Privacy-preserving analytics for the securitization market: a zkLedger application

Sophie Meralli
MIT Digital Currency Initiative

Abstract

A Zero-knowledge proof or protocol is a cryptographic technique for verifying private data without revealing it in its clear form. zkLedger [1] is a zero-knowledge protocol developed by the MIT Media Lab and the first system that protects privacy while providing provably correct analytics to participants using a distributed ledger. In this paper, I evaluate the potential for applications using zkLedger to solve problems in the asset-backed securitization market. To frame this inquiry, I conducted market data analyses, a literature review with special attention to the 2008 financial crisis, stakeholder interviews with investors, originators and issuers, and collaboration with blockchain engineers and researchers. In a world abuzz about blockchain technology, much interest involves the use of blockchains as a secure source of record. From this rises an ongoing debate regarding public versus private data accessibility, permissionless versus permissioned systems, and on-chain versus off-chain data storage. In securitization markets, one of the main challenges in using current blockchains is lack of privacy: data stored in the blockchain is viewable by all participants or is encrypted but does not support data analytics on hidden data. This impedes the ability to store confidential data in a blockchain and simultaneously provide access to multiple distrusting parties (e.g. trading partners or competitors) – key conditions for scaling blockchain applications at the industry level. As a result, existing blockchain-based products in the securitization market are limited to a few types of participants and therefore cannot support interactions between the sell-side and the buy-side of the industry. I explain how the adoption of the zkLedger protocol might resolve these privacy concerns. It could enable all market participants in the securitization lifecycle (e.g. investors, rating agencies, regulators and 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.
Introduction

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 [2]. zkLedger [1] is an experimental system developed by the MIT Media Lab Digital Currency Initiative that uses zero-knowledge proofs to provide provably correct analytics without revealing the actual data. Through its flexible privacy settings, zkLedger can address the trade-off between the need for transparency and privacy, therefore providing secure timely information to market participants. This paper evaluates the potential for zkLedger’s application to the securitization market, an industry with no near-real time analytics services currently available. 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.

The $10 trillion US 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. 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. This lack of transparency prevents investors from performing their investment decisions independently and efficiently and has led to significant regulatory reforms 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 one of the most compelling use cases for a zkLedger application. In the past couple of years, financial institutions and regulators in the industry have looked into blockchain technology’s potential [3][4] and applications have already emerged in China [5]. Blockchain technology may enable market participants to store and update securely the information of thousands of individual loans on a near-real time basis, without the need for reconciliation among each party’s database. It has the potential to bring secure, traceable near-real time performance data to the industry. However, blockchain adoption faces privacy concerns: current blockchains are either entirely viewable to all participants or are encrypted but do not support verifiable analytics on masked data. As security issuers do not have the incentive to reveal sensitive, proprietary loan-level data to investors and third-parties, current 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 subtility of current market interactions.

Through the combination of zero-knowledge proofs and distributed ledger technology, zkLedger can 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 provable market analytics in a timely manner. zkLedger has applications throughout the value chain: in the security construction and issuance steps, zkLedger 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 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, the application of zkLedger could reduce asymmetry of information and improve transparency in the securitization market.

For the purpose of assessing zkLedger’s potential impact on the securitization industry, "blockchain" and "distributed ledger technology" are used throughout this paper interchangeably.

I. 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, which can be primarily attributed to the incentive structure of the securitization model. 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 [3][6] [4].

Overview. Today, the US securitization market represents $10 trillion [7] 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 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”)2 to investors. By transferring the credit risk of the loans to the SPV in return for

---

1 See section III for more details.
2 We use a broad definition of asset-backed securities, which includes securities backed by mortgages (“MBS”) and by any other
Figure 1. Overview of the securitization process

Securitization allows investors to get exposure to specific risk profiles, providing larger portfolio risk diversification.

Sources: Report to the President: A Financial System That Creates Economic Opportunities. US Department of Treasury. October 2017

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 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 Figure 1). Because there are multiple parties involved, there are time lags before investors get notified about the loan payments or defaults.

**Misaligned Incentives.** The market inefficiencies can be primarily attributed to the incentive structure of the securitization model. 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. Due to their different business models, these parties have misaligned incentives that may amplify the systemic risk of the industry: loan originators collect commissions on loan issuance and aim to offload their credit risk by selling the loans to investors [8]. 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 [9]: 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 [9]. 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. Moreover, 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 securitization allows investors to get exposure to specific risk profiles, providing larger portfolio risk diversification.
noting that risk retention rules 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.

**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 [10]. Through our interviews with the trading desks of institutional investors\(^4\), 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 [9]. 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). 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 investor interviewees\(^5\) pointed out:"it would be great to have online analytical 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.

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 [11].

**II. 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 distrustful 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 Figure 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 the data-tape, with asset-level information, it is rather on an occasional basis. Investors may get curated off-chain information on an aggregate 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 [1] 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 analyt-

\(^4\)Interviews of ABS buy-side trading desks from several major financial institutions, March-April 2018

\(^5\)Interview with a buy-side trader on the US asset-backed security market, March 2018
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. zkLedger is an instance of a zero-knowledge protocol which combines several cryptographic primitives to preserve privacy of the ledger while still allowing to compute provably correct measurements over the data in the ledger. zkLedger uses a cryptographic primitive called Pedersen commitments, which are schemes that let someone commit to a specific chosen value (e.g. a transaction amount), while keeping it hidden to others. Instead of storing plain text transactions on the ledger, participants store hiding commitments to the transaction values. These commitments can be homomorphically combined (e.g. the product of the commitments can be opened to compute sums and averages on hidden data) and perfectly hides the committed data (even in the presence of quantum computing). The zkLedger protocol includes a suite of analytics (e.g. sums, averages, correlations and market concentrations). See the zkLedger paper [1] for in-depth explanations and limitations about the technology.

III. Applying zkLedger to the securitization industry

The securitization industry would benefit from zkLedger 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.

1. Architecture and governance system

This paper does not intend to recommend any blockchain 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 – “zkABS” – to analyze the benefits of zkLedger for the participants. Such a simplified architecture would have the following components:

A permissioned 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 zkLedger, participants cannot equivocate (assuming the consensus model is sound), therefore the information in the ledger is secure and publicly verifiable by participants. Figure 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 loan-level payments, pool-level performance and rating information.

Figure 2. Privacy Limitations of Current Blockchain Applications in the Securitization Industry
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.

- 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 Rating Agencies have access to loan-level data (read access for the Auditors and Rating Agencies 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.** The goal of this paper was 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. A smart contract layer could reduce operational errors and speed up data processing, particularly at the Servicer level.

2. 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. As we discussed in section I, 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. 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 Figure 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. Moreover, 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.

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 Figure 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 Figure 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

**Figure 4.** Sample of loan-level record

<table>
<thead>
<tr>
<th>Data type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE</td>
<td>Auto loan</td>
</tr>
<tr>
<td>assetNumber</td>
<td>0001694010 - 000001</td>
</tr>
<tr>
<td>reporting date</td>
<td>Real-time</td>
</tr>
<tr>
<td>originationDate</td>
<td>7/1/2011</td>
</tr>
<tr>
<td>originalLoanAmount</td>
<td>$27,694.00</td>
</tr>
<tr>
<td>Annual Payment</td>
<td>$542.11</td>
</tr>
<tr>
<td>loanMaturityDate</td>
<td>8/1/2017</td>
</tr>
<tr>
<td>originalInterestRatePercentage</td>
<td>12%</td>
</tr>
<tr>
<td>underwritingIndicator</td>
<td>TRUE</td>
</tr>
<tr>
<td>vehicleManufacturerName</td>
<td>GMC</td>
</tr>
<tr>
<td>vehicleModelName</td>
<td>TERRAIN</td>
</tr>
<tr>
<td>vehicleModelYear</td>
<td>2011</td>
</tr>
<tr>
<td>vehicleValueAmount</td>
<td>$24,237.00</td>
</tr>
<tr>
<td>obligorCreditScoreType</td>
<td>Credit Bureau Score</td>
</tr>
<tr>
<td>obligorCreditScore</td>
<td>548</td>
</tr>
<tr>
<td>paymentToIncomePercentage</td>
<td>8%</td>
</tr>
<tr>
<td>obligorGeographicLocation</td>
<td>IL</td>
</tr>
<tr>
<td>remainingTermToMaturity</td>
<td>8</td>
</tr>
<tr>
<td>nextReportingPeriodPaymentAmount</td>
<td>$539.84</td>
</tr>
<tr>
<td>reportingPeriodInterestRatePCT</td>
<td>12%</td>
</tr>
<tr>
<td>nextInterestRatePercentage</td>
<td>12%</td>
</tr>
<tr>
<td>servicingFeePercentage</td>
<td>2%</td>
</tr>
<tr>
<td>Monthly interest rate</td>
<td>3%</td>
</tr>
<tr>
<td>scheduledPrincipalAmount</td>
<td>$494.88</td>
</tr>
<tr>
<td>ActualEndBalAmnt</td>
<td>$4,513.54</td>
</tr>
<tr>
<td>ScheduledPmntAmnt</td>
<td>$539.84</td>
</tr>
<tr>
<td>totalActualAmountPaid</td>
<td>$1,080.00</td>
</tr>
<tr>
<td>actualInterestCollectedAmount</td>
<td>$102.67</td>
</tr>
<tr>
<td>actualPrincipalCollectedAmount</td>
<td>$977.33</td>
</tr>
<tr>
<td>currentDelinquencyStatus</td>
<td>0</td>
</tr>
<tr>
<td>loanToValue</td>
<td>61%</td>
</tr>
</tbody>
</table>
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 [3], 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 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.” [3] 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.

zkABS is just one example of the many industry applications that could be developed using the zkLedger protocol. zkLedger could power innovative solutions for decentralized digital platforms where market participants must perform data analysis based on confidential transactions.

IV. 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, regulators will 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". 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 (per-
formed 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

Blockchain 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 the data accuracy. We propose to adopt a privacy-preserving protocol, zkLedger, that addresses the tradeoff between privacy and transparency. In the securitization market, zkLedger could alleviate market inefficiencies, such as the lack of transparency over the quality of the underlying assets backing these securities. Using widely accepted cryptographic zero-knowledge proofs, zkLedger preserves the transparency of transaction at a granular level, while providing third-parties with a suite of near-real time analytics on asset pool performance (net cash flow balances, average credit scores, variances, etc.). Among the potential benefits, zkLedger 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.

Acknowledgments

During the course of this project, we solicited the input of MIT Digital Currency Initiative member, Deloitte & Touche LLP. The view and perspectives in this paper are not necessarily the views of Deloitte & Touche LLP. We would like to thank in particular Seth Connors, Ann Perrin, Jeremy Simon and Peter Taylor for their guidance. In addition, research elaborated in this paper could not have been performed without the oversight and thought leadership of Simon John-son, Kevin Lee, Joshua Lester, John Levonick, Neha Narula, Mark Weber and Nabeel Younis.

References


Appendix I – 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 [5]. 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.