March 1st-12th

Tasks

1. Explore solutions for simulating a network of computers on single or multiple VMs. With the goal of deploying a test network for development.
    a. Your Recommendation:
        i. Familiarize yourself with docker
    b. Actions:
        i. Went through a tutorial provided by docker, have a general idea of how microservices works.
        ii. Also learned about docker swarm, container management software, and Kubernetes, a competitor.
    c. Comments:
        i. To simulate nodes on docker, need to set up an overlay network which connects the containers. There are tutorials for this.

        Hyperledger:

        1. Hyperledger Fabric on IBM cloud with Kubernetes
            a. Pre
            b. Must use IBM cloud? However, “allows you to create a free cluster that comes with 2 CPUs, 4 GB memory, and 1 worker node. “
        2. Hyperledger Fabric on Vmware's VSphere

        Ethereum

        3. Dapp development framework called Truffle suite
            a. Truffle: Tools for writing Smart contracts
            b. Ganache: Provides a blockchain (simulated?) for development to deploy contracts
            c. Drizzle: Front End library
        4. Pyethereum
            a. Provides a test network
            b. Python ethereum, although depreciated.
2. Setup Helios server
    a. Your recommendation:
        i. Run the server and get familiar with the codebase
    b. Actions:
        i. Cloned the code from GitHub, set up the the Postgresql database, ran the server code on the desktop. Ran the unit tests.
        ii. Went through some basic HTML, css and Django framework tutorials to understand how the crypto interfaces with the backend/frontend.
    c. Comments:
        i. The codebase is quite large, still, don’t completely understand how all the modules interface to create the election.

Questions and Thing's I'm not clear about

- The exact protocol for the election, using homomorphic encryption isn't spelled out explicitly anywhere. Perhaps we can go through the crypto in the election.

  Adida cites Cohen 1985 in Helios v2.0 paper, which switches to homomorphic encryption.

  Josh Cohen is Josh Benaloh.. Probably the first proposal of using homomorphic encryption for elections?

  However, the election seems to follow CDS97 paper, which extends elections using disjunctive proofs.

  Adida also provide a verification procedure, in his documents:

  https://documentation.heliosvoting.org/verification-specs/helios-v4

  [CF85] "Josh D. Cohen and Michael J. Fischer. A robust and verifiable cryptographically secure election scheme. In FOCS, pages 372–382. IEEE Computer Society, 1985."

  [CGS97] "Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. 1997. A secure and optimally efficient multi-authority election scheme. In Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques (EUROCRYPT'97)"

  "Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios Adida, et al 2009"

Next Step:

- Toy app in hyperledger fabric and ethereum.