EXHIBIT 2

Rebuttal Report

Jeremy Clark, Ph.D., P.Eng.

1 Assignment

I have been engaged by Lead Plaintiff Bradley Sostack ("Plaintiff"), through his counsel, to respond to expert testimony in the case captioned *In re Ripple Labs Litigation*, Case No. 4:18-cv-06573, pending in the United States District Court for the Northern District of California. Lead Plaintiff has retained me to independently analyze and opine on the expert reports from Prof. Yesha Yadav and Prof. Allen Ferrell. My qualifications and other background information is set forth in my previous expert report.

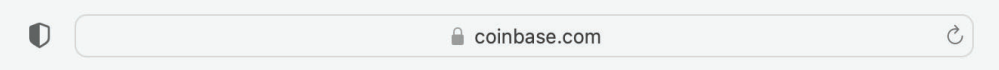
2 Location of Exchanges

Prof. Yadav uses a variety of methods (*e.g.,* business registrations, terms of service, and media reports) to establish where a company behind a website is located, and opines that the following exchanges are based in the United States: Coinbase, Kraken, Poloniex, and Bittrex.[1] I agree with this assessment. While Prof. Yadav does not perform any analysis of Binance.US, the same factors utilized in her analysis of the other U.S.-based exchanges show that Binance.US is also based in the United States.[2] (Binance.US represents itself as a Delaware Corporation. Its Terms of service is governed by the State of California. Binance.US has an office in San Francisco, California).

[1] Yadav Report at 65, 66, 70, and 71.

[2] BAM-SDNY2_00001; BAM-SDNY2_00015; BAM-SDNY_00034

For all five exchanges above, I use an additional method to confirm these details. For security reasons, exchange services offer their websites over an encrypted channel between the users' browser and the server of the website. The presence of encryption is denoted in the browser with a lock beside the URL.



The protocol used is called `https://` and it provides three properties: (1) encryption to keep data on the channel confidential, (2) message integrity to ensure data on the channel is not undetectably modified, and (3) server authentication to ensure the channel from the user's browser ends at the actual website they are accessing. In order to provide server authentication, the website is required to produce a certificate that attests to the user's browser that it is fetching the correct cryptographic keys for the website. Certificates are issued by organizations called certificate authorities (CAs). Although it is not necessary, many businesses elect to include information such as their address or location in their certificate, which is then signed by the CA. Recently issued certificates are logged by servers in a protocol called certificate transparency (CT).

Coinbase. The website `https://www.coinbase.com/` has many certificates in CT. Some are through a load-balancing service called Cloudflare and others have been issued directly by Coinbase. In its most recent direct certificate, valid 12 June 2023 – 12 June 2024, Coinbase lists the following information:[3]

[3] "ID 9966495721," crt.sh, Retrieved Aug 2023.

```
Subject:
    1.3.6.1.4.1.53087.1.4 = 6687920
    1.3.6.1.4.1.53087.1.3 = US
    1.3.6.1.4.1.53087.1.13 = Registered Mark
    commonName                = Coinbase, Inc.
    organizationName          = Coinbase, Inc.
    streetAddress             = 548 MARKET ST STE 23008
    localityName              = SAN FRANCISCO
    stateOrProvinceName       = CALIFORNIA
    countryName               = US
    serialNumber              = 5154317
    businessCategory          = Private Organization
    jurisdictionStateOrProvinceName = Delaware
    jurisdictionCountryName   = US
```

This information overlaps with the FinCEN money service business (MSB) registration for Coinbase, Inc., although there the address is listed as 430 California Street, San Francisco.[4]

Kraken. The website `https://www.kraken.com` has many certificates in CT and most of these certificates do not list a business address or country. However some subdomains have certificates with information. As one recent example, Kraken lists in a certificate for `api.futures.kraken.com`, valid 1 Jun 2023 – 1 Jun 2024, the following information about the company (Payward, Inc) that operates the website:[5]

```
Subject:
    commonName                = api.futures.kraken.com
    organizationName          = Payward, Inc.
    localityName              = San Francisco
    stateOrProvinceName       = California
    countryName               = US
```

This information matches the FinCEN MSB registration for Payward Ventures Inc. (DBA Name: Kraken) which adds the street address 100 Pine Street, Suite 1250, San Francisco.[6]

Poloniex. The website `https://poloniex.com` has many certificates in CT. A few recent, but no longer valid, certificates do such as one valid 26 Jul 2019 – 26 Jul 2021 which presents

[4] 31000203925685, MSB Registration Status Information, FinCEN, Signed: 11/30/2021

[5] "ID 9542433278," crt.sh, Retrieved Aug 2023.

[6] 31000239561651, MSB Registration Status Information, FinCEN, Signed: 03/22/2023

the following information:[7]

```
Subject:
    commonName                = poloniex.com
    organizationName          = Poloniex, LLC
    localityName              = Boston
    stateOrProvinceName       = Massachusetts
    countryName               = US
    serialNumber              = 5959580
    jurisdictionStateOrProvinceName = Delaware
    jurisdictionCountryName   = US
    businessCategory          = Private Organization
```

This information matches the FinCEN MSB registration for Poloniex LLC which adds the street address 99 High Street, Suite 1701, Boston.[8]

Bittrex. The website `https://bittrex.com` has many certificates in CT and most of these certificates do not list a business address or country. However for one subdomain `https://trust.bittrex.com` the certificate, valid 28 Feb 2023 – 30 Mar 2024, lists the following information:[9]

```
Subject:
    commonName                = trust.bittrex.com
    organizationName          = Bittrex, Inc
    localityName              = Seattle
    stateOrProvinceName       = Washington
    countryName               = US
```

This information matches the FinCEN MSB registration for Brittrex Inc which adds the street address 701 Fifth Avenue, Suite 4200, Seattle.[10]

Binance.US. The website `https://www.binance.us` has many certificates in CT such as the most recent one, valid 11 Aug 2023 – 10 Sep 2024, where Binance.US lists the following information:[11]

[7] "ID 1716208029," crt.sh, Retrieved Aug 2023.

[8] 31000204884335, MSB Registration Status Information, FinCEN, Signed: 12/14/2021

[9] "ID 8763262277," crt.sh, Retrieved Aug 2023.

[10] 31000233518921, MSB Registration Status Information, FinCEN, Signed: 12/27/2022

[11] "ID 10116234857," crt.sh, Retrieved Aug 2023.

```
Subject:
    commonName                = *.binance.us
    organizationName          = BAM TRADING SERVICES INC.
    localityName              = Palo Alto
    stateOrProvinceName       = California
    countryName               = US
```

This information matches the FinCEN MSB registration for BAM Trading Services Inc which adds the street address 611 Cowper Street Suite 400, Palo Alto.[12]

3 Clarifications on Blockchain Technology

The bulk of Prof. Yadav's expert report deals with centralized exchanges. The report also describes the technology behind blockchain systems. It does so without specifying a specific system it is describing, and many details can vary between systems. I will base my clarifying comments on things that are true within the XRP Ledger, as well as the two leading blockchains: Bitcoin and Ethereum.

Centralized Exchanges. Most centralized exchanges in the United States operate similar to the following. Users deposit the digital asset they wish to trade prior to trading. The exchange then takes custody of the asset until the trader wishes to withdraw. To deposit a digital asset on a typical exchange, the user first creates an account with the exchange and is then provided a unique blockchain address where they can deposit their assets through the blockchain system. Once the deposit is finalized on the blockchain system, the exchange will update the user's balance on the exchange itself.

Subsequent trading on the exchange is accounted for within the exchange's internal accounting system and not reflected through transactions on the blockchain. For housekeeping, the exchange may use blockchain transactions to sweep cryptoassets from the user-specific deposit addresses into more general addresses that pool assets with well-defined internal controls. Such actions are initiated by the exchange, invariant to the user's activity as the assets at this point are in custody of the exchange. However, when a user withdraws a

[12] 31000229445266, MSB Registration Status Information, FinCEN, Signed: 10/31/2022

digital asset, the exchange will send the user the digital asset through an on-chain transfer to an address provided by the user. This transaction would be reflected on the blockchain. In short, depositing and withdrawing are the primary user-initiated actions that require a blockchain transaction.

Identities. Prof. Yadav's report discusses the components on a blockchain payment, noting the validators on the blockchain check certain key components of the transaction including determining, "[the payer's] digital identity" and "the identity of the payee." As described in my expert report, funds are held in addresses which are numerical representations of the cryptographic data needed to confirm digital signatures. Users are free to generate as many addresses as they want and some software clients (in particular in Bitcoin) generate new addresses automatically without direct indication to the user. Blockchain validators only confirm transactions are properly signed, they do not validate anything beyond that concerning the "identity" of the sender. For payees, nothing is checked beyond the fact that the receiving address is in the correct digital format. The address might not belong to any user or exist. Sometimes users purposely "burn" their assets by sending them to an address that does not exist (called "proof of burn" by protocols that deploy this feature).

Immutability. Prof. Yadav's report asserts that blockchain "offers several advantages to its users, including: (i) transparency by allowing the entire ledger to be examined; and (ii) immutability and irreversibility of the transaction record."

It is correct that blockchains generally provide a public copy of the entire ledger but inspecting it is subject to validators retaining at least one copy of the ledger. As a counter-example, the earliest transactions in the XRP Ledger have been lost and are unavailable for examination. This is described in more detail in my expert report.

It is correct that blockchains provision immutability and irreversibility but it is with an important and missing caveat: enough (a quorum) validators need to agree to enforce these properties for them to hold. If enough validators agree to change a transaction or reverse a transaction or break any rule of the protocol, the protocol is capable of doing so. An

example would be the decision of Ethereum validators to reverse the consequences of a $50M USD hack on a smart contract called *The DAO* in 2016, which broke the immutability of the blockchain to recover the stolen funds.

This event is later described on Page 30 of Prof. Yadav's report, although the report positions the response of the validators as being "forced" when it was in fact a freely made decision. In fact, some validators decided against it and continue, to this day, operating a variant of Ethereum called Ethereum Classic that does not reverse this attack. Additionally, the decision was made by the validators themselves and becomes realized when enough (a majority in Ethereum's case) implement the change. The Ethereum Foundation suggested the change and provided the software to the valdiators that implements the change, but the Ethereum Foundation itself cannot actuate the change. This is in contrast to Prof. Yadav's report which asserts, "Ethereum's leadership used a 'hard fork' to reverse the hack and reset users' balances."

Privacy and Encryption. In describing the network of validators that operate in a blockchain system, Prof. Yadav's report asserts that "...networks rely on encryption to engineer user and transaction privacy. Encryption must be strong enough throughout to prevent determined actors from breaking the code and uncovering underlying information in the blocks as well as about the users." It also adds,"encryption ought to also prevent theft of information and maintain user privacy." These assertions are made with citation to the MIT Technology Review article, "How secure is blockchain really" by Mike Orcutt (25 Apr 2018).[13]

Contrary to Yadav's assertion, encryption is not used in blockchain networks and no data confidentiality provisions are provided by default in Bitcoin, Ethereum or the XRP Ledger. In fact, Orcutt's article makes no mention of either encryption or privacy, and describes blockchain technology accurately.

Blockchain systems use cryptography, which is often confused with encryption. Cryptography is a broader suite of primitives to assist with keeping data confidential (*e.g.,* en-

[13]Note that Prof. mistakenly cites the title of the article as 'How secure is bitcoin really."

cryption) and preventing undetectable modification to data (*e.g.,* digital signatures). Some primitives offer both (*e.g.,* hash functions). Blockchains use digital signatures and hash functions only, they do not use encryption. The use of digital signatures and hash functions are only to ensure data integrity: that data cannot be modified without detection. While encryption can be layered onto a blockchain system to provide confidential transactions, major blockchains (like the XRP Ledger, Bitcoin and Ethereum) do not use encryption natively.

The consequence of this is that blockchains do not prevent determined actors from "breaking the code", "uncovering underlying information in the blocks," or "uncovering underlying information . . . about the users." In fact all transaction records in all blocks are public. This enables validators to perform their necessary checks on the data.

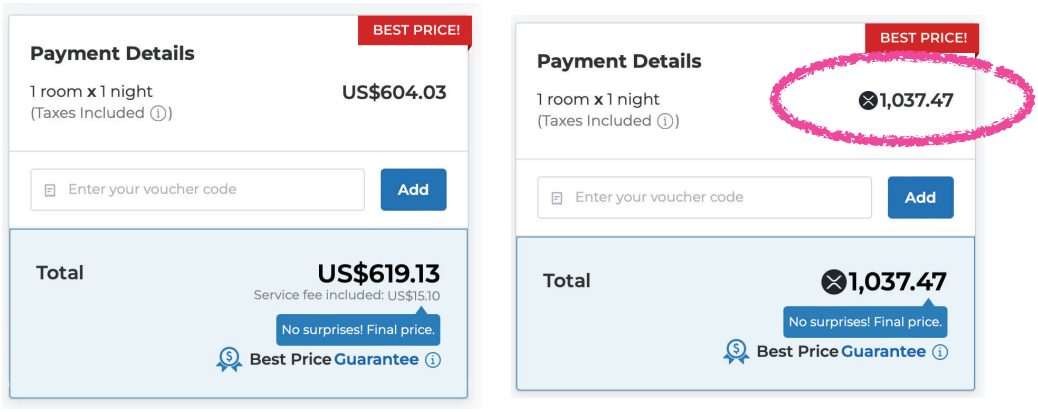
4 Currencies

Unit of account. On page 34 of Prof. Farrell's expert report, a discussion is presented on whether XRP fulfills the three properties of money. One of the three properties is "unit of account." A currency that is used to denote the value of assets and liabilities is said to fulfill this property. For XRP, Prof. Farrell offers two examples: "Hostsailor (a web-hosting service) accepts XRP as payments. Another example is the travel site Travala, which quotes the price of a hotel room in XRP and accepts XRP as payment."

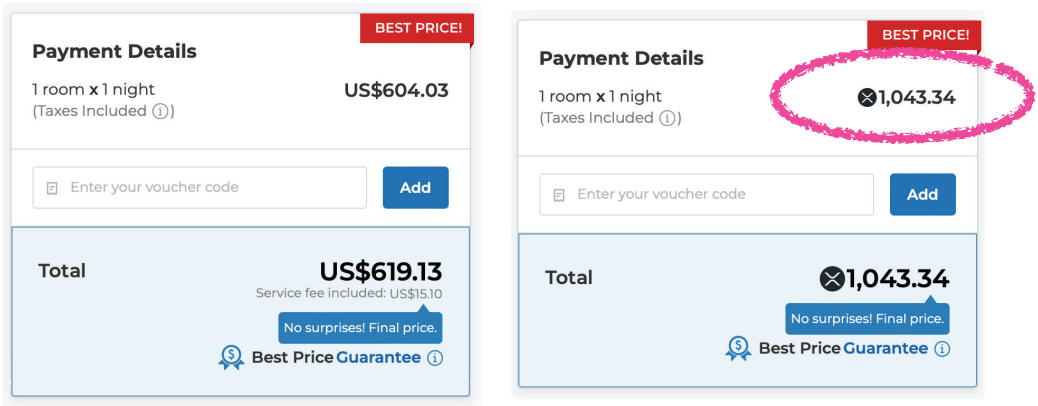
In fact, these examples illustrate that XRP is *not* a unit of account. In both cases, the prices are first quoted in USD. Upon checkout, opting to pay in XRP results in the website determining the price of XRP in USD and offering a quote in XRP. Since the price of XRP in USD changes, the quote itself will change as well. As a consequence, Hostsailor notes,"you will have 20 minutes to make the transaction.[14]" Similarly on Travela, waiting on the payment confirmation screen results in a warning "You've scored a great price for this room. If you leave now, we can't hold the room and rate for you" and ultimately, "the prices and availability have expired. Please refresh to receive the latest search results." Refreshing the page, the price in USD is unchanged but proceeding to the payment screen and selecting

[14] "How to buy host with cryptocurrencies?," Hostsailor, Retrieved Aug 2023.

XRP results in a slightly different quoted price:



1 PM



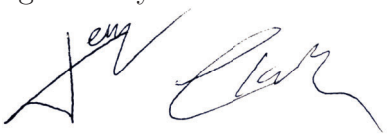
2 PM

In the figure, requesting a hotel room is quoted at $604.03 USD plus fees for $619.13 USD. Selecting XRP results in a quote of 1037.47. An hour later, the room is still $604.03 USD (plus fees) but selecting XRP now results in an updated quote of 1043.34 because the price of XRP in USD has decreased over the hour. This illustrates that the website maintains the price of the room in USD and therefore USD (a currency) is the unit of account. While XRP can be used for payment instead of USD, because it is not the unit of account, the website does not have an inherent price in XRP for the room. So it instead uses a spot conversion and offers to accept the quote in XRP for a limited time in order to protect the site against volatility in the USD price of XRP.

Finally note that neither Hostsailor or Travala are well-known sites. Similarweb (NYSE: SMWB) is a company providing website rankings. Hostsailor is ranked 1360932[15] and Travala is 171282.[16] By comparison, GoDaddy is ranked 899[17] and Expedia is 290.[18]

5 Declaration

The opinions expressed in this report are based on my review and analysis of the documents I cite. I reserve the right to supplement my report and analysis based on any new evidence brought to my attention.



August 30, 2023

Montreal, QC, Canada

[15] "hostsailor.com ranking," similarweb, Retrieved Aug 2023.

[16] "travala.com ranking," similarweb, Retrieved Aug 2023.

[17] "godaddy.com ranking," similarweb, Retrieved Aug 2023.

[18] "expedia.com ranking," similarweb, Retrieved Aug 2023.

6 List of Additional Materials Considered

Expert Reports

- Expert Report of Joel Seligman (6/7/23)
- Expert Report of Steven Feinstein (6/7/23)
- Expert Report of Steven Feinstein (8/4/23)
- Expert Report of Alan Schwartz (7/18/23)
- Expert Report of Allen Ferrell (7/18/23)
- Expert Report of Bradley Borden (7/18/23)
- Expert Report of Peter Easton (7/18/23)
- Expert Report of Yesha Yadav (7/18/23)

Public Court Filings

- *In re Ripple Labs Inc. Litigation*, Case 4:18-cv-06753-PJH (N.D. Cal.) dkt 264 (Order Granting Motion for Class Certification)
- *SEC v. Ripple Labs*, Case 1:20-cv-10832-AT-SN (S.D.N.Y.) dkt 874 (Order)
- *SEC v. Ripple Labs,* Case 1:20-cv-10832-AT-SN (S.D.N.Y.): Motions for Summary Judgment (including oppositions and replies) and supporting documentation and exhibits

Online Materials

- Binance.US, available at https://www.binance.us/
- Bittrex, available at https://bittrex.com/.
    - Additionally cited at https://trust.bittrex.com/
- Coinbase, available at https://www.coinbase.com/.
- Hostsailor, available at https://hostsailor.com/.
- Hostsailor, How to buy host with cryptocurrencies?, available at https://hostsailor.com/how-to-pay-with-cryptocurrencies/.
- "ID 1716208029" (Jul. 28, 2019), available at https://crt.sh/?id=1716208029. Retrieved Aug. 2023.
- "ID 8763262277" (Feb. 28, 2023, available at https://crt.sh/?id=8763262277. Retrieved Aug. 2023.

- "ID 9542433278" (Jun. 1, 2023), available at https://crt.sh/?id=9542433278. Retrieved Aug. 2023.
- "ID 9966495721" (Jul. 22, 2023), available at https://crt.sh/?id=9966495721. Retrieved Aug. 2023.
- "ID 10116234857" (Aug. 11, 2023), available at https://crt.sh/?id=10116234857. Retrieved Aug. 2023.
- Kraken, available at https://www.kraken.com/.
    - Additionally cited at https://api.futures.kraken.com/.
- Orcutt, Mike; How secure is blockchain really? (Apr. 25, 2018); available at https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/.
- Poloniex, available at https://poloniex.com/.
- Similarweb, "expedia.com ranking," available at https://www.similarweb.com/website/expedia.com/. Retrieved Aug. 2023.
- Similarweb, "godaddy.com ranking," available at https://www.similarweb.com/website/godaddy.com/. Retrieved Aug. 2023.
- Similarweb, "hostsailor.com ranking," available at https://www.similarweb.com/website/hostsailor.com/. Retrieved Aug. 2023.
- Similarweb, "travala.com ranking," available at https:// https://www.similarweb.com/website/travala.com/. Retrieved Aug. 2023.
- Travala, available at https://travala.com./

Produced Documents

- BAM-SDNY2_00001
- BAM-SDNY2_00015
- BAM-SDNY_00034
- RPLI_02089389

Other Materials

- 31000203925685, MSB Registration Status Information, FinCEN, Signed: 11/30/2021

- 31000204884335, MSB Registration Status Information, FinCEN, Signed: 12/14/2021
- 31000229445266, MSB Registration Status Information, FinCEN, Signed: 10/31/2022
- 31000233518921, MSB Registration Status Information, FinCEN, Signed: 12/27/2022
- 31000239561651, MSB Registration Status Information, FinCEN, Signed: 03/22/2023

Any and all other materials referenced in my report.