Stablecoins





Sergey Ivliev, Lykke, Perm State National Research University Perm Summer School 2018

'Good money' fundamentals



- Store of value
- Medium of exchange

Durable

Divisible

Fungible

Portable

Relatively scarce

Resistant to counterfeiting

Unit of account

Price discovery

Price signalling

- Privacy
- Censorship resistant
- Adoption / network effect
- Scalability

US Dollar



- Short-term stable: 0.18% 90-d volatility to basket (SDR)
- Store of value: >63% of currency reserves
- Payment method: >50% of payments (SWIFT)
- Unit of account of choice

...but

- Long term halving every 20 yrs
- Not private (except for cash)
- Not resistant to censorship
- Not suitable for microtransactions



http://www.imf.org/en/News/Articles/2017/03/31/pr17108-IMF-Releases-Data-on-the-Currency-Composition-of-Foreign-Exchange-Reserves

Fiat currencies



- 27 years average life expectancy of a fiat currency
- 20% failed through hyperinflation, 21% destroyed by war, 12% destroyed by independence,

24% were monetarily reformed



Good golly, Miss Bolí!

Venezuelan bolívar to the \$ Implied PPP* conversion rate, inverted log scale





- Consensus on emission (minting, mining)
- Fast (but probabilistic) finality, cost of 51% attack defines upperbound
- Not much scalable: <10-15 tps
- Market adoption is growing: >100m cryptocurrency users... but not mainstream
- Expensive to transact when network is congested (especially micropayments)
- Bubble-crash price dynamics



- 3.5% 60-d volatility of BTC/USD, up to 7% and more (>100% annual)
- 2x-10x compared to EUR/USD or Gold
- Other ccs are even more volatile





- Other ccs are even more volatile
- 7.5% sample std.dev for ETH returns, 8.2% sample volatility for Bitshares, etc.
- Heavy tails: **3x** sigma price drops are pretty frequent





Intraday price jumps (shocks) are severe: >10% in less than 1 hour





• Liquidity is spurious on many exchanges (slippage > 0.25% for \$50k order)



Slippage = f(Volume), OKex, Kraken, Bitfinex, GDAX

Volume (\$ million)

10

Stablecoins

Must have's

Price stability (low volatility)

Nice to have's

- Transparent structure and governance
- Little counterparty/ tail event risk
- Fiat gateway
- Market liquidity
- Scalability
- Privacy
- Censorship resistance
- Adoption



Stablecoins



- Centralized IOUs (e.g. Tether, TrueUSD, etc.)
- Decentralized collateral-backed (e.g. Bitshares bitUSD, MarketDAO DAI, etc.)
- Algorithmic-stable coins (e.g. Basis)

Centralized IOUs **Tether**

大 Lykke

- Symbol: USDT
- Issuer: Tether International Limited
- Most popular stablecoin
- Launched in 2014 (Realcoin)
- Colored coin (OMNI protocol)
- Redeemable for fiat (Kraken, OTC)
- Ties with Bitfinex

F	TetherUS created by 5ed3694e8a4fa8d3ec5c75eb6789492c69e65511522b220e94ab51da2b6dd53f
Total	3,020,000,000.00 Tokens
Name	TetherUS
PropertyID	#31
Created	10/6/2014 9:39:15 PM
Data	The next paradigm of money.
Sender	3MbYQMMmSkC3AgWkj9FMo5LsPTW1zBTwXL
Category	Financial and insurance activities
Divisible	True
URL	https://tether.to
Raw Data	Click here for raw info

13

Centralized IOUs Tether

• **\$2.5B** USDT in circulation





Centralized IOUs **Tether**



• 2.58% 3m-volatility of USDT/USD, 25.8% max drawdown



Avg. USDTUSD

Centralized IOUs Tether

Proof of reserve

USD₮	
Total Assets	\$2,508,665,722.36
Liabilities (Tether in Circulation on Omni)	
Total Authorized	\$3,020,000,000.00
Less: Authorized but not issued	- \$510,960,153.48
Less: Quarantined Tether	- \$30,950,010.00
Liabilities (Tether in Circulation on Eth)	
Total Authorized	\$60,109,502.10
Less: Authorized but not issued	- \$108,983.00
Total Liabilities	\$2,538,090,355.62
Shareholder Equity	-\$29,424,633.26



MONITOR AND REVIEW:

Pursuant to the above terms of Engagement, and the discretion provided by Tether, FSS selected the date of June 1st, 2018, and received the following balance information from Tether's two banks as of the close of the banking day. FSS received the following confirmations from the respective banks by sworn and notarized statements provided by duly authorized personnel.

BANK 1: \$1,968,538,584.82 USD (unencumbered)

BANK 2: \$576,528,652.00 USD (unencumbered)

TOTAL: \$2,545,067,236.82 USD

In conjunction with receiving the above balance information, FSS requested the Chief Financial Officer and the General Counsel of Tether to certify, by sworn statement, the amount of fully-backed USD Tethers that were in circulation as of the close of business on June 1st, 2018. The amount certified to FSS was \$2,538,090,823.52 USD Tethers. According to Tether's transparency page (https://wallet.tether.to/transparency), the amount of fully-backed USD Tethers in circulation as of June 1st, 2018 was equal to \$2,538,090,823.52 USD Tethers. FSS did not provide the Tether personnel with any advance notice, nor did FSS provide Tether the account balance information gathered from the two banks prior to receiving the Tether balance information.

https://wallet.tether.to/transparency

https://tether.to/wp-content/uploads/2018/06/FSS1JUN18-Account-Snapshot-Statement-final-15JUN18.pdf

Centralized IOUs **Tether**

- Aggregate flow between major addresses
- USDT are issued at private address
- Sent to Bitfinex
- Bittrex and Poloniex are close allies



Griffin, John M. and Shams, Amin, Is Bitcoin Really Un-Tethered? (June 13, 2018). SSRN: https://ssrn.com/abstract=3195066

Centralized IOUs **Tether**



• Controversy: "Less than 1% of hours with such heavy Tether transactions are associated with 50% of the meteoric rise in Bitcoin and 64% of other top cryptocurrencies."



Griffin, John M. and Shams, Amin, Is Bitcoin Really Un-Tethered? (June 13, 2018). SSRN: https://ssrn.com/abstract=3195066

Centralized IOUs TrueUSD

- Symbol: TUSD
- Issuer: TrueCoin LLC
- Launched in 2018
- ERC20 token
- Redeemable for fiat (>\$10k)
- Collateral is held at escrow account
- Audited by professional firm

A stablecoin that you can redeem 1-for-1 for US dollars 1 USD = 1 TrueUSD T TrueUSD Backers foundation capital a16zcrypto BLOCKTOWER DISTRIBUTED GLOBAL JumpCapital SIGNIA VENTURE **GGV**CAPITAL FOUNDERS FUND Stanford University SLOW VENTURES ZhenFund Stanford-StartX Fund



19

Centralized IOUs TrueUSD

• **\$61M** TUSD in circulation





Centralized IOUs TrueUSD

Proof of reserve

TrueUSD Attestation Reports

TrustToken has engaged Cohen & Company, a Top 50 public accounting firm with cryptocurrency expertise, to independently confirm that the TrueUSD assets the independent fiduciaries hold in escrow adequately collateralize the outstanding TrueUSD coins that have been issued. All the attestations that have been published since the launch of TrueUSD can be viewed below.



TRUECOIN LLC 325 9th Street San Francisco, CA 94103

ESCROW HOLDINGS REPORT

JULY 16, 2018

Balance of Escrow Account(s):

\$ <u>79,051,658.66</u>

NOTES

- 1. The issued and outstanding TrueUSD tokens on the blockchain as of 5:00 pm ET on July 16, 2018 do not exceed the balance of the Escrow Account(s) reported above.
- The USD balance in the Escrow Account is held at Prime Trust, LLC (the "Escrow Agent") for the benefit of the TrueUSD token holders as agreed to within the Escrow Agreement(s).
- In the event of Escrow Agent's insolvency, recovery of the USD Balance in the Escrow Account with the Escrow Agent may be limited to account insurance or other protection afforded such deposits.
- 4. As agreed to within the Escrow Agreement(s), TrueCoin LLC and the Escrow Agent are not entitled to any funds at any time and no amounts deposited into the Escrow Account(s) shall become the property of TrueCoin LLC, the Escrow Agent, or any other entity, or be subject to any debts, liens or encumbrances of any kind of TrueCoin LLC, the Escrow Agent, or any other entity.

- Symbol: BitUSD
- Issuer: Bitshares protocol
- Launched in 2014
- Bitshares asset (bitasset)
- Collateralized with Bitshares (BTS)
- No fiat gateway (yet)





 1 BitUSD is created as loan or short position when at least \$2 worth of BTS is locked (200% collateral)







- bitUSD tracks Bitshares (BTS) price
- Price feed is written to blockchain by witness nodes: <u>https://github.com/xeroc/bitshares-pricefeed/</u>
- Price is normally a weighted average from various sources: <u>https://github.com/xeroc/bitshares-pricefeed/tree/master/bitshares_pricefeed/sources</u>
- Each witness can decide frequency on its own .. usually they have something like this: publish
 new price feed if price moves more than x% or my feed is older than 12h
- bitUSD has a feed expiration of 24hrs
- Median of prices is taken as settlement price



- 1 bitUSD collateral always worth at least \$1 equivalent
- bitUSD holder can order forced settlement (delivery of the underlying)
- Executed in **24 hours** at market price
- The collateral is taken from those traders that have the lowest collateral ratio (hence improve it)
- Minor fee is paid (1%, goes to the shorter)
- When BTS price is up everything is great! Collateral \$ value increases
- What happens when the price goes down?



- Every "shorter" maintains their own call positions and has its own collateral ratio (collateral/debt)
- The least collateralized positions are queued for margin call
- Margin call is executed when collateral value falls below Maintenance Collateral Ratio (currently MCR=175%)
- Protocol evaluates how much collateral has to be liquidated to get out of the margin call regime
- Protocol tries to liquidate collateral (BTS) on Bitshares DEX: sends limit order with feed price corrected by Short-squeeze protection (10%)

→ ~ uptick calls USD			
acount	debt	collateral	call price ratio
+	685.3596 USD 18,084.8006 USD 1,150.0000 USD 31,100.6691 USD 59,242.7016 USD 113,956.4076 USD 84.1624 USD 144,482.3367 USD 31,797.8167 USD	6,940.11591 BTS 183,148.42598 BTS 11,650.00000 BTS 315,107.99223 BTS 600,242.57223 BTS 1,154,699.82907 BTS 853.00000 BTS 1,464,685.52551 BTS 322,601.94979 BTS	5.786422952 BTS/USD 1.76 5.786972482 BTS/USD 1.76 5.788819876 BTS/USD 1.76 5.789641029 BTS/USD 1.76 5.789671070 BTS/USD 1.76 5.790183173 BTS/USD 1.76 5.791524142 BTS/USD 1.76 5.792840679 BTS/USD 1.76 5.797378262 BTS/USD 1.76
stk87	0.8000 USD	8.11979 BTS	5.799850000 BTS/USD 1.76





- Suppose price = 1 bitUSD / 10 BTS (p = 0.1)
- Alice is shorter. Alice borrows 100 bitUSD for 1800 BTS. Collateral ratio = 1.8 (>MCR=1.75).
 Minimum required collateral = 100*MCR/p = 1750 BTS
- Suppose price goes down to 1 bitUSD / 11 BTS (p = 0.091)
- Alice position is undercollateralized now. Minimum required collateral = 100*MCR/p = 1925 BTS
- Suppose Bob wants to buy BTS worth of 20 bitUSD and sends limit order at price 1 bitUSD / 12 BTS (p = 0.082)
- Protocol evaluates how much collateral has to be liquidated to improve MCR and sends 20
 bitUSD sell order at the price of 1 bitUSD / 12.1 BTS (+10% max squeeze). They match with Bob and swap 20 bitUSD vs. 240 BTS.
- Alice now owes less 100-20=80 bitUSD and holds 1800-240=1560 BTS collateral.
- She is OK. Collateral ratio = 1.77 (>MCR=1.75). Minimum required collateral = 80*MCR/p = 1540



- If any (least collateralized) call position goes below 100% collateral the blackswan event is triggered, a.k.a. "Global Settlement"
- This happen when BTS valuation drops significantly and no one is willing to short-sell at a +10% premium until the least collateralized position reaches 100%



The consequences are:

- no more margin calls on bitUSD/BTS
- no more borrowing of bitUSD
- last available price is tagged
- ALL call positions are moved over to the issuer account (committee)
- committee write-offs debt and collateral, excess collateral is paid out to the original shorters,
 e.g. If you have a call position at 200% at the time of a black swan, you will a) get half of the collateral paid out, b) lose the other half, but c) also drop the liability/debt.
- trading continues as usual
- bitUSD forced settlement continues as usual
- The collateral in the committee account is then used to cover those settlements



This situation stays as long as either:

- BTS price recovers so that the collateral (now owned by the committee) covers the debt (also owned by committee) with 175%, or
- market participants have place sufficient bids to 'buy' the debt&collateral so that the ratio goes to 175% too (BSIP18 <u>https://github.com/bitshares/bsips/blob/master/bsip-0018.md</u>)

There were a few blackswans: bitNZD, bitSEK, bitRUB, bitBTC, bitGOLD, bitSILVER.

Most of them recovered when BTS went up again.

bitGOLD was recovered through BSIP18 (which means people have placed bids to buy up the entire collateral and debt that was left).

bitBTC has not recovered.



Significant changes in market properties on July 19:

- BSIP30: Always Allow Increasing Collateral Ratio If Debt Not Increased
- BSIP31: Update Short Position's Margin Call Price After Partially Called Or Settled
- BSIP32: Always Match Orders At Maker Price
- BSIP33: Maker Orders With Better Prices Take Precedence
- BSIP34: Always Trigger Margin Call When Call Price Above Or At Price Feed

https://www.bitshares.foundation/announcements/2018-06-18-bitshares-core-release-2-0-180612



• **\$12m** bitUSD in circulation





• 3.7% 3m-volatility of bitUSD/USD, 6.1% sample std.dev (vs. 6% and 8.2% respectively for BTS)



Oct '14	lan '15	Apr '15	lun '15	Aug '15	Dec '15	6 Mar	'16 May	v'16 lu	1'16 Oc	t'16 De	c'16 M	ar'17 M	av '17	lul '17 Oc	t'17 De	c'17 Ma	ar'18 Ma	av '18 lu	ul '18 Aug '17

bitUSD normally is growing >\$1
 during bear markets as
 speculators tend to reduce their
 leverage and buy back bitUSD



🛨 Lykke



• bitCNY is more liquid recently (\$34m bitCNY issued), volatility is comparable to bitUSD



大 Lykke

Useful links:

- <u>https://bravenewcoin.com/assets/Whitepapers/bitshares-financial-platform.pdf</u>
- <u>https://bitshares.org/technology/price-stable-cryptocurrencies/</u>
- <u>http://bytemaster.github.io/article/2014/12/18/What-are-BitShares-Market-Pegged-Assets/</u>
- http://bytemaster.github.io/guest/2014/12/22/How-BitShares-Works/
- <u>https://github.com/bitshares/bsips/blob/master/bsip-0018.md</u>
- <u>https://www.reddit.com/r/BitShares/comments/6684x1/can_somebody_explain_bitusd_please_t_hanks/</u>

- Symbol: DAI
- Issuer: MakerDAO
- Launched in 2018
- ERC20 compatible token
- Collateralized with Ethers
- Pegged to USD/SDR
- Coupled with MKR "Stakercoin"

Equity

- Buy back program
- Governance (voting on parameters)
- Tail risk exposure

MAKER





- Dai is created by locking ETH in smart contract (called collateralized debt position or CDP)
- ETH \rightarrow Wrapped ETH (ERC20 for ETH) \rightarrow Pooled ETH (allows dilution and burning)
- Locked collateral can be recovered at any time by paying back the borrowed Dai (plus a stability fee)

My CDPs	Open CDPs	Un	safe CDPs	Closed CDPs	All CDPs						
CDP Id S	Stability Debt (DAI)	Governan	ce Debt (MKR)	Locked (PETH)	% Tot (PETH)	% Ratio	Avail. DAI (to draw)	Avail. PETH (to free)	Liquidation Price	S tatus
2642	41,237	.000		0.001	220.057	0.063%	235.693%	23,558.374	80.008	277.379	Safe
2643	0	.000		0.000	0.000	0.000%	-	0.000	0.000	-	Closed
2644	19,698	.960		0.000	98.663	0.028%	221.213%	9,352.177	31.761	295.537	Safe
2645	30	.000		0.000	0.150	0.000%	220.835%	14.167	0.048	296.042	Safe
2646	19,549	.770		0.000	98.663	0.028%	222.901%	9,501.367	32.268	293.298	Safe
2647	10	.000		0.000	0.045	0.000%	198.751%	3.250	0.011	328.936	Risk
2648	180	.000		0.000	0.986	0.000%	242.136%	110.563	0.375	270.000	Safe



The first Dai instance has been deployed with the following parameters:

System Status

Status	System Col	lateralizat	tion Deb	t Ceiling Ratio	PETH/ETH	Total Liquidity Available from forced CDP liquidations							
Active	275.590%		55.2	93%	1.013	Sell 0.000 DAI Buy 0.000 PETH	Sell 0.000 PETI Buy 0.000 DAI	Η					
ETH/USD	MKR/USD	DAI/USD	Liq. Ratio	Liq. Penalty	Debt Ceiling	Spread (Join/Exit)	Spread (Bust/B	oom) Total	l Bad Debt	Deficit	Safe	Stability Fee (365 days)	Governance Fee (365 days)
435.844	620.608	1.000	150.000%	13.000%	100,000,000.000	0.000%	-3.000%	0.000	0	NO	YES	0.000%	0.500%
DAI Target	Rate (365 da	ys)											
0.000%													
Stats													
CDPs Open	ed CDPS (closed Bi	ite Counter	Give Counter	Tot PETH Locked	d Tot PETH Freed	Tot DAI Drawn	Tot DAI Wipe	ed				
2295	666	38	80	737	401,159.936	89,952.667	88,157,322.885	31,884,651.28	85				



Liquidation

- If CDP reaches Liquidation Ratio the Maker platform will acquire and liquidate the collateral.
- The CDP owner receives the value of the leftover collateral *minus* the debt, Stability Fee and Liquidation Penalty
- The PETH collateral is set for sale in the Liquidity Providing Contract, and keepers can atomically purchase the PETH by paying Dai



Price oracles

- MKR voters choose a set of trusted oracles to feed this information to the Maker Platform through Ethereum transactions
- Oracles submit underlying asset prices to blockchain
- Price Feed Sensitivity Parameter protects oracles from collusion and price manipulation
- This restriction ensures there is enough time to trigger a global settlement



"Global Settlement"

- Global Settlers are external actors similar to price feed oracles and are the last line of defense for the Dai Stablecoin System in the event of an attack.
- The set of global settlers, selected by MKR voters, have the authority to trigger global settlement.
- When triggered it stops CDP creation and manipulation, and freezes the Price Feed at a fixed value that is then used to process proportional claims for all users.
- After Global Settlement has been activated, a period of time is needed to allow keepers to process the proportional claims of all Dai and CDP holders based on the fixed feed value.
- Each Dai and CDP holder can call a claim function on the Maker Platform to exchange their Dai and CDPs directly for a fixed amount of ETH that corresponds to the calculated value of their assets, based on the target price of Dai. There is no time limit for when the final claim can be made.



• **\$55m** DAI in circulation





• 1.1% 3m-volatility of bitUSD/USD, 1.3% sample std.dev





Pros

- ERC20 compatibility is a huge advantage: Dai is going to be used by Ethereum-based projects: DEXs, remittance, prediction markets, etc.
- Decentralized governance and transparent structure
- Achieved better stability than other stablecoins

Cons

- The process is pretty complicated
- Not clear how efficient CDP liquidation will function in severe bear markets (liquidity?) and during blackswan Global Settlement events
- Oracles and Global Settlers are points of failure
- No partial settlement of CDPs



- Worst N-days returns for Ether price: -27% in a day, -45% in 2 days, -60% in a month
- Current DAI pool collateral-debt ratio is 275%: -45% to breach 150%, -63% to breach 100%



46

Algorithmic-stable coins **Basis**

- Issuer: Intangible Labs
- Just raised \$133m
- Stable cryptocurrency with algorithmic central bank

6 BASIS



🛨 Lykke

Three-token system:

Basecoin.

Pegged to the USD and are intended to be used as a medium of exchange. Their supply is expanded and contracted in order to maintain the peg.

Base Bonds.

Auctioned off by the blockchain when it needs to contract Basecoin supply. Each bond promises 1 Basecoin at some point in the future under certain conditions. Newly-issued bonds are sold on open auction for prices of less than 1 Basecoin (yield curve).

Base Shares.

Shares supply is fixed at the genesis of the blockchain.

Their value stems from their dividend policy.

When demand for Basecoin goes up and the blockchain creates new Basecoin to match demand, shareholders receive these newly-created Basecoins pro rata after all outstanding Base Bonds have been redeemed.

大 Lykke

Expansion:

- Happens when Basecoin >\$1
- Blockchain orders outstanding Base Bonds according to when they were issued, with the oldest first (Bond Queue) as well as outstanding Base Shares.
- Blockchain creates N new Basecoin tokens and distributes them as follows:

1) Bondholders are paid first, and in first-in-first-out (FIFO) order. Blockchain converts bonds into coins, one-for-one, according to their order in the Bond Queue.

2) Shareholders are paid after bondholders. If there are no more outstanding Base Bonds, the system issues any remaining new coins to shareholders, pro rata, as a dividend.

🛨 Lykke

Expansion (example):

- Suppose there are 500 bonds in the Bond Queue, 200 of which were created more than 5 years ago. Additionally, suppose there are 1,000 shares in circulation.
- Suppose the system needs to create **1,000** new coins.
- The system expires the **200** oldest bonds, leaving **300** bonds in the queue.
- The system redeems **300** bonds.
- The system distributes 700 more coins evenly across the 1,000 shares. Each share receives 700 / 1,000 = 0.7 coins.



Contraction:

- Basecoin < \$1
- Blockchain tries to lock up existing Basecoins in exchange for future payoff
- Blockchain runs a Dutch auction in which bidders specify a bid and bid size for Base bonds
- Then it chooses the orders with the highest bids and converts the holders' coins into bonds until sufficient Basis has been destroyed
- Price floor is 0.10 Basis per bond



Contraction (example):

- Suppose the system wants to auction **100** bonds.
- Suppose that there are three buy orders on the order book: One bid for 80 bonds at 0.8 Basis each, one bid for 80 bonds at 0.6 Basis each, and one bid for 80 bonds at 0.4 Basis each.
- The system will compute the clearing price, which is a single price at which all offered bonds would have been bought at. Here, the clearing price is **0.6** Basis.
- The system will fill the winning bids at the clearing price: The first user will receive 80 bonds in exchange for 80 * 0.6 = 48 coins, and the second user will receive 20 bonds in exchange for 20 * 0.6 = 12 coins.
- Both winners will have to wait until their bonds matures to receive 80 and 20 Basecoins, but no longer than 5 years (when both bonds defaults)



Pros

• Interesting approach to solve the cryptocurrency deterministic supply problem

Cons

- Will it work?
- Probably will not help short-term stability
- Blockchain technology part is completely out of scope

Algorithmic-stable coins **Face-to-face**



	Tether	bitUSD	N MAKER	6 BASIS
Price stability	2.6%	3.7%	1.1%	ŚŚŚ
Transparent structure	No	Protocol code	Smart contract	Likely
Counterparty risk	High	Little	Median	Little
Tail event risk	High	Medium	Medium-rare	May be high
Fiat gateway	Yes	Not yet	Not yet	ŚŚŚ
Market liquidity	High	Low	Growing	ŚŚŚ
Scalability	Low	Quite high	Low, but Plasma	ŚŚŚ
Privacy	KYC required	Ok	Ok	ŚŚŚ
Censorship resistance	No	Yes	Yes	ŚŚŚ
Adoption	High (\$2.5b)	Low (\$11m)	Low, but grows (\$55m)	ŚŚŚ
	7	9	13	