

Oracle for Research Blog

Customer Success, Recent Posts

UC Davis use OCI to boldly reimagine the fabric of blockchain

December 7, 2022 | 4 minute read



Mohammad Sadoghi

Associate Professor, Department of Computer Science, University of California, Davis



There's been a lot of media discussion about blockchain over the last several years, particularly in the context of the ever-fluctuating cryptocurrency market. But what is blockchain technology really? Put simply, blockchain is a computer network that grant uniform privileges for the computers in a given network. In a totally decentralized system, no one computer has more privileges than any other. This results in an equitable system free from administrators and managers regulating the network according to their own set of rules. Instead, the participating computers must all follow the same rules, or 'protocols', to take part in the network.

When a majority of the computers in the network agree on the validity of a transaction, this is called 'consensus.' Blockchain systems should be in agreement about the validity of transactions periodically using consensus algorithms, such as Proof-of-Work (PoW) or [Practical Byzantine Fault Tolerance \(PBFT\)](#), to continue operating even if some of its nodes fail or act maliciously. In addition, some computers may not conform to the rules of consensus protocols, so this possibility needs to be accounted for during the blockchain network design phase.

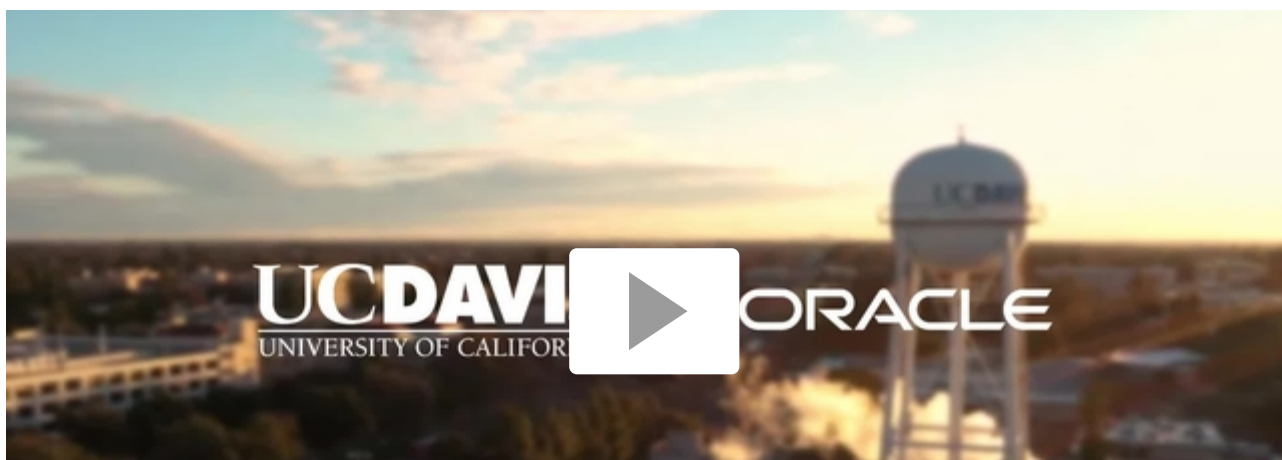
Blockchain is proving to be a powerful technology with the potential to disrupt diverse fields such as finance, commodity trading, agriculture, identity management, land ownership, aid delivery and health care. This widespread interest is rooted in the fundamental guarantees that blockchain offers, namely, transparency, integrity, and resiliency, all of which must be inalienable data rights of citizens. I would argue these rights can be respected through the decentralization and democratization processes that are the cornerstones of today's modern society. The inception of Bitcoin and blockchain have renewed the vision of a democratic and decentralized computational paradigm, ingraining privacy, integrity, transparency and accountability into the very fabric of the computational model. Recent developments in blockchain technology have also inspired innovative new designs in resilient distributed and database systems.

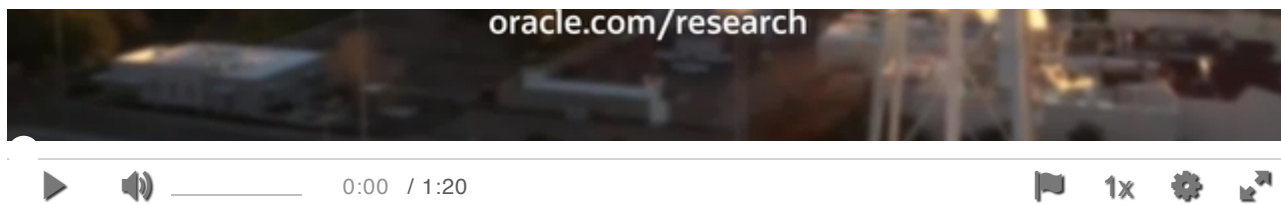
At the heart of this paradigm shift lies a family of Byzantine-tolerant consensus protocols, a classical distributed theory problem that has failed to fulfill the needs of high-performant modern applications. Unfortunately, existing consensus protocols are not designed to deal with geographically diverse deployments in which many networked computers spread across a geographically large area participate in consensus.

Reinforcing democracy and decentralization in blockchain

To close this gap, my team at UC Davis have boldly re-imagined the entire blockchain fabric through a scale-centric lens in [ResilientDB](#). For this project, we're focusing on a new data management landscape centered around a democratic and decentralized model, a catalyst for verifiable computational trust, by developing a global-scale, fault-tolerant blockchain fabric. We re-architected and re-imagined the modular system design from scratch, embedding parallelism and deep pipelining at every layer to fully exploit modern hardware and cloud infrastructure globally. At the core of our project lies a replicated data model - a 'distributed ledger' - on which the truth can only be derived and persisted by consensus among participants, a process resilient to any malicious minority.

UC Davis boldly reimagine the fabric of blockchain with OCI





Despite the recent growth of blockchain technology, many platforms continue to rely on unsustainable protocols [such as Proof of Work \(PoW\)](#) for deciding how and what should be added to the ledger. PoW protocol requires its participants to perform massive computations and leads to massive energy wastage. Existing solutions to replace the PoW protocol make use of the Proof-of-Stake (PoS) protocol or traditional BFT consensus protocols. However, the safety of the ledger created by PoS or BFT protocols is at the mercy of the long-term safe-keeping of the private keys of participants subject to long-range attacks. To ameliorate this situation, we have developed a novel HybridChain architecture, which requires each client transaction to undergo two consensus protocols: a BFT consensus followed by our novel [Power-of-Collaboration \(PoC\)](#) protocol that gives rise to sustainable collaborative mining. On a large-scale Oracle cloud deployment, we observe that our HybridChain system outperforms state-of-the-art blockchain systems yielding up to 2000x higher throughput and 10^5 times less energy costs.

The broader societal impact of our new blockchain system will be to eliminate the need for a centralized data gatekeeper that can overcome the trust barrier, and instill the power of privacy in the hands of the rightful owners of the data, the people. We have facilitated the creation of an undergraduate club called [Blockchain At Davis \(BAD\)](#), taken an advisory role to [Blockchain Acceleration Foundation \(BAF\)](#), and partnered with MouseBelt Blockchain Accelerator, all aimed at diversifying blockchain education across campuses. We are fostering interdisciplinary collaborations among undergraduate students, out of which we plan to mentor projects focused on sustaining our environments (e.g., building decentralized applications to incentivize water and waste management over a blockchain). The final key outcome of this project will be to substantially enhance infrastructure through the commitment of maintaining ResilientDB as [an open-source project](#).

Oracle for Research assists with technical collaboration and scalability

In the past 6 years of using various cloud solutions, no other provider offered a team of Research Advocates and Solutions Architects to help get our projects up and running on the cloud. Christine, Nathan, and Bryan really stood out with lots of great ideas and helpful communication that made the experience so warm and personal.

From a technical perspective, OCI stood out for its bare metal offering – this enabled our low-

level programming close to the kernel. These bare metal servers also provided the isolation, visibility, and control we needed by using dedicated compute instances. Oracle’s servers provided high core counts, large amounts of block storage and SSDs, and high bandwidth, accommodating hundreds of replicas. We simply couldn’t have accessed this type of scalable compute power in house.

~

[Oracle for Research](#) offers products, capabilities, and resources purpose-built for research to simplify the research process and accelerate discovery around humanity’s most urgent needs. Through our research-first, partner-centric approach, we make computing paradigms more powerful and user-friendly, data easy and accessible, and community resources invaluable and actionable. We help researchers in academic, commercial, and federal settings, across all research disciplines, explore novel ways to achieve ground-breaking results to make the world a better place.



Mohammad Sadoghi
Associate Professor, Department of Computer Science, University of California, Davis

Professor Sadoghi’s research spans all facets of secure and massive-scale data management. He leads the ExpoLab Research Group with the aim to pioneer a resilient data platform at scale, a distributed ledger centered around a democratic and decentralized computational model that further aims to unify secure

[Show more](#)

[◀ Previous Post](#)

Resources for	Why Oracle	Learn	What's New	Contact Us
About	Analyst Reports	What is Customer Service?	Try Oracle Cloud Free Tier	US Sales 1.800.633.0738
Careers	Best CRM	What is ERP?	Oracle Sustainability	How can we help?
Developers	Cloud Economics			Subscribe to Oracle Content

Investors	Corporate	What is	Oracle COVID-	Try Oracle Cloud
Partners	Responsibility	Marketing	19 Response	Free Tier
Startups	Diversity and	Automation?	Oracle and	Events
	Inclusion	What is	SailGP	News
	Security	Procurement?	Oracle and	
	Practices	What is Talent	Premier	
		Management?	League	
		What is VM?	Oracle and Red	
			Bull Racing	
			Honda	