Vandeveer Chair Public Lecture In Economics

Bitcoin's Legacy and Blockchain's Future

John P. Conley
Vanderbilt University

November 10, 2022

SIU Southern Illinois University
CARBONDALE

Money and Banking

Your money is not yours.

At least you don't really control it.

Money and Banking

- Banks decide what your account balance is.
- Banks can shut down your access.
- Banks are centralized custodians of **Fiat Currency** issued by Central Banks, and answer to them.
- Banks can make mistakes and authorize transactions you did not agree to.
- Banks can be hacked, or be sloppy with their security systems.
- Banks can simply be dishonest.

Money and Banking

Banks almost always comply with the demands of courts and governments.

Money and Banking

- China has locked millions of customer accounts in response to a liquidity crisis.
- Canada locked accounts of protesting truckers.
- Banks refuse to work with the cannabis business.
- PayPal often locks merchant account balances, or closes accounts, at whim.
- Visa refuses to process charges for companies or political organizations they disagree with.

Fiat Money and Privacy

Even if you have access to your accounts, and your money, everything you do is tracked and recorded by some combination of:

- The Fed's **Automatic Clearing House (ACH)**.
- Visa, Master Card, and American Express.
- Google, Apple, or other wallet providers.
- Your bank.

Fiat Money and Privacy

- You, and everyone you deal with, has had to pass **Know Your Customer/Anti-Money Laundering (KYC/AML)** checks.
- You have no privacy.
- All your financial activities are tied to your true, verified, identity.
- Many of your transactions are reported to the government as a matter of course.
- all are discoverable by government order.

Does it Matter?

How would your survive if your
phone, credit cards, and bank account
were locked?

At best, you would have live entirely cash-based existence.

You would be cut off from the internet, access to capital.

You could not work for anyone who won't pay cash.

What you financial information say about you?

- How much do you drink?
- What prescriptions do you buy?
- Who do you donate to (politics, religion)?
- What books do you read?
- What sites do you subscribe to?
- Do you have children in your home, or aging parents?

What you financial information say about you?

There not much to know about you that is not evident in your financial life.

This may show that you are "wrong" sort of person to be a school teacher, a banker, to work for the government, or join the military or police force.

What you buy today may lower your future social credit rating.

Yikes!

Money is the leading example of how vulnerable we become when we rely on centralized systems.

Yikes!

- If there is no competition, we live at the pleasure of the central authority in control.
- Or worse, the government and other entities that have coercive power over these authorities.
- You have to agree to any terms of service they offer.
- In the case of fiat finance, this means complete surveillance, and no financial privacy.
- Your data may or may not be shared routinely, you can never know.

What to do?

Bitcoin started in 2009

Provides a decentralized, digital currency alternative to fiat or central bank currencies like the dollar.

Bitcoin

- Well-defined, and independently verifiable, rules for what makes transactions valid.
- The ledger is public and auditable.
- Once a transaction if marked as valid in a block, it is irrevocable.
- No one can change a balance in a ledger account record
- No one can prevent the person with the correct credentials from accessing the account.
- No one can prevent you from transacting with any other account.

Decentralized Consensus

Bitcoin uses a consensus mechanism called **Proof of Work (PoW)**.

PoW incentivizes nodes/miners/validators to:
maintain and update the ledger honestly
agree on a correct consensus view of its contents

This contrasts with the "my view or the highway" approach of commercial banks.

Why Decentralization?

The goal is to

- Allow People who have never met and have no reason to trust each other, to transact securely without the need for an intermediary, such as a bank.
- Limit financial surveillance.
- Allow exchanges of value to take place without the need for the permission of the government, a bank, or any other central authority.

But Bitcoin Boils the Oceans!

Bitcoin is a big step in these directions, but has a number of flaws.

- It is only pseudo-anonymous.
- It is difficult to use.
- It has certain flaws in its incentive structures that may ultimately cause it to fail.
- It is expensive, recently one to 2 dollars per transaction.
- It is slow, at most, 5 transaction per second, and can't scale up.
- It uses a huge amount of electricity, 132 TWh of energy in 2021, about the same as Argentina.
- It is mostly limited to exchanges of value, that is financial transactions.

Ethereum Saves the Day?

Ethereum started in 2015

Used about 76 TWh in 2021 for its PoW consensus mechanism.

Is slightly faster, up to 12 TPS.

Is more costly with transactions fees ranging from $.50 to $20.

Otherwise, Ethereum has similar features and flaws as Bitcoin, with one major difference:

How amazing are Smart Contracts!

Nick Szabo's idea of capturing the intentions of two untrusting parties in code that can be executed remorselessly, without fear or favor, on a blockchain is powerful.

In principle, **Turing Complete** programing languages like **Solidity** for smart contracts make blockchain capable of anything.

I'll detail examples below, but here is an incomplete list:

- Crypto-tokens that power thousands of blockchain projects, carbon credits, loyalty points, etc. (ERC20).
- Non-Fungible Tokens, Bored Apes, IP rights transfer, and more (NFT).
- Decentralized currency exchanges (DEX).

- Decentralized finance, peer to peer borrowing and lending (DiFi).
- Logistics, provenance, and chain of custody (Decentralized Business Processes).
- Government and corporate transparency and accountability (Attestation Services).

Unfortunately, all is not well in paradise.

What’s Wrong?

PoW is costly, environmentally questionable, and can’t scale to the level needed to have any meaningful widespread impact.

Many alternative consensus mechanisms have since been developed:

- Proof of Stake (PoS)
- Proof of Authority (PoA)
- Proof of Honesty (PoH)
- Various lightning, bridge, and sidechain solutions
- Many other variations on these

These are cheaper, can scale to a greater extent, and have smaller environmental impact.

What's Wrong?

Ethereum recently moved to from a PoW to a PoS Consensus mechanism largely for environmental reasons.

Unfortunately, the security models are often not as good.

Implicit centralization, or least, de facto concentration of power, and the creation of single points of failure, are common.

But, Smart Contracts, Right?

Executing smart contracts on a **World Computer**, with thousands of machines, is resource intensive.

Smart contacts make too many things possible.

They have proven to be a major attack surface and point of failure.

Oh, Well

In practice, smart contracts rely on implicit trust layers regarding the honesty and competence of contract developers. The results are mixed at best:

- DAO, June 17, 2016: 3.6 million ETH worth $79.6 million, (now about $6 billion)
- Parity, July 19, 2017: 150,000 ETH, worth, $30 million. (now $259 million)
- Estimated total losses in 2021: $680 million (Exploring Security Practices of Smart Contract Developers, T Sharma, Z Zhou, A Miller, Y Wang, arXiv preprint arXiv:2204.11193, 2022 – arxiv.org)
- Estimated losses in the first half of 2022: $1.25 billion. (Defiyield rekt database)

What is Blockchain Really about?

The legacy is may be mixed, but the future is much more promising.

A <u>decentralized currency</u> was the first application of Blockchain.

This was chosen because what blockchain really provides a generalized a data technology with a number of very special properties:

- Secure
- Auditable
- Immutable
- Difficult to censor
- Distributed and decentralized

What is Blockchain Really about?

Put another way: blockchain is a data service.

Provides: trustless, reliable, and verifiable **Source of Consistency**

Without: the need for a centralized, **Trusted Data Intermediary** (TDI) such as your bank, Google, or Oracle.

Blockchain Use Cases

Some examples of what Blockchain as Data Service can provide:

Logistics Provenance, and Chain of Custody services.

Consider the movement of a container of bananas from Honduras to a Walmart warehouse in Chicago. The container is packed by a farmer, picked up by a trucker, inspected and cleared by Honduran customs, loaded by longshoremen, transported on a cargo ship, unloaded … trains … trucks … Walmart … a bowl of cornflakes.

- Who keeps the records of that track the location of, and responsibility for, the container?
- Who decides who gets access to these records, and who gets to update them?
- Why would any of these actors trust one another not to alter or censor records?
- How do the different the data systems of all these stakeholders even communicate effectively?

Decentralized Data Services are the Future

Blockchain allows the creation of **Cryptographically Signed Attestations**.

An agent starts with a document, a receipt, an acceptance of custody, agreement to a contract, a reading from a sensor, or anything else.

- Signing it makes it non-reputable.
- Putting it into a blockchain that makes it immutable, and publicly visible, to all parties.
- In the logistics application, each agent cryptographically signs an attestation that he received the container in a certain condition, in a certain place, at a certain time.
- If this attestation does not appear in the ledger, it is clear to all parties where the holdup is.
- If the attestation does appear, then the signer, is responsible until the next agent in the system signs an attestation of acceptance.

More

You can see how this might be used in similar applications:

- Distribution/Chain of Custody for opioids and other controlled substances.
- Proving the provenance of organic produce.
- Distributed business processes like real-estate transactions.
- **Internet of Things (IoT)** telemetry produced by alarms, monitors, medical devices, power transformers that may spark and cause wildfires, and so on.

Even More

Blockchain can do many other things:

Fungible Tokens (ERC20, in the case of Ethereum) that can fund activities on blockchain and decentralized application platforms, serve as loyalty points, poker chips, backed scrip for microcredit, development, or disaster recovery projects. TDIs are not required. In fact, these currency-like applications do not require any all between parties to be effective.

Non-Fungible Tokens (NFT) that might represent ownership of art, music, or IP rights. More interestingly, NFTs can represent stocks, shares of physical assets, or deeds and titles to real property.

- Blockchain allows provable, secure ownership without a government entity or other TDI.
- Transfer of ownership is entirely in the hands on the owner. mediated and provable on the public, immutable ledger, and cannot be manipulated by governments or other powerful entities. Exchange is governed decentrally.

Transformative Value Chains

Accepting credit cards requires a merchant account, KYC/AML, and paying a fixed fee of $.25 + 3% per credit card transaction.

Content creators would have to be large enough to make it worthwhile to get a merchant account, and even then, payments of less than $1 are either infeasible, or not worthwhile.

Credit cards, and all other existing payment rails, cannot be used for the small, sub-dollar payments required for direct user to creator markets to exist.

Legacy Platforms

Google and YouTube exist largely because they are effective transactions aggregators.

You can’t collect tenths of a cent from someone who watches a video. Revenue models depend on either paid subscriptions or advertising.

Platforms can accept credit card payments for subscriptions.

Platforms can also negotiate deals for advertising and again collect multi-dollar payments.

Platforms can then divide some part of this among their content creators. Again, the payments are measures in dollars.

Micropayments and the Peer-to-Peer Economy

If blockchain can be made to scale (thousands or hundreds of thousands of transactions per second) and become cheap (hundredths of cent per transaction), something entirely new becomes feasible:

Micro-Value Chains

Who Needs the Center?

Cheap, scalable, blockchain makes **Micropayments** a reality.

If a blockchain makes it possible for a user make a micropayment of 1/10¢ for a 1/100¢ transaction fee, a world of decentralized peer-to-peer exchange becomes possible.

The Amazons, YouTubes and Instagrams lose the financial leverage that allowed them to become gatekeepers.

Users can make small, one-time payments, or stream small payments to service providers for content, search services, personal services (piano lessons, or tutoring, for example), or storage and distribution of their own content.

This kind of blockchain will be a key part of the foundation of the decentralized, privacy protecting vision for Web 3.0 that many hope for.

We have to Walk before we Run

Blockchain is still is a young technology, but is rapidly evolving. We are heading in directions that make blockchain:

- Cheap
- Scalable
- Much greener
- Easier to use
- At least as secure as PoW using better consensus mechanisms
- More decentralized and immutable
- Crucially, able to offer more than just simple currency transactions without exposing users to the many attack vectors of Smart Contracts.

Conclusion

The world is becoming more centralized every day, and this disempowers us all.

Blockchain is the only significant, emerging, technology that moves us away from centralized power and control.

It creates the possibility of living in a world where financial surveillance has no place, and where central powers do not control all the key crossroads that make modern technological existence possible.

Building on blockchain make is possible to take power back from the center, and live our lives as we wish without asking permission.

Many thanks for your Attention!

Bitcoin's Legacy and Blockchain's Future

Abstract

The world is becoming increasingly centralized. We have fewer platforms to choose for our financial, social, technological, of informational needs every day. We have to accept whatever terms and conditions they impose. Bitcoin uses blockchain to break free of this in the financial realm. While Bitcoin has many limitations, it is only one possible use of more generalizing distributed ledger technology. New developments expand these possibilities to all types of trustless, decentralized interactions. Blockchain is fundamentally a source of data consistency that offers a foundation for new types of platforms that empower individuals, and allow us to live our lives as we choose without requiring permission from central authorities.