, intermediaries (e.g. issuers), third parties (e.g. credit rating agencies, servicers, underwriters, regulators and trustees) and investors. The incentives of these participants are not aligned with each other, which becomes the primary attribution of market inefficiencies. Loan originators collect commissions on loan issuance and aim to

[3] We use a broad definition of asset-backed securities, which includes securities backed by mortgages ("MBS") and by any other types of loans than mortgages ("ABS").
[4] A "Tranche" is defined as a group of claims in the asset pool principal repayment. The word derives from the French word "tranche" which means "slice".

offload their credit risk by selling the loans to investors (Fligstein and Roehrkasse 2013). However, they are not directly evaluated based on subsequent loan performance and therefore may have incentives to misrepresent the quality of the loans and to engage in opportunistic behavior (European Central Bank Publication N. 975 2008): since originators' profits increase based on the volume sold, they seek to achieve a high turnover of selling assets with reduced efforts in screening and monitoring borrowers (European Central Bank Publication N. 975 2008). Unlike investors, originators will not be directly impacted if the quality of the loans subsequently deteriorates. Intermediaries collect transaction fees based on volume processed and have little incentive to balance the risk/reward trade-off that investors are seeking. Further, third parties such as credit agencies and servicers may not be inclined to perform downgrades or act upon loan delinquency in a timely manner as they are closely involved with the issuers. Finally, investors aim to maximize their returns and mitigate risk using correlation indexes while delegating the management of their securities to intermediaries and third parties. Due to these misaligned incentives and asymmetry of information, investors bear the main risks and tend to rely on the reputation of the originators, issuers and servicers as well as rating agencies to support their investment decisions. It is worth noting that risk retention rules (Code of Federal Regulations Title 17 Commodity and Securities Exchanges Chapter II Part 246 Credit Risk Retention 2017) which have already gone into effect have been designed to particularly put a stop to the originate-to-sell model and reduce the misaligned incentives. Securitization usage has significantly dropped since their enforcement (Wheeler et al 2017).

Lack of Timely Information These misaligned incentives are amplified by the lack of timely information available to investors. Investor due diligence is a necessary component of an efficient market (OICV-IOSCO Technical Committee 2012). Through our interviews with the trading desks of institutional investors[5], we established that investors lack the price and liquidity discovery online tools to perform their due diligence independently and efficiently. Investors receive information at the issuance stage (i.e. in the prospectus), but receive fewer and non-standardized asset-pool performance statistics through the life of the asset (European Central Bank Publication N. 975 2008). The information reported in servicer reports lack standardization across servicers: some servicers still do most of their work on paper and scan document copies, which are then stored in siloed databases (servers, data warehouses, government offices) (Sindle et al 2017). This makes it increasingly difficult to reconcile the information among originators, intermediaries, investors, rating agencies and regulators, and results in market inefficiencies such as information delays, operational errors, and a lack of independence among the different parties. The performance updates are often released with significant time lags (e.g. there is a time lag of several weeks between the date of non-payment of consumer and the date the investor gets notified of the non-performance of his pool). Such delays can be especially significant in the case of a transfer from one servicer to another, due to difficulty in reconciling data. In consequence, buy-side traders often have to download scanned documents from many servicers and standardize the data themselves to perform their analysis, which is very time consuming and requires a high degree of expertise. As one of our institutional

[5]Interviews of ABS buy-side trading desks from four major financial institutions, March-April 2018

investor interviewees[6] pointed out: *"it would be great to have online analytics tools to monitor loan performance and track the record of originators in a timely manner."* The lack of timely information is even more pronounced in the secondary market, where often there is no price listed on market platforms or it is outdated by several weeks. In addition, there is opacity in tracking the flows of collateral and security ownership throughout the value chain and in financial markets. For instance, investors that manage arbitrage or relative value strategies are interested in information about security ownership such as concentration or composition for a specific collateral that they own partially. Today, the investors would have to carefully search dealer inventories or speak to dealers in order to find the exact collateral. Therefore, investors lack the information tools to make their investment decisions efficiently. In US, secondary markets for ABS are much smaller compared to agency MBS (Bloomberg database 2018). For ABS, the difficulties and delays in accessing information on the underlying loans may be one of the main reasons to drive investors away from these securities or demand a higher risk premium. The possible 'near-time' solution of zKABS may reduce these issues, encourage more investors and thus increase the size of the ABS market.

Overall, the market suffers from a combination of misaligned incentives and information asymmetry, which impedes market growth and liquidity. Solving for all of these inefficiencies may be challenging, however we believe that the market would benefit from more transparency. One solution could be to implement a database managed by the issuer that would update and share loan-level information to all participants simultaneously to ensure transparency. The problem with such a solution is that the issuer controlling the data enjoys significant market power over other participants and may prevent the collaboration of multiple competing servicers, issuers and originators. Another potential solution could be a new type of decentralized digital platform, such as the one powered by a distributed ledger. Under such a system, no unique party has full control of the platform and its data. Rather, the platform's ownership and governance can be shared among all the participants. Such a system could reconcile this need for transparency and efficiency without assigning the same degree of control to the intermediary operating and facilitating transactions in the market, therefore separating the benefits of network effects from the agency costs they entail in terms of market power (Catalini and Tucker 2018).

ZkLedger, a privacy-preserving protocol

Current distributed ledger solutions are either entirely viewable to all participants or are encrypted to hide sensitive data but do not support data analytics without revealing the content of the data in the ledger. For instance, in order to calculate the net balance of monetary transactions in a private blockchain with distrusting participants, one would need to download all transactions to verify their integrity. This raises privacy concerns for market participants in the US securitization industry (see Fig. 2). Due to the information asymmetry and diverging incentives between issuers and investors, there is a high degree of confidentiality and intellectual property surrounding the structuring of asset-backed securities. Although investors can get access to loan tapes[7], with loan-level information, it is rather on an occasional basis and may present data quality issues (i.e. completeness, accuracy) (OpenRisk). Investors may get curated off-chain information on an aggregate

[6] Interview with a buy-side trader on the US asset-backed security market, March 2018
[7] A loan tape denotes an electronic file or set of files that captures loan data from a financial institution's systems.

Market Participant	High-Level Considerations	Impact
Originators	Originators compete against each other to provide consumer credit and raise funds from investors. Therefore, they do not want to reveal sensitive loan information among themselves.	Multiple originators cannot participate in the same blockchain.
Issuers/SPV	Issuers have proprietary risk valuation and pooling methodologies to package loans into ABS products and sell them to investors. Therefore, they do not want to reveal sensitive information at loan-level basis to investors.	Investors and issuers cannot participate in the same blockchain if it includes sensitive information.
Investors	Investors buy ABS product to get exposure to specific types of risk. They base their investment decision on their ability to price risk and therefore value real-time performance data.	Investors cannot get access to real-time information without putting their trust in the issuer as they lack direct access or the tools to perform publicly verifiable analytics themselves.

Fig. 2 Privacy limitations of current blockchain applications in the securitization industry

basis but are not expected to join the issuers' blockchain and thus will lack the tools to perform their due diligence independently. Similarly, current blockchain applications do not yet allow for multiple competing issuers to join the same universally agreed-upon ledger and therefore face limitations for applications at the industry level.

zkLedger Overview zkLedger (Narula et al. 2018) is an open source protocol developed by the MIT Media Lab Digital Currency Initiative that solves the trade-off between transparency and privacy of current blockchains. It is the first system to generate cryptographically verifiable answers to arbitrary analytics queries without revealing confidential information. Currently no other permissioned ledger allows for the ability to run analytics on masked data. Other permissioned ledgers only share information on a need-to-know basis, thus there is no universally agreed upon ledger within these systems. The incompleteness of each participants ledger means query responses cannot be verified unless all transactions are announced to the verifier. The combination of zero-knowledge proofs and a distributed ledger is critical to developing flexible privacy settings and selective visibility. Using a secure zero-knowledge proof scheme, zkLedger provides its users with analytical tools that can run on hidden data. As a result, ledger participants do not need to access all the sensitive data in clear form in order to perform provable data analysis.

Security Goals zkLedger maintains privacy: parties non-involved in a transaction cannot see transaction details. In addition, zkLedger ensures completeness through its novel table architecture: when running analytics on the hidden data, the verifier can be ensured that no transactions are omitted. Finally, zkLedger maintains integrity by enabling distrusting parties to perform publicly verifiable analytics.

Architecture zkLedger works as an append-only ledger. The ledger can be represented as a table with each row being a transaction and each column a category of information (participant name, transaction amount, currency, etc.). The information stored on the ledger is not in plain text but hidden using *commitments* detailed below. Figure 5 illustrates the table design for security issuers and investors in the securitization market. The

ledger could be maintained by a third-party (who would not have access to the underlying data) or as a distributed ledger maintained by the participants (Narula et al. 2018). It can potentially be built on top of existing permissioned ledgers – such as Hyperledger Fabric[8]. The zkLedger protocol includes a suite of analytics (e.g. sums, averages, correlations, variances, outliers, ranges and market concentrations) that each participant can query at any point in time.

How it works A zero-knowledge proof is a protocol defined between a prover and a verifier, such that a prover can convince a verifier of the validity of its knowledge of a secret, without revealing anything else beyond the assertion of this knowledge. Zero-knowledge is a broad field in cryptography with many different instances defined (Wang and et al 2019). In this paper, we focus on the cryptography behind zkLedger and do not cover protocols that use other types of zero-knowledge proofs such as zk-SNARKS and bulletproofs (Wang and et al 2019) in Zcash[9]. zkLedger is an instance of a zero-knowledge protocol which combines several cryptographic primitives to preserve the privacy of the ledger while still allowing to compute provably correct measurements over the data in the ledger. Zero-knowledge proofs can be either interactive (e.g. Schnorr's three-move sigma protocol (Cramer et al. 1994; Schnorr 1991)) or non-interactive (Bernhard et al. 2012; Feige et al. 1988); for the latter the prover only sends his proofs and the verifier decides to accept or reject the statement without any further interaction (Bernhard et al. 2012). zkLedger can be implemented as an interactive or non-interactive protocol. In our design, we adopted the interactive version for security reasons (a party cannot perform an analytics query without approval from the party that it is trying to query). For simplicity purpose we do not outline in this paper the exhaustivity of the zkLedger protocol's design. See the zkLedger paper (Narula et al. 2018) for in-depth explanations and limitations about the technology. Below, we describe the two main cryptographic primitives used in zkLedger.

Schnorr's protocol Schnorr's identification protocol (Cramer et al. 1994; Schnorr 1991) is an interactive three-move signature scheme between a prover and a verifier which allows the prover to prove the knowledge of a discrete logarithm (in our case, the prover's secret key) without leaking information about its value. Consider a cyclic group H with prime order $|H|$ = q. Using Schnorr's protocol, one can prove that he knows the discrete log x of an element z to the base h, i.e., that he knows x such that $z = h^x$ (Maurer 2009). The mechanics of the Schnorr protocol are widely described in the cryptography literature (Schnorr 1991; Maurer 2009; Wang and et al 2019). In zkLedger, every participant generates a Schnorr signature keypair consisting of a secret key sk and public key $pk = h^{sk}$, where pk is public to all participants.

Pedersen commitment zkLedger combines Schnorr's protocol with Pedersen commitments (Pedersen TP 1992), which are schemes that let someone commit to a specific chosen value (e.g. a transaction amount), while keeping it hidden to others. Let v be the transaction amount in plain text. Then a Pedersen commitment to v is formed as $cm := COMM(v) = g^v h^r$, where g and h are two random generators belonging to the same cyclic group of points and r is a random integer that ensures semantic security. g and h are

[8] https://github.com/hyperledger/fabric#releases
[9] https://z.cash/

visible to all participants and common to all the entries, while r is hidden and generated randomly for each new entry. For each new entry j in a row, instead of broadcasting plain text transactions on the ledger, the following items are broadcasted to each participant i: a Pedersen Commitment $COMM(v_j) : g^{v_j}h^{r_j}$ and a Verifier Token $VF(i,j) = pk_i^{r_j}$. We will see below how the verifier can use these tools to perform analytics on hidden data. Pedersen commitments have three important characteristics. First, they are perfectly hiding: they do not reveal anything about the committed data v (even in the presence of quantum computing). Second, Pedersen commitments are computationally binding: for the same r and two amounts v and v', one can verify whether v and v' are equal by calculating the discrete logarithm $log_h(g)$. Third, unlike hash functions, Pederson commitments can be homomorphically combined (e.g. the product of the commitments can be opened to compute sums and averages on hidden data). For two commitments *cm1* and *cm2*, the product *cm1* x *cm2* is equal to $cm := g^{v1}h^{r1}g^{v2}h^{r2} = g^{v1+v2}h^{r1+r2}$, which allows for linear computation on masked data. In other words, if $v1 = 1$, $v2 = 2$ and $v3 = 4$, then $COMM(1) \times COMM(2) \times COMM(4) = COMM(7)$.

Illustration for private sums We take the example of a prover who wants to prove a verifier that $v_1 + v_2 + v_3 = 100$, without revealing anything about v_1, v_2 or v_3. The verifier knows g, h, sk and pk. He also knows for each entry v_i, $COMM(v_i)$ and the verifier token pk^{r_i}. However, he does not know anything about v_i or r_i.

In order to verify that $v_1 + v_2 + v_3 = 100$, the following equation must be satisfied based on the additive homomorphic properties of Pedersen commitments:

$$g^{\sum_1^3 v_i} \times h^{\sum_1^3 r_i} \div g^{100} = h^{\sum_1^3 r_i} \tag{1}$$

Since $pk = h^{sk}$, then:

$$pk^{\sum_1^3 r_i} = h^{sk \times \sum_1^3 r_i} \; and \; h^{\sum_1^3 r_i} = pk^{\sum_1^3 r_i \, / sk} \tag{2}$$

Therefore (1) can be written as follows:

$$g^{\sum_1^3 v_i} \times h^{\sum_1^3 r_i} \div g^{100} = pk^{\sum_1^3 r_i \, / sk} \tag{3}$$

Since $pk = h^{sk}$, then:

$$sk = \log_h(pk) \tag{4}$$

Combining (3) and (4) and applying the discrete logarithm, the following equivalence must be satisfied to verify that $v_1 + v_2 + v_3 = 100$:

$$log_{\left(g^{\sum_1^3 v_i} \times h^{\sum_1^3 r_i} \div g^{100}\right)} \left(pk^{\sum_1^3 r_i}\right) = \log_h(pk)$$

Although the verifier does not know v_i and r_i, he can compute the product of the Pedersen Commitments $g^{\sum_1^3 v_i} \times h^{\sum_1^3 r_i}$ and the product of the Verifier Tokens $pk^{\sum_1^3 r_i}$. Therefore, he is able to solve the equation above and verify that $v_1 + v_2 + v_3 = 100$ without knowing any information on v_1, v_2 or v_3. If the equation does not hold, this simply implies that the prover is lying about the sum $v_1 + v_2 + v_3$. Using this logic, zkLedger supports any type of publicly verifiable linear computations on hidden data.

Applying zkLedger to the securitization industry

In this section, we introduce zkABS, a platform based on zkLedger that aims to reduce the information asymmetry in the market. In our use case, zkABS is used as a model to share loan electronic records among distrusting participants in a secure and confidential way without compromising the independent verifiability of the data. We argue that the securitization industry would benefit from this technology in order to allow all market participants, including investors, to join the ledger while preserving confidential information. zkLedger could allow investors and issuers to interact on the same decentralized digital platform and get access to near-real time updates about ABS products' performance while preserving the confidentiality of the underlying loan-level data.

Architecture and governance system

This paper does not intend to recommend any DLT architecture for the securitization industry as this would be an ambitious separate problem to address for each step of the securitization lifecycle, but rather, to provide a simplified architecture and governance system and analyze the benefits for market participants. Such a simplified architecture would have the following components:

A permisioned ledger Due to the sensitive nature of the information disclosed and the types of participants involved in the securitization market, we adopted the framework of a permissioned ledger with a consensus protocol for append-only information which globally orders all valid transactions. Financial institution consortia are considering the use of permissioned ledgers as they offer efficiency and security. Under these settings, the consortium is responsible for operating the ledger, validating transactions and granting access to new entrants. In zkABS, participants cannot equivocate (assuming the consensus model is sound), therefore the information in the ledger is secure and publicly verifiable by participants. By "publicly" verifiable, we imply that anyone with the permission to access zkABS and get a full copy of the ledger can verify the inputs and outputs. Figure 3 illustrates zkABS's permissioned distributed ledger architecture for an ABS product issued by an SPV and backed by auto-loans from the Originator. Each participant in zkABS has two dimensions of flexible settings: write/read permissions and privacy settings.

Read/Write permissions Participants that contribute to building and updating asset-backed securities (e.g. the SPV and Servicer) have modification rights to update loan-level payments, pool-level performance and rating information. Other participants have read-only rights.

- Append permission: the SPV has the right to create new loan ID and append initial information to the ledger.
- Edit permission: the Servicer has the right to update information of current loans using a checkpoint system. At regular intervals defined by the system (e.g. near-real time), all the cryptographic commitments are updated and re-posted in the ledger with initial order preserved. Reposting the complete set of commitments to the ledger guarantees that no one can see which loan data points have been updated. Each checkpoint is recorded in the system as an immutable time-stamped log.

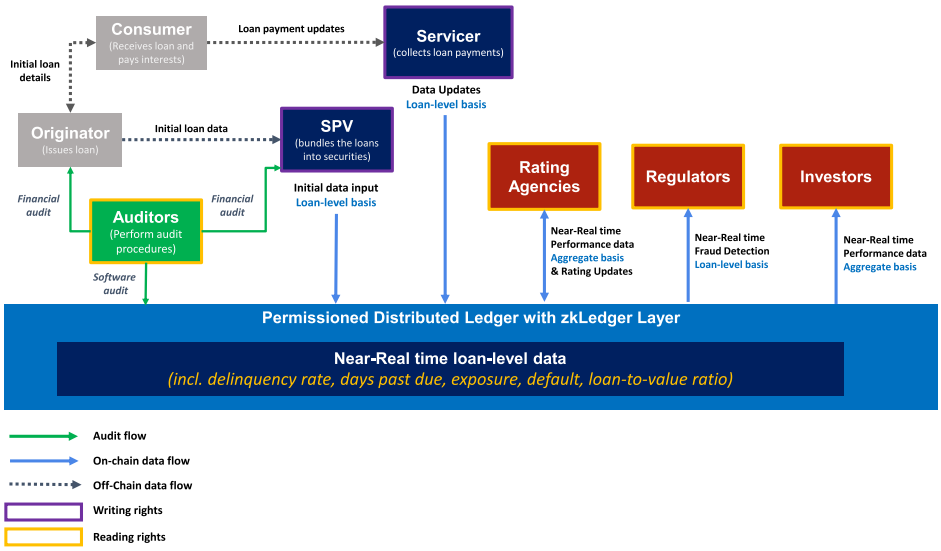

Fig. 3 zkABS Architecture

- Read permission: read permissions are given to Rating Agencies, Investors, Regulators and Auditors of Issuers and Investors in order to perform their data analysis. They act as observatory nodes in the network.

Privacy and Selective Visibility zkLedger introduces the concept of selective visibility. Each participant has access to either loan-level data (loan-level basis access) or asset pool-level data (aggregate basis access). In zkABS, the SPV, Servicer, Auditors and Regulators have access to loan-level data (read access for the Auditors and Regulators and write access for the SPV and servicer), while investors and rating agencies have only read access to asset pool-level data. This is for illustrative purpose and it is possible to have different privacy settings for each actor within a specific category. For instance, certain investors could get loan-level data access in exchange for a premium charge.

Near-real time updates We want to caution the reader about the notion of real-time updates. Often times, proposed blockchain solutions include the promise of delivering real-time information to market participants. This raises privacy concern and security vulnerability as real-time updates might leak transaction contents. For instance, if an investor monitors the performance of an ABS product every second, he could identify which loan in the pool was updated and reconstruct loan-level records. To preserve tuneable privacy, we introduce the concept of near-real time updates. In near-real time settings, the frequency of information release allows for multiple loan-level data points to be updated before they get published in the platform, therefore maintaining the privacy of the loan-level data. In the securitization market, loan-level data updates follow a cyclical pattern which depends on the type of underlying asset backing these securities: an auto-loan typically has monthly payments while a credit card loan has a revolving structure and could be paid back any day. In addition, investors may have different needs depending on their risk profile: central banks and traditional banks usually invest in AAA Tranches with very low default rate and are therefore usually focused on monthly updates. Hedge funds

and private holders who may invest in riskier tranches and short-term investments may be interested in more frequent updates about loan performance. Near-real time should therefore be taken as a broad and flexible definition. In our use case, we take the case of auto-loan ABS, which have monthly payments. Originators offer consumers usually two payment dates (beginning or end of month), therefore near-real time frequency is defined as biweekly. As the platform scales and hosts multiple asset classes with different payment collection cycles (credit card loans, revolving loans etc.) and multiple types of investors, near-real time could be defined as daily.

Industry-wide platform In our use-case, we focus on one underlying asset class: auto-loans. As the platform grows, zkABS's flexible privacy settings could host multiple originators and ABS asset classes (e.g. credit card loans, receivables, etc.) on the same platform while maintaining loan-level data privacy among competing originators and issuers. Since zkABS is used as a means to store loan-level records, the data storage required is reasonable (e.g. the number of loans in an asset-backed security is typically constant until maturity). Therefore, the scalability limitations of zkLedger would not be an issue. zkABS could host all the participants of the US securitization market, and thus power a new type of decentralized digital platform with online analytics and benchmarking tools for the industry.

Smart contracts A "smart contract" refers to transactional terms and conditions embedded in computer code which allow automatic execution of the relevant transaction once precise conformity with those terms and conditions has been established (Dong et al. 2018). When used in conjunction with blockchain technology, the code itself is replicated across multiple nodes and, therefore, benefits from the security, permanence and immutability that a blockchain offers (Dong et al. 2018). A simple example of a smart contract is the automatic payment of monthly interests on a loan when the due date arises. The goal of this paper is to focus on zkLedger application to reduce asymmetry of information among participants rather than to address the potential efficiency and security gains of automating the business logic of the securitization process. zkABS architecture currently does not have a smart contract layer due to the lack of legal framework surrounding their application and the ongoing research on privacy-preserving smart contracts. However, we can imagine that a smart contract layer could be added later in order to automate and bring on-chain several steps of the securitization lifecycle, such as collecting loan payments directly from the consumer, identifying non-performing loans, pricing and rating security. As mentioned in "The inefficiencies of the securitization market" section, zkLedger is agnostic to the DLT used and could be implemented as a set of smart contracts on top of an existing DLT which already has a smart contract layer and then could easily link other smart contracts into zkABS. A smart contract layer could reduce operational errors and speed up data processing, particularly at the Servicer level.

Near-real time analytics about loan performance for investors

In this section, we focus on a particular use case for zkLedger: the potential for investors to get access to publicly verifiable near-real time analytics about asset-pool performance, without compromising individual loan data.

Near-real time analytics tools Currently, there are no available solutions on the market that enable investors to get near-real time performance data[10]. As we discussed in "Introduction" section, investors have to perform cumbersome data standardization and offline analysis to price risk and perform benchmarking for this type of securities. In addition, they do not get asset pool performance updates in a timely manner, which can result in suboptimal investment decisions and a lack of liquidity in the secondary market (Sindle et al 2017). With zkABS, financial information about each individual loan is stored and updated in near-real time on zkABS decentralized platform. This information includes loan principal, annual payments, delinquency rates, credit scores, remaining term to maturity and other information (see Fig. 4 for a sample of loan-level records for an auto-loan) and serves as a base for issuers to disclose periodic information to investors and regulators (e.g. offering prospectus, TRACE reports).

This information is highly sensitive and issuers may not have the incentive to disclose such data at individual loan-level in near-real time to investors. Further, investors may not want to see the loan-level data points and consumer information in clear form as they would become subject to data privacy regulations[11].

Through our interviews, we confirmed that investors would be interested in getting timely updates about the performance of ABS products at the asset pool level (aggregate basis as opposed to loan-level basis) and may be willing to pay a premium for this kind of ABS offering. There is currently no solution in the market that would enable issuers to provide **publicly verifiable** timely information at pool level, without revealing loan-level information.

If they adopt zkABS, the issuers' incentive to include investors in their blockchains may change. With zkABS, issuers can hide sensitive loan-level data on their blockchain and still allow investors to perform analytics on the hidden data in order to get secure aggregate balances and ratios about the performance of their ABS products.

As shown in Fig. 5, investors see a hidden view of the ledger and cannot track loan performance at loan-level, thus zkABS protects the issuers/SPV's proprietary and sensitive data such as borrower names and individual loan performance. However, investors can still perform analytics on the hidden data at the pool level as in Fig. 6, which allows them to monitor the performance of their loans and improves their ability to price risk efficiently and independently. **It allows investors to build their own queries at any point of time.** For instance, an investor could query trends about loan default in Texas for one particular asset class instead of waiting for the servicer reports. All queries (sum, mean, correlation, etc) are interactive and the party that the investor is trying to query must exchange information with the investor otherwise he cannot query the table, another form of information control for issuers and servicers.

Pricing efficiency zkABS allows multiple SPVs to join the same platform, which will push for data standardization and provide investors with easy-to-compare near-real time information across issuers and related asset-backed securities. As pointed out in the Structured Finance Industry Group's report (Sindle et al 2017), this could fundamentally improve pricing efficiency and deepen the securitization market: "security pricing could become more accurate with a potential narrowing of spreads as investors gain the ability

[10] Expert interviews of ABS buy-side trading desks from four major financial institutions, March-April 2018
[11] Expert interview of one attorney representing investors in the securitization market

Data type	Example
TYPE	Auto Loan
assetNumber	0001694010 - 000001
reporting date	Real-time
originationDate	7/1/2011
originalLoanAmount	$ 27,694.00
Annual Payment	$ (542.11)
loanMaturityDate	8/1/2017
originalInterestRatePercentage	12%
underwritingIndicator	TRUE
vehicleManufacturerName	GMC
vehicleModelName	TERRAIN
vehicleModelYear	2011
vehicleValueAmount	$ 24,237.00
obligorCreditScoreType	Credit Bureau Score
obligorCreditScore	548
paymentToIncomePercentage	8%
obligorGeographicLocation	IL
remainingTermToMaturity (Months)	8
nextReportingPeriodPaymentAmount	$ 539.84
reportingPeriodInterestRatePCT	12%
nextInterestRatePercentage	12%
servicingFeePercentage	2%
Monthly interest rate	1%
scheduledPrincipalAmount	$ 494.88
ActualEndBalAmnt	$ 4,513.54
ScheduledPmntAmnt	$ 539.84
totalActualAmountPaid	$ 1,080.00
actualInterestCollectedAmount	$ 102.67
actualPrincipalCollectedAmount	$ 977.33
currentDelinquencyStatus	0
loanToValue	61%

Fig. 4 Sample of loan-level record

zkABS SPV Plain View

ABS ID	Loan ID	Net Balance	Credit Score	Delinquency Status	Loan-to-Value
B	1	27,030	568	0	61%
A	1	34,100	540	28	54%
B	2	23,050	625	12	23%
...	...	...	...	...	...
C	10,000	45,320	486	0	75%

zkABS Investor Encrypted View

ABS ID	Loan ID	Net Balance	Credit Score	Delinquency Status	Loan-to-Value
B	xxx	xxx	xxx	xxx	xxx
A	xxx	xxx	xxx	xxx	xxx
B	xxx	xxx	xxx	xxx	xxx
...	...	...	...	...	...
C	xxx	xxx	xxx	xxx	xxx

Fig. 5 zkABS plain and hidden views

Investor Near-Real Time Analytics

Metric	ABS A	ABS B	ABS C
Outstanding Principal Balance	$164 M	$156 M	$116 M
Weighted Average Interest Rate (% p.a.)	4.93%	5.23%	6.56%
Weighted Credit Score	621	520	490
Average Weighted Delinquency Status	0.1	0.9	1.3
Defaulted Amounts	$34.9 K	$67.2 K	$75.5 K

Fig. 6 Example of analytics available to investors

to make near-real time assessments of security values by tracking shifting patterns in loan-level payments. The pool disclosure–the loans, with their performance and yields–in the security's offering documentation could also be automatically and almost instantly updated to reflect the very latest portfolio performance." (Sindle et al 2017) Compared to another permissioned blockchain with the right access rights, zkLedger provide investors the ability to perform **anonymized** analytics that are **publicly verifiable**, which provides additional security, transparency and reduces asymmetry of information in the market.

Limitations

There are several significant limitations to our research findings. First, there are some practical limitations about the implementation of zkABS. This paper does not provide a cost analysis of implementing and running zkABS. While we expect the benefits to outweigh the costs as more participants join the platform, each participant should perform a cost analysis and evaluate the return on investment before shifting to this type of technology. In addition, we do not discuss which actor(s) (e.g. industry consortia, third-party notaries, government, fintech company) would be leading this initiative, the legal implications and resulting consensus mechanism. DLT may be slower to adopt due to its decentralized nature and the industry is still exploring different types of operational and consensus mechanisms. In the finance industry, financial institutions have performed experimentation with their own DLT or via the creation of a consortium that operates on a same DLT (e.g. Corda, Hyperledger Fabric, Ethereum Enterprise). In this paper, we do not recommend a specific infrastructure nor discuss the integration protocol: participants could leverage the existing DLTs above to operate zkABS or create a new DLT. Second, there are some technical limitations to the underlying technology: zkLedger can guarantee the traceability and immutability of the information in the ledger, however the information's veracity can only be as good as its input data (an issue common to DLTs). If there are manual errors during the input phase, the information in the ledger will not

be accurate. The use of smart contracts and automation from the loan inception phase will greatly minimize the need for manual input and alleviate this concern but is out of the reach of this paper. Finally, there are risks over data security breach when performing analytical queries in a repeated manner: a participant may be able to perform reverse-engineering and guess changes in individual loan level datapoint by querying certain types of analytics (averages, sums, etc.) at high frequency. There is a need to define a limit of number of queries and interval of time between two queries for each asset in order to prevent this threat.

Future work

This paper focuses on the benefits to investors in the securitization market of having access to near-real time performance data to perform their due diligence independently and efficiently. Nevertheless, there are potential benefits for other participants that we do not address in details in this paper. For instance, as introduced by Kou et al. (2019), recent advances have been made in the use of machine learning methodologies, such as network-based models (Kou et al. 2019) and clustering (Kou et al. 2014), to assess and regulate systemic financial risk and provide early warning for risk exposure. These models consider various types of indicators including securitization market conditions and could therefore benefit from the near-real time network-level data collected through zkABS. Regulators would be able to track fraud behavior and abnormal correlations using a customized suite of zkLedger analytics; a benefit that they value significantly: "From a regulatory perspective, access to a constantly updated, auditable set of agreed-upon data can also allow a myriad of regulatory benefits, including more efficient Know-Your-Customer (KYC) and Anti-Money Laundering (AML) checks. Currently, complying with KYC requirements creates a great deal of duplicative data and work; whereas, if industry participants and regulators could agree on a consensus-based ledger as the repository of relevant data, it could allow for new service providers to facilitate KYC compliance and permit regulators greater insight into the relevant data and processes" (U.S. Chamber of Digital Commerce SFIG 2017). Another example would be rating agencies or credit scoring agencies, which could get access to performance data and update their ratings in near-real time accordingly. Finally, through the implementation of smart contracts, issuers would also be able to export their data into the TRACE regulatory database in a seamless and low-cost fashion. Currently, zkLedger does not support private smart contracts, which is an ongoing area of research. A critical part to the success of blockchain applications in this industry is to ensure through assurance services (performed by an independent CPA auditor) that the underlying technology and analytics tools are designed and operating effectively. This is particularly important for zero-knowledge technology due to the privacy goals. Current assurance services include examination of Service Organization Controls, such as SOC 1, 2 and 3 reports. A SOC 1 report is a report on Controls at a Service Organization which are relevant to user entities' internal control over financial reporting. A SOC 2 report focuses on a business's non-financial reporting controls as they relate to the AICPA's Trust Services Principles: security, availability, processing integrity, confidentiality, and privacy of a system. A SOC 3 report covers the same areas as a SOC 2 report but is a shorter report for general public use. A future contribution to the zkLedger project would be to explore the types of assurance services required for zkLedger applications and their characteristics.

Conclusion

Distributed ledger technology has the potential to fundamentally change the way markets operate, by reducing agency costs while bringing more transparency and accountability to each market interaction. In order to unlock such potential, there needs to be flexible privacy settings that can preserve confidential, proprietary information while allowing participants to verify data accuracy in a timely manner. We propose to adopt a zero-knowledge protocol, zkLedger, that addresses the tradeoff between privacy and transparency. We introduce zkABS, a simplified architecture of a decentralized market platform based on zkLedger and designed for the securitization industry. Using widely accepted cryptographic zero-knowledge proofs, zkABS preserves the transparency of transaction at a granular level, while providing distrusting market participants with a suite of anonymized timely analytics on asset pool performance (net cash flow balances, average credit scores, variances, etc.). We argue that zkABS could alleviate market inefficiencies related to the lack of transparency over the quality of the underlying assets. Among the potential benefits, zkABS allows investors to better price risk, regulators to monitor fraud and systemic risks and rating agencies to update their ratings in near-real time, making the securitization market more efficient. While our study shows promising applications, privacy solutions for distributed ledgers are an ongoing research area, which we believe open the path towards opportunities for future related work.

Appendix A – existing blockchain initiatives in the securitization industry

This Appendix presents some of the existing blockchain initiatives in the securitization industry. In 2017, the Structured Finance Industry Group and the Chamber of Digital Commerce commissioned Deloitte and Touche LLP to examine applications of blockchain technology for the securitization industry. This work resulted in the hypothesis that this technology can indeed be used to streamline processes, lower costs, enhance transparency, increase transaction speed and fortify security. The Financial Industry Regulatory Authority (FINRA) has responded positively as well, commenting on blockchain's potential to reduce fraud and power timely analytics solutions in the industry. Among the potential benefits, blockchain technology may bring transparency and accountability to the system due to its immutable and traceable audit trail, which prevents fraudulent data alteration. It also helps streamline data processing as it allows participants to store and securely update the information of thousands of individual loans on a timely basis, without the need for reconciliation among each party's database. Any update to the underlying assets – such as payment delinquency – and related securities, could be consistently broadcasted to all participants in the ledger, which would give investors, rating agencies, auditors of issuers and investors, and regulators timely access to performance data. Several applications of securitized blockchains have emerged in China, led by giant technology companies such as JD Finance and Baidu. In Fall 2017, Baidu announced its first blockchain-based ABS product publicly trading on the Shanghai Stock Exchange (Jingli 2017). The ABS is backed by consumer auto-loans and valued at CNY 400 million ($60.4 million), with preferred Tranche A of CNY 340 million and Tranche B of CNY 24 million. Baidu built a blockchain as a service for the security, with all participating institutions on this permissioned consortium blockchain, including Baidu Finance, the security provider, the brokers, the rating agency and the law firm. The technology uses decentralized storage, cryptography and a consensus algorithm to enable each participant to have a node

in the blockchain and gain access to timely information about the underlying assets at different stages of the securitization process. Unlike zkABS, this platform supports only participants on the sell-side (issuers, brokers, etc.) and does not support the buy-side of the industry (investors, auditors of investors, etc.). Therefore, investors would not be able to verify independently the data accuracy or trade directly on the platform.

Abbreviations

ABS: Asset-backed securities; AICPA: American institute of certified public accountants; AML: Anti-money laundering; FINRA: Financial industry regulatory authority; KYC: Know-your-customer; MBS: Mortgage-backed securities; SOC: Service organization controls; SPV: Special purpose vehicle

Acknowledgements

We would like to thank Neha Narula, Simon Johnson, Nabeel Younis, John V. Levonick, Joshua R. Lester and Yutong Zhang for their guidance during the research.

Authors' contributions

The research was conducted by myself and the manuscript was written entirely by myself. The author read and approved the final manuscript.

Funding

We received funding solely from our institution to perform this research.

Availability of data and materials

This manuscript has not been published and is not under consideration for publication elsewhere at this moment. We have no conflicts of interest to disclose.

Competing interests

I do not have any competing interest.

Received: 27 October 2018 Accepted: 13 January 2020
Published online: 25 January 2020

References

Bernhard, Pereira, Warinschi (2012) How not to prove yourself: Pitfalls of the fiat-shamir heuristic and applications to helios. In: Wang X, Sako K (eds). ASIACRYPT 2012. LNCS, vol. 7658. Springer, Heidelberg. pp 626-643

Bloomberg database (2018). Accessed in March-April 2018

Catalini C, Tucker C (2018) Antitrust and costless verification: an optimistic and pessimistic view of the implications of blockchain technology. MIT Sloan Research Paper No. 5523-18:3. http://ide.mit.edu/sites/default/files/publications/SSRN-id3199453.pdf

Cramer, Damgard, Schoenmakers (1994) Proofs of partial knowledge and simplified design of witness hiding protocols. In: In Advances in CryptologyŮCRYPTO Š94, Vol. 839 of Lecture Notes in Computer Science. Springer-Verlag. pp 174-187

Code of Federal Regulations Title 17 Commodity and Securities Exchanges Chapter II Part 246 Credit Risk Retention (2017). https://www.govinfo.gov/app/details/CFR-2016-title17-vol4/CFR-2016-title17-vol4-part246

European Central Bank Publication N. 975 (2008) The incentive structure of the originate and distribute model. ISBN 978-92-899-0370-7 (online) https://www.ecb.europa.eu/pub/pdf/other/incentivestructureoriginatedistributemodel200812en.pdf

Dong X, Mok RCK, Tabassum D, Guigon P, Ferreira E, Sinha CS, Prasad N, Madden J, Baumann T, Libersky J, McCormick E, Cohen J (2018) Blockchain and emerging digital technologies for enhancing post-2020 climate markets (English). World Bank Group, Washington. http://documents.worldbank.org/curated/en/942981521464296927/Blockchain-and-emerging-digitaltechnologies-for-enhancing-post-2020-climate-markets

Feige, Fiat, Shamir (1988) Zero-knowledge proofs of identity. J Cryptol 1(2):77-94

Financial Industry Regulatory Authority (FINRA) (2017) Report on distributed ledger technology: Implications of blockchain for the securities industry, FINRA Publications. https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf

Fligstein, Roehrkasse (2013) All of the incentives were wrong: Opportunism and the financial crisis. Paper presented at the annual meeting of the American Sociological Association Annual Meeting, Hilton New York and Sheraton New York, New York, NY Online August 2013 975:22. https://www.ecb.europa.eu/pub/pdf/other/incentivestructureoriginatedistributemodel200812en.pdf

Goldwasser, Micali, Rackoff (1989) The knowledge complexity of interactive proof systems. SIAM Journal on Computing 18(1):186-208. https://doi.org/10.1137/0218012

Jingli S (2017) Baidu joins global group to advance blockchain technologies. http://ChinaDaily.com.cn. Accessed Mar–Apr 2018

Kou G, Peng Y, Wang G (2014) Evaluation of clustering algorithms for financial risk analysis using mcdm methods. Inf Sci 275:1-12

Kou G, Chao X, Peng Y, et al. (2019) Machine learning methods for systemic risk analysis in financial sectors. Technol Econ Develop Econ 25(5):1-27

Maurer (2009) Unifying zero-knowledge proofs of knowledge. In: Preneel B (ed). Progress in Cryptology AFRICACRYPT 2009, LNCS 5580. Springer, Berlin, Heidelberg. pp 272-286. Lecture Notes in Computer Science, vol 5580

Narula N, Vasquez W, Virza M (2018) zkLedger: Privacy-Preserving Auditing for Distributed Ledgers. In: 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18), USENIX Association. https://www.usenix.org/system/files/conference/nsdi18/nsdi18-narula.pdf
OICV-IOSCO Technical Committee (2012) Principles for ongoing disclosures for asset-backed securities. https://www.iosco.org/news/pdf/IOSCONEWS224.pdf
OpenRisk Loan tape. Open Risk Manual. www.openriskmanual.org. Accessed Mar–Apr 2018
Pawczuk, Massey, Schatsky (2018) Deloitte's 2018 global blockchain survey, findings and insights. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/gx-us-fsi-2018-global-blockchain-survey-report.pdf
Pedersen TP (1992) Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In: J. Feigenbaum (ed). Advances in Cryptology Ů CRYPTO Š91. CRYPTO 1991. Lecture Notes in Computer Science, vol 576. Springer, Berlin, Heidelberg. pp 129-140
Pemberton, Levy (2018) The reality of blockchain. Gartner. https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/
Schnorr (1991) Efficient signature generation by smart cards. J Cryptol 4(3):161-174
SIFMA database (2018). Accessed Mar-Apr 2018
Sindle et al (2017) Applying blockchain in securitization: opportunities for reinvention. U.S. Chamber of Digital Commerce Structured Finance Industry Group SFIG. https://digitalchamber.org/assets/sfig-blockchain-report.pdf
The World Bank (2018) Blockchain & distributed ledger technology (DLT) brief. https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt
U.S. Chamber of Digital Commerce SFIG (2017) Comments' on finra's report on distributed ledger technology. https://www.finra.org/sites/default/files/Blockchain-SFIG-Comment.pdf
U.S. Department of Treasury (2017) Report to the president – a financial system that creates economic opportunities, capital markets
Wang L, et al (2019) Cryptographic primitives in blockchains. J Network Comput Appl. 1 February 2019 127:43-58
Wind database (2018). Accessed in March-April 2018
Wheeler et al (2017) Ten years after the financial crisis, global securitization lending transformed by regulation and economic growth. Standard and Poors Ratings Direct. Structured Finance Research. Issue 1888500-300871285:5. https://www.spratings.com/documents/20184/1393097/SF10Years/b0f1300a-5ed5-407d-8d3b-77fdc3b1f20c

Publisher's Note