Incentives and Governance Model for a Decentralised Crypto Asset Exchange

Final Project Presentation
First Internal Fund Call for Project Proposals on Distributed Ledger Technologies at the UCL Centre for Blockchain Technologies, 20 February 2020

Giacomo Livan, University College London
Francesco Pierangeli, King’s College London/National University of Singapore
Moritz Platt, King’s College London
Simone Righi, University College London

Agenda

1 Centralised and Decentralised Exchanges

2 Protocol

3 Outlook

Cryptocurrency Market Capitalisation

	Name	Market Cap	Price	Volume (24h)	Supply
1	Bitcoin	$184,210,229,903	$10,116.92	$35,794,231,987	18,208,125 BTC
2	Ethereum	$25,093,191,977	$228.89	$14,936,061,883	109,628,359 ETH
3	XRP	$12,352,182,524	$0.282670	$2,268,819,803	43,698,224,662 XRP
4	Bitcoin Cash	$8,219,158,862	$449.89	$4,127,089,476	18,269,163 BCH

[CoinMarketCap2020]

- Bitcoin [Nakamoto2009] and the subsequent creation of “Altcoins” introduced the problem of exchanging cryptocurrencies
- Exchanges are fundamental for the long-term development of a diverse and robust cryptocurrency ecosystem [Gandal2014, Wisniewska2016, Franke2019]

Centralised Cryptocurrency Exchanges by Trade Volume

#	Name	Adj. Vol (24h)	Volume (24h)	Volume (7d)	Volume (30d)	No. Markets
1	BKEX	$3,125,835,625	$3,125,835,625	$18,384,841,662	$74,523,857,893	100
2	Fatbtc	$2,871,214,657	$2,871,214,657	$16,112,553,023	$66,644,916,873	114
3	BiKi	$2,411,115,558	$2,411,115,558	$13,565,814,043	$57,659,250,867	92
4	BitForex	$2,410,459,099	$2,410,459,099	$15,161,964,438	$60,694,131,095	153

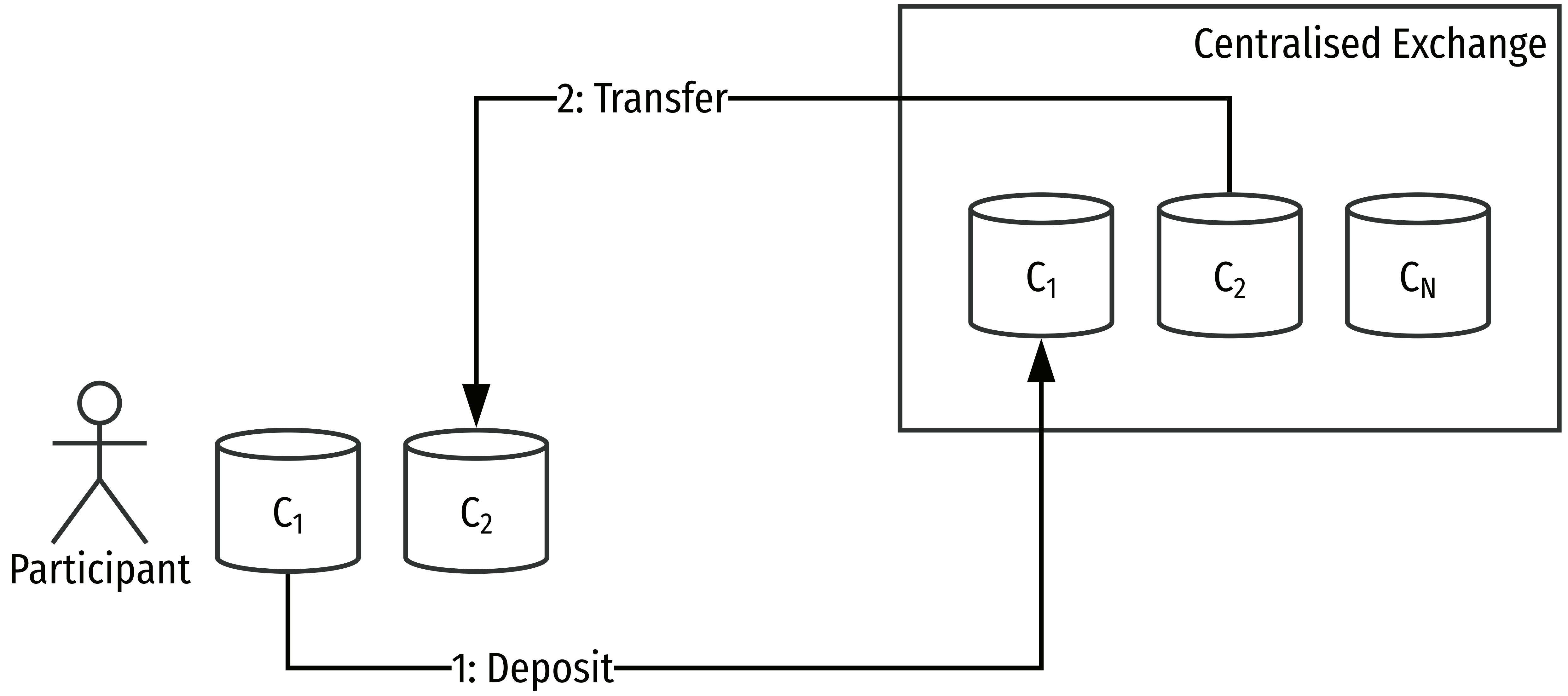
[CoinMarketCap2020]

□ All commercially relevant exchanges on the market today operate in a centralised manner

□ Centralised exchanges provide market-making capabilities by holding a reserve of crypto-currencies, standing ready to buy currency and to sell

□ Well understood model based on the same principles as foreign exchange spot trading of fiat currencies

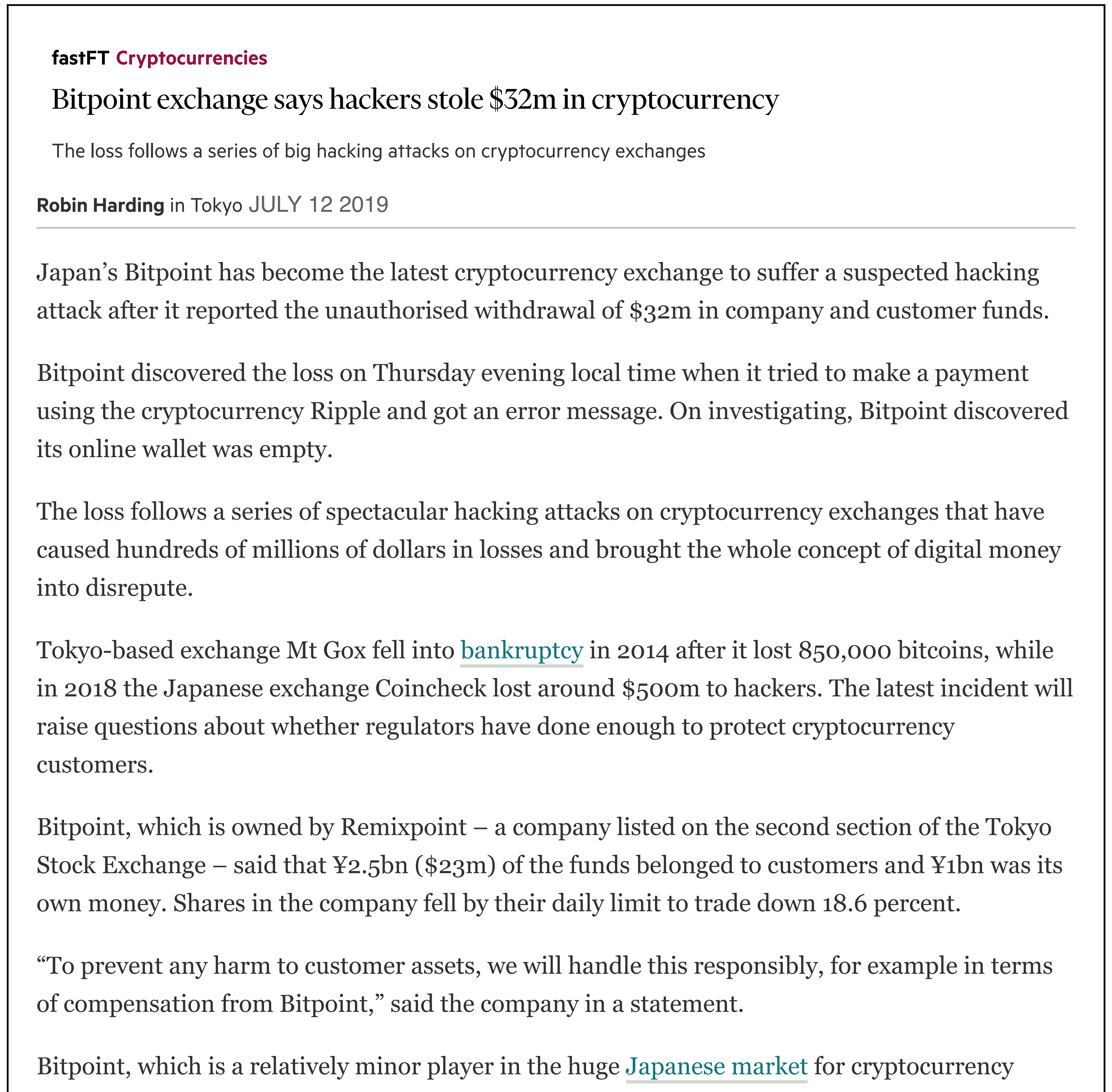
Centralised Cryptocurrency Exchanges



- □ Participants deposit currency into exchange account
- □ Exchange pays out funds at agreed rate to recipient account
- □ Business model reliant on fees and bid-ask-spread [Bundi2019]

Risk of Misappropriation of Funds in Transit

The recent past has provided several examples of the loss of assets in the exchange process, either due to theft or exchanges shutting down [Bolici2016, Chohan2018].



fastFT Cryptocurrencies

Bitpoint exchange says hackers stole $32m in cryptocurrency

The loss follows a series of big hacking attacks on cryptocurrency exchanges

Robin Harding in Tokyo JULY 12 2019

Japan's Bitpoint has become the latest cryptocurrency exchange to suffer a suspected hacking attack after it reported the unauthorised withdrawal of $32m in company and customer funds.

Bitpoint discovered the loss on Thursday evening local time when it tried to make a payment using the cryptocurrency Ripple and got an error message. On investigating, Bitpoint discovered its online wallet was empty.

The loss follows a series of spectacular hacking attacks on cryptocurrency exchanges that have caused hundreds of millions of dollars in losses and brought the whole concept of digital money into disrepute.

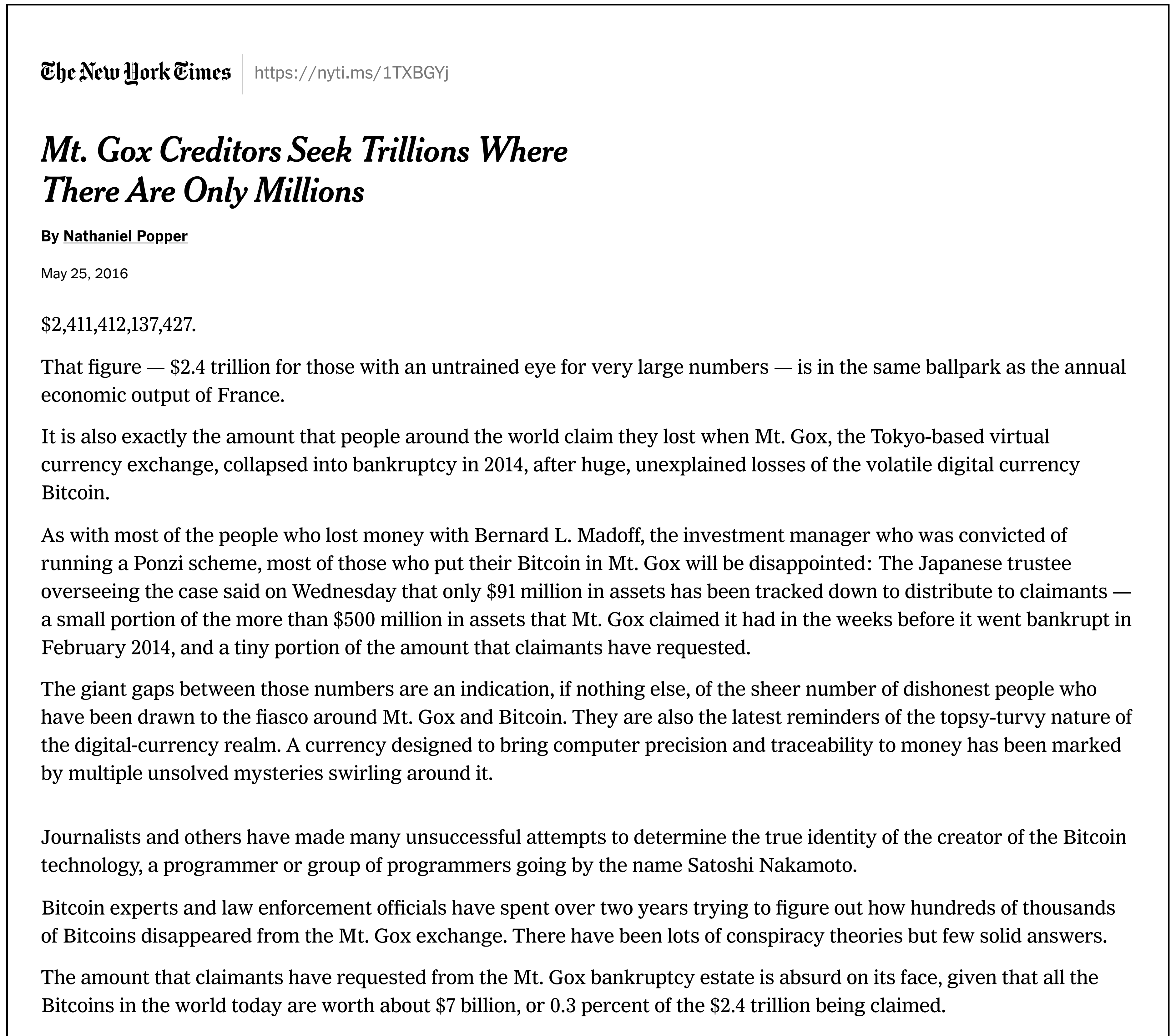
Tokyo-based exchange Mt Gox fell into bankruptcy in 2014 after it lost 850,000 bitcoins, while in 2018 the Japanese exchange Coincheck lost around $500m to hackers. The latest incident will raise questions about whether regulators have done enough to protect cryptocurrency customers.

Bitpoint, which is owned by Remixpoint – a company listed on the second section of the Tokyo Stock Exchange – said that ¥2.5bn ($23m) of the funds belonged to customers and ¥1bn was its own money. Shares in the company fell by their daily limit to trade down 18.6 percent.

"To prevent any harm to customer assets, we will handle this responsibly, for example in terms of compensation from Bitpoint," said the company in a statement.

Bitpoint, which is a relatively minor player in the huge Japanese market for cryptocurrency

[Harding2019]



The New York Times https://nyti.ms/1TXBGYj

Mt. Gox Creditors Seek Trillions Where There Are Only Millions

By Nathaniel Popper

May 25, 2016

$2,411,412,137,427.

That figure — $2.4 trillion for those with an untrained eye for very large numbers — is in the same ballpark as the annual economic output of France.

It is also exactly the amount that people around the world claim they lost when Mt. Gox, the Tokyo-based virtual currency exchange, collapsed into bankruptcy in 2014, after huge, unexplained losses of the volatile digital currency Bitcoin.

As with most of the people who lost money with Bernard L. Madoff, the investment manager who was convicted of running a Ponzi scheme, most of those who put their Bitcoin in Mt. Gox will be disappointed: The Japanese trustee overseeing the case said on Wednesday that only $91 million in assets has been tracked down to distribute to claimants — a small portion of the more than $500 million in assets that Mt. Gox claimed it had in the weeks before it went bankrupt in February 2014, and a tiny portion of the amount that claimants have requested.

The giant gaps between those numbers are an indication, if nothing else, of the sheer number of dishonest people who have been drawn to the fiasco around Mt. Gox and Bitcoin. They are also the latest reminders of the topsy-turvy nature of the digital-currency realm. A currency designed to bring computer precision and traceability to money has been marked by multiple unsolved mysteries swirling around it.

Journalists and others have made many unsuccessful attempts to determine the true identity of the creator of the Bitcoin technology, a programmer or group of programmers going by the name Satoshi Nakamoto.

Bitcoin experts and law enforcement officials have spent over two years trying to figure out how hundreds of thousands of Bitcoins disappeared from the Mt. Gox exchange. There have been lots of conspiracy theories but few solid answers.

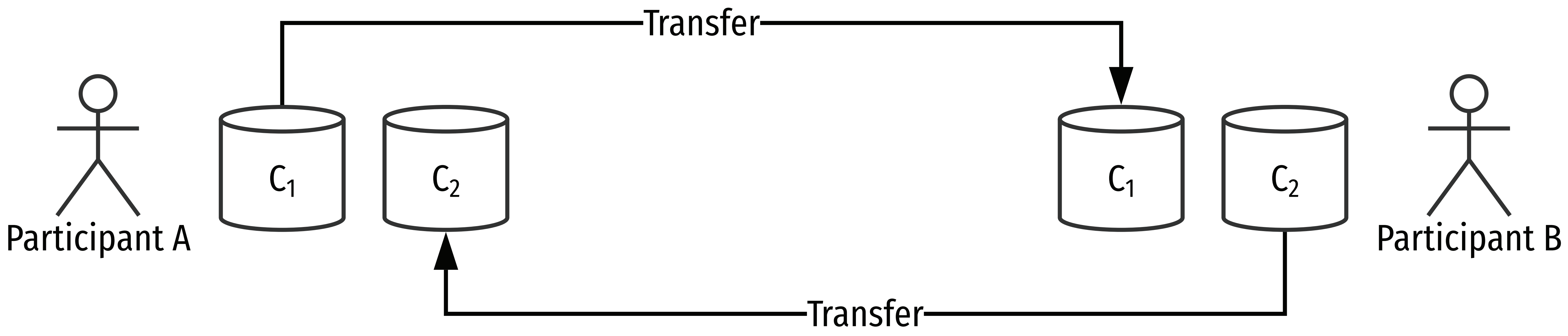
The amount that claimants have requested from the Mt. Gox bankruptcy estate is absurd on its face, given that all the Bitcoins in the world today are worth about $7 billion, or 0.3 percent of the $2.4 trillion being claimed.

[Popper2016]

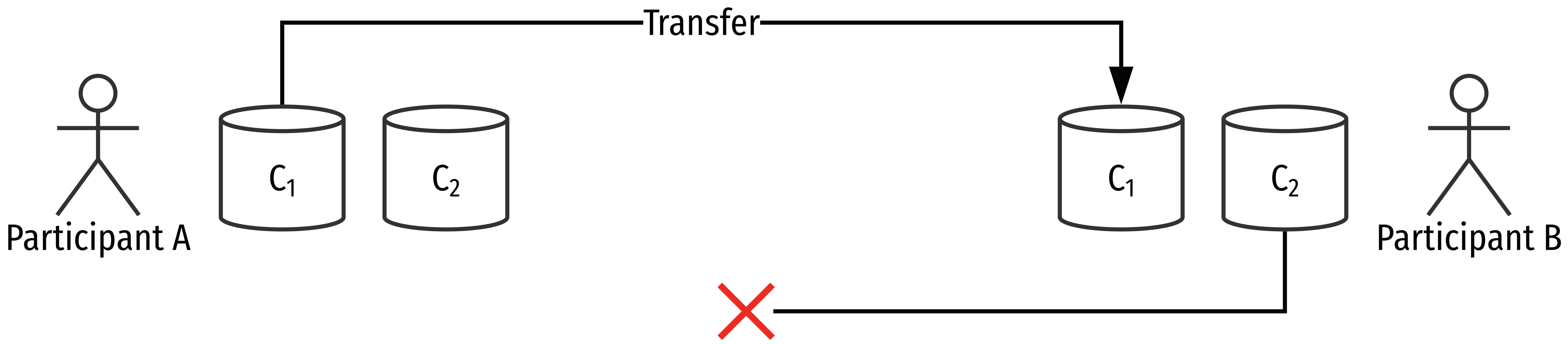
Exclusion of Participants

- Centralised Exchanges choose who they do business with
- Exclusions can be introduced for various reasons
  - Anti-Money Laundering legislation
  - “Know Your Customer” laws
  - Geoblocking [Wilmoth2018]

Decentralised Cryptocurrency Exchanges

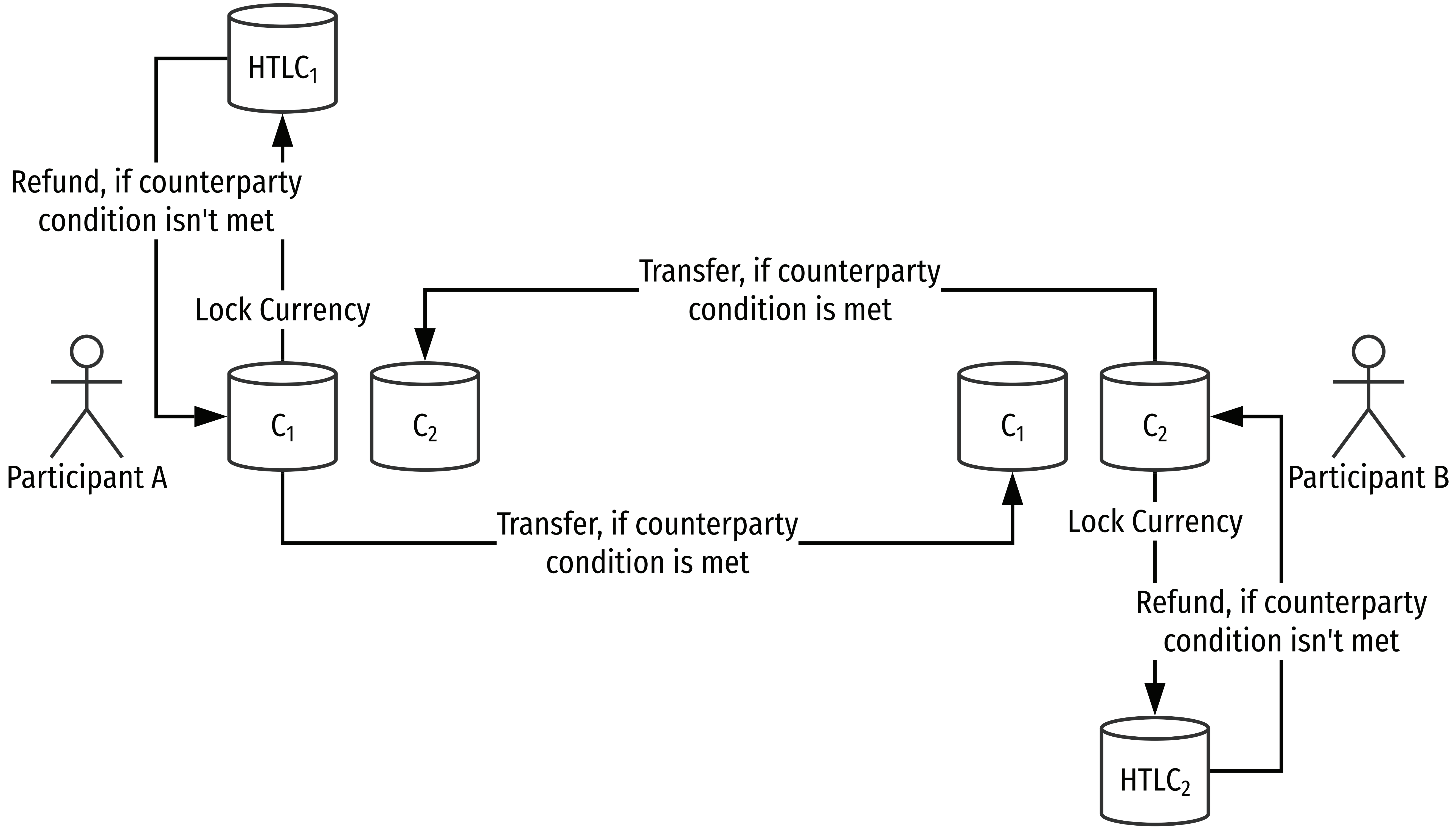


- □ *A* transfers a previously agreed amount of C_1 to *B* who in turn transfers a previously agreed amount of C_2 back to *A*
- □ Transactionality of transfers is key



Transactional Cryptocurrency Transfers

- □ Atomic swaps between different cryptocurrencies are hard
- □ The prevalent paradigm utilised to enable them are “Hashed Time-Locked Contracts” (HTLC)
- □ Most commercially relevant cryptocurrencies can be connected via HTLC [Griffith2019]


HTLC$_1$
Refund, if counterparty condition isn't met
Lock Currency
Transfer, if counterparty condition is met
Participant A
C$_1$
C$_2$
C$_1$
C$_2$
Participant B
Transfer, if counterparty condition is met
Lock Currency
Refund, if counterparty condition isn't met
HTLC$_2$

Downsides of Atomic Swaps

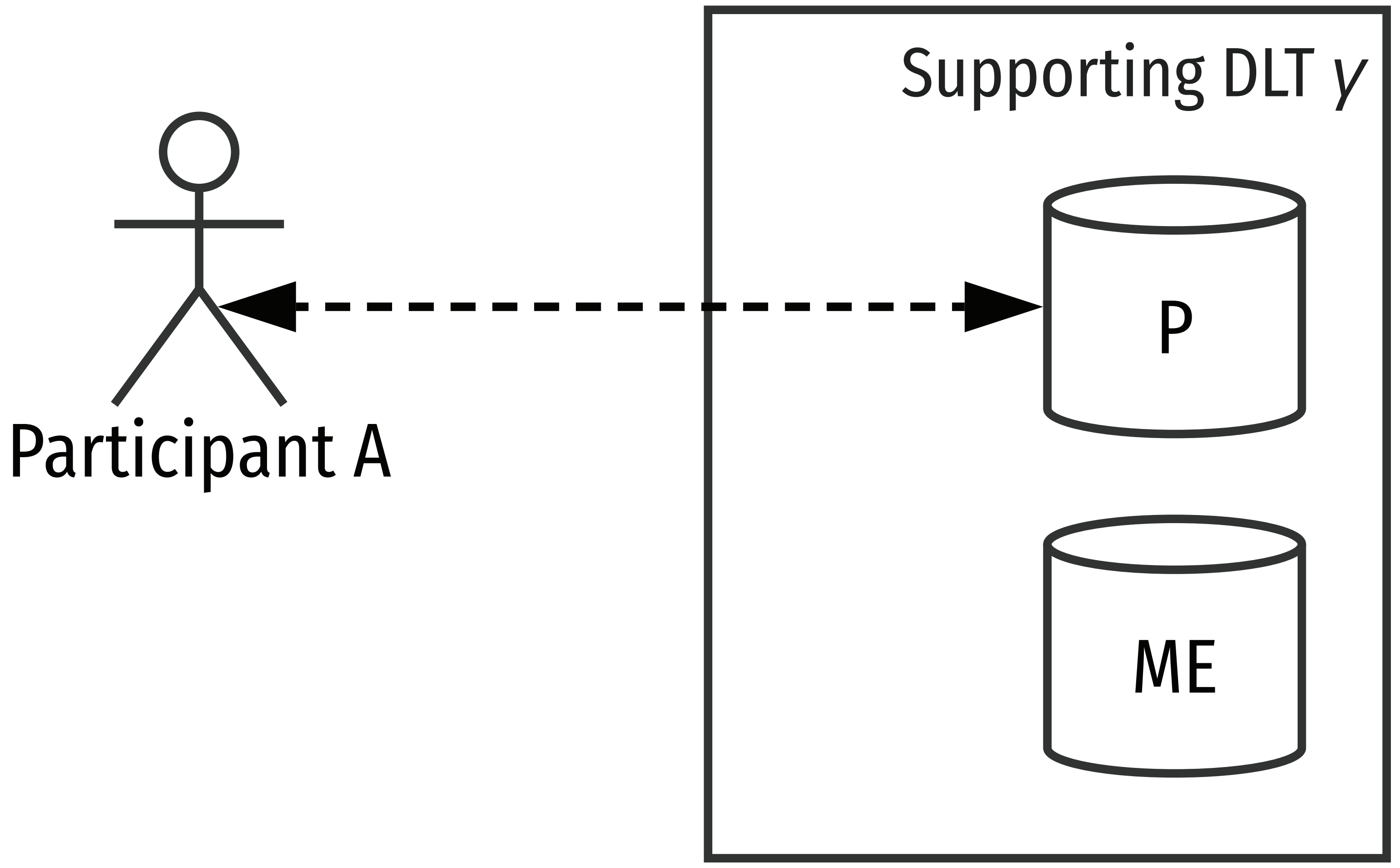
- No exchange rate discovery mechanisms
- Manual matching of the buy and sell sides necessary (i.e., how can interested traders find each other)
- Protocols that lock collateral can incur opportunity costs for the participants in cases where trades that were previously agreed upon fall through

Protocol Implementation

- Multi-stage protocol that facilitates HTLC-based decentralised exchanges
- Designed to alleviate the downsides of decentralised exchanges;
  - Complicated trading partner discovery
  - Opaque exchange rates
  - Opportunity costs incurred from failed trades
- Introduces a “supporting distributed ledger” to facilitate trades
- Supporting ledger is not involved in the actual execution of trades, thus maintaining the advantages of decentralised exchanges
  - No risk of misappropriation of funds in transit
  - No direct trading costs
  - Censorship resistancy

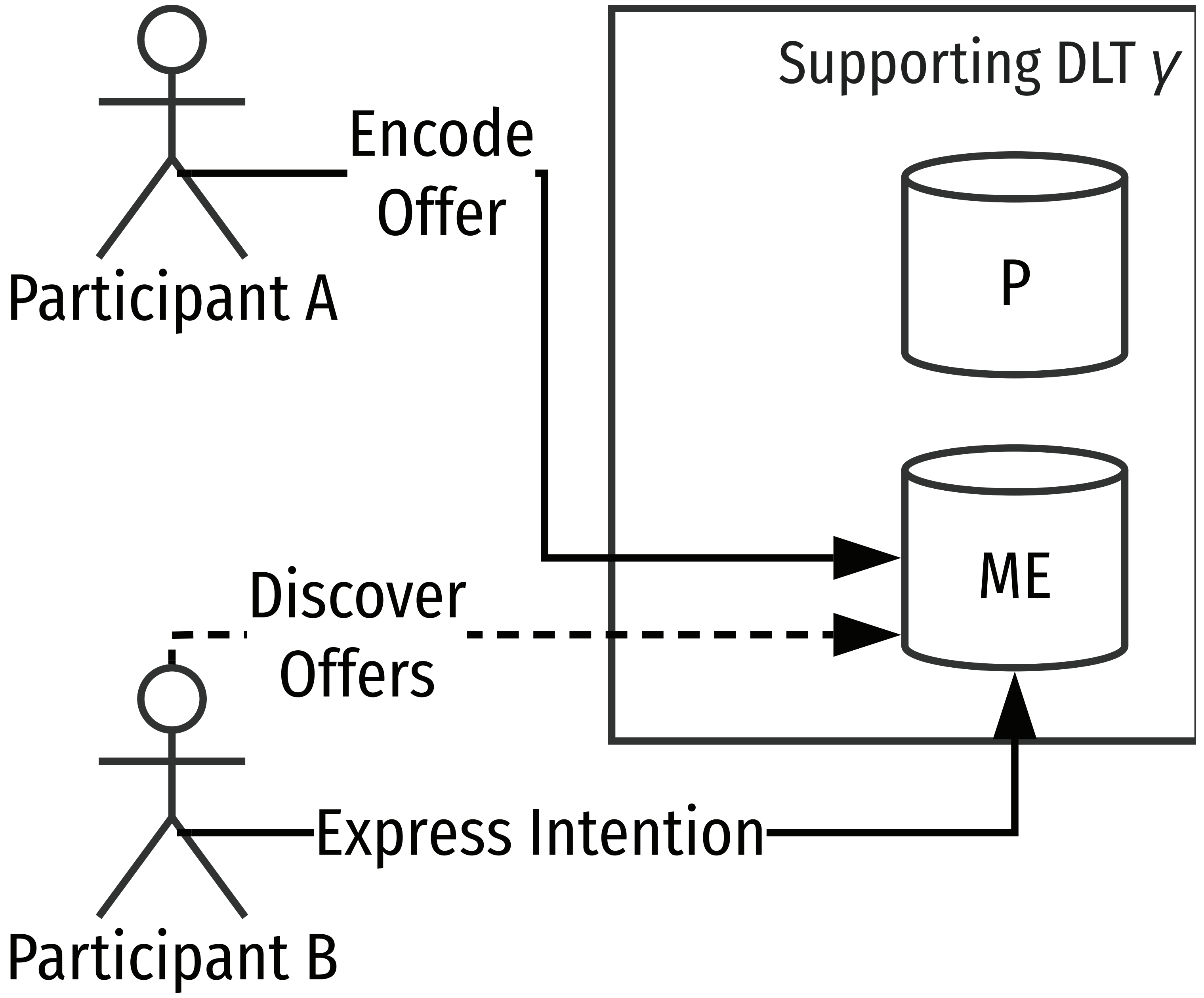
I — Exchange Rate Discovery

- Optional first step of the protocol
- Participants can query a price-reporting facility *P* deployed in *γ* for the exchange rate between two given currencies (*a*, and *b*) at the current time.
- This facility can be used by both parties of an exchange, e.g., both *User$_I$* holding *a* and a potential counterparty holding *b*, to determine a fair exchange rate
- The price reporting facility utilises verified trade data to publish a rolling benchmark rate



II — Order Matching

- □ Order-driven market; a market in which heterogeneous agents trade via a central order-matching mechanism
- □ Central order matching is provided by a matching engine deployed in γ
- □ To encode an order for exchanging a defined amount of one cryptocurrency for another, any account holder on γ can post an order message using the matching engine (e.g. A)
- □ The order posted using the matching engine includes the parameters relevant to the trade (units offered and units sought) and the technical parameters necessary for performing the trade via an HTLC

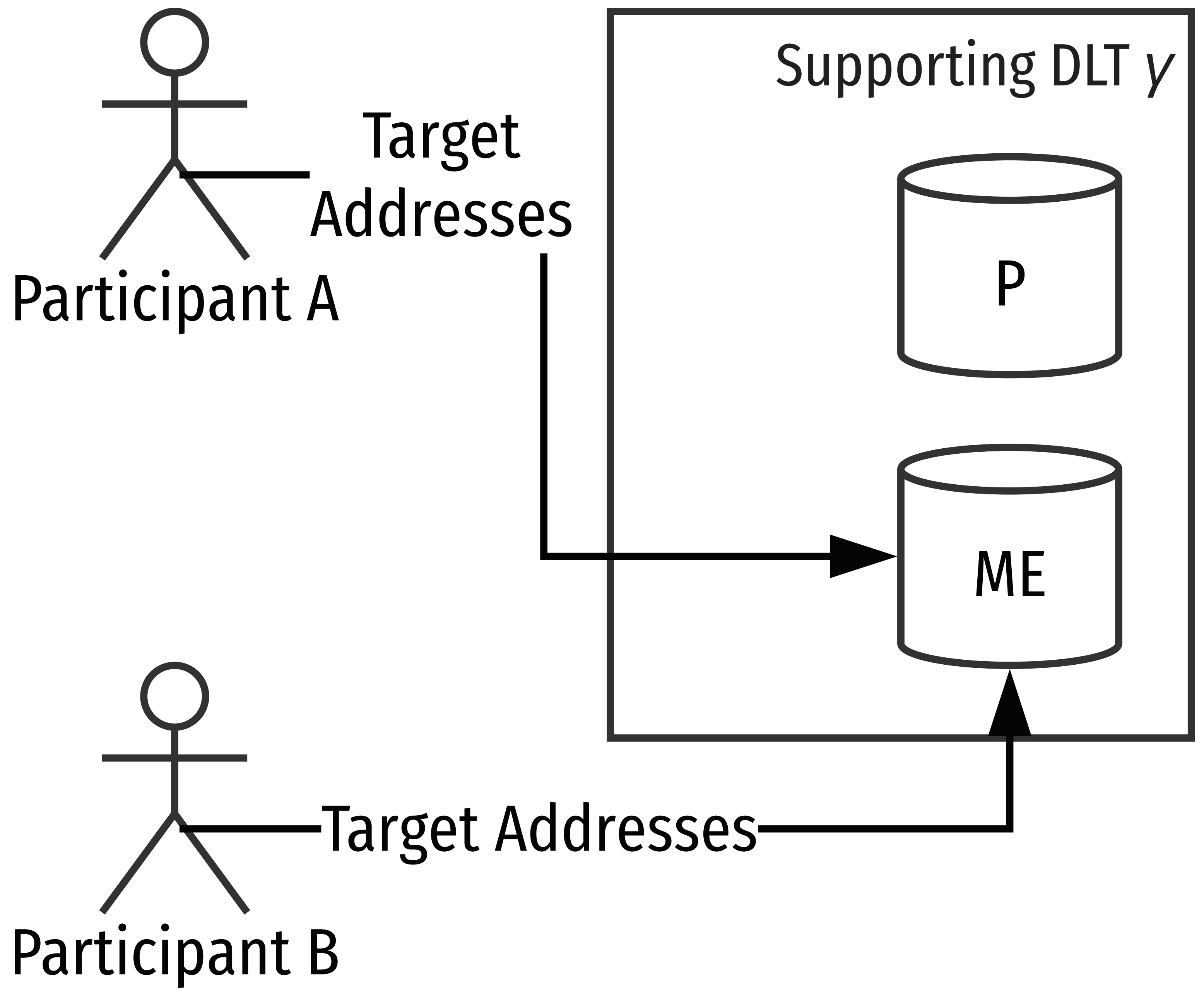


II — Order Matching

- *A* will include a minimal performance rating t in the order
- This value is used as a threshold to exclude participants whose past performance was below expectations
- Buyers (e.g. *B*) can query the matching engine for orders that are of interest to them
- Should they qualify based on their performance rating, some aspects of the relevant orders are made available to them
- Once a buyer expresses their intention to engage in a particular trade–as referenced by its offer ID– this trade will no longer be visible to other potential buyers

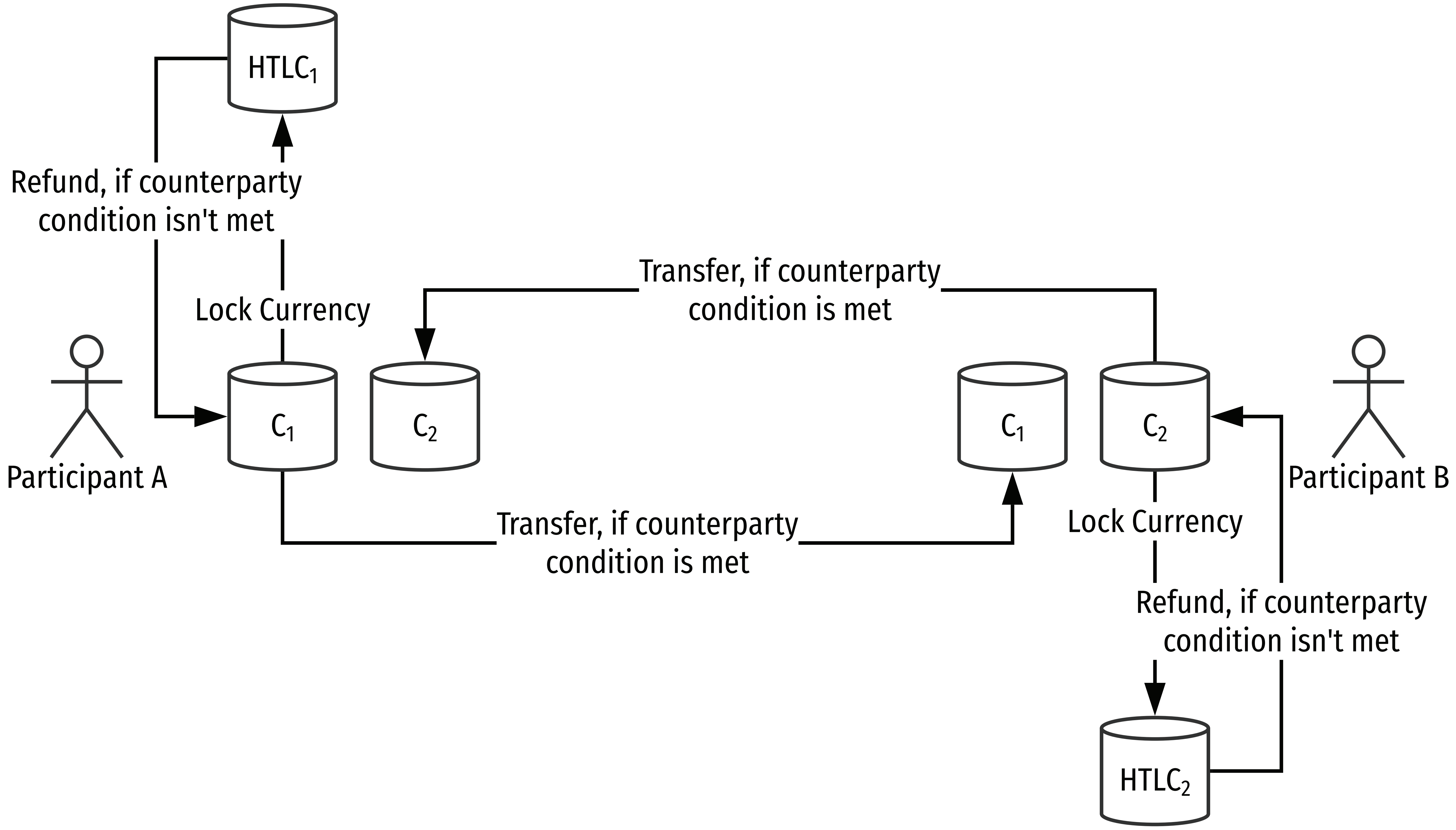
III — Exchange

- The order book of the matching engine will be updated and the details of the trade (addresses and locking secret hash) will be made available to the buyer
- The buyer also needs to communicate their success address (where they seek to receive funds) to the seller
- The matching engine will be a witness to this transaction to allow for judging whether the transfer was executed as expected later on
- This message concludes the message flow necessary to establish a decentralised exchange.



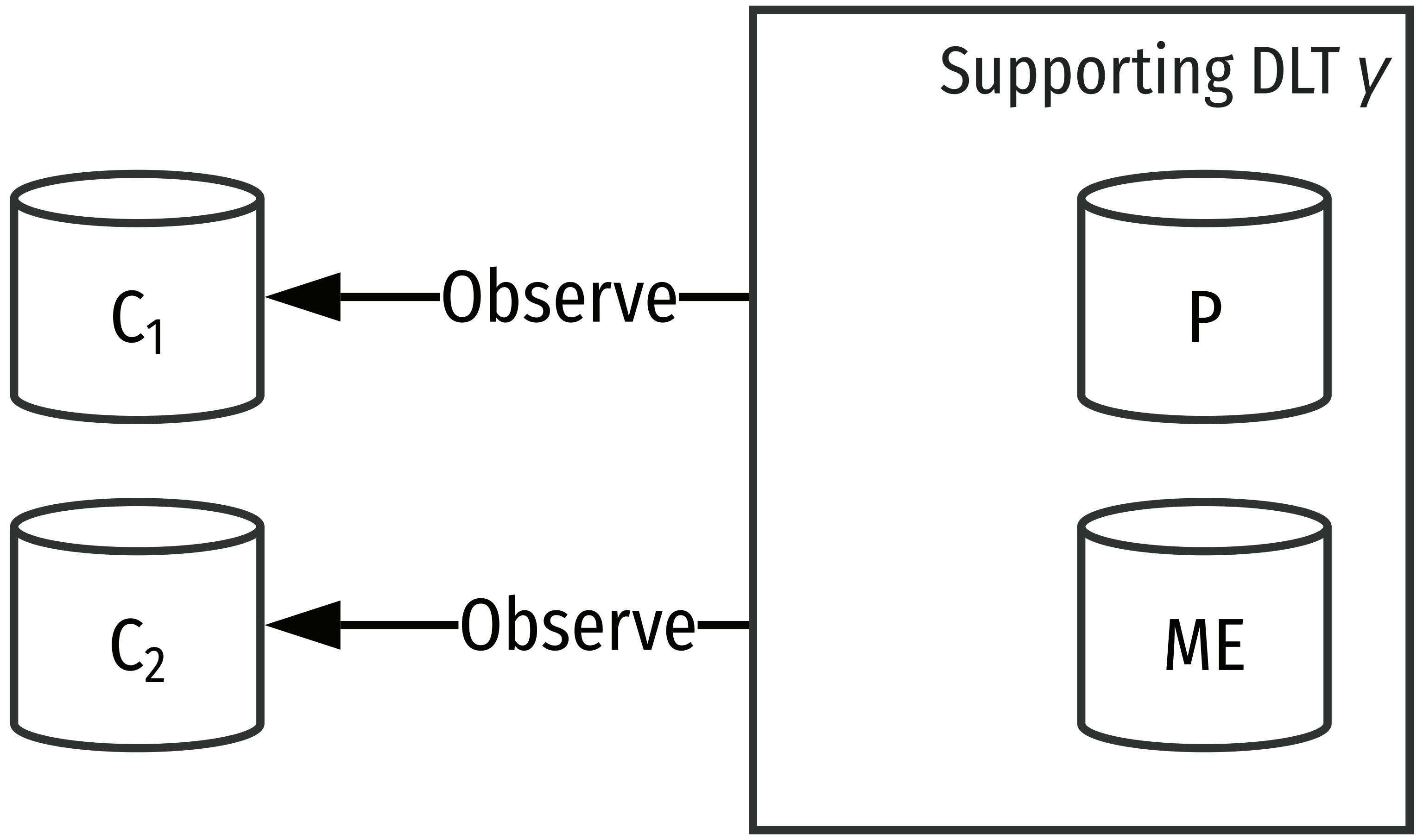
IV — HTLC

- *A* and *B* then engage in an exchange by following the respective HTLC protocol connecting blockchains C_1 and C_2


HTLC₁
Refund, if counterparty condition isn't met
Lock Currency
Transfer, if counterparty condition is met
Participant A
C₁
C₂
C₁
C₂
Participant B
Transfer, if counterparty condition is met
Lock Currency
Refund, if counterparty condition isn't met
HTLC₂

V — Execution Monitoring

- γ offers key data in two dimensions to its users
  - a trustworthy exchange rate
  - a participant performance rating
- γ observes transactions on C_1 and C_2
- A participant's performance rating is computed using the total volume of their successfully fulfilled obligations in relation to the total volume of their failed trades
- Execution monitoring allows one to understand which of the two legs of a trade fell through, thusa positive score can be attributed to an honest counterparty of a failed trade



Conclusion

- □ We show how combining centralised elements with decentralised technology can ease trading partner discovery, thus lowering the friction during the preliminary phase of a trade
- □ We show how performance scoring can lower opportunity costs by reducing the risk of trades falling through
- □ We identify economic trade-offs faced by users in both CEX and DEX
- □ Taking the underlying conditions of an order-driven market into account, we show how a rolling benchmark rate of verifiable trades can establish a trustworthy exchange rate between cryptocurrencies

Outlook

- □ Formal validation of the economics of the proposed protocol
- □ Decentralisation of more aspects of the system (i.e. credit scoring) through Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARK) with the ultimate goal of removing any central entity

Bibliography

WWW (CoinMarketCap2020)
CoinMarketCap
Top 100 Coins by Market Capitalization
2020
https://coinmarketcap.com/coins/

Misc (Nakamoto2009)
Nakamoto, S.
Bitcoin: A peer-to-peer electronic cash system
2008

TechReport (Gandal2014)
Gandal, N. & Halaburda, H.
Competition in the Cryptocurrency Market
NET Institute, NET Institute, 2014

TechReport (Wisniewska2016)
Wisniewska, A.
Altcoins
Institute of Economic Research, Institute of Economic Research, 2016

InBook (Franke2019)
Franke, J.; Härdle, W. K. & Hafner, C. M.
Financial Econometrics of Cryptocurrencies
Statistics of Financial Markets: An Introduction, Springer International Publishing, 2019, 545-568

Article (Bundi2019)
Bundi, N. & Wildi, M.
Bitcoin and market-(in)efficiency: a systematic time series approach
Digital Finance, 2019

InProceedings (Bolici2016)
Bolici, F. & Rosa, S. D.
Torre, T.; Braccini, A. M. & Spinelli, R. (Eds.)
Mt.Gox Is Dead, Long Live Bitcoin!
Empowering Organizations, Springer International Publishing, 2016, 285-296

Article (Chohan2018)
Chohan, U.
The Problems of Cryptocurrency Thefts and Exchange Shutdowns
SSRN Electronic Journal, Elsevier BV, 2018

WWW (Harding2019)
Harding, R.
Bitpoint exchange says hackers stole $32m in cryptocurrency
2019
https://www.ft.com/content/c23930d4-a474-11e9-974c-ad1c6ab5efd1

WWW (Popper2016)
Popper, N.
Mt. Gox Creditors Seek Trillions Where There Are Only Millions
2016
https://www.nytimes.com/2016/05/26/business/dealbook/mt-gox-creditors-seek-trillions-where-there-are-only-millions.html

WWW (Wilmoth2018)
Wilmoth, J.
Decentralized[?] Ethereum Exchange IDEX Waves Goodbye to New York Traders
2018
https://www.ccn.com/decentralized-ethereum-exchange-idex-waves-goodbye-to-new-york-traders/

WWW (Griffith2019)
Griffith, T.
Atomic Swap Readiness
2019
https://swapready.net/

InProceedings (Lausen2019)
Lausen, J.
Regulating Initial Coin Offerings? A Taxonomy of Crypto-Assets
Proceedings of the 27th European Conference on Information Systems (ECIS), 2019

Picture Credit

Assorted color shape and denomination coin lot
Photo by Benjamin Lambert on Unsplash
https://unsplash.com/photos/KxdO8elL5_c