DeFi and the Future of Finance:
2. DeFi Infrastructure

Campbell R. Harvey
Duke University and NBER

Outline

- Blockchain
- Cryptocurrency
- Smart contracts
- Oracles
- Stablecoins
- dApps

Blockchain

What is blockchain?

- Blockchains are fundamentally software protocols that allow multiple parties to operate under shared assumptions and data without trusting each other.
- These data can be anything, such as location and destination information of items in a supply chain or account balances of a token.
- Updates are packaged into “blocks” and are “chained” together cryptographically to allow an audit of the prior history, hence the name.

Blockchain

Why are blockchains special?

- Blockchains have consensus protocols (a set of rules that determine what kinds of blocks can become part of the chain and become the “truth”.)
- Once in a blockchain, the data remains there forever. This is the immutability property.
- These consensus protocols are designed to be resistant to malicious tampering up to a certain security bound.

Blockchain

Proof of work

- Ethereum currently relies on *Proof of Work (PoW)* consensus protocol, which relies on a computational lottery to determine which block to add. The participants agree that the *longest chain* of blocks is the truth.
- An attacker needs to amass 51% of the network computational power (this is the boundary of PoW security).
- Given the massive computational power of the Ethereum and Bitcoin networks, it is extremely unlikely that a malicious actor (or even an entire country) can attack these networks. This is not true for other less popular networks

Blockchain

Mining

- The computational lottery involves cryptographic hashing.
- Miners group transactions together, make sure they are valid, and add a small piece of metadata called a nonce. They run a hashing function (SHA-256 in Bitcoin and Keccak-256 in Ethereum) and try to get a very small value of the hash by cycling through different nonces.
- This task is computationally burdensome. However, when a miner wins it is very fast to verify that the transactions + nonce = winning hash. When verified, a new block is added.

Cryptocurrency

What is cryptocurrency?

- Cryptocurrency is a digital token that is cryptographically secured and transferred.
- Asymmetric key cryptography is a crucial component. Owners of cryptocurrency have a private key which is essentially a long random number.
- A public key is mathematically derived from the private key. This is a one way operation (you cannot – using today's technology) derive the private key from the public key)

Cryptocurrency

What is cryptocurrency?

- Public addresses are derived from the public key
- If currency is transferred, the sender uses a digital signature algorithm to sign the token over to someone else's address. The signature mathematically reveals that the sender has the private key associated with the senders public address.
- The token will now reside with the receiver and it can be transferred again using the receivers digital signature based on the receiver's private key and a new party's address.

Cryptocurrency

What if you lose your private key?

The New York Times

Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

By Nathaniel Popper

Published Jan. 12, 2021 Updated Jan. 14, 2021, 4:25 p.m. ET

Cryptocurrency

What if you lose your private key?

The New York Times

Of the existing 18.5 million Bitcoin, around 20 percent — currently worth around $140 billion — appear to be in lost or otherwise stranded wallets, according to the cryptocurrency data firm Chainalysis. Wallet Recovery Services, a business that helps find lost digital keys, said it had gotten 70 requests a day from people who wanted help recovering their riches, three times the number of a month ago.

https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html

Smart contracts

Enhanced capabilities

- Bitcoin is a payments technology.
- Ethereum is the primary example of a smart contract platform.
- A smart contract is code that can create and transform arbitrary data or tokens on top of the blockchain of which it is a part.
- The concept is powerful because it allows the user to trustlessly encode rules for any type of transaction and even create scarce assets with specialized functionality.

Smart contracts

Trustless

- Many standard business contracts can be algorithmically encoded and algorithmically enforced
- These contracts run on the Ethereum blockchain and are run on every node.
- This is not just useful for finance. For example, supply chains are another good example

Smart contracts

Gas

- Users of smart contracts need to pay a fee, called gas.
- The gas price depends on the complexity of the calculation (think of a fee for using a cloud computing platform)
- Gas fees also help protect attacks on the system that cause an infinite loop of code (known as a halting problem)

Smart contracts

Turing complete

- The car analogy is useful
- Suppose the car is stuck on auto pilot. The limiting factor is the gas. When the gas runs out, the car stops.
- Gas plays a very important role. A malicious attack would be prohibitively expensive.
- Ethereum is Turing complete – Bitcoin is not

Smart contracts

ERC

- Ethereum Request for Comment or ERC refer to standard interfaces for different types of functionality
- Most popular is ERC-20 which defines an interface for tokens whose units are identical in utility and functionality. It includes behavior such as transferring units and approving operators for using a certain portion of a user's balance.

Smart contracts

Important ERCs

- ERC-20 is a fungible token. Traditional examples in fiat are $1 bills all have equal value (though different serial numbers) and 10 $1 bills are equal to a $10 bill
- ERC-721 are non-fungible. Each token is associated with a particular asset (for example, a loan).
- The benefit of these standards is that application developers can code for one interface, and support every possible token that implements that interface.

Oracles

What are oracles?

- Ethereum blockchain only knows what happens on the Ethereum blockchain. What is information is needed from outside the Ethereum blockchain? An oracle solves this problem.
- An oracle, in the context of smart contract platforms, is any data source for reporting information external to the blockchain.
- How can we create an oracle that can authoritatively speak about off-chain information in a trust-minimized way? This is known as the oracle problem.

Oracles

Oracle implementations

- An application might host its own oracle. This does not solve the trust problem
- One Ethereum-based platform known as Chainlink is designed to solve the oracle problem by using an aggregation of data sources. The Chainlink whitepaper includes a reputation-based system that is decentralized.

Stablecoins

What are stablecoins?

- Bitcoin and Ethereum are excessively volatile
- Stablecoins are intended to maintain price parity with some target asset, e.g., USD. Stablecoins provide the necessary stability that investors seek to participate in many DeFi applications
- They also allow a cryptocurrency native solution to exit positions in more volatile cryptoassets.
- They can even be used to provide on-chain exposure to the returns of an off-chain asset if the target asset is not native to the underlying blockchain (e.g., gold, stocks, ETFs).

Stablecoins

Fiat collateralized stablecoins

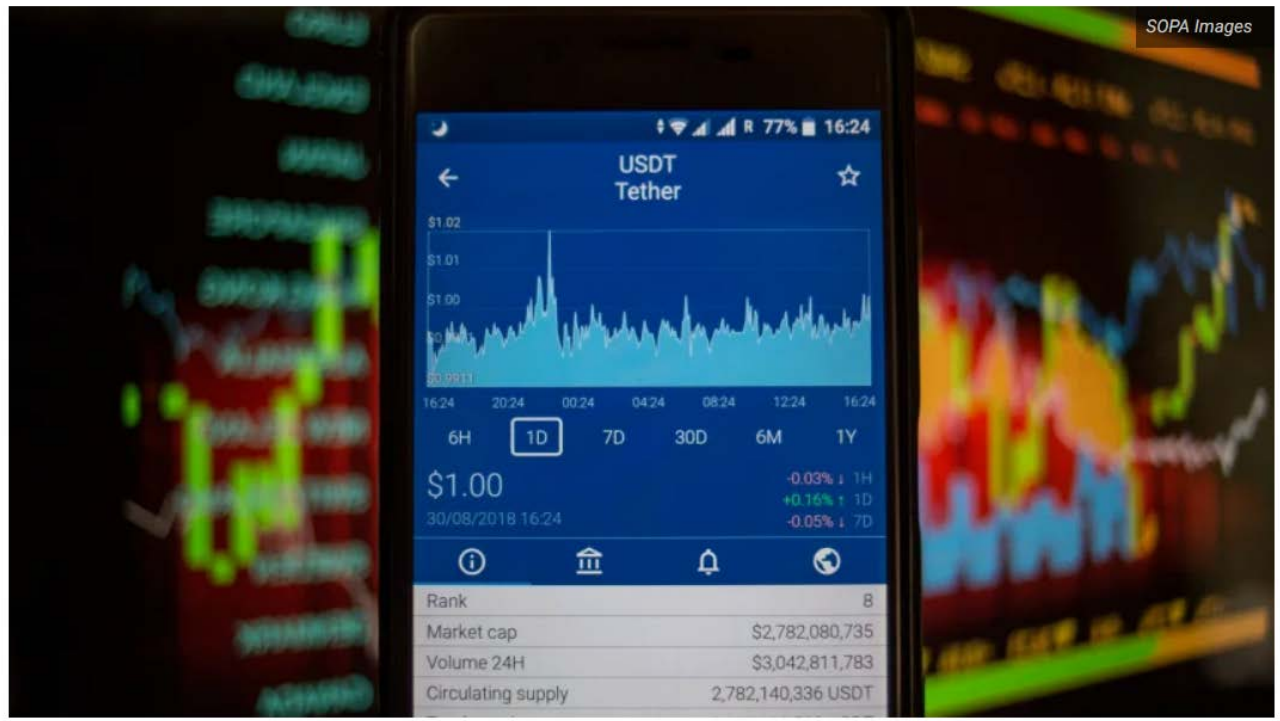
- Fiat collateralized stablecoins are the most popular and are backed by an off-chain reserve of target asset.
- Tether (USDT) is largest but has a complicated history. Further, there is no regular audit of the reserves. It has a $24b market cap and daily trading volume of $112b.
- USDC is the second largest and back by Coinbase and Circle. It has a $5b market cap and daily trading volume of $2b.
- Both of these stablecoins are centralized.

CRYPTOCURRENCY

NY Bans Tether, Bitfinex Over False Statements About Dollar Backing and Losses

The state's attorney general said both Tether and Bitfinex made false statements about their financial position and losses

Published 3 hours ago • Updated 3 hours ago



BANGKOK, THAILAND – 2018/08/30: In this photo illustration, a smartphone displays the Tether market value on the stock exchange via The Crypto App. (Photo Illustration by Guillaume Payen/SOPA Images/LightRocket via Getty Images)

Cryptocurrency companies Tether and Bitfinex will be barred from doing business with New Yorkers, and will pay heavy fines, for false statements about Tether's backing and for covering up losses at Bitfinex, the state attorney general's office said Tuesday.

Stablecoins

Crypto collateralized stablecoins

- MakerDAO DAI is the most popular crypto collateralized stablecoin with a $1.5b market cap and $0.5b daily volume (more details later)
- sUSD is another popular stablecoin that is linked to the Synthetix and is backed by the Synthetix network token, SNX (more details later)

Stablecoins

Non-collateralized stablecoins

- These are not backed by any underlying asset, and use algorithmic expansion and contraction of supply to shift the price to the peg.
- They often employ a seigniorage model where the token holders in the platform receive the increase in supply when demand increases.
- When demand decreases and the price slips below the peg, these platforms would issue bonds of some form which entitle the holder to future expansionary supply before the token holders receive their share.

Stablecoins

Decentralized, scalable stablecoin

- It is still an open problem to create a decentralized stablecoin which both scales efficiently and is resistant to collapse in contractions.
- Further, there are regulatory issues which we will discuss later.
- Fei Protocol is an example of a new initiative that is both decentralized and scalable.

dApps

Decentralized Applications

- dApps are similar to traditional software applications except they live on a decentralized smart contract platform.
- The primary benefit of these applications is their *permissionlessness* and *censorship-resistance*. Anyone can use them, and no single body controls them.

dApps

Decentralized Autonomous Organization

- A decentralized autonomous organization (DAO) has its rules of operation encoded in smart contracts that determine who can execute what behavior or upgrade.
- It is common for a DAO to have some kind of *governance token,* which gives an owner some percentage of the vote on future outcomes.
- More detail later.

DeFi primitives

Next

- Explore the DeFi primitives including transaction mechanics, fungible tokens, non-fungible tokens, custody, supply adjustment, incentives, swaps, collateralized loans and flash loans

Contact: Follow me on LinkedIn

http://linkedin.com/in/camharvey

cam.harvey@duke.edu

@camharvey

SSRN: http://ssrn.com/author=16198

PGP: E004 4F24 1FBC 6A4A CF31 D520 0F43 AE4D D2B8 4EF4