How Banks are Modernising to Approach Open Source

Rob Moffat
Senior Technical Architect at FINOS

FINOS

Professional Open Source

When you think of open source, do you see visions of coders hacking away in an attic late at night, headlines about vulnerabilities being discovered (like Log4Shell), or hordes of zealous individuals at conventions such as FOSDEM or KubeCon?

The fact is, open source software infiltrated the firm long ago—the Synopsis OSSRA report (2023) estimates that 96% of all codebases contain some open source software and that 76% of all code is open source. Projects like Linux and Kubernetes are now key components in most firms' cloud strategies.

It is perhaps surprising to learn that a lot of open source software development is also now happening within the enterprise. Corporations are rolling up their sleeves and assigning staff to work on these projects, freely donating their time and resources to further the "common good" of open source projects that they deem to be "too important to fail".

Big Players

Datamation's 2023 report gives some idea of the main movers and shakers in professional open source: Amazon, Apache, IBM, Google, Intel, Microsoft, RedHat, Meta, Oracle, and so on. These are the big tech names you would expect to see here.

Google is of particular note; their strategic approach to open source is outstanding. When faced with a competitor they want to challenge, their strategy is "let's build an open source alternative to that". This is a strategy called "Commoditizing Your Complement", attributed to Joel Spolksy back in 2002. When considering how to compete against Microsoft's Internet Explorer, Google started Chromium (an open source browser). Faced with Apple's iPhone, Google started Android, and when it wished to compete against Amazon's AWS, which had a considerable head-start, Google open-sourced Kubernetes.

Financial Services

At the time of writing (early 2024), Big Tech is at its biggest ever. The valuations of the top firms are staggering—and increasing. However, the financial services industry is no small fry either. According to Statista, financial services contributed just under 50% of the total net income generated by global financial services, fintech, and Big Tech in 2018.

Financial services companies and Big Tech—as well as many others—are growing increasingly similar all the time; they are becoming software companies. In the words of Marc Andreesen, *Software is eating the world*. Netflix is a software company that happens to be in the business of showing TV and movies. Spotify is a software company that happens to be in the business of playing music, and financial services firms are software companies that happen to be in the business of money.

Financial services firms have plenty of software know-how: consider the software you interact with every day, such as Internet banking, ATMs, card payments and so on. There's also a lot going on behind the scenes—settlements, balance sheets, electronic trading, risk management and know-your-customer systems. Because of this, financial services firms are as reliant on and invested in open source as anyone else.

Strangely, financial services firms don't appear in the list of open source "Big Players" we looked at earlier. Where are they?

Three Problems

Financial Services firms are the "Hotel California" of open source: code goes in, but (at least until recently) nothing comes back out. Why is this? Here are three main reasons:

1. Culture

The first and most obvious thing that blocks open source contributions is culture. Banks are famously secretive. The more secretive your bank is, the better! Internally, there is a culture of caution—information is provided on a need-to-know basis. Staff are taught to question why someone might be calling and asking for the name of a manager. Access control systems abound for controlling data resources or processes. This is not an accident; these systems have grown in response to the risks faced in the financial services environment. However, this is in stark contrast to the culture of open source.

2. Regulations

Many financial services firms are regulated. Market forces and competition can erode systems of trust, so it is up to governments and regulators to set and enforce rules to make sure our financial systems are stable.

For example, regulated firms are required to keep detailed logs of messages to clients. In 2022 the SEC fined several major firms for un-monitored communications using WhatsApp, to the tune of $1.1bn. These are important regulations to ensure the fairness of markets and avoid insider dealing. The size of the fines underscores this.

Thus, a large part of the effort of running a financial services organisation goes into following regulations to avoid these kinds of fines. Whether they are related to anti-money laundering, counter-terrorism, security or the safety of personal information, avoidance is key.

In protecting bank IP and customers' personal information, it is clearly better to err on the side of caution, and in doing so, often open source is the casualty.

3. Rules

To meet regulations and control risks around confidential information and reputation, firms enact policies, procedures and rules. For example: it would be easy to accidentally or deliberately divulge confidential information in a Facebook post or a Google Doc. So, broadly, sites which could be involved in this are "firewalled" or blocked internally.

Likewise, the penalties for sharing confidential information (source code included) via email are strict.

From this perspective, a site like GitHub (commonly used for open source development) is just as likely a vector as Facebook, WhatsApp or Google Docs. Usually, these are locked down tightly.

In summary, there are lots of things standing in the way of open source participation in financial services. It's worth looking at what is lost as a result of this.

What Is Lost

It would be very easy at this point for financial services firms to throw in the towel and decide that there are too many barriers standing in the way of open source contribution. But it's worth reflecting on what is lost by doing this. Let's look at four of the most obvious problems:

1. Dependencies and Vulnerabilities

Financial Services firms are auditing their open source dependencies and discovering that sometimes, key projects are maintained by "that one guy in Nebraska" to quote the XKCD comic strip.

This is a driver for open source contribution, as staff can argue: "We have a dependency risk issue here. These are some of the threats that we have to figure out. We should be investing in open source and we should be adding maintainers to these projects to keep track of these things."

It makes sense for financial services firms to help maintain code and keep projects up-to-date. This way, the code is there for the future when they need it, rather than it getting abandoned by its maintainers. Abandoned code creates more work for firms since they then have the costs of migrating to new solutions.

2. Excessive Internal Forks

The alternative to the abandonment problem is *forking projects internally* and maintaining those. At first glance, this seems like a way to mitigate risk and keep control of your codebase—but then you have to maintain all the forks. Every time the upstream, open source version changes, you have to update the internal versions and you're in a massive maintenance hell.

Typically this happens when an engineer discovers a bug or missing feature in an open source project and can't supply the fix. They then fork internally. Worse still, this can happen multiple times within the same firm. Imagine having development staff spending their time maintaining multiple, different out-of-date versions of (say) the React project just because each developer discovered a different bug that needed fixing.

3. Strategically Compromised Positions

As discussed earlier, major companies like Google are using open source as a strategic lever. There is always a risk that another firm might build a vital open source piece of software that changes the finance industry. For example, what if a major bank introduced something along the same scale as Kubernetes, but for finance instead of cloud computing?

Any firm that doesn't have a way for its teams to engage with that open source project would be unable to influence its future. This would limit the value they could get from it, which could be strategically damaging. A firm that doesn't "do open source" can't help steer the ship—they're either stuck as a passenger or they're stuck watching the ship go by without them.

Another analogy which is helpful when thinking about open source as a strategy is to consider the Peloton in cycling: rather than every cyclist battling air resistance, they work together and slipstream each other. They are all competing with one another, but at the same time, they're working together. If a firm isn't engaged in an open source effort, they're battling the wind all by themselves. A single firm is unlikely to be able to commit the resources to compete with a "Peloton" of other firms in the industry.

Given that "software is eating the world" this is a strategically compromised position.

4. Talent

Consider the case where a firm builds a product on an open source project. As discussed before, if the project is critical enough to that product, the firm should appreciate the key dependency risk involved in the open source project.

One strategy they might adopt to mitigate that risk is to hire one of the project's maintainers to come and work for them. That way, they have the talent on hand should issues arise with the dependency.

There is a critical flaw in this plan: if the company isn't set up to allow open source, that new staff member won't be able to engage with the project they maintain! So, they're faced with a choice: either leave the firm or leave the open source project. Furthermore, if they choose the latter, this is also bad for the firm, since it *increases* the dependency risk on that open source project. The project now has one less maintainer!

A further argument in favour of open source in this area is that talented developers are attracted to open source. They want to work on quality projects that enhance their profile and open source is a great way to do this. Allowing open source contributions is an employment benefit.

FINOS

FINOS is the FinTech Open Source Foundation and part of the Linux Foundation. Its membership (around 80 entities at the time of writing) comprises various firms across the financial services industry and its suppliers. FINOS has Platinum, Gold and Silver members, all corresponding to the different membership fee levels and benefits. Many of the platinum and gold-level members are exactly the sort of heavily regulated firms I've described above: they are all-in on the potential value of open source software. They see the risks and issues posed above by not contributing to open source and want FINOS to help resolve them.

But that's not all: FINOS hosts many open source projects that financial services firms want to take advantage of. As well as trying to fix the issues described above, there are some huge prizes for the industry if it can collaborate on open source projects. Let's look at some:

1. Open RegTech

According to International Banker, financial institutions spend $270 billion per year on complying with regulations. When a regulatory agency imposes a new requirement, the firms all have to comply or face fines. Largely, the work building systems to meet new regulations is repeated in every firm.

The idea of firms collaborating on open source implementations of regulations represents a huge opportunity for cross-industry cost-saving.

2. Cloud Computing Standards

FINOS has two projects, Common Cloud Controls and Compliant Financial Infrastructure aimed at allowing financial services firms to get the most out of the cloud. Building a cloud platform that complies with worldwide financial regulations is a big ask, so why not collaborate with your peers to share the cost?

Additionally, "given enough eyeballs, all bugs are shallow" (to quote Linus Torvalds), the more cross-industry collaboration that occurs on these projects, the better the quality of them will be.

This is not just true for FINOS' cloud computing standards but for other standards such as FDC3 (financial desktop interoperability) and CDM (a financial services Common Domain Model).

3. Emerging Technologies

The technology landscape is not only changing extremely rapidly but the rate is not slowing down. With this in mind, organisational strategy needs to be constantly on the lookout for external technological disruption and innovation.

FINOS' Zenith project is all about looking at innovation and trying to map it back to the financial services industry. How does AI intersect with finance? Where is it best deployed? What about blockchain, augmented reality or quantum computing?

4. Open Source Best Practices

FINOS runs Open Source Readiness, which gets financial services' open source advocates together every couple of weeks. FINOS helps document the path to adoption and excellence in open source and provides a way for firms to share best practices and approaches. In 2024, FINOS are starting to look at best practices around open source AI and focus more closely on supply chain security measures.

Baby Steps

An attitude shift has to happen before change can pick up pace. Financial Services firms are heavily using standards such as FDC3 behind their firewalls. But to maximise their benefit and improvements to the standard, they need to contribute back.

While there's a long path ahead before most internal teams can make contributions and truly adopt open source, many firms are taking the first steps. For example:

1. Trial Projects

The organisation will grant a board-level agreement for a project. Teams can use open source on it and run a risk analysis. Instead of doing it entirely in-house or going to a third party and getting a proprietary solution, they try open source and see how that works and take it from there.

2. Tackling Policies and Regulations Head-On

This means working with all of the organisation's policies to understand them and try to chart a way through them to allow for open source. Often, it's hard for firms to even craft a policy around open source which doesn't either infringe on existing policy or overstep regulations. For this reason, FINOS has worked with its members to produce a sample policy (open sourced from one of its member banks) and annotations, explaining why the policy has been crafted the way it has.

3. Technology

FINOS projects such as GitProxy allow a compliant, DLP-aware workflow for pushing code to public repositories.

4. Training

FINOS has just released LFD137 - Open Source Contribution in Finance. A free Linux Foundation training course aimed at teaching developers in financial services firms the best practices for contributing to open source. This is starting to see acceptance within regulated firms.

5. Certification

FINOS (and the Linux Foundation) have just released FSOSD - Financial Services Certified Open Source Developer, a proctored, on-line certification allowing candidates to prove that they understand the risks associated with open source contribution and the best industry practices for mitigating them.

Conclusion

Every project is not going to become an open source project. This includes projects which help integrate internal systems, projects which contain the algorithmic "secret sauce" of the business and projects which might be vital but aren't going to be of interest to the open source community in general. These "in-house" projects will always exist.

There is now compelling evidence that in-house by default is being challenged, however. In the future, we should expect to see financial services choose between in-house and open source based on merit.

If you're working in financial services and are interested in understanding your firm's open source journey, why not get in touch with FINOS via their email help@finos.org. They would be happy to hear from you and put you in touch with like-minded individuals within your organisation.

Flagsmith

Get in Touch

Flagsmith is an open source feature flag software that lets developers release with confidence. We work with banks and financial institutions across the world to help them transition to modern feature management and software development, offering on-premise deployments, security features, and technical support to cover your needs. We also partner with OpenFeature to support open standards and prevent vendor lock-in.

"Our development speed and velocity have increased. Mainly, though, I just feel good about releases. I know when I ship something to production it's going to be safe and I won't have to do a thousand tests to make sure I don't miss something. When things are behind a feature flag, I know what is and isn't enabled in production and I have the visibility I need."

Vontobel

Globally active investment firm with Swiss roots

Flagsmith.com