White Paper

Confidential Computing
Intel® Software Guard Extensions (Intel® SGX)

Securing open banking with blockchain and Intel® SGX technology

With SilentData, Applied Blockchain uses confidential computing technology inside Intel® SGX to help banking data stay private during computation.

Contributors

Adi Ben-Ari
Founder & CEO, Applied Blockchain

Mark Green
Industry Technology Specialist, Intel UK

Ian Butcher
UK Energy & Utilities Account Manager, Intel UK

Paul O'Neill
Director, Strategic Business Development, Intel UK

Table of Contents

Executive summary

The open banking initiative "connects banks, third-parties and technical providers – enabling them to simply and securely exchange data to their customers' benefit."[1] These benefits include improved choice for customers, new payment services, as well as more convenient ways to manage their finances online. A core use of the technology is providing digital proof for a future transaction. This can range from proof of funds to proof that debt is being serviced.

As useful as all this can be, once access has been granted, what happens to shared banking data can pose a risk to privacy. Information can move out of customer control and there's always the potential for private information to be leaked.

We live in an age when cyberattacks and data breaches are becoming more frequent and sophisticated. Any vulnerabilities in third-party open banking apps or weak/repeated customer passwords can result in fraud and identity theft. However, technologies like SilentData from Applied Blockchain can make open banking systems even safer.

Applied Blockchain has created its Confidential Computing platform, SilentData, to address these security issues. It uses Intel® Software Guard Extensions (Intel® SGX) to help provide secure and private access to proof of properties of financial data, using trusted certificates rather than sharing the data itself. Utilising open banking while protecting privacy, SilentData offers trust and data privacy without sacrificing connectivity and flexibility.

Privacy and open banking

Open banking is a relatively new banking practice that connects banks, third parties and technical providers, so that they can simply and securely exchange data. The idea is that customers, both private and business, can select who can access their data, which can then be used for a variety of purposes. For example, access to an account can be used for proof of funds or the ability to service a loan.

In principle, open banking should make life easier, sparking a raft of innovative new solutions, products and services. It should also make many financial operations faster to execute and help to reduce fraud. Yet, open banking can reveal banking data and one potential area of concern is the level of access that third parties may have to that data.

The stats behind open banking

6 billion

The volume of open banking API calls increased from 66.8 million during 2018 to nearly 6 billion in 2020.

2.5 million

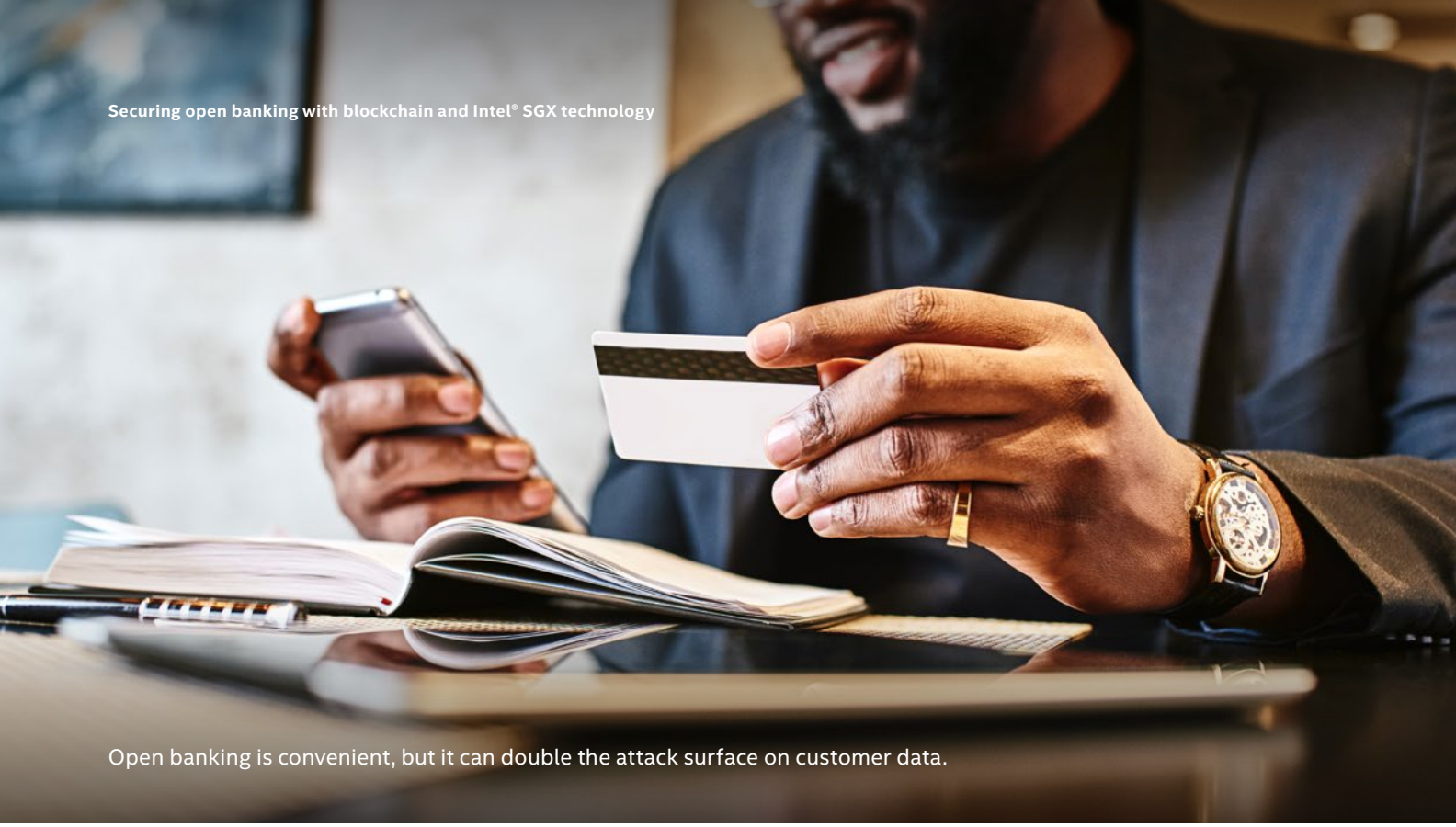
More than 2.5 million UK consumers and businesses now use open banking-enabled products regularly.

300

The number of third party providers that have joined the open banking ecosystem in the UK.

90

The number of days that third parties are able to store, process and retrieve open banking data.



Open banking is convenient, but it can double the attack surface on customer data.

As Adi Ben-Ari, the founder and CEO of Applied Blockchain, explains. “In the UK and Europe, the regulator introduced regulation[2] to instruct the banks to expose APIs to bank accounts of individuals and businesses when requested.” Applied Blockchain’s technology expertise lies in distributed ledgers, advanced cryptography and confidential computing. Its work to date encompasses solutions ranging from enterprise blockchain and confidential computing to Non Fungible Tokens (NFT) and decentralised finance (DeFi).

As Adi Ben-Ari sees it, there’s a potential problem with open banking. “Individuals and businesses can be asked whether they're willing to give people access to their accounts. But when they do, it's generally an all or nothing approach, giving access to all of their banking data.”

He is keen to point out that access to a bank’s API is secure and permission must be given. But open banking can allow full access to accounts for up to 90 days[3]. Furthermore, data processing takes place outside of the bank. So, by opening up their APIs, potentially banks have also opened up a greater attack surface to cyber criminals.

“If I want to access a service, and that service needs to see my bank account,” says Ben-Ari, “then I'm giving it access to my transactions. That basically means that this third party can see transactional data from my bank account.

"Once access is granted to a third party, that third party can continue to access the data on an ongoing basis until permission is revoked. So, I’ve just doubled the attack surface [on my data] and that data is being stored somewhere where I no longer have direct technological control.”

For individuals, the risks are personal, with financial leaks able to destroy relationships and reputations, even careers. In a wider context, having financial data stolen and leaked can lead to severe repercussions for companies. “If, for example, my company bank account was exposed,” says Adi Ben-Ari, “all the employees would see what the other employees are being paid. All of my customers would see what we’re charging the other customers. We’d be completely undermined, because everyone will have leverage against us with that information.”

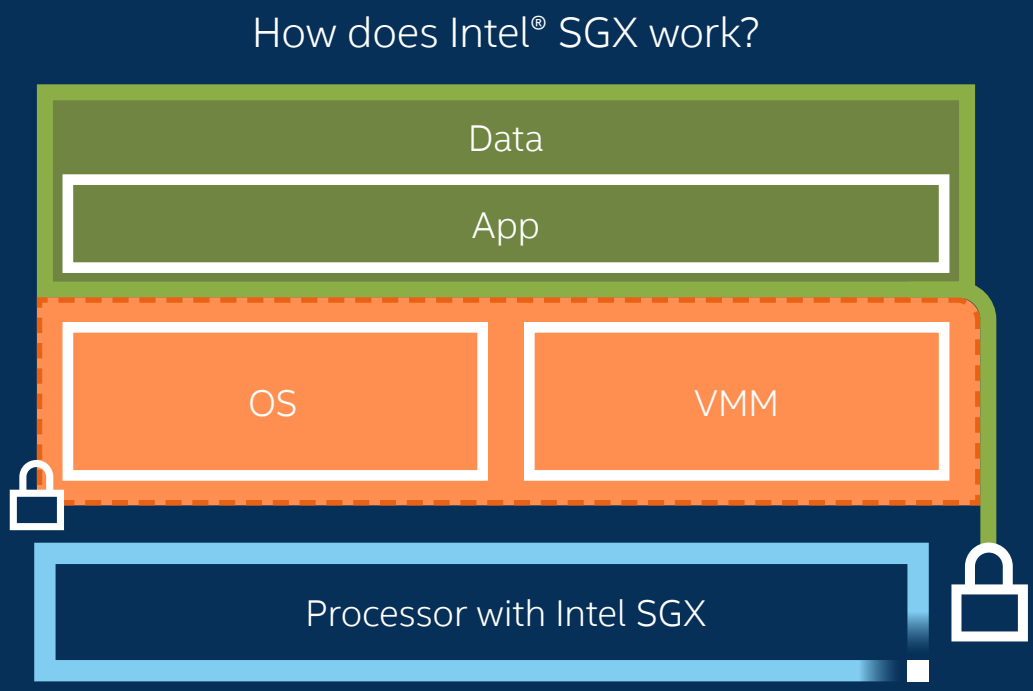
Privatising transactions with blockchain

It’s clear that we need both secure access to data and a better way of protecting open banking information. Applied Blockchain first looked at doing this as a way of protecting data on the blockchain.

With a blockchain, the trust ring is far larger, making the issues of altering or undermining data far harder. As Adi Ben-Ari explains: “The larger the group, the broader the group, the harder it is to change the historical data. With blockchains, you get that out of the box. In most of them, you get well-distributed infrastructure that would be very costly or very hard to undermine.”

But while blockchains provide extensive security by locking data histories, they lack the same degree of security for data privacy. In fact, any data shared on a blockchain is usually shared with the network of validating parties, multiplying the attack surface.

One example where Confidential Computing can be used to enable safer blockchain transactions is in the case of



Intel® SGX technology enables the aggregation of senstive data in secure enclaves.

high value online (e.g. NFT) sales. Here, payment uses 'real' fiat currencies, so there's often a need for 'proof' of funds before a bid can be accepted or a sale can take place. "On the blockchain," says Ben-Ari, "you don't want to start putting sensitive bank account data on there. But you do want to be able to prove key credentials to other actors on that blockchain. You might want to prove that someone has a bank account, for example, and that they have fiat funds available to proceed with a sale."

The SilentData approach with Intel® SGX

To provide this proof, Applied Blockchain has developed a platform called SilentData. It's designed to offer any financial proof required, furnished by open banking. Yet it's also able to restrict how that data is accessed and shrouds actual transactions behind a privacy curtain. "We think that the future of protecting data is being able to process it where it resides and avoid moving it at all," says Ben-Ari. "That way the underlying data is never shared, and the risk of data theft is greatly reduced."

SilentData works on the principle that you can provide the underlying proof while securely restricting access to data. This keeps real financial transactions hidden from all third parties. At its heart, SilentData must still access financial transactions through open banking APIs. For real trust, there needs to be proof that this data isn't being misused, stored outside the bank or shared publicly. This is where Intel® Software Guard Extensions (Intel® SGX) plays a crucial role.[3]

Intel SGX technology is incorporated into 3rd Gen Intel® Xeon® Scalable Processors, enabling applications to be partitioned into processor-hardened 'enclaves'[4]. These enhance the protection of selected applications or data from disclosure or modification. In SilentData's case, the confidential enclaves ensure that open banking data is never revealed or permanently stored. "We extract encrypted data from the bank into an Intel SGX enclave. Encryption/decryption of that data happens inside that enclave, which means that we (the data processor) never get to see it," explains Ben-Ari.

While Intel SGX helps to protect selected code and data from modification using these hardened enclaves[4], there's still an issue of trust to address. Technically, outside of this private processing, a malicious operator could still write code that spits out private data, bypassing the point of the enclave. It's why the second component to Intel SGX is just as important as the technical implementation: attestation

Attestation Services for Intel® SGX

Intel's attestation capabilities check code and issue certificates for applications that meet the privacy requirements. It provides proof from a trusted and respected source of end-to-end privacy. Remote attestation gives the relying party increased confidence that the software is running inside an Intel SGX enclave and on a fully updated system at the latest security level. Attestation results, meanwhile, provide the identity of the software being

Beyond Banking: SilentData Everywhere

SilentData has already been showcased by the UK regulator in the FCA Digital Sandbox[5], and has won industry awards including an Open Banking Expo award. Although SilentData has initially been designed for adding privacy to open banking transactions, it can go beyond this. As we've discovered, one of the benefits of SilentData and its Intel SGX technology is that no changes need to be made at the data source. Common APIs can be used to access the information more securely. This opens up SilentData to working with any type of data.

"We started with bank account data," explains Ben-Ari. "But we can join different data sources as well, all inside the privacy-preserving environment powered by Intel SGX. So, for example, if you're querying a company, you could query that company's bank account or other systems that hold data about that company. And you could reconcile it in the Intel SGX environment without having access to any of that data. That's something that we're already doing on SilentData. So that goes beyond the bank."

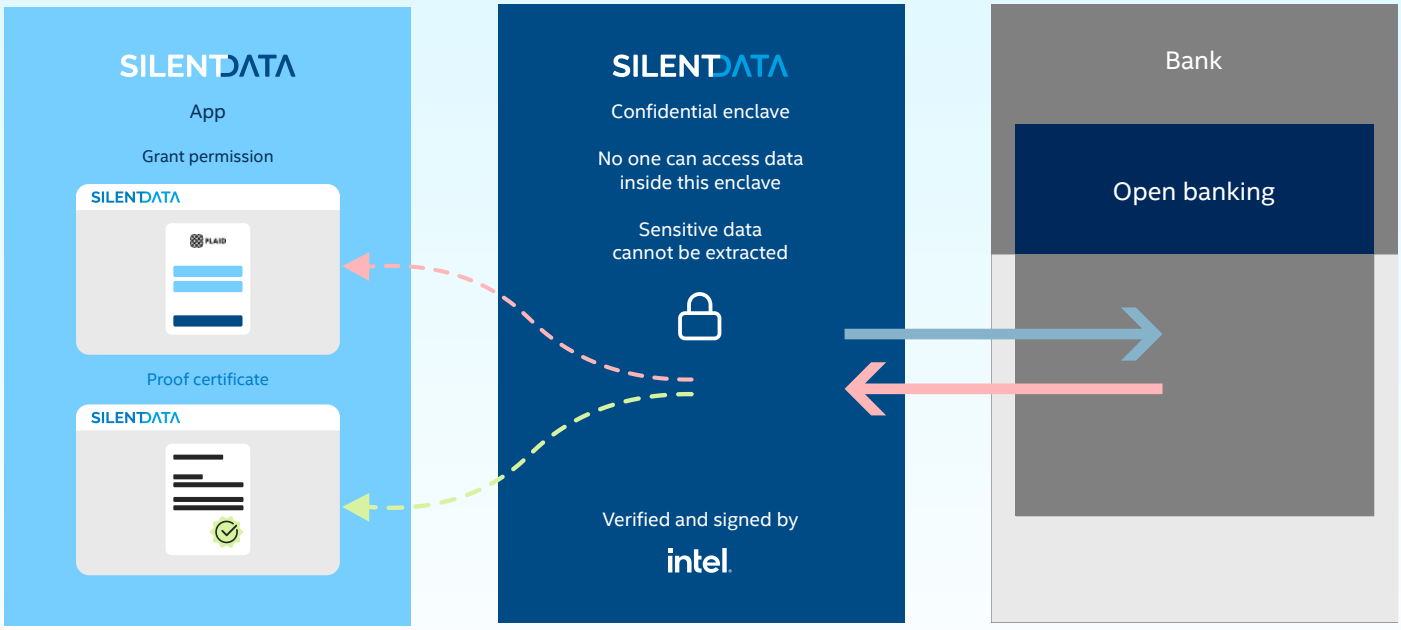
An increase in blockchain use should also see a rise in demand for SilentData, as it is able to provide digital proof in a privacy-preserving environment. One of the big growth areas is blockchain and confidential computing for energy and carbon trading. Applied Blockchain has already built a downstream exchange with Shell[6].

While energy trading exchanges are centralised today, liquidity is limited to participants of that market, and illiquid assets are typically traded directly with counterparts. These illiquid markets are hard to price, so third parties aggregate trade and publish prices. But they need to be trusted with the trading data of each party.

With blockchain, assets can be traded and processed independently of any particular exchange, increasing liquidity, while the tokenization of energy assets can include proof of provenance. The SilentData approach is well-suited to this market.

"SilentData could be used in order to conduct privacy-preserving credit assessments on trading counterparts," reveals Ben-Ari. "This may involve, for example, ongoing bank account assessments without anyone having direct access to the bank account data. In addition, SilentData could also be used to generate ESG or other privacy-preserving data proofs for tokenized energy and carbon assets. This is to prove credentials using data held by the other party that is too commercially sensitive to share."

Powered by Intel SGX, SilentData allows wider access to data while preserving privacy. It expands what's capable, adding trust and proof to trading systems, without ever having to reveal confidential information.



SilentData uses Intel® SGX to perform bank account checks in a hardware secure enclave for maximum data privacy.

attested and details of an unmeasured state (such as the execution mode). They can also give an assessment of possible software tampering.

“It's not just the privacy aspect that’s important,” says Adi Ben-Ari. “It's the fact that there's someone attesting to the integrity of what's going on inside the box. And that means we can process data in this environment and others can be assured of what's going to happen in that environment.

"After [data is processed], we can prove to them how it was done. They don't have to take our word for it. because Intel has provided assurance to the end user that the computed results cannot be manipulated within the SilentData platform, and that it retains technological control over the data and the results.”

Intel SGX enables security and privacy without complicated changes at a data source. Before Applied Blockchain moved to Intel SGX, it had looked at software-based encryption. Zero-knowledge proofs are another way of preserving data, but that technology is in its infancy. Given that open banking has a well-defined API, requiring banks to implement new technologies for each party that it interacts with is unfeasible. Intel SGX solves this by requiring no changes at either end.

“What we can do with Intel SGX is something that we've developed ourselves for SilentData,” says Ben-Ari. “We can direct the traffic that wasn't designed to interface into a privacy-preserving environment, without needing the bank to do anything. With a zero-knowledge proof solution, for example, the bank would have to generate these proofs.

Conclusion

Digital proof and access to data is a requirement of the modern world, and open banking provides a simple API that can enable that. However, any sharing of data with third parties can put that data at risk.

SilentData harnesses the power of Intel SGX technology, which helps to protect selected code and data from modification using a hardened enclave[4]. Here, data can be queried but not viewed, outputting secure proof that exposes no private data. Thanks to attestation, Intel SGX code is certified by Intel as being private, introducing that crucial layer of trust that secure applications need.

And, Intel SGX doesn’t require any fundamental changes to banks for SilentData to add privacy, keeping the fundamental open access point of open banking alive. It’s proving a concept that can be applied to other areas of finance too. For auctions, it could be used to request privacy-preserving proof of funds or it could perform real-time credit control for online trading platforms.

“Intel SGX is almost a get out of jail free card for solving these types of problems,” says Ben-Ari. “The best cryptography is often slow and it requires a lot of processing power. It’s also not standardised and the solutions become very complex and bespoke.

"But with Intel SGX we’ve got a highly scalable environment that we can use out of the box, with a minimal performance overhead. It gives us the ability to produce solutions that enable better data privacy for everyone.”

Learn More

You may find the following resources useful:

- Intel Software Guard Extensions
- Intel Attestation Services
- Silentdata.com
- Appliedblockchain.com

[1] https://www.openbanking.org.uk/
[2] https://www.openbanking.org.uk/regulatory/
[3] https://standards.openbanking.org.uk/customer-experience-guidelines/ais-core-journeys/90-days-reauthentication/latest/
[4] https://www.intel.co.uk/content/www/uk/en/architecture-and-technology/software-guard-extensions.html
[5] https://www.fca.org.uk/publication/corporate/digital-sandbox-joint-report.pdf
[6] https://www.shell.com/inside-energy/blockchain.html

Solution provided by

intel®

appliedblockchain