Lecture 1: Private Money & Stable Coins

*Current State of Affairs: Traditional Finance*

Not Universally accessible, Expensive, Technologically Complex, Cross border payments are slow

*Private Money* Not controlled by any central entity, Clear definition of value, Trustless

*What do we need from money?* Wide availability, Low to no cost, Transparency, Value clearly defined

*What do blockchains offer?*

Availability, Transparency, Speed, Security, need solution to value

*Stablecoins* Digital assets backed by real assets, Designed to maintain a stable value

* Like Defi because independent, low cost, fast
* Like Tradfi because low vol, familiarity?

Medium of Exchange, Store of Value

* They are cryptocurrencies and software
* Value is governed by smart contracts

*Trilemma*

1. Capital Efficiency 2. Stability (vol) 3. Decentralization

*Four Types of stablecoins:*

1. Fiat-collateralized stablecoins

* Backed by reserve of fiat currency (ex: USD)
* Benefits: simple, stable, low vol
* Cons: counterparty risk, lack of regulations
* High levels of capital efficiency and stability but managed by a central entity

1. Crypto-collateralized stablecoins

* Backed by a basket of other cryptocurrencies
* Benefits: decentralized, doesn’t require a custodian, no regulations

Cons: crypto backed is more complex, must be over-collaterized

* Offer stability, decentralization, but not capital efficient

1. Algorithmic stablecoins

No association with collateral: algorithms maintain the peg

* Price discovery and supply adjustment
* Benefits: No collateral is required, so extremely capital-efficient
* Disadvantages: complex implementation often requires a governance coin
* Offer high-level of decentralization and capital efficiency, little stability guarantees via complex logic

1. Commodity-backed stablecoins

Backed by a reserve of commodities: gold, real estate or oil

* Benefits: real assets, relatively stable, tokenization brings more liquidity to the market
* Cons: centralized, must undergo audit

Lecture 2: Crypto as an Asset Class and Blockchain Innovation

*What is the value?*

Money? Commodity (something with intrinsic value or utility)? Equity?... separate asset class!

Blockchain: way to arrange bits of data (aka transactions) such that they depend on each other, this dependence is based on their content and temporal order

Transactions are batched into blocks. Subsequent block contains a “fingerprint” (hash) of the previous block, so they are linked in a linear sequence

Blockchain DAG: a transaction ledger!

*Distributed Ledger & Consensus*

Shared by multiple independent actors: everyone has the same copy

Reaching a consensus: having everyone agree on transactions and their sequences

* Must trust either each other or 3rd parties
* If 3rd parties: pay them for services, rely on honesty, share data with them

Trustless consensus: no intermediaries. Problems are: big world, world is parallel, miscommunication, malfunction, malicious actors

Byzantine General Problem: game theory, scenario 1: coordinated attack leading to victory, scenario 2: uncoordinated attack leading to defeat

Classic consensus: too much communication, more actors = harder to achieve consensus

Nakamoto consensus: proof of work: distributed consensus protocol where independent network participants perform “work” to build and broadcast blocks and validate transactions, growing the chain and getting rewards for the work done.

Only one, the longest chain, is selected as the “true” one at any time.

If honest participants are majority, the combined resources they commit outweigh the resources of the bad actors, securing the network. No need to communicate.

Bitcoin innovation: trustless decentralized consensus

Lecture 3: Blockchain Innovation Continued…

Decentralized consensus: goal is to make it impractical for any single malicious actor to have enough resources to attack the network. In true decentralized network you cannot force them, but you can incentivize them!

Proof-of-stake: committing something else instead of physical resources, blocks added by committing money

Blockchain -> global distributed state machine

Distributed computer -> state machine as well

Generalization … transaction = smart contracts

*What is the key innovation of Ethereum?*

Expand blockchain state to be generic and add programs that manipulate it

Smart contracts: programs that operate on the distributed state machine of blockchain, causing state transitions -> new computing platform

* Bitcoin also has “smart contracts” … not so smart
* Each network node executes smart contracts so they know the state… nodes compensated trough fees (explicit cost)
* Code resides on the blockchain, created by a special transaction

Blockchain is secured by trustless consensus. Anyone can join. Anyone can program. Anyone can support & get rewarded.

Network participants = the identity… this is key!

Cryptography: A way to prove the identity without revealing it, data proofs, data representation and linking, way to compress the data history

Lecture 4: Asset Tokenization

Everything is an Asset.

*How is asset ownership recorded?*

Traditionally, Many middleman involved, lots of paperwork, transfer is complex and costly, ownership is nor divisible

Blockchain: transparent, provable, reliable, easy transfer, visible to everyone, but only the owner can manipulate.

*Tokenization of Real World Assets?*

Virtual counterparts of physical assets like property, art, and treasuries

Converting rights to assets into digital tokens makes them tradeable on a blockchain

Benefits: securely and reliably bought, sold, and traded using blockchain tech, effectively increase liquidity as well as lower costs and transaction times across markets, operate with speed and efficiency, democratized ownership, better transparency and global accessibility, can buy fraction of total

One of the fastest growing segments of DeFi

Currently a market of 1 trillion in 2023, 2030 expected to be at over 16 trillion

Captures the essential and specific properties of an asset such as measurements, expiration date, underlying price, entitlements

1. “off-chain” representing ownership of physical asset
2. “on-chain” token, solely existing within the digital realm

*RWA Tokenization Infrastructure*

Blockchain Technology, Legal and Regulatory frameworks, Security and Identification, Blockchain network data (on chain data), Oracles (off chain data)

*Tokenization Process*

Identify and Verification -> Legal Structuring and Compliance -> Token and Smart Contract Creation -> Distribution and Trading

*Benefits of Tokenization*

1. Tokenizing RWA creates opportunities for both asset managers and investors by offering cost savings, expediting transaction processes, and creating more equitable market
2. Efficient transactions
3. Greater Liquidity
4. Lowered Costs
5. Transparent environment
6. New financial products

Lecture 5: Chain Properties and Value

*Chain Properties*

1. Scalability

Many things happen in parallel, how to achieve one shared state quickly? Fork reconciliation takes time, to solve this without sacrificing decentralization -> Scalability: level 2 : do not “commit” them to the chain right away, batch of conflate them first… this can be done on a localized blockchain

Ex: multiple buys and sells on the same account, the balance shrinks and grows back and forth, final balance is recorded as a single change, bitcoin lightning is like this.

Partitioning

* Subnets: custom rules for network nodes, security model (Avalanche, cosmos, Polkadot)
* Shards: partition by various criteria to cope with transaction volume

1. Decentralization: a big deal?

* Limited control over resources and costs. Everyone competes for the same network resources
* Generic security, by not trusting anyone, you trust everyone

1. Centralization (to some degree)

* Common rules of engagement and participation
* Super nodes: well known entities that everyone trusts

1. Security

* Bitcoin has never been broken or hacked
* Often most popular is one that succeeds!

*Value Factors*

1. Specific purpose it serves: payment method? Trading?
2. Consensus: expensive to run? Vulnerabilities?
3. Adoption rate, usage: some not more than white paper

Killer app: something lacking at moment

1. Technical strength: speed, cost, attacks
2. Governance: how easy to make changes to the code

*“Off-chain” factors*

Supporters, funding and treasury, profit generated, media coverage, institutional investor interest

Lecture 6: Price Discovery and Market Places

*Price Discovery*… price matters only together with quantity that is being offered, price without quantity is meaningless

Slippage and Volatility: commitment to buy/sell large quantity has more “weight,” large orders can absorb more demand/supply

Liquidity: aggregated quantity at different price levels

* Higher liquidity -> better price stability, better execution quality
* Lower liquidity -> high volatility (price movement)

*Supply/Demand Interplay. Market Makers*

* Higher demand: buyers compete and bid higher prices to attract sellers
* High supply: buyers lower their prices and wait for sellers to hit their bids… sellers offer lower to attract buyers

An important service because it provides liquidity

*Price transparency*

Transparent process: everybody sees bids and offers changing

* Transactions are informed: price is fair

*CEX Centralized exchange:* the traditional way

Order Book: collection of standing orders form

“Centralized” book: the exchange maintains the books and server as intermediary

* Controlled by a concrete authority that defines rules

CEX Advantages: speed, central authority is a guarantor of rules, mediating “disputes” protecting against bad actors, vital for institutional and retail: managed counterparty risk, simplicity of use, enforced know-your-customer

CEX disadvantages: central point of failure, lack of transparency in how the central authority operates, security risks: loss of client data, trader money is locked in the exchange custody, the central authority keeps the clients’ funds in its own wallet

*Decentralized exchanges (DEX):* not your keys – not your money…marketplace in which trading activities are blockchain transactions, the exchange is a smart contract, orders are transactions sent to the exchange’s contract

DEX advantages: the key feature is participants interact with one another on a peer-to-peer basis, no intermediary and no entry barriers: market access for all, fewer parties interacting – less risk, safety and security of the blockchain, anonymous, lower fees

DEX disadvantages: lower speed, blockchain transactions are (still, relatively) slow, easier arbitrage: takes time for price information to propagate between different marketplaces, low liquidity levels (less popular for now) -> lower price stability, high volatility, unpredictable fees, dependent on the network load, intrinsic front-running opportunities, bugs and scams

Lecture 7: Crypto Market Places and Market Makers

Transactions are a signal (even if unconfirmed

Funds moving from wallets to exchanges: bear signal

Dark Pools: submitted transactions are visible to all … go off-chain, private, permissioned mempools

Private pools -> loss of transparency of the network, concentration of control

Automated Market Makers… attempt to solve a problem of low liquidity and high cost of trading (through fees).. get code to help with liquidity … price determined algorithmicly

* The relative price of an asset against another asset is a direct reflection of the supply/demand (im)balance

AMM disadvantages: “impermanent loss”: price depends only on asset balance in the pool, it can fluctuate significantly from the “real” market price and can also be manipulated, large trade causes significant price impact, front running in the CPAMM is always profitable … intrinsic problem. UST (Luna) Failure

WHAT IS HERE?!?