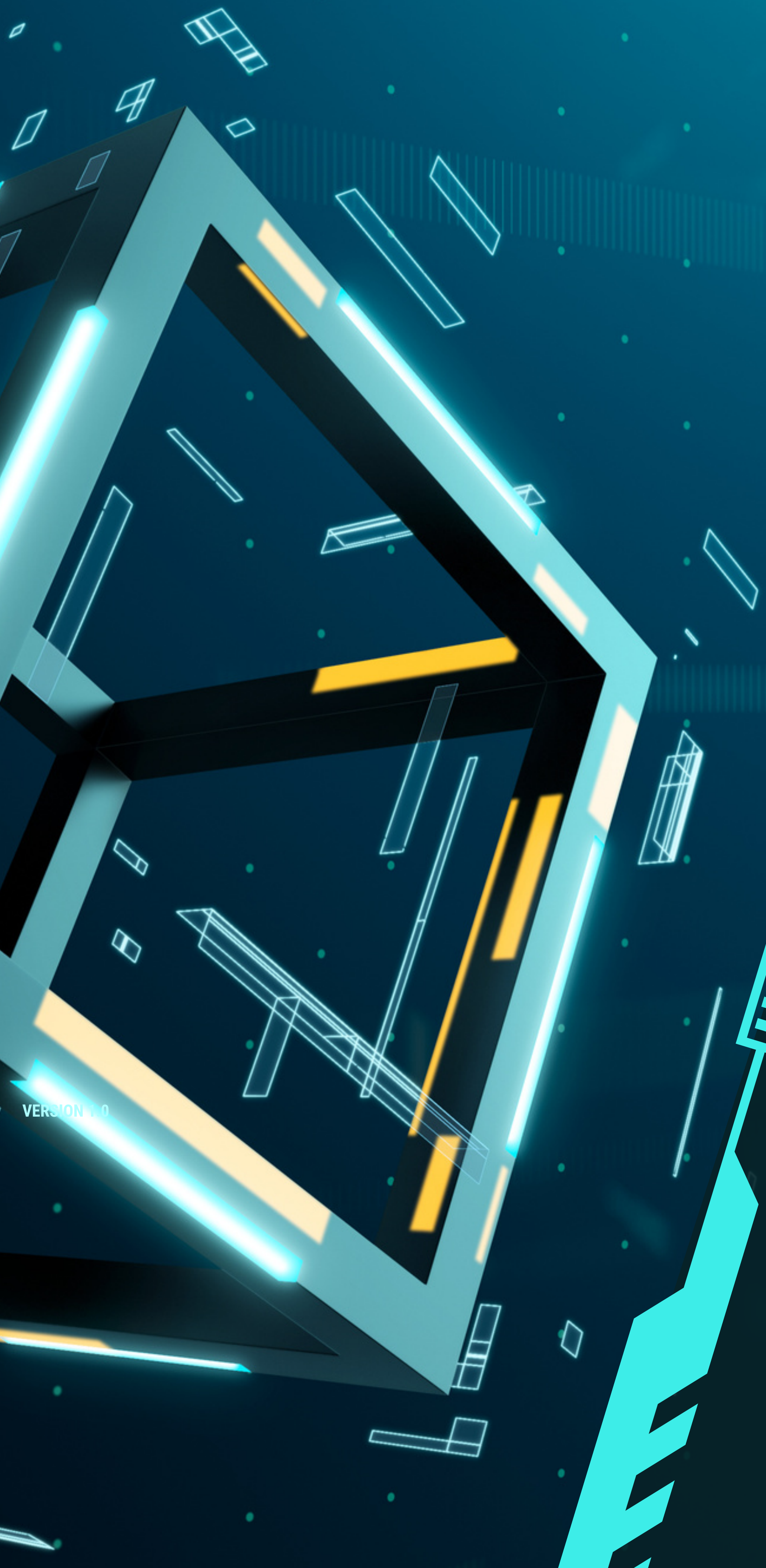


POLY ZKP

SOLUTION FOR BLOCKCHAIN PRIVACY

WHITEPAPER

version 1.11

Content

Background

In 2008 at the height of the financial crisis, a mysterious figure released a message to the world. This message was about Bitcoin, a new electronic cash system that was fully peer-to-peer without any third party involved.

Satoshi Nakamoto—an individual or group of individuals (or artificial intelligence, even?)—announced that they had managed to solve the double-spending problem that had plagued previous digital currencies or cryptocurrencies. Nakamoto did this by bringing together numerous technologies and assembling them in novel ways. Those technologies and concepts involve cryptography, game theory, economics and algorithms, to name a few.

At the time Bitcoin was released, the term 'blockchain' wasn't used to describe this new ledger technology. Satoshi's creation enabled a user of Bitcoin to digitally transact directly with another user without relying on a single, centralised intermediary (such as a bank) to validate the transaction. This was a breakthrough that previous digital transaction systems had failed to achieve.

Blockchain vs Bitcoin

Blockchain is the technology that underpins Bitcoin. A blockchain is a decentralised ledger that records transactions (or information in general) within a network of participants. A ledger is a set of permanent records that are updated sequentially. A decentralised ledger is one where no single authority is able to control what is written onto the shared ledger. Blockchains coordinate information amongst multiple participants.

The transactions, records or information on a blockchain are immutable, made so through cryptographic functions and timestamps. Immutability means that the records are tamper-resistant—very difficult to alter once they have been written into the ledger.

Pain point

The growth in popularity of free internet applications used by billions of people worldwide has resulted in most user information and data being controlled by large technology companies, often resulting in an abuse of users' privacy.

Blockchain technology, like Ethereum, was created to bring control back to the users where a user data is owned by them as well. However, apart from being pseudo anonymous, it does not have many ways to protect the privacy of users.

For example, if a user purchases something from someone with his wallet address, his wallet address is now known by that someone, and he will know everything that the user did in the past and the future, including what else he bought, or how much he has, etc, creating a real privacy concern for real-world adoption.

To combat this, Ethereum and various protocols are looking to implement zero-knowledge proofs (ZKP) to improve privacy for users.

What is ZKP?

Simply put, zero-knowledge proofs (ZKP) uses encryption to prove something is true without revealing more than necessary, greatly improving privacy.

ZKP was invented in 1985 and is popularly defined as “A zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that something is true, without revealing any information apart from the fact that this specific statement is true.”

There are two main types of zero-knowledge proofs, interactive and non-interactive. We will provide some examples of ZKP later to make it easier to understand.

With the growing popularity of blockchains, ZKP is becoming popular due to the great benefits it brings when implemented together with blockchain technology as it will improve privacy, speed, and security, without impacting decentralization.

But how effective is it in real life and could it be the answer to our data privacy issues?

ZKP is a type of cryptographic evidence that allows a "prover" to demonstrate to a "verifier" if the prover is aware of certain values, without disclosing the actual answer to the verifier.

The zero-knowledge as a concept comes from the fact that no information is provided by the prover but still able to convince the verifier that the truth is being told. This secures your communication so that no one else can see what you are talking about or what files you're exchanging.

Since ZKPs make it possible to verify a computational assertion, there are many use cases for it such as, a lender can use ZKP techniques to confirm that the borrower has a sufficient amount in their bank account to eventually return the money without learning further information about their balance. This takes away the need to reveal information or have a witness to prove the validity of any claims.

Types of ZKP

There are two main types of zero-knowledge proofs, interactive and non-interactive.

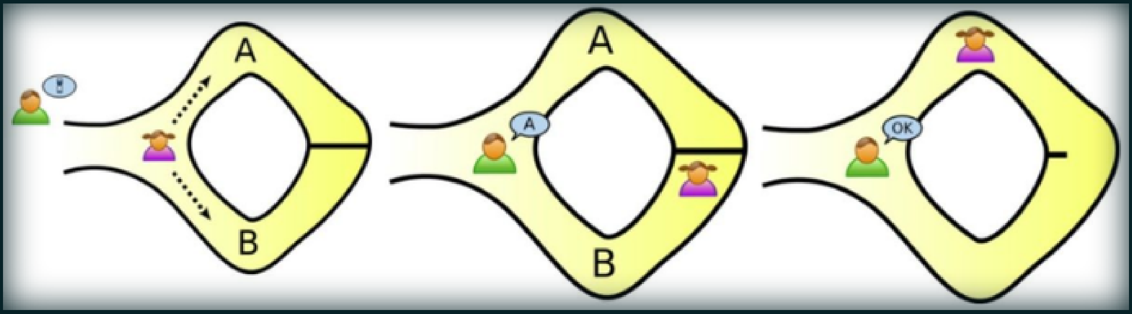
1.Interactive Zero-Knowledge Proofs

Interactive ZKPs allow the prover and the verifier to interact several times. The verifier challenges the prover, who provides replies to these challenges until the verifier is convinced.

A famous example of interactive zero-knowledge proof is "The Ali Baba Cave".

In the story, there is a cave with a magic locked door. Peggy (the prover) wants to prove to Victor (the verifier) that she knows the secret phrase to open the magic door in the cave without revealing the phrase. Both of them know that this cave has a circular path with a single entrance and exit and the magical door is at the end blocking the path in the middle and the only way to open it is by saying the magic phrase.

How can Peggy prove to Victor that she knows the magic phrase without telling him what the phrase is?



They label paths A and B from the entrance, and Victor waits outside the cave as Peggy goes in. Peggy can either take path A or B, but Victor is not allowed to see which path she takes. Victor can then shout which side of the path he wants her to use to return randomly. If Peggy really does know the magic word, this would be easy, as she will be able to open the door and return along the chosen path.

However, if Peggy does not know the magic phrase, she has a 50% chance of exiting via the path Victor chose. By repeating the test, her chances of tricking Victor would become exponentially slimmer, and the only way to guarantee that she always takes the correct path is by knowing the magic phrase. After a few attempts, the probability that Peggy really knows the magic phrase approaches 100%. Although it can never be 100%, the idea is to minimize the chances that someone is lying to you.

In summary, interactive ZKPs, as the name suggests, require interaction with the prover and verifier. For example, Victor uses interactive ZKPs to verify the validity of Peggy's statement through back-and-forth communication between provers and verifiers.

However, interactive ZKPs have limited utility and transferability as it relies on the interaction between two parties and the proof would be unavailable for a third party to verify.

If Peggy brings another friend to the cave, she would have to go through the entire process to proof again, which is time-consuming and not scalable.

2.Non-Interactive Zero-Knowledge Proofs
Non-interactive ZKPs were created to show that the prover is aware of certain information without really revealing it.

A popular example of non-interactive proof uses the game 'Where's Wally'.

Imagine a competition of 'Where's Wally', even the organizers do not know where Wally is. Whoever can prove that Wally exists receives a prize. You found Wally but you do not want to point him out with your finger because that would show the location of Wally to everyone and end the competition immediately.

To prove that you know where Wally is and that he really does exist, you take a giant piece of paper, many times the size of the Wally photo, and cut a small hole in it. You then place the small hole on top of Wally. This shows that Wally does exist, but because the big piece of paper blocks all other context information, Wally's location has not been revealed and is still a mystery.

In summary, the above example is just an analogy for non-interactive ZKPs, but it showcases how they are non-interactive, as anyone that sees the hole showing Wally will agree that it is enough proof that Wally exists without you having to repeat any action, unlike in interactive ZKPs.

In reality, a non-interactive zero-knowledge proof is made by putting the secret data into a certain algorithm and running it. When the verifier gets this proof, he or she uses a different method to make sure that the prover knows the secret information.

Non-interactive ZKPs also make the prover and verifier share a key so that verification can be done by someone other than the prover and verifier.

Since the verifier can only check the information once at any given time, this takes more processing power than interactive ZKPs.

Polygon zkEVM

Polygon zkEVM is a decentralized Ethereum Layer 2 scalability solution that uses cryptographic zero-knowledge proofs to offer validity and quick finality to off-chain transaction computation, also known as a ZK-Rollup.

The ZK-Rollup executes smart contracts transparently, by publishing zero-knowledge validity proofs, while maintaining opcode compatibility with the Ethereum Virtual Machine.

Given that Ethereum is subject to the DLT (distributed ledger technology) trilemma, it cannot scale beyond its transaction threshold without sacrificing decentralization or security. This is where Polygon zkEVM comes into play.

Polygon zkEVM is a virtual machine designed and developed to emulate the Ethereum Virtual Machine (EVM) by recreating all existing EVM opcodes for transparent deployment of existing Ethereum smart contracts and exponentially improve the scalability and transactions per second (TPS) of Ethereum.

In order to prove that the off-chain computations are correct, Polygon zkEVM employs verifiable zero-knowledge proofs as validity proofs. Although the Layer 2 zero-knowledge proofs are based on complex polynomial computations to provide validation and finality to off-chain transactions, the validity proofs are quick and easy to verify.

As a state machine, zkEVM carries out state changes, which come from executions of Ethereum's Layer 2 transactions that users send to the network, and subsequently produces validity proofs attesting to the correctness of the state change computations carried out off-chain.

Although taking on this revolutionary design approach was a hard decision to make, the objective is to minimize the user and developer friction while using the solution. It is an approach that requires recreation of all EVM opcodes for the transparent deployment of existing Ethereum smart contracts.

Benefits of Polygon zkEVM

- EVM-equivalence
- Ethereum security
- ZKP-powered scalability

Polygon zkEVM is a Layer 2 scaling solution for Ethereum that leverages the scaling power of zero-knowledge proofs while maintaining Ethereum compatibility. Developers and users on Polygon zkEVM can use the same code, tooling, apps, etc that they use on Ethereum, but with much higher throughput and lower fees.

Developers will deploy their existing contracts to the zkEVM, and users can deposit assets from Ethereum and transact off-chain. These transactions are grouped into batches with zero-knowledge proof attesting to the validity of each transaction. This ensures that the operators of the zkEVM can't steal user funds, so we can say that it inherits the security of Ethereum.

Polygon zkEVM offers compatibility and scalability without compromise.

Why Polygon ZKP on Bep20

The Polygon zkEVM is the first zero-knowledge scaling solution compatible with the Ethereum Virtual Machine to integrate smart contracts and developer tools. Polygon as a Layer 2 protocol is already faster and more scalable than Ethereum; however, the launch of the zkEVM feature is bound to make it even more scalable.

The launch of the zkEVM tool is a significant milestone that is bound to push Polygon ahead in the race for dominance among the top Layer 2 protocols on the Ethereum blockchain. From Optimism to Arbitrum and much more recently, Shibarium and Base from Coinbase Exchange, Polygon will now rank as the first L2 to launch a zkEVM tool in the crypto ecosystem.

In contrast, zkEVM has not been developed enough on the Binance Chain for the time being, and the market is relatively blank. At the same time, the development of ZKP requires users to continuously trade to verify its validity and stability, so the Polygon team deployed ZKP on Binance Chain, aiming to fill the temporary defects of Binance Chain in zkEVM.

Conclusion

Polygon zkEVM is a new technology, the first zero-knowledge scaling solution equivalent to the EVM, where existing smart contracts, developer tools, and wallets can work seamlessly. Polygon zkEVM leverages zero-knowledge proofs to reduce transaction costs and increase throughput while inheriting the security of Ethereum.

Transactions in the zkEVM network (L2) are compiled into batches, these batches are then sequenced in Ethereum smart contracts, after which their state transitions are proven and verified on Ethereum, reaching a trusted state.

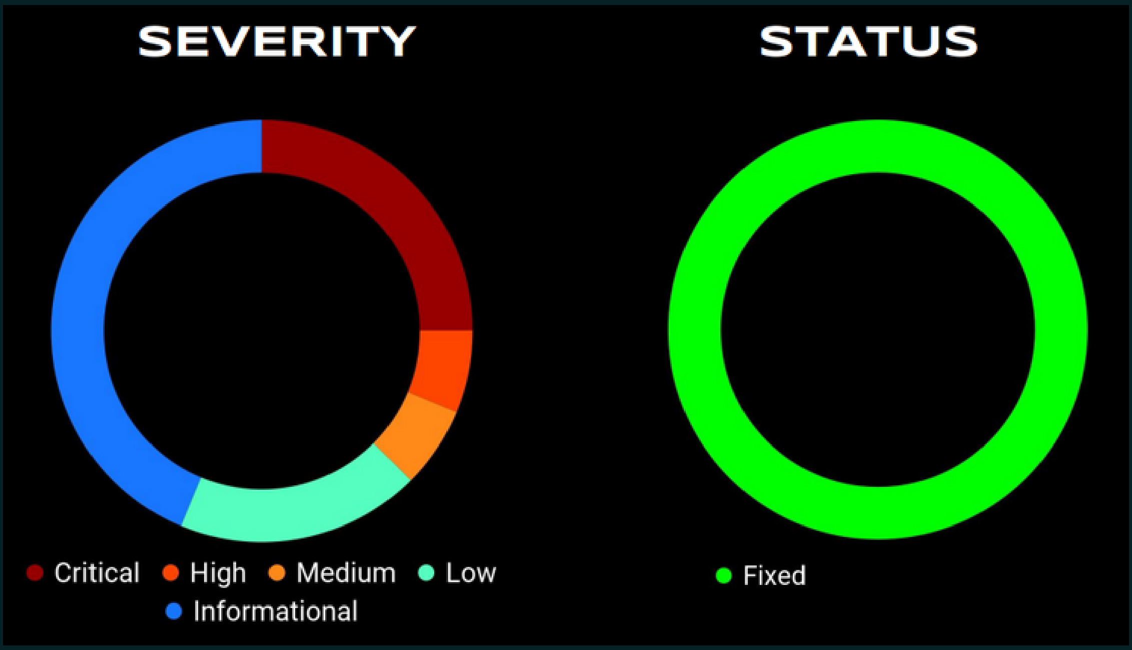
zkEVM has multiple operational layers:

Network layer: where the Sequencer and Aggregator run.

ROM layer: zkEVM uses a new language called zkASM to implement the EVM, making EVM state transactions provable.

Hardware layer: zkEVM uses a new language called PIL to create polynomial identities and constraints to guarantee complete and well-executed zkASM ROM.
L1 Ethereum Smart Contract: Bridges assets between networks and implements PoE (Proof of Efficiency) consensus, ensuring correct state transitions for batches.

During the security review, the Hexens team covered the most critical attack surfaces, including smart contracts, PIL hardware and zkASM ROM, unexpected differences between EVM and zkEVM, and more.



Due to its complexity and composability, the review requires a wide range of expertise and mindsets across different areas of cybersecurity. The final conclusion is that the overall security and code quality are at a high level.

Tokenomics

Token (Ticker): ZKP
Total supply: 1,000,000
Initial token price: 1 MATIC
Initial market cap: 1,000,000 MATIC
Contract:
0x2aD9C7Eccda25861f11D8b1D96Ba7B5101f199f3

Token Allocation:
Ecosystem rewards: 75% (with burning mechanism, all the remaining will be burned when the ZKP exchanger launch)
Treasury / Liquidity Reserve: 8% (12 months lock up, then unlock 8% per month)
Marketing & Partnerships: 3% (6 months lock up, then unlock 15% per month)
Adoption Incentives: 3% (per network activity)
ZKP Exchanger Launch Liquidity: 8%
Team & Recruitment: 3% (24 months lock up, then daily for 12 months)

Stay tuned for further details.

Roadmap

Our roadmap outlines some important stages in our product development cycle that will provide the best value possible to Poly ZKP users. Please note that the roadmap can be updated as new priorities emerge and is meant to serve as a guidepost for us as we continue to build financial products that will onboard the next wave of users onto Poly ZKP.

2023 Q1

- Scale up development & design team
- UI/UX design
- Smart Contract Development

2023 Q2

- Audit Smart Contracts
- Frontend development Stage 1/3
- Testnet Launch

2023 Q3

- Node Presale
- Dapp 1.0 version publishment
- BSC ZK Exchanger development 1/3

2023 Q4

- Frontend development Stage 2/3
- Price Feed integration & Internal Testing
- Complete technical documentation

2024 Q1

- BSC ZK Exchanger development 2/3
- UI/UX design 2.0 version
- Frontend development 3/3 (Completed)

2024 Q2

- Dapp 2.0 version
- BSC ZK Exchanger Testnet 1/3

2024 Q3

- BSC ZK Exchanger dev 3/3 (Completed)
- BSC ZK Exchanger Testnet 2/3
- Merchants Association（HK/Dubai）
- Mint ZKP Exchanger NFT

2024 Q4

- BSC ZK Exchanger Testnet 3/3 (Completed)
- BSC ZK Exchanger launch

Terms of Use

1. Introduction Please read these Terms of Use ("Terms") carefully before using the Poly ZKP platform ("Platform") operated by Poly ZKP ("us," "we," or "our"). Your access to and use of the Platform is conditioned on your acceptance of and compliance with these Terms. These Terms apply to all visitors, users, and others who access or use the Platform.

By accessing or using the Platform, you agree to be bound by these Terms. If you disagree with any part of the Terms, you may not access the Platform.

2. Open Source and Smart Contract Use Poly ZKP may provide open-source resources, including but not limited to smart contracts. Users are solely responsible for ensuring that their use of our resources is in compliance with all applicable laws, regulations, and rules.

3. Disclaimer of Warranties The Platform is provided on an "as is" basis. Poly ZKP makes no warranties, expressed or implied, and hereby disclaims and negates all other warranties, including without limitation, implied warranties or conditions of merchantability, fitness for a particular purpose, or non-infringement of intellectual property or other violation of rights.

4. Limitation of Liability In no event shall Poly ZKP or its suppliers be liable for any damages (including, without

limitation, damages for loss of data or profit, or due to business interruption) arising out of the use or inability to use the materials on the Platform, even if Poly ZKP or a Poly ZKP authorized representative has been notified orally or in writing of the possibility of such damage.

5. Intellectual Property Rights All intellectual property rights, including but not limited to trademarks, logos, and copyrights, related to the Platform are owned by or licensed to Poly ZKP. Users are not granted any rights to use such intellectual property without the express written consent of Poly ZKP.

6. Governing Law These Terms shall be governed and construed in accordance with the laws of the jurisdiction in which Poly ZKP is based, without regard to its conflict of law provisions.

7. Changes to the Terms of Use We reserve the right, at our sole discretion, to modify or replace these Terms at any time. If a revision is material, we will try to provide at least 30 days' notice prior to any new terms taking effect. What constitutes a material change will be determined at our sole discretion.

By continuing to access or use our Platform after those revisions become effective, you agree to be bound by the revised Terms. If you do not agree to the new Terms, please stop using the Platform.

8. Ending Our Relationship
8.1 Termination by You You may terminate your relationship with Poly ZKP and discontinue the use of the Platform at any time. To do so, simply stop using our

Platform and any associated services. Upon termination, you remain responsible for any outstanding obligations or liabilities that may have arisen during your use of the Platform.

8.2 Termination by Poly ZKP Poly ZKP reserves the right to terminate or suspend your access to the Platform without prior notice, for any reason, including but not limited to breaches or violations of these Terms or applicable laws, or if we believe that your actions may harm or threaten the safety and security of our Platform, other users, or any third parties. In the event of termination or suspension, your right to use the Platform will immediately cease, and you must promptly discontinue any use of our Platform and services. We will not be liable to you or any third party for any termination or suspension of your access to the Platform.

8.3 Consequences of Termination Upon termination of your relationship with Poly ZKP, any licenses granted to you by Poly ZKP will be revoked, and you must cease using all materials and resources provided by us. Termination will not affect any rights, obligations, or liabilities that accrued before the termination date.