CS+ Decentralized Finance: Blockchain and Cryptocurrency on the Internet Computer

Meeting Minutes

7/8/2021 10:00 – 11:00 AM EST

Present:

Prof. Luyao Zhang - Lead

Prof. Kartik Nayak – Co-Lead

Prof. Yulin Liu – Co-Lead

Derrick Adam – Graduate Mentor

Dylan Paul – Full-Time Researcher

Urjit Banerjee – Full-Time Researcher

Oum Banerjee – Full-Time Researcher

Malika Rawal – Full-Time Researcher

Tianyu Wu – Research Support

Elliot Ha – Research Support

Saad Lahrichi – Research Support

Ray Zhu – Research Support

Anika Suman – High School Student

Dylan & Malika:
Team Name: Icy – play on words Internet Computer and it being icy

Dylan presented the following:

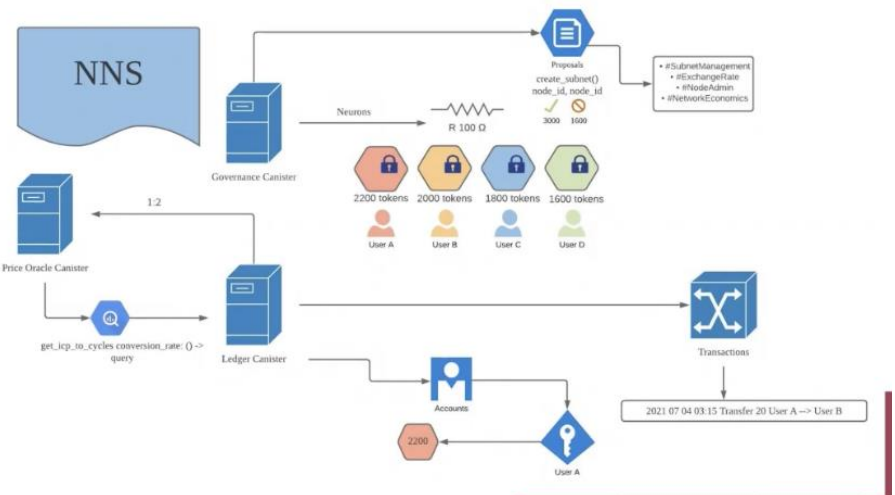
Week 3 Research - Dylan Paul

- Narrowed down research question: How does Ethereum's gas model compare to Dfinity's 'reverse gas model' and how do these models affect developers and users on these platforms?
  - Goals for the research
    - Analyze and compare gas models
    - Analyze and give overview of each blockchain structure(consensus mechanism, tokenomics, validators, etc.)
    - Future outlook for users and developers
- My research this week was a deep dive into each blockchains structure and how their gas fees work on their network
  - Broke down Internet Computer roles of NNS, Canisters, Cycles, ICP Tokens, subnets, subnets, data centers, nodes. This ultimately led into research on how their reverse gas model operates.
  - Looked into what ethereum gas is, why gas fees exist, the gas limit, block gas limit, and their 'fee market'. Researched solutions that ethereum is working on for scalability issues leading to high congestion and thus fees.
- Methodology to analyze economic impact of gas models: eventually deploy ICy on the Internet Computer and test out different revenue models (user pays vs. in-place reverse model)
- Code Update:
  - Worked on but have not yet completed database canister to incorporate accounts to go around issue faced with getting transactions to work.

Malika presented the following:

Week 3 Research - Malika Rawal

- Narrowing down Chain and Key Technology to NNS and implementing it on the Price Oracle Canister
- Tokenized open governance system that manages the Internet Computer.
- Stake-Based Model
- Reward System
- Stores what nodes belong to which subnets, and how to update nodes/what happens when they crash. Essential in chain and key recovery of node process.

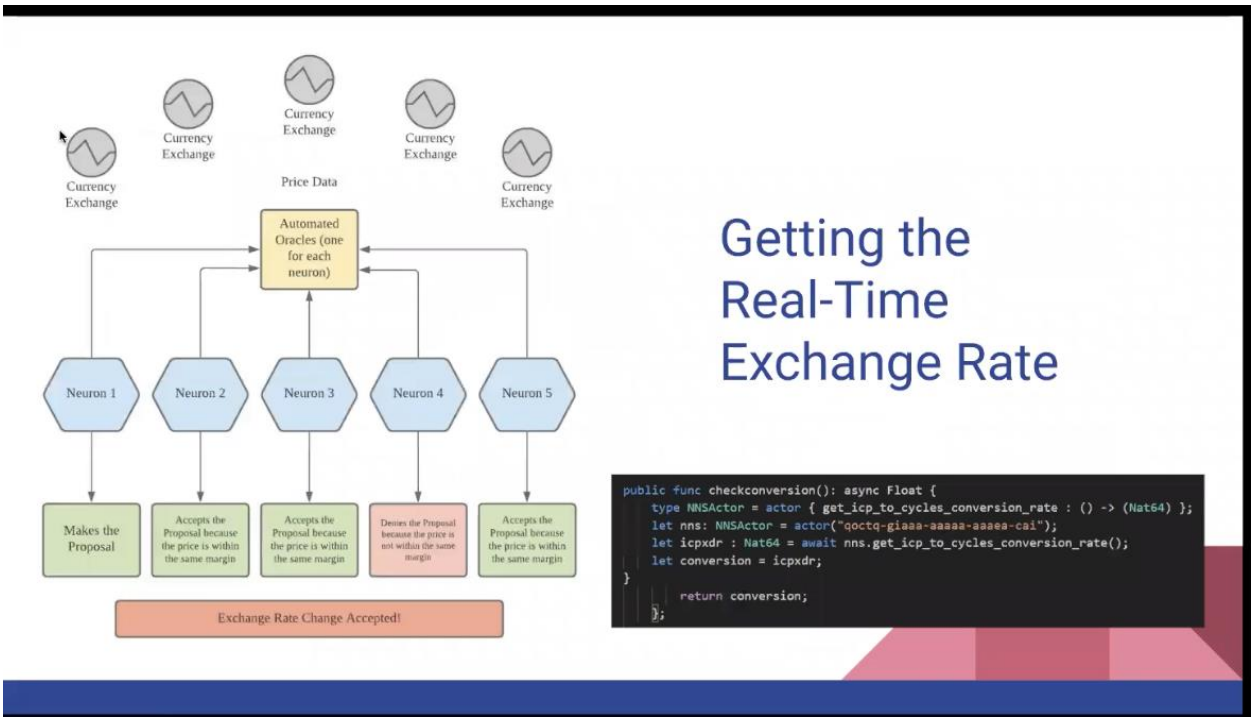


Prof. Yulin Comment:
In bitcoin and Ethereum they have the off-chain governance system. The code base changes all the time, but who can change the code, paramters, and who can make decisions? The comes through the governance system. The off-chain governance system means decisions are made off the chain and the developers first make the code change and the miners decide whether or not to adopt the change or not. Users of bitcoin and Ethereum have no say in the system. In that sense, it's still a centralized system. Only a small number of developers and a large mining pool have the voting power on how bitcoin and Ethereum evolve over time. Sometimes these two parties have different opinions on the system. That is why Bitcoin is hard forked many times, e.g. Bitcoin-gold, Bitcoin-cash, Bitcoin-diamond, Bitcoin-platinum. That's the problem of the off-chain governance system – users/token holders do not have a say and the decision-making is slow and centralized. For this reason, Ethereum is thinking of switching to the On-chain governance system.

For DFINITY's Internet Computer, the governance system starts with NNS. Here, token holders are the users of the system, so they should have voting power. But you don't want them voting on short-sighted proposals for short-term interests. If you want voting power, holding tokens is not enough. You need to stake your token in the system for a minimum of 1 year. Voting power is proportional to the number of tokens you keep in the system. The longer you stay, the more voting power you have. The longer you log, the more voting power you have to give poor users more voting power if they are willing to lock their tokens for longer. If you lock 1000 tokens for 7 years, then you have the same voting power for those who lock 7000 tokens for 1 year.

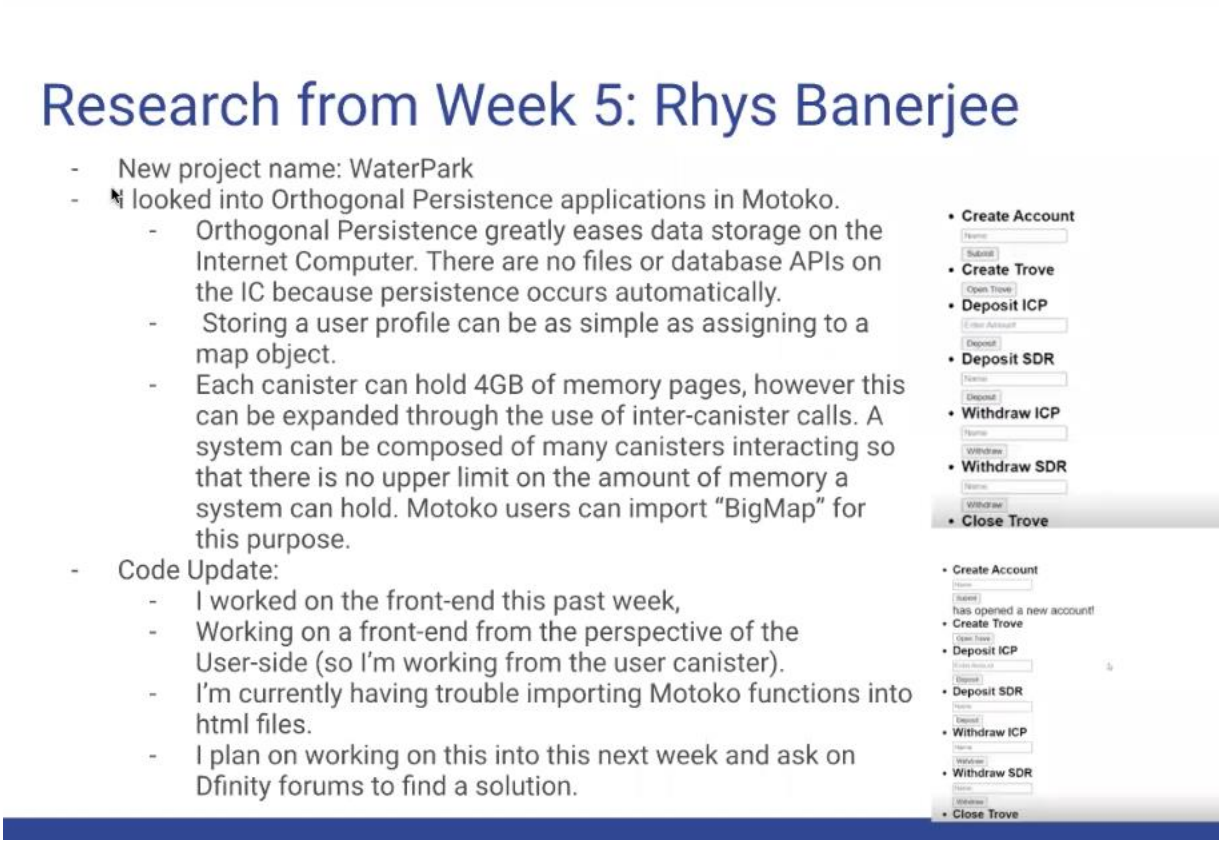
The second difference is DFINITY has a different democratic system. Most people don't care for the voting power, but more for the monetary incentive. Voting is costly if there is a proposal – for example Bitcoin should increase the size of the block or reduce the block time. This requires research and most people do not have the expertise. For that reason, most people don't want to vote. To incentivize the turnout rate for voting, DFINITY gave a voting reward with an economic incentive. Secondly, the system is liquid democratic meaning you could dedicate your vote to someone is an expert in a certain field. On the NNS, there is a dashboard. There are different proposals related to economics and technical aspects. You could dedicate your vote to an economist for economics related proposals or delegate your vote to technical experts for technical related topics. If there's a proposal you think you have expertise in, you could vote on this proposal. If you are unhappy with some of the experts you delegated to, you could withdraw your vote in the delegation any time.

Malika presented:



Liquity Team: Rhys & Oum
New Team Name: WaterPark

Rhys presented:



Prof Nayak Question:
You write each canister can hold 4GB of memory pages and and you can use inter-canister calls. Does this mean that if want 40GB I use 10 canisters?

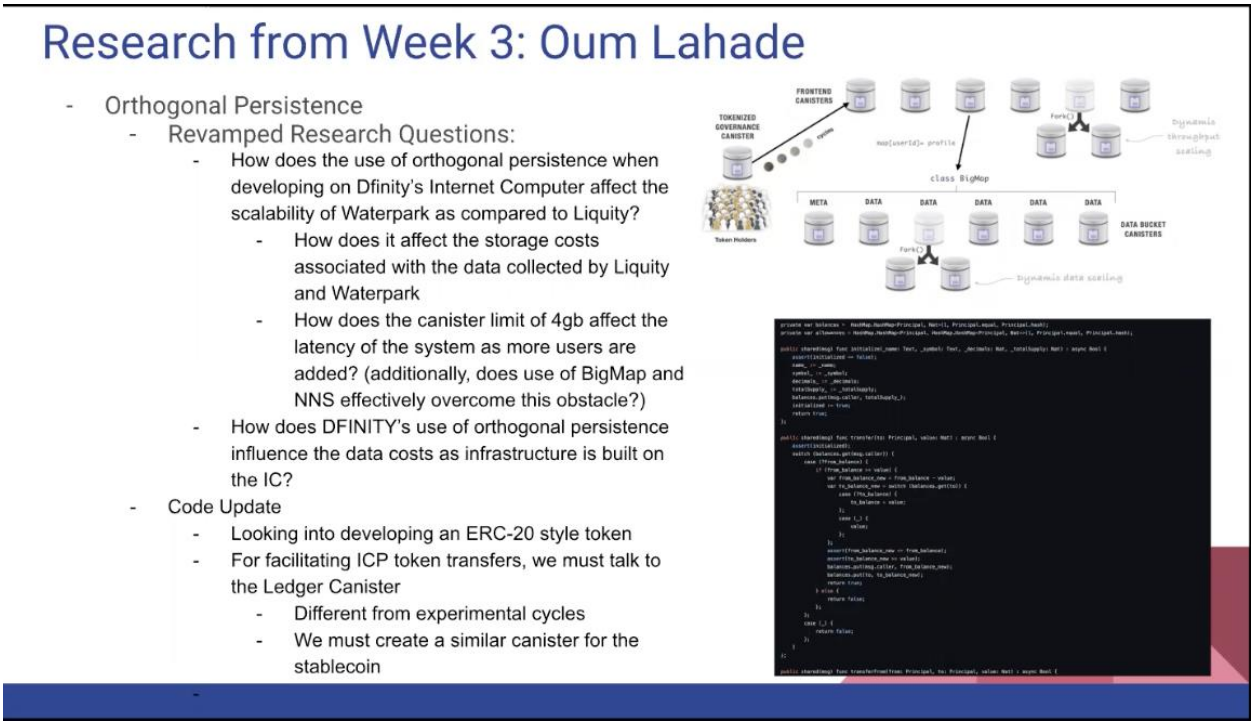
Rhys:
If you want more, you import BigMap and use multiple canisters.

Prof Nayak:
1 canister vs. multiple canisters – why does it matter? If use 10 canisters because to make them 40GB then these nodes need to store that amount of memory anyway.

Rhys:
Will do more research into this question.

Prof. Yulin Further Research Questions:
Is there any reason why it's 4GB? If the canister exceeds the memory of 4GB, the canister could create a new canister as its sub-canister. There is one central canister with many sub-canisters which is how it becomes scalable. How do canisters interact with one another? What is the difference inside a canister and an inter-canister call? If the application is too big to be hosted by 1 subnet, it might be expanded to several subnets. There are inter-canister and inter-subnet calls. Are there differences time-wise and cost more or less? BigMap is to facilitate canisters to search for information. How does it work and further explain it?

Oum presented:



Will use storage costs as a proxy for measuring efficiency