INTERMEDIATE PLANNING DOCUMENT

Senior Design Project
Blockheads
Credentials and Identity Manager

Project

Our team, BlockHeads, is developing an android phone application called CredHub. The application allows the user to store important documents such as IDs and credentials for a subscription fee.

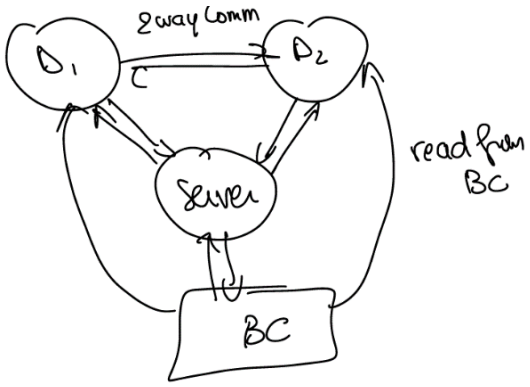
A description of your minimum viable project. What is it that you absolutely need and can deliver by April of 2024?

- Our minimum viable product:
  - Target verifying one or both a Wyoming driver's license/ID and a UW degree,
  - Login, 2FA, and recovery of passwords,
  - An android interface,
  - Smart contracts to interact with blockchain and blockchain to store IDs and credentials,
  - A server to interact with devices and the blockchain,
  - A database for temporary and system data mirrored between a device and the server, and
  - A procedure to verify with UW and Wyoming.

Detailed descriptions and diagrams of your system, sub-systems/components, and expected user interactions.

Our System and Subsystems

- These are our systems, potential languages to use, and primary and secondary team members responsible for that area.
  1. Android UI/UX, Java/Kotlin – Megan (Selma)
     - User profile, settings, preferences, and support.
  2. Security and Authentication, Java/Kotlin – Selma (Megan)
     - Document capturing and authentication.
     - Document sharing and permissions.
  3. Server, Python/C++ – Kellen (Megan)
     - API, security protocols, and data processing.
  4. Database, SQL – Tamara (Selma)
     - User data storage, and data retrieval.
  5. Blockchain and Smart Contracts, Solidity – Kellen (Tamara)



- Integration of Blockchain, data storage and integrity.

6. Validation (contacting organizations) – Tamara (Selma)
    - Integration of external organizations, verification, and tracking.

Expected User Interactions

- The user will enter username and password and use facial recognition built into android phones. First-time users will enroll in 2FA. In case a password is forgotten, the user will be able to reset their password via pin code sent via text that will have a set expiration date. A stretch goal would be a twelve-word recovery phrase.
- The user will begin the process of verification. They will enter information about a type of ID or credential and possibly upload images of that credential. The app will interface with the issuing organization to verify it.
- We will establish a process with each organization to verify on our app.
- The home screen will have a button for each ID or credential, and the user will use a pin code (the same one for all) to access these to ensure security.
- Each ID or credential will have an expiration date and prompt the user to confirm or renew, if needed.
- The user will give permission for IDs and credentials to be accessed and viewed.
- The user can show the identity on the screen of their phone, which will be locked so that an official or other person cannot access the phone without permission.
- We will ask the issuing organization to put a page on their website that verifies the legitimacy of our app, which we will link to on our app. And so, if a person viewing an ID or credential questions the validity of the app, they can click that button and see that it is legitimate.

A rough start of mapping out specific tasks and dependencies between tasks that need to be completed in order for you to implement the systems and subsystems you have listed in 2. You do not need to assign team members to those tasks yet, but you should be thinking about the constraints, dependencies, and requirements needed to complete a task.

- See our detailed description above, as well as the pitch document, status updates, and meeting notes (attached), to see specific tasks and functionality and who is tentatively responsible for each.
- We are researching our areas to come up with more specific approaches, and we are planning on beginning programming before the end of the semester and/or over winter break to get a head start.
- Constraints: We need make sure we don’t expand our project to far. We are constrained by the requirements of Android, App Store, AWS, Ethereum blockchain, a SQL database, and the verifying organizations.
- Dependencies: We are developing these as we are developing our approach.
- Requirements: We have outlined our minimum viable product and tentatively decided on approaches. Now we each will be investigating the requirements on our area.
- Tentative Timeline:

- January: Continue developing each of our portions, dividing work, and building the app.
- February: Continue development process as well as reach out to resources and mentors for assistance. Making changes according to the feedback provided. Begin work on interoperability of components.
- March: Finalize our project, bring it all together, and start vigorous testing.
- First two weeks of April: Bug fixes, finalize presentation, and put everything together.

ATTACHED:

- Pitch Document
- Status Update #1
- Meeting Notes
- Team Contract

PITCH DOCUMENT

Senior Design Project
Blockheads
Credentials and Identity Manager

1. Group information

   i. Title/Name of your project. This should be descriptive and not "My Senior Design project."

   CredHub: Protecting Your Credentials

   ii. All members of your group.

   Megan Steeves, Selma Samet, Kellen Mentock, and Tamara Linse

2. Develop Your Team "Brand" [name/tagline] & Bio (This will also be your Group Name.)

Blockheads
Tagline: You've Got Cred

BlockHeads is creating the next-gen identity and credentials manager CredHub. Our team includes programmers Selma Samet, Megan Steeves, Kellen Mentock, and Tamara Linse of the University of Wyoming.

Our project
CredHub: Protecting Your Credentials
Tagline: You've Got Cred

3. Project Summary

   i. Summary of the project

   CredHub is an identity and credentials management app that gives users full control over their personal data and credentials. It relies on either an API or physical confirmation to verify each ID or credential with the issuing organization. It uses blockchain smart contracts and data storage for the user to establish and maintain their credentials and to provide secure credentials to outside parties.

ii. What problem the project aims to solve or what niche it intends to fill. E.g., why would someone who to use your project.

The problem: We as a society are transitioning our lives to the digital world, but our IDs and credentials are still in paper form. CredHub aims to solve this problem.

Why would someone want to use CredHub:

- **Accessibility and convenience**
- **Security and privacy of sensitive data**
- **Organized personal information that is easy to track thanks to the blockchain technology**
- **Reduction in the amount of paperwork needed to get a task done**
- **One-stop shop for all verification needs and simplification of daily tasks, which saves time and energy**
- **Quicker processing**

iii. Major components used by the of the project and any resources you plan to use for the project.

AWS web server

4. What do you specifically plan to do. A very rough project planning and timeline. Remembering you only have until mid-April to complete this project.

January: Continue developing each of our portions, dividing work, and building the app.

February: Continue development process as well as reach out to resources and mentors for assistance. Making changes according to the feedback provided. Begin work on interoperability of components.

March: Finalize our project, bring it all together, and start vigorous testing.

First two weeks of April: Bug fixes, finalize presentation, and put everything together.

STATUS UPDATE #1

Senior Design Project
Blockheads
Credentials and Identity Manager

1. **Recap:**
   Over the past few weeks, we've dedicated time to conducting research on the core concepts we want to focus on for our website's functionality and features. Later, we gathered to discuss and develop these ideas and address any questions or challenges that arose during our pitch day.

   During our meeting, we thoroughly explored how the website will operate from the user's perspective. We ensured that our verification and security measures are robust while maintaining a user-friendly approach. We also talked about reaching out to potential partners to establish collaborations for our service.

   Since blockchain technology plays a critical role in our project as it facilitates trust between users and hosts, we had a detailed discussion on how and where we plan to implement blockchain within our website.

   Please see the attached meeting notes for details.

2. **Tasks completed:**
   - Megan reached out to Steven Lupien, director of Center of Blockchain and Innovation, to help answer some of our questions related to integration of blockchain into our project.
   - Tamara took charge of keeping notes of our progress and updating our meeting records.
   - Kellen looked into Truffle boxes and how we can implement them in our project.
   - Selma looked into the UI/UX portion of the project for ideas to create a user-friendly website.

3. **Successes:**
   i. **Group accomplishments:**
      - Pitching ideas and finding solutions to some of verification and authentication issues.
      - Development of robust security measure ideas.

   i. **Other things tried:**
      - n/a

4. **Challenges:**
   i. **Describe the challenges:**
      - Since we are just starting our project, we're developing our ideas, so there are plenty of challenges. What functionality do we want? We need really good security, so how will we implement that? Who will be in charge of what? What resources do we have? Details on how big of a part will Blockchain play and in what areas?

ii. **Did you overcome them or are there challenges left?**
    - We are talking through these challenges as we develop our ideas and trying to find solutions for them as the project progresses.

iii. **Do you need help? Can mentor help or external help is needed?**
    - We have you and Steve Lupien as our mentors at the moment. We may need other mentors as we get further in our project.

5. **Changes/deviations:**
   We don't really have any changes from the pitch document. We are just adding more details and authentication/verification measures to ensure security.
6. **Confidence:**
   We are confident that we will be able to develop and implement this project.
7. **Group dynamics:**
   Our group is working great together. Each member is actively contributing during meetings, sharing ideas, conducting appropriate research, and fulfilling their roles/tasks. We are very excited about this project.

MEETING NOTES

Senior Design Project
Blockheads
Credentials and Identity Manager

Megan Steeves
Selma Samet
Kellen Mentock
Tamara Linse

Meetings: 10.17.23 (Standup, EERB 255), 10.24.23 (Coe 264), and 10.31.23 (with Jim, EERB 255) - Selma, Megan, Kellen, and Tamara

Summary

- Our minimum viable product:
    - Target verifying one or both a Wyoming driver's license/ID and a UW degree,
    - Login, 2FA, and recovery of passwords,
    - An android interface,
    - Use smart contracts to interact with blockchain and blockchain to store IDs and credentials,
    - A server to interact with devices and the blockchain,
    - A database for temporary data mirrored between a device and the server, and
    - A procedure to verify with UW and Wyoming.
- We will assume that the user is only connecting one device.
- We decided a phone app would be more appropriate than a website and with consultation with Jim decided to design for android.
- We made a list of functionality, potential programming languages, and then designated a lead and a backup for each area, with the understanding that if we need help or need to hand it off to someone that will be okay.
    - Database, SQL – Tamara (Selma)
    - Blockchain and Smart Contracts, Solidity – Kellen (Tamara)
    - Android UI/UX, Java/Kotlin – Megan (Selma)
    - Server, Python/C++ – Kellen (Megan)
    - Security and Authentication, Java/Kotlin – Selma (Megan)
    - Validation (contacting organizations) – Tamara (Selma)
- Security and authentication are important and may be challenging, so we need to be on top of that.
- We will each do research on our areas to firm up our approach, including developing diagrams.
- We reached out to the State of Wyoming to develop a procedure for validating driver's licenses/IDs (Tamara, with group added to email). We completed the contact form, called, emailed per the phone call contact's instructions to helpdesk@wyo.gov, and followed up with email, but we have not yet heard back. We will continue to follow up.

- We reached out to the University of Wyoming to develop a procedure for validating credentials—degrees received. We (Tamara, with group added to email) first emailed the registrar (Lane Buchanan) and he referred us to IT (Brett Williams). We then emailed IT and did not get a response. We followed up and got a response. Brett is out of the office after surgery and isn't able to meet yet but will be able to soon. Megan and Selma will be meeting him.
- Brett said he had concerns about student data privacy, but since we're only asking for degrees—which are public information—that are connect to a person and it's that person who is asking for it, it should be okay.
- We also will need to develop language and then ask the State of Wyoming and University of Wyoming to put a page on their website that can be accessed by people verifying identification and credentials that says that our product is legitimate.
- In consultation with Jim, we decided to develop our server on the AWS platform.
- We firmed up our security and authentication plans.
    - For first-time login, the user will enter username and password plus facial recognition that is built in to android devices.
    - They will also enter their phone number and enroll in two-factor authentication.
    - If they forget their password, they can reset their password with a code (that expires after a period of time) sent via text to their phone that will be entered into the interface.
    - A stretch goal would be to also offer a twelve-word recovery phrase.
- Memory management will be via a database and a blockchain. The database will store process, account, and temporary information, while the blockchain will store identities, credentials, and long-term information.
- Our model for communication and memory:
    - There will be two-way communication between devices and the server.
    - The server will have two-way communication with the blockchain, but devices will only be able to read from the blockchain.
    - Each person's database will be mirrored between their device and the server.
- Our mentors so far are Jim Ward, Steve Lupien, and Danny Radosovich.

Action Items

- Continue to follow up with the State of Wyoming about validating driver's licenses or IDs (Tamara).
- Do research on how Colorado sets up their digital ID system (Tamara and Megan).
- Continue to follow up with the University of Wyoming about validating UW degrees (Selma, Megan, and Tamara).
- We will all so research into our designated areas and firm up our approach, including diagrams and models.
- We will develop a flow chart of security/login/authentication and the related technologies (Selma).
- We will research which database language to use, PostgreSQL or MySQL (Tamara).
- We will research server setup and decide on a language, Python or C++ (Kellen).

- We will research Truffle boxes and smart contracts and how they apply to our project (Kellen).
- We will research the android interface, store, messaging for password recovery, and face recognition (Megan).
- We'll attempt to do some programming before the end of the semester and over the holidays to get ahead of next semester.
- We are developing the Intermediate Planning Document and, possibly, a team contract.

Meeting with Jim: 10.10.2023, EERB 255 - Selma, Megan, Kellen, and Tamara

Summary

- We gave our status report to Jim
- Jim let us know expectations for status report and the course going forward – status reports every so often, be able to hand off project to another team at end of semester if it was necessary, planning docs, working through details
- We don't necessarily need to divide the project evenly by 4, just everyone work on their strengths and speak up if one of us feels like we're taking on too much and hand things off as necessary
- We need to limit the scope of our project as much as possible or we won't be able to finish it
- Maybe focus just on Wyoming ID and UW credentials
- We're now thinking a phone app (dApp) as opposed to a website
- Talked through what we'd decided about security and keep it to a minimum
    - First login – ID and facial recognition if possible, otherwise just verify id number
    - Login after that – bio such as facial recognition or username and password
    - Have logins expire and timeout
    - Use text messages for recovery
    - Can offer the user choices of they they want for security (trust this device, how long before timeout, how to send pin code)
    - Not having to give phone number or email is a stretch goal
- Think outside the box and think about failures and backup plan
- Minimum viable project in April
- Our status report is done (status report + these meeting notes) and we've turned it in on WyoCourses and GitHub

Action Items

- Megan and Selma will give verbal status update next week (standup, 3-5 min max, wins and losses and failures and what we've tried and what others can learn from it), with support from Kellen and Tamara
- After next class period, we will do the same thing we did this past two weeks. The first week during the class period we'll meet in Coe to further develop the project. The following week we'll meet with Jim in the classroom for an update.
- Everyone will continue to research things
- Intermediate planning document due 11.3
- He also suggests a team contract 11.3
- Next status doc due 11.27
- Final planning doc and retrospective due 12.7

Meeting: 10.3.2023, Coe 264 - Selma, Megan, Kellen, and Tamara

Summary

- We addressed the great questions that came up in class from other members of the class
- We talked a lot about processes for security
    - Megan came up with idea to solve our initial login problem – When someone initially logs in, they take a photo of themselves and their id. Facial recognition plus validating their ID (e.g., quick API validation with driver's license through DMV) will allow them to create an account
    - Not sure we will be able to get facial recognition working in time, but we had some suggestions for open-source facial recognition
    - User's login will automatically log them out after a certain time period (4 days? 2 weeks?)
    - Once a browser is logged in, they will be able to get back in with a pin
    - They will only be able to login on two trusted devices (the independent pages send to other people to show ID will not count in this)
    - If they forget their pin but they are logged in, they can reenter their login info to create another pin
    - If they forget their login information, we will need to have password recovery option
    - We talked about a number of things for password recovery and login
    - We have the options of having them enter their phone number, an email address, and a recovery phrase
    - They won't need both phone number and email unless they want it
    - A number of us were in favor of using a recovery phrase as first-line login, with the possibility of not making them enter a phone number or email
    - However, in order to make the app work, we most likely need at least one piece of contact information, most likely (for 2FA)
    - Users may need a trusted third party or emergency contact to be able to access this, or one partner may be the one in charge of both partners' online data—therefore, we need a way to have a trusted contact
    - We could do trusted and/or emergency contact through a smart contract with asymmetric cryptography
    - We need to talk through all this with Jim
- Once again, we are assuming we are creating a website (not a phone app, tho that would be the most useful to user)
- Multiple ways of doing things is good
- We decided to limit the scope of the IDs we will test, with the understanding that with each agency would have to establish a relationship. We will focus on one at first.
    - We will focus on credentials with UW
    - If possible, we may add Wyoming Driver's License
    - Probably won't get to it but also a national ID such as Passport
- We will need 2FA
- We will have multiple ways to show an ID to someone
    - It will have a time out

    - One way is a QR code that takes the person asking to a web page not linked to any of our other login
    - One QR code for each type of ID
    - There will be a verification permission sent to user via text (reply Y or N) or another way such as a popup from the app so they can confirm to show that page to the outside person
    - Other ways to share an ID may be text or email with link that goes to that web page display
- The home page will have buttons to each ID, and after button press, the user will need to enter a pin (even tho they are logged in)
- We need to further figure out how to just show the info they need and not expose the whole ID unless necessary
- We will test, for example, at liquor store with valid (of age) ID and invalid (underage) ID
- Because those wanting to see the ID won't know if this is legit, we will have a button on the viewing page they can press that will go to the ID agency web page, and we would ask the agency to put up a page with a brief description of CredHub and saying that it's legit
- We'll start with UW and talk to Registrar's Office (Tamara will email Lane, the Registrar)
- Selma said she'd like to do the UI/UX portion
- Megan has been talking about the project with Steve Lupien for ideas
- Kellen has been looking into Truffle boxes
- We will set up reminders for updates

Action Items

- We will meet with Jim next class period (10.10) in our classroom in the EERB
- Selma will begin our Status Update #1 and have it to us by Sunday, then the rest of us will go through and edit and add so that we can turn it in on Tuesday (10.10)
- Tamara will upload these notes
- Tamara will email the Registrar's Office
- We will continue to develop and parse out responsibility for parts of the project

Meeting. 9.19.2023, Coe 310 - Selma, Megan, Kellen, and Tamara

Summary

- Our project:
    - CredHub – Protecting your credentials
    - Tagline – You've got cred
    - Group name – BlockHeads
    - We will develop a web application (dApp) (mobile interface reserved for future due to limited development time)
- Everyone has their logins to the group on WyoCourses, Discord group, and GitHub
- Tamara and Selma had started the pitch document before the meeting
- We all developed the pitch document to be fairly complete during the meeting
- Jim is our advisor
- For now, all we need is a server
- Selma proposed our name be CredHub - Protecting your credentials
- Tamara proposed the tagline You've got cred
- Megan showed us an example app from Colorado state government that holds credentials that we can partially use as a model
- Kellen suggested we not only have a blockchain to store credentials but also we use a smart contract to verify with official organizations
- Types of IDs/credentials: social security number, birth certificate, passport, drivers license/ID card, degrees, marriage license, etc.
- Someone suggested using a QR code for sharing of credentials
- We discussed how to authenticate (2FA?) and what data would be used for user login (SSN? other?) and how to protect against someone getting your data and then spoofing you and creating an account
- Trust and security is going to be very important
- Verification with official organizations may be either through an API or through a analog process
- Reminders to renew ids and credentials will be built in
- As a phone app, will need a lock feature for when a user hands over their phone to someone to show id
- We may need alternate profile options (what someone goes by at work vs in private vs as a name that you go by for other things)
- For blockchain, we may use Solidity and Truffle and Truffle boxes
- Not sure the exact data storage model - blockchains with a database (hybrid)?
- Functionality to consider: authentication, user accounts, security/trust, UX/UI, data storage (blockchain and database), API integration, manual verification, use cases

Action Items

- Selma will edit through the pitch document and send to everyone else to review (Sunday?)
- Then we will submit the pitch document by Tuesday, 9.26, and also do a verbal pitch to the class
- We will meet with Jim sometime in the next two weeks

- We are setting up additional meeting times (during class time?)
- We will complete status update #1 and submit by 10.10
- Future topics – narrow in on functionality, tech stack, and who is doing what

Initial Meeting and Followup on Discord, 9.12.2023 - Megan, Selma, Kellen, and Tamara

Summary

- Tamara, Megan, and Selma pitched idea to class, 9.12.2023
- Kellen joined group and is interested in blockchain
- Selma emailed Jim, and he set up group on Discord and WyoCourses
- Megan is in contact with her prof Steve Lupien, who can help us or connect us with people as necessary

Action Items

- Because we've formed our group, we will not go to class 9.19.2023
- Instead, we'll meet in Coe Library during that time (Tues., 9.19.2023, from 4-5, in Coe 263) to talk about the project and create the pitch document
- We all will bring ideas and what aspect we're good at and what we would like to work on
- Selma is reserving the room in Coe
- Tamara is taking meeting notes

TEAM CONTRACT

Senior Design Project
Blockheads
Credentials and Identity Manager

Group: Megan Steeves, Selma Samet, Kellen Mentock, and Tamara Linse

We agree to do our best to complete our senior design project and to be responsive to our group. We also agree to communicate as soon as possible if we run into problems. We will ask for help and pitch in to help others when needed, and we'll be open to other people's suggestions. We believe in our project and will do our best to achieve our minimum viable product by the deadline. Documents we produce for class will be our guidelines and goals.