PassBook whitepaper

TL;DR

- Enables you to safekeep your passwords locally, while still having convenient access to all your logins across your devices via lightstream technology.

- Lastpass and 1password stores all your eggs in on basket in the cloud. Even if they claim super encryption, history show that encryption often has backdoors.

The premise:

Instead of having illusions about standards being perfectly designed, software being bug free and systems being 100% secure one should accept that this is impossible to achieve in practice for today's complex systems. To mitigate this one should care more about resilience and robustness, i.e. staying safe and secure even if some parts break by layering security, not fully trusting anything and having plans if something breaks.

The solution:

Absolute separation of sensitive data. basically right now your probably using the same master password to access your entire password vault. Be it Keychain, 1password or lastpass. This is bad. As you will need to type in the same password for logging into goodread.com as your online bank. The former you care little about if it gets hacked. the later could ruin your life. The more you use the master password to access your vault, the bigger the attack surface gets. Sure, 1password and lastpass have all these checks and bounds to keep things secure. But the keyword is "all" here. The more complexity you add to a system the bigger the attack surface gets. And getting some sort of attack workflow for lastpass and 1password is something a lot of people is working on right now. If they find even 1 flaw, the world could literally end as we know it. Information leak would be devastating and spreading, increasing in speed as the network effect increases because the hackers would get into more and more services that yields more and more attack vectors. Basically the world would need to shut down the internet if this was to happened. The solution is obvious. Low tech Absolute AirGapping lockers.