

ZKU Report

Kousik Rajesh

Week 28 (24 Aug - 30 Aug):

<https://assorted-bobcat-826.notion.site/24456f347d4143d7a3879fb9134a0e5d?v=50f560f02072496582e12bdd70ddb73b>

This week I went through the code and tested out the final project submissions of c4. I also did some research on conducting a proper round on darkforest in preparation for a beta round soon. I made code and ui changes to finish the porting and merging of betting contracts..

Week 27 (17 Aug - 23 Aug):

<https://assorted-bobcat-826.notion.site/9fa7f2b41ec34d2a930dd5efe9d5728c?v=eaf9437c6d9540c485c3628ded55cf19>

This week I finished the betting part for blueforest. I made an endpoint to fetch bet sizes, and modified some react elements for leaderboard to include the data. I then integrated the endpoint to display bet sizes on the leaderboard itself, so players can make a bet accordingly. I also made a few changes to the betting interface and deployed the final version. With this blueforest is almost ready for a beta round. I also had some discussions with some students on some final project queries they had.

Week 26 (10 Aug - 16 Aug):

<https://assorted-bobcat-826.notion.site/3d5831950beb4369bfb83456b0213b59?v=d6f53d35316947e685ad55e9b8ac75ec>

This week I graded week 5 assignment and had some discussion regarding a few final projects with the students.

I also integrated the betting contract with the frontend of darkforest and deployed it.

The betting interface is now integrated to the df terminal and bets can be placed/changed before game starts.

Moving forward I would like to host a beta round of the fully ported blue forest.

Week 25 (3 Aug - 9 Aug):

<https://assorted-bobcat-826.notion.site/03fe6bc4b2ee4834b42d10020031bdcd?v=d89bfc64405148b4b571b2ee0cc162c9>

ZKU work: This week I held an AMA, graded week 4 assignments, discussed final project ideas with students

ZKDAO work: Ran scraper and updated final transactions from harmony multisig

Df work:

1. Reviewed pull requests from harsh and 0xIws
2. Requested modifications, solved merge conflicts and merged to main repo
3. Coded the betting contract, a functioning basic version of the contracts is complete
4. Started merging betting contract with df repo
 - a. Added to darkforest eth, wrote code for compiling and deploying the contract

Week 23 (27 July - 2 August)):

<https://assorted-bobcat-826.notion.site/9dd1ad8fe5bc4e628ed10480051c0f15?v=4a024dd9e0c841a284098a70cc7dcb1c>

This week I held an AMA, reviewed final project ideas and graded week 3 assignments.

Most of my focus was on df -

1. I coded a basic version of the betting contract
2. checked df nightmarket and how it can be ported to our df version
3. helped debug the df leaderboard issue.
4. Managing df=gameplay

Week 22 (20 July - 26 July)):

<https://assorted-bobcat-826.notion.site/879c4c0c3c3f45e3a73b8fe0ae94ed76?v=9f6a6ecbe5fb498682b742533c4cce38>

This week I graded week 2 assignment submissions. I read and commented on the final project proposals made by c4 students.

For df, I researched various ways that betting systems usually work and devised a strategy for betting that rewards winners based on their initial bet size and also their final leaderboard position. Based on feedback on discord, I modified the strategy a bit

so that it incentivizes users to bet more. A fixed amount of money (5%) will be drawn from this pool for df and zkdao funds so the more people bet the better our revenue model from df.

Week 21 (13 July - 19 July):

<https://assorted-bobcat-826.notion.site/3ac16eb54b9b428784d22ce65cac0be9?v=dc528fc0b0b34aeca53af836c27a21f9>

This week I graded the late submissions for c3 final project. Checked and tested the codebase of suhasbr as it seemed to have some flaws. These were later clarified after cathie's communication with him.

I also held an AMA for week 2, and graded week 1 assignments.

For darkforest, I laid out the future tasks that need to be done and discussed them on discord. I also looking through the codebase to understand how the leaderboard is being fetched and calculated. Fixing the leaderboard will be the first step after which we will focus on implementing the betting logic.

I also tried to understand how the planets were being generated procedurally for the df-frontend team.

Week 20 (6 July - 12 July):

<https://assorted-bobcat-826.notion.site/d56b3cd38b384d8d95394c9e9e009221?v=a5bc32eda11469ab29b76b5f27a3f91>

This week I tested and commented on c3 mainnet submissions

I fixed the artifact issue in the darkforest port and tested gameplay. I also played with the configuration parameters of df to better understand how df could be adapted for smaller game sizes in preparation for beta round.

Week 19 (29 Jun - 5 July):

<https://assorted-bobcat-826.notion.site/5b424daf1a324a428cad3836e20fd196?v=7d7743b5bcf64a4f8a19d4dc11ba52a0>

This week I tested and graded all testnet submissions from c3. I also concluded the alpha round of darkforest, analysed issues in it and laid out future improvements that can be done. Also engaged in discussion regarding zkdao, df, c4, final project discussion on discord

Week 18 (22 Jun - 28 Jun):

<https://assorted-bobcat-826.notion.site/eb86967a2dd547a3a22f521fff78ffad?v=21c60d542564416b8690b7e9ab594123>

This week I launched the alpha round for darkforest. After devnet deployment last week a few small issues had to be fixed

Around 10 zku graduates had registered for the alpha round, but since whitelist has been removed it's free to play. I've also been ~~playing~~ testing the port and almost all features seem functional, transactions are a teeny bit slow (2-4 sec) on harmony but nothing bad for the UX. Artifact minting is the major thing that needs to be fixed, the port doesn't allow to prospect them (say's round finished)

For ZKU work, I graded week 7 submissions, followed up with some of them regarding it, graded background assignments for c4 and started testing testnet submissions of final project submissions.

Also did a bit of zkdao governance work - had a discussion regarding future treasury management and grant approvals.

Week 17 (15 Jun - 21 Jun):

<https://assorted-bobcat-826.notion.site/f38a196754ba4a86ba82cd9320954289?v=cdca8c4ba5d5419c8b8baf8b8925399c>

This week I graded week 6 assignments and followed up with the students regarding the final project progress.

I also ported darkforest to devnet since testnet is now unstable for dapps. Few bugs had to be solved while porting. I also removed the whitelist requirement for darkforest so it's easier to play. This was in preparation for the alpha round of darkforest which would be held starting this saturday.

Week 16 (8 Jun - 14 Jun):

<https://assorted-bobcat-826.notion.site/687480e488dc40bdae029ec8e9622d25?v=9a51f41d2ece4942acd882addc4cdbe8>

This week I graded week 5 assignments, and mostly focused on evaluating final project proposals and discussing with students possible improvements.

I also held an AMA, went through some grant proposals and tested the hongbao project. For zkdao, I updated the scraping script to handle failed txs and updated expenses/income. I'm also talking to re:base for a potential vc interview and pagan for advertising the df port. Discussing with tosin the dao structure for df and about conducting an alpha testing round among zku graduates.

Week 15 (1 Jun - 7 Jun):

<https://assorted-bobcat-826.notion.site/4be16e2ab14e4092933098c0f7b27423?v=0486fd4dc9ba49c7b8d72d80f1bdb594>

ZKU work:

- **Promo work:** Collected and emailed around 15 university blockchain groups regarding c4
 - Promoted in researchdao
- **Academic collaboration:** In talks with research dao and a student from university of michigan regarding possible academic collaboration for seminars
- Graded week 4 assignments and followed up with students on final project feedback

ZKDAO work:

- Read and commented on dao proposals, constitution etc
- Updated dao statement, address mapping and labelled txs
- Formed minimal df dao
- Tested and commented on grant proposals

Week 14 (25 May - 31 May):

<https://assorted-bobcat-826.notion.site/d058f6adcd6948af834d6971d499956a?v=79f31963b160465d97d78b165dea1552>

ZKU work:

- Graded week 3 assignments and gave feedback on project proposals
- Did some data analysis on the gradebook and applications sheet to evaluate the effectiveness of our partnerships and to see where our distinction candidates find out about the course from. C4 promotion can be modified according to these insights

- Discord time - answering queries, reading resources, newsletter, proposing project idea etc.

ZKDAO work:

- Attended the 1dao alliance talk and discussed on multisig issues we face
- Calculated type wise expenses of zkdao for use in funding request for next cycle as requested by kayuet
- Modified account statements to include grant account as well
- Testing and approving grant proposals
- Went through tosins contract for dbi disbursement

Week 13 (18 May - 24 May):

<https://assorted-bobcat-826.notion.site/c5d35acdd71b4a9ba5516ebe806d7b24?v=10b3322cc83e494baf11ac7561412574>

ZKU work

- Hosted AMA
- Answered discord queries
- Graded week 2 assignments
- Studied few papers and blogs

ZKDAO work

- Updated finances on sheet and labelled them
- Promo work for c4 - contacting few blockchain groups
- Tested out and approved c2 final project proposals

Week 12 (11 May - 17 May):

<https://assorted-bobcat-826.notion.site/fa1903f3222943ab8b1d9e85317e026a?v=ce7367dd61c741a7878a5665c75b62f3>

This week I graded my batch of week 1 assignments. I was travelling for half the week (13-16 May) so couldn't get much work done then.

I updated the minimalDf repo contracts, circuits and also added a basic readme.

Also updated the dao finances. The multisig website has some weird bugs which causes it to mix up transaction ID's so I had to update the tx scraping script. Also modified the script to take care of the pagination on the website.

Finally, I read, tested and commented on the launch grant proposals made by c2 students.

Week 11 (4 May - 10 May):

<https://assorted-bobcat-826.notion.site/cf051997e12f4c12a501f30a23c15192?v=739e1b64963946279ae5c9b35ad11b2c>

- Did mostly ZKU TA work
- Answering queries on discord
- Held ama for week 1
- Read the original circom implementation paper
- Went over some final projects

Week 10 (27 Apr - 3 May):

<https://assorted-bobcat-826.notion.site/8e9a65f45efb471baae36054d9cef80d?v=167595b0409f4e49810a22bb61a00fe4>

- This week too most of my work was on the darkforest port. It is now in pretty good shape and most components have been ported completely to harmony
- Also did testing on df and made some frontend changes to the ported version
- ZKU work: Graded some background assignments, worked on minimaldf question for week 3, discord work
- Updated finances of DAO

Week 9 (20 Apr - 26 Apr):

<https://assorted-bobcat-826.notion.site/2bd39d40414049feb7c4ea343be790e9?v=b6753aea599040d2a8e2bf9ebb14dc19>

- Finally managed to get the full darkforest working on harmony testnet!
- The port is deployed at <https://ephemeral-cheesecake-94204a.netlify.app/>
 - If anyone wishes to play and test it out dm with the burner wallet address so I can whitelist you
 - The transaction page still says xdai but ones will be transacted so you need to fund the burner with some drip from the one faucet
- Other than porting work, I did some zku work - looking at 0xparc projects such as zk-mnist, providing final project feedback to some students

Week 8 (13 Apr - 19 Apr):

<https://assorted-bobcat-826.notion.site/ac812717bc9e4cfcb0ccafdce10689ca?v=6c2b098e854745589c32cfb85ca22d97>

- Most of the week was spent in scheduling and interviewing students for the ta position in next cohort
 - Interviewed k15n, Globallager, Thanks Skeleton, Alien Flip, Sigrid, 0xlws
 - Feedback in #hiring channel
- Started creating dao for minimaldf
- Did some study on solidity exploits. Re-entrancy attacks etc. so I can self-audit my code before mainnet launch
- Some promo work, contacted university blockchain groups about the next cohort. NTU responded and forwarded it to students.
- Reviewed project proposals and contacted them to provide suggestions
- Some zkdao admin work, updated dao expenses on sheet, modified script a bit.
- Restarted work on porting darkforest. Still running into some errors when switching networks to harmony

Week 7 (6 Apr - 12 Apr):

<https://assorted-bobcat-826.notion.site/35804fb09aaa471eb431ee9db70fcbe1?v=c49dbc73df114cd8b41127766f1d1ef7>

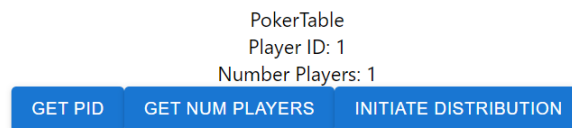
- Modified bookkeeping script. Separate expenses and income and store them separately for easy updation on sheets.
 - Updated records
- Some promo work. Mailed a few blockchain groups who had responded for last cohort promo
- Plagiarism detection
 - Research into possible moss alternatives
 - Jplag
 - Wrote a script for basic plag checking in two files
 - Won't account for variable name changes etc. but would flag direct copies of assignments
 - Issues documented in conversation with cathie on #teaching-staff-general and #LMS
- Interviewed tomo and setup interview with k15n for ta positions
 - Interview feedback:
 - 📄 Interview feedback

Week 6 (30 Mar - 5 Apr):

Timesheet:

<https://assorted-bobcat-826.notion.site/3ed6d699f82e41e08e1b836f9d5271f6?v=91b105af73a7489ba59f5e5de05c991d>

- Worked on bookkeeping.
 - Finalized a book keeping template relevant to zkdao with tosin. Template was derived from brians template.
 - Multisig harmony website doesn't provide an easy way to download all transaction data. Manually adding each of the 50 transactions metadata to the book keeping sheet is time-consuming and not scalable in the future.
 - Made a scraping tool that scrapes transactions and relevant metadata (address, amount, tx hash) from the site and converts it to a csv format.
- Did research on plagiarism detection software. Moss should work great for our purposes. Moss-taps is a modification of moss which accepts multiple assignments and compared all (not pairwise). So more scalable. Will try out both on sample submissions this week and share results
- Worked on poker project. Implemented a basic frontend and tested the smart contract functionality and integration with frontend.



Week 5 (23 Mar - 29 Mar):

Timesheet:

<https://assorted-bobcat-826.notion.site/511fd513833a4747bc55d11c59327058?v=7c533083c72c44ea84cb219da5514054>

TA duties

- Done with week 3. Graded all assignments including late ones, noted questions in doc and DM'ed results
- Tried something different this time, while grading submissions I noted down feedback, and while DM'ing results also sent the feedback on where they went wrong. Probably not feasible for all assignments and/or if the cohort size is bigger as it took some time. But I felt that it is quite helpful to students especially this week as some of the questions were theoretical and they should know why the solution wouldn't work when actually implemented.

ZKDAO

- Management work for zkdao
 - Went over proposals and commented
 - Consolidated all doc links in one place
 - Went over zkcross whitepaper and added questions
 - Looking into bookkeeping sheets
- In talks with an Indian based coding tutorial company with some focus on web3 courses for a contract to onboard more students next cohort. Will share more details once they show full interest.
- Started looking into mechanism behind auditing so we can audit each other's codes for mainnet launch

Learnt some more reactjs(Rendering, component lifecycles etc) for poker project.

Week 4 (16 Mar - 22 Mar):

Timesheet:

<https://assorted-bobcat-826.notion.site/cac1bb1d11f14623871a0c7a9cff86be?v=a838ccb3e25b45548d9f014dc6a5c1ca>

TA duties

- Week 3 TA duties - Solved queries on assignment, held office hour and started grading week 3 assignments

ZKDAO

- Reviewed my darkforest code and finally posted my grant proposal for zkdao.
- Research on investment daos - Came across two types of DAO's, VC DAO's which incubate nascent projects. These have potential for massive returns but are also very risky and require lots of research. Ex: VentureDAO. The other type of DAO's invest in assets, liquidity pools and other defi instruments. These seem more relevant to our operations. Basically, a basket of assets is chosen by dao member voting. Finally, these assets are weighted on market cap and sentiment. The sentiment component is derived from research and analyses the roadmap, potential etc of the project to arrive at a score. Both these metrics are combined and a portfolio is chosen that minimises risk

Darkforest

- Revisited porting of darkforest and made some progress. This time managed to deploy contracts to testnet and deploy the frontend. There are still issues in connecting both. I kept running into a transaction underpriced error. Will try to resolve it soon. Atleast for now the whitelisting mechanism is working.

Week 3 (10 Mar - 15 Mar):

Timesheet:

<https://assorted-bobcat-826.notion.site/8ef396a9b92944458008de1de86ec16e?v=70327b83ab094dc0ba0795d6297b8498>

TA duties

- Finished making assignment 3. Went for a different style where the questions are more solution oriented than implementation heavy. So far students gave positive feedback regarding the assignment.

- Graded Week 1 assignments. It was a cumbersome process. I realized that to scale the course we need better tools - proper course management software to handle, grade, and return assignments.

ZkDAO

- Went through the proposal and constitution of zkdao and suggested changes
- **Grant proposal**
 - Started preparing the last cohort final project for grant proposal. Checked for bugs etc.
 - Writing the proposal for MinimalDF.

Project

- Learning react for project frontend
 - Explored mui library for components
- In the last project, I made the frontend code was a mess as a result of randomly copying components and setting up events. This time learning it formally, so that frontend is more systematic.

Week 2 (3 Mar - 9 Mar):

<https://assorted-bobcat-826.notion.site/d59281d350864ec8be4698be1d500030?v=e30ba2362c7f4589993788c3266c3e3a>

TA duties and market research

- Worked on week 3 resources and assignment
- Went through the code of MACI and darkforest again.
- Mostly rewrote assignment 3. Questions seem more interesting now. Added a coding assignment for darkforest as well. The other question is focused on zk card games to emphasize on the 'fairness' theme of this week.

- Read an interesting paper on ZK-ML <https://eprint.iacr.org/2021/673.pdf>
Most of ml relies on matrix multiplications. Circom lacks templates for matrix operations, I feel there could be a strong demand for it soon. Cathie also needed such operations in her zkphoto application. If none of the students take up the project, I wish to work on this after my poker application
- Ethdatamarketplace - Cannot find a deployment of this. Pretty cool idea but not sure how useful it would be actually. Nevertheless, should be deployed on harmony. Another possible project a student can pick up.
- Went through the zkdao proposal. Excited to be a part of a DAO for the first time. The plan seems solid and sustainable. Hakwan is a meticulous planner! :D

Project

- Mostly done with the card shuffling and picking part. Not sure how long it would actually take on mainnet. The next step is to build and integrate the frontend.
- Finally received an invite key and played a bit of darkforest. Personally, not a huge game addict but their front end is very nice and addictive. The next week, me and shada will try again to deploy df to harmony testnet.

Week 1 (23 Feb - 3 Mar):

Timesheet

<https://assorted-bobcat-826.notion.site/cc5ed84a0f364911a0534ce2efacd71c?v=79070206eec2493498b9f06f0ab1dfc8>

Coursework and TA duties

This week too I was mostly involved in TA duties. Hopefully, after next week I should have more time to focus on my product launch and market research.

- Went through resources for week 3. Learnt about VRF's, multiparty computations, MACI, quadratic voting and Interrep
- Added a basic sketch for week 3 assignment. Making original questions for assignments is harder than I expected.

- Held first office hour.
- Graded week 0 assignments.

Product

- Done mostly with the smart contract part. Will start working on the frontend and integration next.
- Worked with shada and deployed the darkforest contracts to harmony testnet. The contracts are deployed but the game isn't functional yet. Hopefully, the errors will be sorted soon.

Market research

Two interesting zk products I read about are
ethdatamarketplace <https://github.com/nulven/EthDataMarketplace>
Stealthdrop <https://stealthdrop.xyz/>

The first one: eth data marketplace was particularly interesting. It seems to be a more general version of Cathie's zkphoto. A prover can submit a proof of any general property about the data for a verifier to verify and later buy the data.
Will follow up more on this product next. Could also potentially be deployed on harmony.

Week 0 (13 Feb - 22 Feb):

Timesheet:

<https://assorted-bobcat-826.notion.site/f428a0d08f8b415b8a6d9f1bfaba3d70?v=fdd24c7fc7bd4ae090589e9e817a55f3>

Coursework and TA duties

For most of this week, I gathered resources and designed assignments.

Onboarding - Collected and emailed around 20 university blockchain groups regarding the course. Unfortunately, only a few got back and forwarded the message to their members. This is probably because most groups were no longer active, or the website

displayed outdated information. Nevertheless, quite a few joined the course from the universities that got back, so it was a partial success.

Week 1 - I, along with Cathie and Shada worked on week 1. I went through blogs that explained aspects of zkp and Merkle trees for the resources section. I could find only a few good-quality blogs. Technical writing for zkp is one possible area with scope, especially as zkp gains more mainstream adoption.

We also wrote and finalized the assignment. I worked on formulating Q1 of the assignment, which was on circom. It was pretty fun to come up with questions for it. I finally settled on one that involved proving Merkle roots from leaves using circom. Since it also connects to zk-rollups, it would be a good thinking exercise for students.

The resources for circom are also pretty scant, the best one being the docs. There were no demonstration videos for it. I find tutorial videos the best way to learn a new concept/language. Hence, I made a short demo video for circom, which will be provided as week 1 resource. <https://youtu.be/Yx80SQ-AvMI>
Expanding on this and making more tutorials can be one possible contribution from zku.

Product

I launched the final project (darkforest) made for the previous course on mainnet. It wasn't as smooth as I expected it to be. Since it was pretty straightforward to deploy on the testnet, I assumed mainnet deployment would involve just changing the chain parameters. But some deployment errors kept cropping up, which magically disappeared when I tried redeploying 4-5 times.

I am also working on a mental poker game to deploy on harmony. This is quite a challenging and exciting problem. The public nature of blockchains makes incomplete information games almost impossible. Darkforest gets around this using zkp, but poker is very different. Perhaps the most challenging part is distributing a non-intersecting and random set of cards to players on a public ledger without them knowing each other's cards.

The solution seems to be using commutative encryption functions. I plan to use SRA, which is just a slight modification of the well-known RSA encryption such that it becomes commutative.

One thing I realized recently is how new this space is. There is minimal support and functionality for most tools. For example, one very frustrating issue is that there is no easy way to auto-sign small value transactions on metamask. When building

applications like games, the user frequently interacts with the contracts and generates transactions. If they need to approve each of them, manually, it can become quite frustrating.

Market research

I did not get much time for this, but I plan to take it up in the coming weeks when TA duties are fewer.