02/25/2022

Meeting started at: 4:00pm

Present:

- **Raven Zucchelli**
- **Abigail Zucchelli**
- **Wasif Siddiqui**
- **Kumail Bukhari**
- **Aiden Nguyen**
- **Cedric Lee**
- **David Eddy**

Notes:

- GitHub Documents UML
    - Ways to do version control without having to do it directly on GitHub instead of doing the pdf
    - Uml documentation
    - Cedric created updated UML Markup language for our documents/deliverables
    - PlantUML
        - Focus on the data rather than the
        - GitHub
            - Output - contains images
            - UML - contains the UML code
        - SVG - Scalable Vector Graphic
            - Don't lose clarity of the image - scalable
- Message Signing
    - Depending on message signature video
    - Digital signature - what should it look like? How would digital sign?
        - Different ways of doing it
            - Employer providing Unique ID field
                - Click a button, application sign the message, respond back with some string that includes a timestamp and public key
                - Random message with some structure
                - Copy message to third party tool, and create the signature
                    - Submit the form, got a message ,copied and pasted, signed it
                    - Another field to paste signature into it
                    - Single transaction go to the block chain
                - Encrypting message with the public key
            - ID access management system - a lot of systems
                - Passcode is the digital signature through that code
                - Know that it's you
                    - Won't get access until get the code
                - Account associated with a public key
                    - MFA is a pointer to it to know who you are
                - Do we want to, do digital signature or do we pass static digital signature?
                    - Concept:
                        - Once block chain receives it, it will decrypt message with public key and that would result in the original message
                        - Submit the transaction

                - Public key, message signed with public key and original message
            - Employer is encrypting message with the private key with public key
                - Input - survey info, employer public key, signature, original message
                - Block chain receives, decrypt message with the public key must match
        - Block chain has listener, sending transaction expecting the parameters
            - Must do signature - implement signing it digitally and sending it to the block chain
                - Act of signing of message is manually off the system/application
                - They are signing it themselves
    - Employer experience
        - Open form, enter public address message appears, employer would sign, with auto generated message try to do same thing but with receiver
        - Sending the signature public key, signature, message and survey
            - Block chain receiving it and verifying the transaction
            - Message signature test is decrypting the signature
        - and then ensure its the right personMessage - unique every time
            - Main thing - timestamp, unique across public key is included
        - Make call to block chain and give response, know its in the block chain and save it to the database
            - Some risk, might never get to database
    - Ask signature when they input public key, the message will appear underneath the employer id and signature will be on the same line
        - Message appears, put signature box and go off take message sign it and past, and now the form has everything they need
        - Provides some uniqueness to the message
        - API to blockchain- limited amount of time, message has expiration about 5 minutes - blockchain API does that - can change time
- Next steps:
    - Implement changes to the screen/mock-up
    - Designate a team for blockchain API
        - Good if one or two takes a particular keen interest in block chain code
            - Familiarize - represent block chain api team
                - Can make changes to the code
            - When submitting the survey, what is the data-structure of the survey
                - Block chain receiving a string, are we talking about putting string in json?xml? What are we receiving back?
        - Whomever is on team, coordinate to get the code running on their machine
    - Ripple effect to database to referral table [update database mock-up]
        - Message, message signature
    - Some of code template code - udacity - don't present any of that as own, if cite david or udacity do it
- Blockchain code
    - Creating docker containing and running code in container, put image in AWS
        - Set up Container registry and container service

            - Future infrastructure
            - Different server/domain space, calling the API, there is something called cores policy, protecting inline client side javascript
                - Browser security - post somewhere from a browser different from server that its from, then security risk
    - As long as there is a way to normalize score so if question is added old scores may become invalid
        - Known limitation, pick a question thoughtfully chosen to have normal distribution, lack of fairness to early adapters
        - Assume to only post score