Zero Knowledge Technology as a future of Banking and Verifiable Autonomous Financial Protocols

Author: Sergey Kozlov, PhD
Co-authors: Oleksandr Kurbatov, Bogdan Gryekhovodov

Banking as we know it today in the classical sense is about procedures, control and risk management. For the past 10-20 years there was a huge shift in banking from business to compliance and control in the two layer banking system where the central bank supervises layer of commercial banks.

As a market response to this compliance avalanche and tightening control from central banks and governments we saw the rise of FinTech industry and crypto as a new technology which opposes control by the means of decentralisation. DeFi or Decentralised Finance is the very last tech stack built on blockchains which challenges the traditional highly regulated approach with decentralisation, trustless environment and immutability to any possible fraud or market manipulation.

But DeFi and blockchains today have serious technical limitations in throughput and computing capabilities in comparison to traditional banking centralised systems. That is why not everything we have now in CeFi (Centralised Finance) is possible to bring to DeFi but definitely, full Turing complete blockchain virtual machines are the future of financial accounting systems. We may say that DeFi appeared in 2018-2019 since the first Automated Market Maker introduction and the whole industry is just 4-5 years old. It had a good start with explosive growth and 2020 DeFi Summer but still all protocols are just primitives due to its youth with very limited functionality and number of users tens of thousands at best but not millions or tens of millions which we have now in traditional banking.

That is why we need some roadmap and clear path on how to overcome current blockchain limitations in cost, speed of transactions and its quite limited functional capabilities preserving trustlessness and immutability. How we can have control and compliance, privacy and scalability for tens of millions daily users with significantly less expenses than our traditional banking system now worth.

The answer to these questions is Zero Knowledge Technology (ZK). In general terms this technology is a way of proving the validity of a statement without revealing the statement itself. 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.

In what way can we connect this trivial ZK Tech definition to our complex banking problem? Let's have a simple uncollateralized consumer loan example. Traditional bank after receiving a consumer loan application from a customer goes through a predetermined algorithm of checks and calculations. First of all bank requests customer credit history from credit bureau, checks it for absence of overdue loans, than checks the validity of customer ID, calculates amount of loan according to customer income and existing loans, calculates overall customer credit rating by the formula from customer data and if the rating is higher than certain threshold approves the consumer loan.

This is a fully centralised process which is now in most of the banks close to 100% automated, especially if we talk about online loan applications. If a bank regulator or internal bank audit wants to check the process it is possible via access to archives and computer logs of what was done and why.

In a new world of self regulated **Verifiable Autonomous Financial Protocol (VAFP)** we might imagine the same consumer loan process look like this:

1) The off chain process
    - Customer sends a request for a loan to VAFP via decentralised front end hosted on IPFS or other decentralised storage
    - This application should be signed by the customer's digital signature and might not contain the private customer data (Name, Surname, Date of Birth, etc.)
    - With application customer provides ZK proof that he/she does have positive credit history higher than a certain required by algorithm level
    - Customer provides ZK proofs that he/she has a certain required citizenship and other required by credit scoring credentials (lives in a certain city, does not have criminal record, etc.)
    - VAFP gets all required for credit scoring information in the form of ZK proofs and does not know the customer name or even living address (if it is not necessary)
    - If the credit scoring algorithm given customer data gives a positive result VAFP generates Credit Process ZK Proof confirmation
2) The Credit Process Zero Knowledge Proof generation
    - Special ZK circuit is used to generate Credit Process ZK Proof which confirms to any interested party that all credit process was fulfilled according to procedure without revealing to this third party of a specific details
3) On chain loan disbursement
    - VAFP sends transaction to blockchain to disburse a loan to specified by customer address with Credit Process ZK Proof
    - On chain smart contract verifies Credit Process ZK Proof and if the verification result is TRUE sends a loan to the customer address

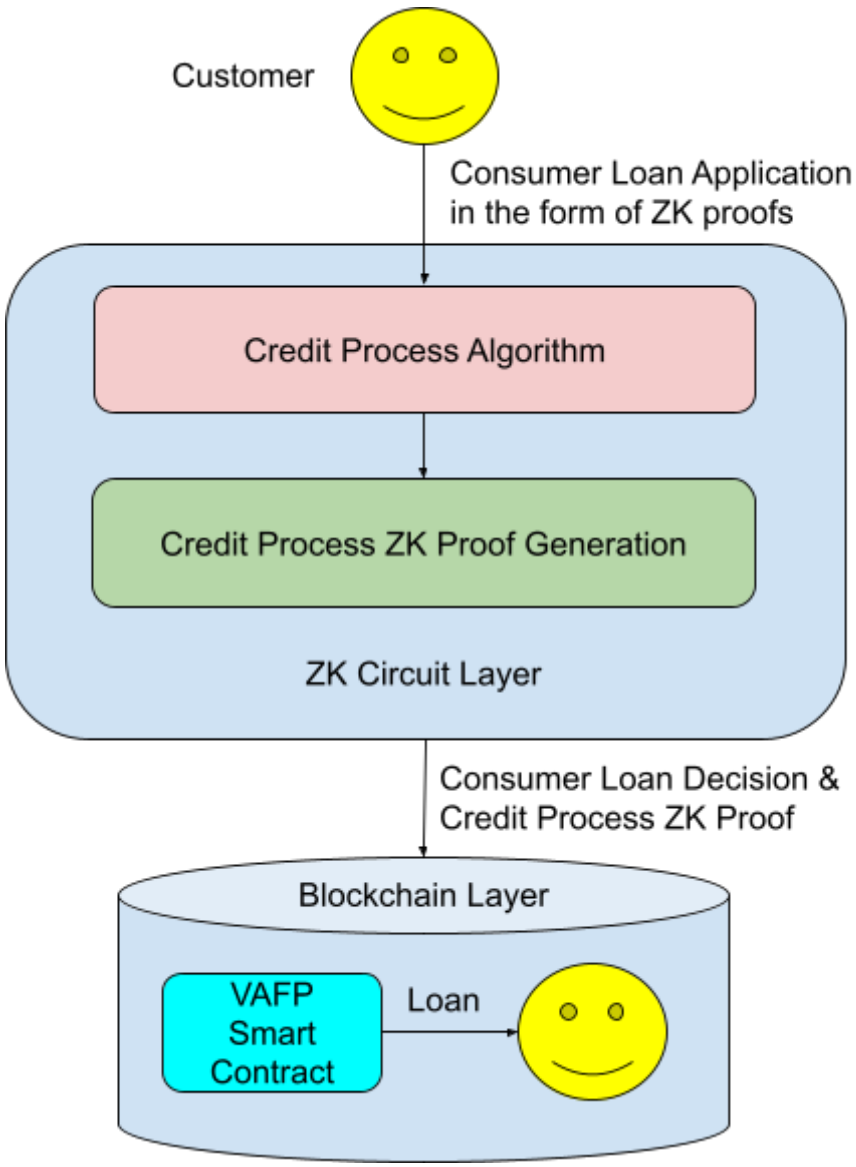
Let's compare these two processes. First in VAFP process we request only needed for the loan process information in the form of ZK proofs, we do not request customer for unnecessary and excessive information for which traditional banks are quite often request their customers. VAFP does not request excessive private customer data so it does not have it preserving customer privacy. To understand the difference let's assume we want to check if a customer is on the sanctions list. Traditional way is to request customer name, surname

and check it for match on sanction list, ZK way is to get from customer directly ZK proof that the customer is not on sanctions list. The ZK way is better because we get the answer we want without revealing any additional private information from the customer.

Second by generation Credit Process ZK proof VAFP implements self audit before the loan is disbursed to the customer and not after it. In traditional banks only post mortem audit is possible. In VAFP case if the credit process is breached the ZK proof will not be generated and loan will not be disbursed.

The third advantage is that all required data for analysis is obtained directly from the customer in the form of ZK proofs. VAFP does not interact directly with credit bureau or any government agency. In traditional banks on the contrary all data provided by the customer is verified by some third party.

Generalised two layer VAFP architecture will look like this.



In our proposed architecture we also have two layers of ZK proofs usage. First when we get application data in the form of ZK proofs from customers. Second when we confirm credit process validity and generate Credit Process ZK Proof. Of course a customer on his/her own can not generate ZK proof from personal data. For this to happen we need some trusted ID Issuer capable of working with ZK proof. Before a customer can make any loan application and generate ZK proof concerning his/her personal data, the customer should get a Claim (ID) from ID Issuer. So this is a matter of building the whole ecosystem grounded on Zero Knowledge Technology where government agencies should be able to generate ZK Claims for its citizens. If this purpose is achieved and the customer shares only ZK proofs required for loan application approval without revealing customer private data we can add additional security level to the system letting any independent node to verify the whole process of making a decision and further loan disbursement. Independent nodes could do it for a rewards and be a part of VAFP internal consensus.

Nevertheless it is possible to simplify VAFP architecture and have only a second layer of Credit Process ZK Proof while receiving loan application in a traditional way with customer query and further centralised requests from VAFP to credit bureau and other government agencies and centralised databases. In this case we make sure by ZK proof that the credit process was conducted according to procedure.

Any existing banking product that has a comprehensive algorithm and procedure could be converted to proposed VAFP two layer ZK architecture making it more private for the end customer and upfront completely verifiable on chain.

It is hard to imagine that banking algorithms and procedures will not use Artificial Intelligence or Machine Learning. According to the article in the sources “Checks and balances: Machine Learning and zero-knowledge proofs” it is possible to use ZK proofs for authenticity checking of AI and Machine Learning models in use.

Finalising our solution to banking of the future problem we give definition to **Verifiable Autonomous Financial Protocol** which is the protocol that uses blockchain as its accounting system and uses Zero Knowledge Proofs for on chain validation of any off chain calculations, algorithms and/or procedures preserving customer privacy and aimed at providing financial services to customers autonomously.

Sources:

Checks and balances: Machine learning and zero-knowledge proofs
https://a16zcrypto.com/posts/article/checks-and-balances-machine-learning-and-zero-knowledge-proofs/