CS 856 Advanced Topics in Distributed Computing

Blockchain: Foundations and Applications

Summary

- Proposed term: W'19
- Instructor: S. Keshav
- Area: Systems and Networking
- Prerequisites: CS 454 (Distributed systems) or equivalent
- Enrolment cap: 22 (this is strict, since there will be 44 papers in the course)

Overview and objectives

This is a seminar course that examines foundations and current research into distributed ledger (blockchain) technologies and their applications. It will primarily consist of reading, reviewing, and presenting research papers. Once completed, students should be able to integrate blockchain technologies into their own research.

There will be two papers assigned to each class period (4 papers/week), selected from the following topics (a preliminary paper list can be found at the end of this document):

1. Blockchain basics
2. Bitcoin and its variants
3. Ethereum and smart contracts
4. Other permissionless blockchain technologies
5. Permissioned blockchains
6. Consensus
7. Byzantine fault tolerant consensus
8. Applications
9. Scalability proposals
10. Scalable consensus protocols
11. Blockchain in the world

Students are expected to carefully read assigned papers and come to class prepared to take part in classroom discussions. To ensure this, they must submit an online review for both papers before class. The review should summarize the paper and the issues the student plans to discuss in class. Students do not need to submit a review for the paper they are themselves presenting.

Each paper will be presented by one student in a 20-minute conference-style presentation. The presenter must submit draft slides of their presentation for the instructor to review. Comments will be returned well before class.

The student presenting the paper will also lead the class in a discussion of the paper, with assistance from the instructor, taking about one hour or so for the presentation and discussion in total for each paper. Presenters should take an adversarial position by pointing out weak and controversial positions in the paper. They should highlight the paper's contributions, any surprises, and other possible applications of the techniques proposed in the paper, while placing the work in the context of other papers covered in the course (and especially the papers covered in that particular week). The presenter should be prepared to get the discussion started by seeding the discussion with open-ended questions and perhaps some controversial statements. They will have access to reviews by their classmates before their presentation, and are encouraged to call on individuals in the class during the discussion to expand or justify their responses, based on these reviews.

All other students evaluate the presenter using anonymous presentation feedback forms, which will be given to the presenter after their presentation.

Attendance alone is not enough for the participation mark. Students must participate: as a rule of thumb, each student is expected to contribute to class discussion at least 1 or 2 times each class by asking a question, commenting on a topic, or clarifying a point. The instructor will keep track of participation by each student, which will be taken into account in computing the final grade.

Projects

Students will work in **pairs** on an original research project on a topic related to blockchain technologies. Each pair will obtain approval for their proposal from the instructor. Near the end of the term, they will present their work to the class in a 30-minute conference-style presentation including five minutes for questions. In addition, by the end of term, they will produce a potentially-publishable workshop-quality paper, 12–15 pages in length, in ACM single-spaced double-column format, describing their project.

Grading

Grades will be assigned as follows:

20% Paper presentations (10% for each of 2 paper presentations)
15% Reviews of papers
5% Reviews of presentations
10% Class participation
50% Project (10% presentation and 40% paper)

Grades will be available after the end of term through LEARN.

Preliminary paper list

The following is a preliminary list papers on the course topics that we will cover in the course. Most of the papers listed below can be accessed on-line from UW servers. Papers published in ACM journals and proceedings can be accessed through the ACM Digital Library while those published in IEEE sources can be obtained from IEEE Xplore. Springer publications (e.g., Lecture Notes in Computer Science - LNCS) can be obtained from Springer LINK.

Reading materials will be augmented by related articles from:
https://a16z.com/2018/02/10/crypto-readings-resources/

Week1: Blockchain basics

[1] Bitcoin, Beyond. "BlockChain Technology." (2015).
[2] Peters, Gareth W., and Efstathios Panayi. "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money." *Banking Beyond Banks and Money*. Springer, Cham, 2016. 239-278.
[3] https://en.wikipedia.org/wiki/Merkle_tree
[4] https://en.wikipedia.org/wiki/SHA-1

Week 2: Bitcoin and its variants

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[2 Tschorsch, Florian, and Björn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." *IEEE Communications Surveys & Tutorials* 18.3 (2016): 2084-2123.
[3] Zerocoin: Anonymous distributed e-cash from bitcoin. Miers I, Garman C, Green M, Rubin AD. S&P '13.
[4] Zerocash: Decentralized anonymous payments from bitcoin. Sasson EB, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M. S&P '14.

Week 3: Ethereum and smart contracts

[1] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151 (2014): 1-32.
[2] Buterin, Vitalik. "What proof of stake is and why it matters." Bitcoin Magazine, August 26 (2013).
[3] "Ethereum": A next-generation smart contract and decentralized application platform. Vitalik Buterin. '14.
[4] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." IEEE Access 4 (2016): 2292-2303.

Week 4: Other permissionless blockchain technologies

[1] Ripple
[2] Stellar

[3] EON
[4] IOTA

Week 5: Permissioned blockchains

[1] Androulaki, Elli, et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018.
[2] Sousa, Joao, Alysson Bessani, and Marko Vukolić. "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform." *arXiv preprint arXiv:1709.06921* (2017).
[3] Vukolić, Marko. *Hyperledger fabric: towards scalable blockchain for business*. Tech. rep. Trust in Digital Life 2016. IBM Research, 2016. URl: https://www. zurich. ibm. com/dccl/papers/cachin_dccl. pdf, 2016.
[4] Androulaki, Elli, et al. "Cryptography and protocols in hyperledger fabric." *Real-World Cryptography Conference*. 2017.

Week 6: Consensus

[1] Lamport, Leslie. "Paxos made simple." *ACM Sigact News* 32.4 (2001): 18-25.
[2] Ongaro, Diego, and John K. Ousterhout. "In search of an understandable consensus algorithm." *USENIX Annual Technical Conference*. 2014.
[3] Howard, Heidi, Dahlia Malkhi, and Alexander Spiegelman. "Flexible paxos: Quorum intersection revisited." *arXiv preprint arXiv:1608.06696* (2016).
[4] Van Renesse, Robbert, Nicolas Schiper, and Fred B. Schneider. "Vive la différence: Paxos vs. viewstamped replication vs. zab." *IEEE Transactions on Dependable and Secure Computing* 12.4 (2015): 472-484.

Week 7: Byzantine fault tolerant consensus: PBFT, Zyzzyva, Tendermint

[1] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." *OSDI*. Vol. 99. 1999.
[2] Kotla, Ramakrishna, et al. "Zyzzyva: speculative byzantine fault tolerance." *ACM SIGOPS Operating Systems Review* 41.6 (2007): 45-58.
[3] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, “Algorand: Scaling byzantine agreements for cryptocurrencies,” 2017.
[4] Tendermint

Week 8: Scalability proposals: sharding, sidechains, payment channels, Bloxroute

[1] Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." International Workshop on Open Problems in Network Security. Springer, Cham, 2015.
[2] Sidechains

[3] Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." *Draft version 0.5* 9 (2016): 14.
[4] Buterin, Vitalik, and Virgil Griffith. "Casper the friendly finality gadget." arXiv preprint arXiv:1710.09437 (2017).

Week 9: Scalable consensus protocols

[1] Li, Jialin, et al. "Just Say NO to Paxos Overhead: Replacing Consensus with Network Ordering." *OSDI*. 2016.
[2] Jin, Xin, et al. "NetChain: Scale-Free Sub-RTT Coordination." *15th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 18)*. USENIX} Association}, 2018.
[3] Rizvi, Sajjad, Bernard Wong, and Srinivasan Keshav. "Canopus: A Scalable and Massively Parallel Consensus Protocol." *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*. ACM, 2017.
[4] Keshav, S., et al. "RCanopus: Making Canopus Resilient to Failures and Byzantine Faults." (2018).

Week 10: Applications: BigChainDB, Storj, Bitcoin Covenants

[1] McConaghy, Trent, et al. "BigchainDB: a scalable blockchain database." *white paper, BigChainDB* (2016).
[2] Wilkinson, Shawn, et al. "Storj a peer-to-peer cloud storage network." (2014).
[3] O'Connor, Russell, and Marta Piekarska. "Enhancing Bitcoin transactions with covenants." *International Conference on Financial Cryptography and Data Security*. Springer, Cham, 2017.
[4] https://www.cybermiles.io/wp-content/uploads/2018/03/Technical-Whitepaper_en-US.pdf

Week 11: Blockchain in the world

[1] Korpela, Kari, Jukka Hallikas, and Tomi Dahlberg. "Digital supply chain transformation toward blockchain integration." *Proceedings of the 50th Hawaii international conference on system sciences*. 2017.
[2] Basden, James, and Michael Cottrell. "How utilities are using blockchain to modernize the grid." *Harvard Business Review* (2017).
[3] Liang, Xueping, et al. "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability." *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*. IEEE Press, 2017.
[4] Hari, Adiseshu, and T. V. Lakshman. "The internet blockchain: A distributed, tamper-resistant transaction framework for the internet." *Proceedings of the 15th ACM Workshop on Hot Topics in Networks*. ACM, 2016.