Sam Korman
Honors Capstone Report
Lookout Finance
Advisor: Xinyu Wang

Introduction

Lookout Finance is a personal finance application designed to help people manage their finances in a more responsible manner. We started Lookout 2 years ago in the summer of 2020, and the product has changed tremendously over time. The whole premise of Lookout is that we want users to ask themselves, and hopefully answer the question, “How am I doing with my money?”. Studies show that money is the number one cause of stress in America. Additionally, 2 out of 3 people do not track their spending. Our goal is to help more people track their spending, which has been shown to help people cut down on their spending in general. Lookout will be able to provide personalized recommendations to people for how to save their money, and will provide people with greater visibility into their finances in general. One critical aspect of Lookout is that we put a large emphasis on privacy and security. Other financial platforms such as Mint and Personal Capital are either very expensive or sell user data, which we feel strongly against. Lookout is designed to be as secure as possible and will never sell user data.

As a college student, I was baffled by how little I knew about personal finance before I started working on Lookout. Throughout this process, I have learned about credit cards, loans, and how to manage my own money. One of my personal goals is to use Lookout to spread this knowledge to as many people as possible, because people in society are often exploited for their lack of financial knowledge. Lookout is not designed for people who have enough money to pay for a full-fledged financial advisor or a very expensive tool (although it might still be helpful to them as well). Instead, it is geared towards people who may not have much experience managing their finances and who might not be able to pay for expensive tools to help them.

The idea behind Lookout is that users will connect their financial institutions - anything from bank accounts to crypto accounts - and will be able to see their finances all together in one place. They will be able to track their spending, savings, income, and expenses, and see how they are trending over time. Our proprietary aggregation technology allows connections with over 48,000 different financial institutions. Additionally, we have built out the functionality for users to add self-custodian cryptocurrency wallets - in case they want to track their crypto assets along with their net worth.

The team currently consists of three members. I am the CTO of the company, and I cofounded Lookout with our CEO, John Mackin. The third member of the team is Ty Foster, our principle designer. Together, we launched a fully functioning beta version of Lookout - which was previously called MoneyPath. We recently relaunched our website under the name of Lookout, with a complete rebranding, and are in the process of onboarding beta users to help us out with testing and feedback. We currently have a waitlist of approximately 100 users and are trying to iron out the kinks in our onboarding process before we start any marketing. Our goal is to get users on the platform to get a sense of whether or not people will use it and enjoy it. If this is the case, we will try to scale up to more users.

How We Started, and Where we are Now

When we started, we made the classic startup mistake of building a fully functioning product without doing full user testing beforehand. We launched Lookout (under the name MoneyPath) for the first time in the summer of 2021. This is before we added Ty to the team, and this is

evident in the UI of the website. Below is a photo of the dashboard of MoneyPath when it was launched.

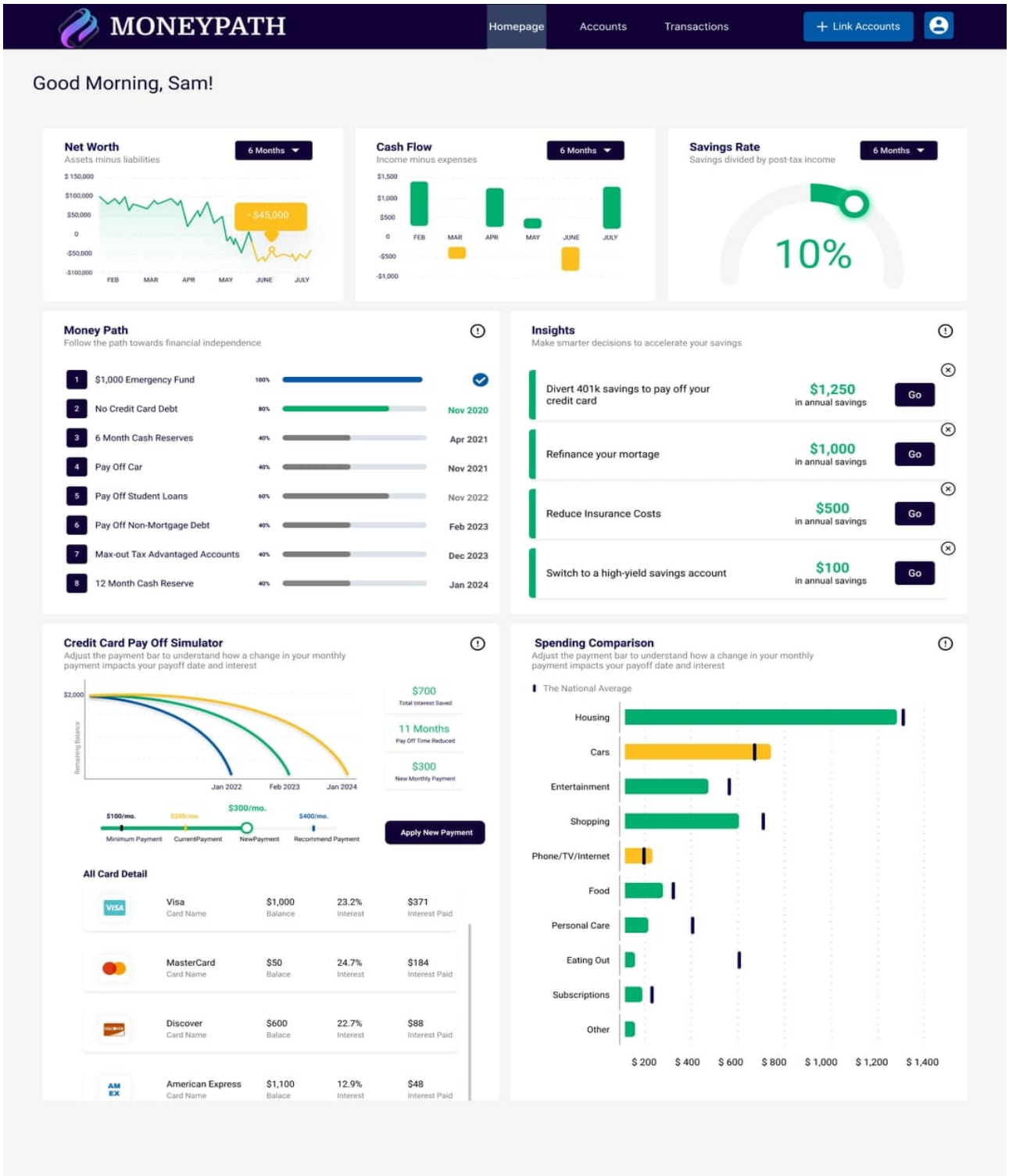

Figure 1: Dashboard for MoneyPath, Launched in 2021

We received a lot of feedback on this product and realized that the connections were not great, there were too many features, and some of the features on the website came across as advertisements. As shown above, MoneyPath had a ton of features built around the data that we received from institutions. After doing a lot of testing, we realized that the data quality we were receiving from our data provider was not sufficient enough to accurately power the features we were planning on providing.

One of the major points of feedback was on the “Insights” section shown above. This section was designed to analyze someone’s finances and determine ways they can save money. It would then recommend different websites they could visit in order to take action on this recommendation. For example, if we detected that someone’s mortgage rates were high, we would send them to Credible to refinance their mortgage. When we conducted user testing, many people expressed distaste in this flow. They thought that we were trying to advertise to them, instead of actually recommending products that we thought were useful.

Overall, the feedback that we received was that many of the features we provided were not useful, and instead people just wanted to know if they were on the right track with their finances. This was the motivating sentiment behind our redesign of the site. We decided to pair down the functionality of the site and really focus on the data quality, the institution connection quality, and the main metrics that people want to see - such as income, expenses, net worth, assets, and debts. With all this in mind, we completed a redesign of the website and launched it in March of 2022. While we haven’t completed everything on our MVP backlog, we decided not to make the same mistake as earlier, and do user testing before building out all the functionality. Below are a couple of screens that show the new and improved version of Lookout.

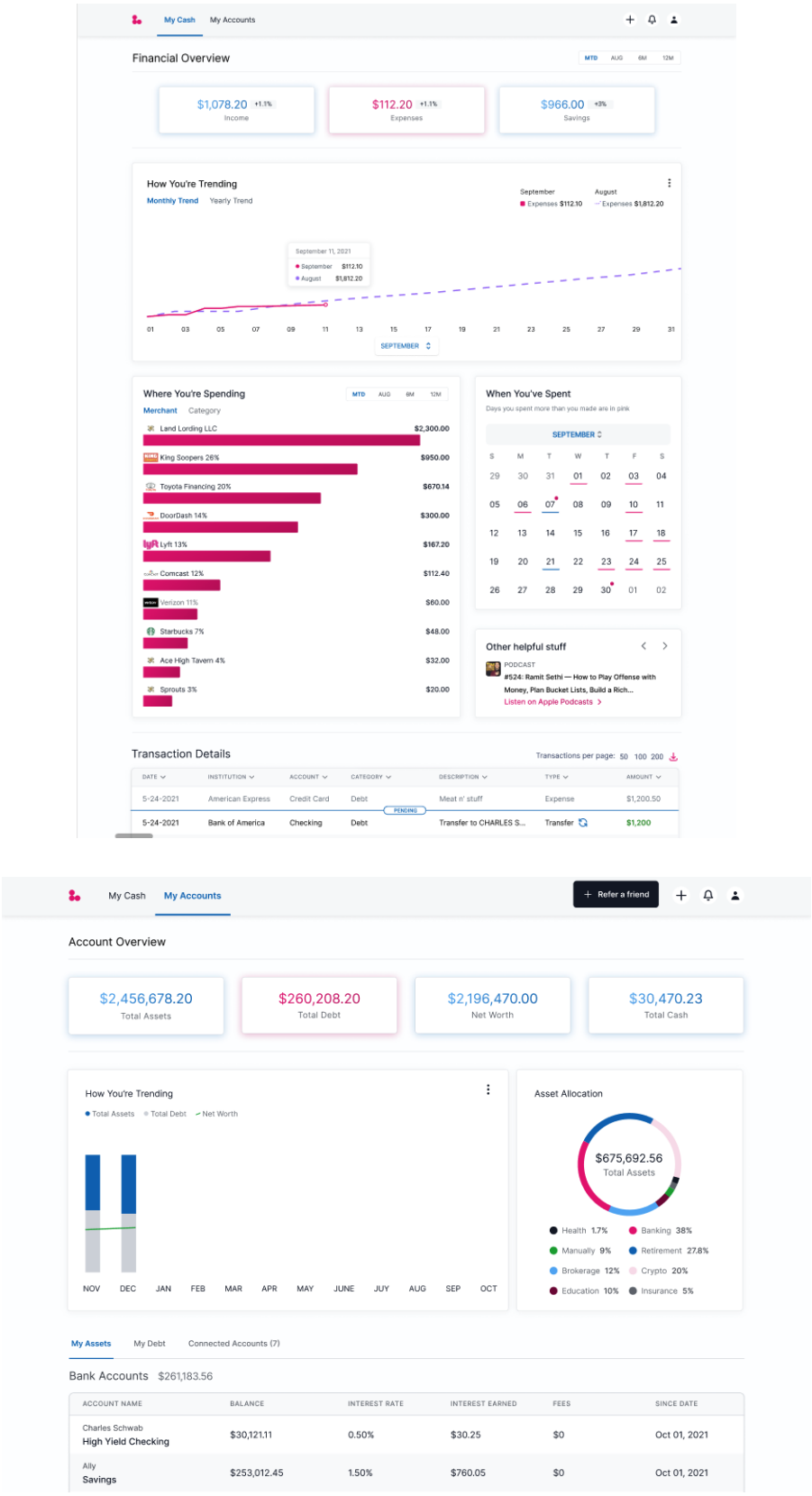

Figure 2: My Cash and My Accounts Page for Lookout

In this new version, we did a complete rebranding of the site to make it look cleaner, more polished, and simpler. Another major change that we made was switching our data provider, which resulted in better connections to institutions and higher data quality.

Technical Details

Determining the technical stack was the most important technical decision of the whole project. While many different stacks would have worked, I chose the stack based on my personal experience and based on recommendations from professors at the University of Michigan. The backend uses Python along with the Flask library for running the web server. I chose this configuration mostly based on my previous experience with Python and online research that endorsed Flask as a scalable and robust web server solution. This decision was reinforced after I took EECS 485 (web systems), which coincidentally uses the same framework for the backend. The database server is a PostgreSQL database, which is one of the most scalable and efficient relational database systems. PostgreSQL is also open-source, which means it is free to use. The backend uses SQLAlchemy and Alembic, two Python libraries that interface with the database. SQLAlchemy handles database management and queries, and Alembic handles database migrations (migrations happen when the schema of the database changes). The frontend of the application is built on React, and the styling is almost entirely done using css, without any libraries. The routing is done through React as well. React provides an easy to use framework which allows for modular creation of components, and is also recommended for use in EECS 485.

One of the largest questions that I have received about Lookout is the way it manages security. This is mostly broken down into two parts: website security and bank security. I will address the web security first.

Web Security

Lookout has many features to protect against various web attacks. Many of the libraries chosen in the technical stack have built in features to aid with security. For example, SQLAlchemy handles query serialization in order to protect against SQL injection attacks. Additionally, Flask does not allow any cross origin requests (CORS), which protects the backend API against cross site request forgery. Flask also encrypts all cookies, which are used for user sessions. Additionally, React has built in safeguards for input fields to protect against cross site scripting. Lookout uses NGinx for web routing, which handles TLS encryption over HTTPS. All HTTP requests are transferred to HTTPS requests so that the communication channel is encrypted. HTTPS uses a combination of asymmetric (RSA) and symmetric encryption.

In terms of encryption, we try to encrypt as much information as possible. Passwords are hashed and salted using the Werkzeug Python security library, using the SHA-256 hash. This is a widely used hashing algorithm and is considered an industry best practice. Additionally, all other personal information, including financial data that we store, is encrypted using AES-256 encryption. This is done through the PyCryptodome Python library. It is vitally important to use libraries for encryption because they have been tested thoroughly against adversaries, and it is very easy to make a mistake in implementation.

Lookout is deployed on AWS servers, which have many different security features built into them, including private key server access, IP whitelisting, and security groups. On the server that serves the web application, all secret keys are stored as environment variables, which

means that even if someone were to obtain access to the server, they would be unable to obtain the secret keys. There are separate keys for the cookie encryption, AES internal encryption, and for the database connection. The database runs on a separate AWS server and uses IP whitelisting to reject any connection attempts other than those originating from the application server. A secret key is also needed in order to access the database. This means that in order to access any data, someone would need to compromise the application server and also know the database secret key. In addition, all the information in the database is encrypted, so an attacker would also need to know the AES decryption key in order to make sense of any of the data.

Bank Security

Perhaps the most critical part of the entire platform is the ability to connect securely to users' financial institutions. For this, we largely use a third party data provider, MX, for the connection. We have an MX widget that we embed inside our website that allows users to search for and connect to their financial institutions. Below is an image that shows this widget.

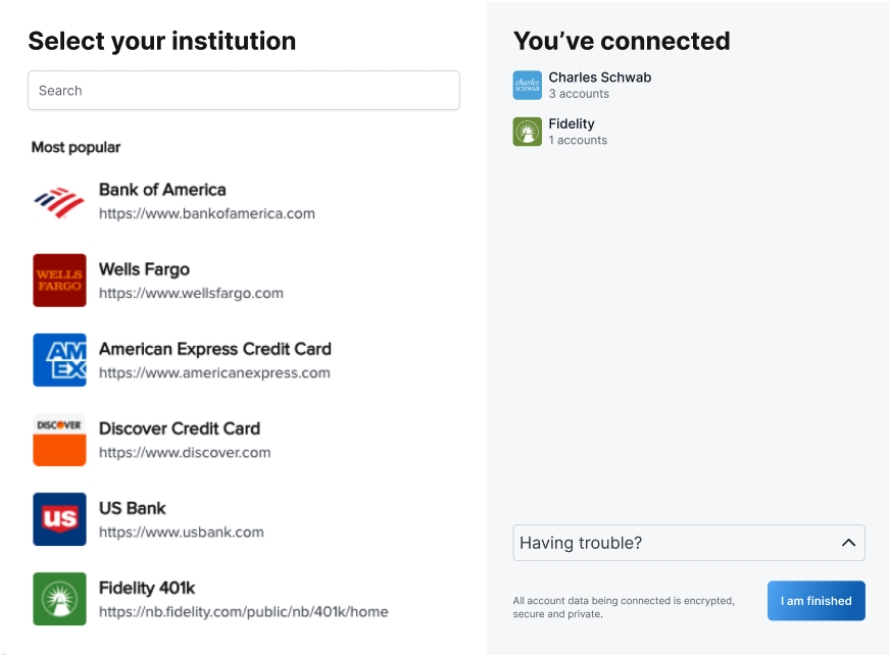

Figure 3: Institution Connection Modal

There are two paths that could happen once a user selects an institution. For the major financial institutions such as Chase, US Bank, and Bank of America, there is an OAuth flow. OAuth means that the user will sign in to the bank directly, and the bank will ask them what information they would like to share. Then, the bank will send the financial data directly to Lookout, so we never have to deal with bank credentials. This is ideal since we don't have to worry about safely storing what is likely the most sensitive information a person can have. We have a registered client ID and API key that are used to access the bank account information from the bank. The information is also protected by IP whitelisting, which is utilized by our application server.

The second path that could happen is a non-OAuth flow, where MX will aggregate the data for us. The users will sign into their bank accounts directly in the MX widget and MX will retrieve their bank data. This option is slightly less preferable because it is often not as durable, although it is still completely secure. We again never have access to any user's bank credentials.

The strength of these connections are a large reason why the new version of Lookout is much better than the old MoneyPath. Additionally, since much of the data comes directly from the bank itself, the data is typically of much higher quality. This is essential for doing the calculations required and providing the insights that are helpful.

Lessons Learned

Overall, this experience has been one of the more incredible learning experiences in my life. Not only have I learned technical skills, but I have also learned a tremendous amount about how businesses are run, how to communicate with different stakeholders, and how to communicate

internally. Aside from that, I've learned much more about my own personal finances and how I can help myself live more financially responsible.

One of the major aspects I've learned throughout this process is how important it is to spend time planning before implementing a solution. The first version of MoneyPath was a bit of a mess code-wise, which caused many unforeseen issues when trying to make changes to our platform. When I rebuilt it as Lookout, I spent much more time planning how the architecture was going to fit together and what design patterns I was going to use. Now, the codebase is much cleaner and easier to work on. Additionally, if we had put more planning and testing into the original version of MoneyPath, we might not have had to build out an entire product just to find out that we needed to change how we were approaching the problem.

Conclusion

Lookout was recently launched in beta version, although we are continuing to work on this project. Right now the goal is to see if people would be interested in using Lookout so that we can scale it to more people. Aside from our future plans, it has been an incredible experience overall and has helped me improve tremendously as a software engineer. If you are interested in Lookout, please feel free to reach out to me (skorman@umich.edu), or you can sign up! (https://lookout.finance).