COMS 4995-001 (Science of Blockchains): Final Project: Proposal Instructions and Some Sample Topics

Project proposal instructions

By 11:59pm on Friday, March 14th, each team should submit a project proposal of length 1–2 pages. (The more specific and concrete the proposal, the better the feedback from the course staff will be.) Submissions will be made via Gradescope.

Potential project topics

Below is a suggested list of potential project topics along with links and citations to relevant sources which serve as good starting points for learning more about the topic. In particular, the links and citations provided are *not* an exhaustive list for the purposes of project requirements, and are listed to serve as gateways for a deeper dive into the topic at hand.

Students are also encouraged to dream up their own project topics (not on the following list), in which case they should run their ideas by the course staff (Naveen/Yuval/Tim) for feedback before submitting a proposal.

1. Deep dive on an existing project. This includes a detailed explanation of how the project handles and carries out consensus, execution, fees, tooling for app developers, the current ecosystem, etc. A non exhaustive list of suitable candidates includes: Ethereum, Solana, Avalanche, Mysten/Sui, Monad, Aptos, Arbitrum, Cosmos. Ethereum, Solana, Avalanche, Uniswap, Monad, Optimism, StarkNet, Arbitrum, polygon, Base, Aptos, Mysten, Espresso, Cosmos, Ritual, Succinct.

2. Ethereum scaling: Wide-ranging survey of the top (e.g. five) Ethereum L2s. [KGC+18, AAB+24], Optimism, StarkNet, Arbitrum, polygon, Base.

3. Ethereum deep dive post merge (Ethereum 2.0), and the future roadmap of Ethereum: Ethereum 3.0, beam chains, native rollups. based rollups, Native Rollups, Orbit SSF, 3 Tier Staking.

4. Survey of approaches to censorship resistance (e.g., FOCIL vs BRAID/multiple concurrent proposers). [But15, TMDM24, bra24, WMT+25, Neu23, FPR23, Fra22, Pra24]

5. Survey on *randomized* consensus protocols for asynchrony, circumventing the FLP impossibility result. [MR17, KNR24, DDL+24] and references within.

6. Deep dive into optimized versions of partially synchronous protocol (like Tendermint): HotStuff, optimistic responsiveness, good-case latency. [YMR+19, AS20, AMN+20, ALS+24, ANRX21]

7. Deep dive into non permissioned consensus: Sleepy model, proof of work, proof of stake, slashing. [Nak08, DKT+20, LR20, MMR23, DNTT22, BLR24, PS17, ET25]

8. Signature deep dive: BLS signatures, Threshold signatures, construction, properties, assumptions, etc. [BLS04, Bol03]

9. SNARK deep dive: Choose a popular SNARK (e.g. Groth16) and explain in detail how it works. [BBB+18, Gro16, GWC19, XZZ+19]

10. Deep dive into Transaction fee Mechanisms: EIP-1559, impossibility results, etc. [BGR24b, Rou24, Rou20, BGR24a, CRS24]

11. Deep dive into the Move ecosystem. Aptos, Mysten, Movement.

12. Deep dive into privacy coins focused projects: Zcash, Monero, IronFish. Zcash, Monero, Ironfish.

13. Deep dive into private smart contracts: Aleo, Aztec. Aleo, Aztec.

14. MEV focused project: In Ethereum (Flashbots, MEV-boost, Proposer-Builder-Seperation structure and ecosystem), or Solana (Jito). Jito, Flashbots, PBS original blog post.

15. Infrastructure project: Contribute to the Solana/Base/Eth ecosystem by building some non trivial tool.

16. Deep dive into L2 interoperability. Espresso.

17. Explore recent alternatives to Tendermint, such as Streamlet/Simplex [CS20, CP23].

18. Account abstraction deep dive (e.g., EIP-3074 vs. EIP-4337 vs. EIP-7702). EIP-4337, EIP-3074, EIP-7702.

References

[AAB+24] Mario M. Alvarez, Henry Arneson, Ben Berger, Lee Bousfield, Chris Buckland, Yafah Edelman, Edward W. Felten, Daniel Goldman, Raul Jordan, Mahimna Kelkar, Akaki Mamageishvili, Harry Ng, Aman Sanghi, Victor Shoup, and Terence Tsao. Bold: Fast and cheap dispute resolution. In *AFT*, volume 316 of *LIPIcs*, pages 2:1–2:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[ALS+24] Balaji Arun, Zekun Li, Florian Suri-Payer, Sourav Das, and Alexander Spiegelman. Shoal++: High throughput DAG BFT can be fast! *CoRR*, abs/2405.20488, 2024.

[AMN+20] Ittai Abraham, Dahlia Malkhi, Kartik Nayak, Ling Ren, and Maofan Yin. Sync hotstuff: Simple and practical synchronous state machine replication. In *SP*, pages 106–118. IEEE, 2020.

[ANRX21] Ittai Abraham, Kartik Nayak, Ling Ren, and Zhuolun Xiang. Good-case latency of byzantine broadcast: a complete categorization. In *PODC*, pages 331–341. ACM, 2021.

[AS20] Ittai Abraham and Gilad Stern. Information theoretic hotstuff. In *OPODIS*, volume 184 of *LIPIcs*, pages 11:1–11:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[BBB+18] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Gregory Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *IEEE Symposium on Security and Privacy*, pages 315–334. IEEE Computer Society, 2018.

[BGR24a] Maryam Bahrani, Pranav Garimidi, and Tim Roughgarden. Centralization in block building and proposer-builder separation. *CoRR*, abs/2401.12120, 2024.

[BGR24b] Maryam Bahrani, Pranav Garimidi, and Tim Roughgarden. Transaction fee mechanism design in a post-mev world. In *AFT*, volume 316 of *LIPIcs*, pages 29:1–29:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[BLR24] Eric Budish, Andrew Lewis-Pye, and Tim Roughgarden. The economic limits of permissionless consensus. In *EC*, pages 704–731. ACM, 2024.

[BLS04] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. *J. Cryptol.*, 17(4):297–319, 2004.

[Bol03] Alexandra Boldyreva. Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2003.

[bra24] BRAID by Max Resnick – Paradigm Research Workshop. Youtube, 2024. https://www.youtube.com/watch?v=mJLERWmQ2uw.

[But15] Vitalik Buterin. The problem of censorship, 2015.

[CP23] Benjamin Y Chan and Rafael Pass. Simplex consensus: A simple and fast consensus protocol. Cryptology ePrint Archive, Paper 2023/463, 2023.

[CRS24] Hao Chung, Tim Roughgarden, and Elaine Shi. Collusion-resilience in transaction fee mechanism design. In *EC*, pages 1045–1073. ACM, 2024.

[CS20] Benjamin Y. Chan and Elaine Shi. Streamlet: Textbook streamlined blockchains. In *AFT*, pages 1–11. ACM, 2020.

[DDL$^+$24] Sourav Das, Sisi Duan, Shengqi Liu, Atsuki Momose, Ling Ren, and Victor Shoup. Asynchronous consensus without trusted setup or public-key cryptography. In *CCS*, pages 3242–3256. ACM, 2024.

[DKT$^+$20] Amir Dembo, Sreeram Kannan, Ertem Nusret Tas, David Tse, Pramod Viswanath, Xuechao Wang, and Ofer Zeitouni. Everything is a race and nakamoto always wins. In *CCS*, pages 859–878. ACM, 2020.

[DNTT22] Francesco D'Amato, Joachim Neu, Ertem Nusret Tas, and David Tse. No more attacks on proof-of-stake ethereum? *CoRR*, abs/2209.03255, 2022.

[ET25] Yuval Efron and Ertem Nusret Tas. Dynamically available common subset. *IACR Cryptol. ePrint Arch.*, page 16, 2025.

[FPR23] Elijah Fox, Mallesh M. Pai, and Max Resnick. Censorship resistance in on-chain auctions. In *AFT*, volume 282 of *LIPIcs*, pages 19:1–19:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.

[Fra22] Francesco D'Amato. Pbs censorship-resistance alternatives, 2022.

[Gro16] Jens Groth. On the size of pairing-based non-interactive arguments. In *EUROCRYPT (2)*, volume 9666 of *Lecture Notes in Computer Science*, pages 305–326. Springer, 2016.

[GWC19] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. PLONK: permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. *IACR Cryptol. ePrint Arch.*, page 953, 2019.

[KGC$^+$18] Harry A. Kalodner, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten. Arbitrum: Scalable, private smart contracts. In *USENIX Security Symposium*, pages 1353–1370. USENIX Association, 2018.

[KNR24] Jovan Komatovic, Joachim Neu, and Tim Roughgarden. Toward optimal-complexity hash-based asynchronous MVBA with optimal resilience. *IACR Cryptol. ePrint Arch.*, page 1682, 2024.

[LR20] Andrew Lewis-Pye and Tim Roughgarden. Resource pools and the CAP theorem. *CoRR*, abs/2006.10698, 2020.

[MMR23] Dahlia Malkhi, Atsuki Momose, and Ling Ren. Towards practical sleepy BFT. In *CCS*, pages 490–503. ACM, 2023.

[MR17] Achour Mostéfaoui and Michel Raynal. Signature-free asynchronous byzantine systems: from multivalued to binary consensus with t< n/3, o(n^2) messages, and constant time. *Acta Informatica*, 54(5):501–520, 2017.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[Neu23] Mike Neuder. No free lunch – a new inclusion list design, 2023.

[Pra24] Pranav Garimidi. A look down ethereum's roadmap: The cases for focil and multi-proposer schemes, 2024.

[PS17] Rafael Pass and Elaine Shi. The sleepy model of consensus. In *ASIACRYPT (2)*, volume 10625 of *Lecture Notes in Computer Science*, pages 380–409. Springer, 2017.

[Rou20] Tim Roughgarden. Transaction fee mechanism design for the ethereum blockchain: An economic analysis of EIP-1559. *CoRR*, abs/2012.00854, 2020.

[Rou24] Tim Roughgarden. Transaction fee mechanism design. *J. ACM*, 71(4):30:1–30:25, 2024.

[TMDM24] Thomas Thiery, Barnabe Monnot, Francesco D'Amato, and Julian Ma. Fork-choice enforced inclusion lists (focil): A simple committee-based inclusion list proposal, 2024.

[WMT$^+$25] Sarisht Wadhwa, Julian Ma, Thomas Thiery, Barnabé Monnot, Luca Zanolini, Fan Zhang, and Kartik Nayak. AUCIL: an inclusion list design for rational parties. *IACR Cryptol. ePrint Arch.*, page 194, 2025.

[XZZ$^+$19] Tiancheng Xie, Jiaheng Zhang, Yupeng Zhang, Charalampos Papamanthou, and Dawn Song. Libra: Succinct zero-knowledge proofs with optimal prover computation. In *CRYPTO (3)*, volume 11694 of *Lecture Notes in Computer Science*, pages 733–764. Springer, 2019.

[YMR$^+$19] Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan-Gueta, and Ittai Abraham. Hotstuff: BFT consensus with linearity and responsiveness. In *PODC*, pages 347–356. ACM, 2019.