Summary Research Note on Circle Internet Financial Ltd.

Contents

Recent Events and the Importance of Taxonomy 1

ANALYSIS - Circle Internet Financial Ltd 2

About Stablecoins, Circle's biggest product, by far 2

How Safe Are Circle's USDC Stablecoins? 4

Can Circle's consistent and increasing losses infect the stablecoins held on balance sheet? 7

Assessng IP covering chains that USDC are offered through... 15

Ethereum 15

Solana 16

Bitcoin as a yield generator and as an asset traded through Circle 17

Disclaimer 20

Recent Events and the Importance of Taxonomy

Bloomberg reports in its Technology section, 'Terra $45 Billion Face Plant Creates Crowd of Crypto Losers' and " 'Everything Broke': Terra Goes From DeFi Darling to Death Spiral" wherein they detail the failure of what they (as an old school concern) say are shortcomings in crypto and DeFi. Terra's problem was very, very simple, yet many either ignore it or fail to understand it. They based their entire system on a methodology that has not proven to work over time, since inception – at least not yet. That methodology is stabilizing digital assets in a "centralized" decentralized market (ex. fractured pricing and liquidity) around a traditional asset that does not exist natively on the blockchain. A shorter way of saying that is algorithmic stablecoin. To my knowledge, and I may be wrong here, every stablecoin that has had significant volume has broken the buck under pressure. Now, physically backed stablecoins have broken the buck as well, but you always have good ole fashion human greed manifested through arbitrage to save the day there. This greed factor works in the opposite direction when it comes to algo coins. This is not a secret hence no one should have been surprised about what happened over there at Terra Labs.

My name is Reggie Middleton, and I'm the storied, founder and patented (US11196566 and JP6813477**)** creator of DeFi.

I'm here to truly educate you…

Bloomberg also reported in its "Finance" section: "The Crisis at Celsius Is Rocking DeFi and Crypto". I mention the sections because nuance is actually very important here. Crypto, and more to the point, DeFi, is nearly purely technology and IP driven. It is not finance, it is technology – a technology that can be used to dramatically improve finance, but technology, nonetheless. Those that fail to understand this are quite likely toing to get their $sses handed to them over time. Further to the title of the article, this has nothing to with DeFi. It is CeFi (centralized finance, yes – that traditional stuff)

which is rocked by this scandal, and it is CeFi which funds, operates and is most effected by the profligate consumption of risk over reward that is common between all three of the aforementioned articles, the extant and current news cycle and unfortunately, this report as well.

The media is not anxious to report the truth and facts, for if it was you would have heard of me a long time ago. The negative and unproven allegations against me actually do catch wind in the media, but the proven and positive accomplishments haven't been covered since 2014, write about the time I invented DeFi - which is also quite unfortunate, Draw from that what you may. I digress, thus back to the topic at hand and the tenor of the Bloomberg articles…

Reference the latest funding rounding Circle Internet Financial – a prominent crypto company that issues the number two stablecoin in the industry, above that of the recently demised UST from Terra labs They are similar in operations to Celsius, BlockFi, Genesis Trading, etc. in that they use the products of DeFi technology to conduct CeFi and TradFi (traditional finance) business. What's wrong with that? Well, imagine tacking a high-powered Tesla Plaid motor onto a horseshoe, then writing articles about the shortcomings of electric care technology when the horse breaks its leg! Yep!

Now, note that DeFi protocols, which are purely (or at least, they're supposed to be) smart contract driven, are humming along just fine.

This goes to show that the media, the management and above all, the regulators, still have no clue as to what this space is about.

It is about technology and IP, just like the internet in 1995. No one should be trying to make IP packets securities and tradeable, speculative SEC-bait, and doing so now will not work any better than doing so then.

ANALYSIS - Circle Internet Financial Ltd.

The Company incurred a net loss of ~USD508mn the year ending December 2021, and said loss is expected to increase soon (likely, already) as further negative mark-to-market adjustments in convertible debt will be required, considering the deteriorating current market conditions. There is a significant doubt (and we believe the Company shares this doubt) that Circle can and will continue as an ongoing concern without a substantial bailout. To be clear, we believe that this is a s*olvency issue*, and not a *liquidity issue*.

About Stablecoins, Circle's biggest product, by far…

Please note that Circle-issued USDC is the number two stablecoin in the entire crypto market, even though its' issuer is apparently insolvent, from what we were able to gather, albeit on very short notice and cursory observation.

About 90 days ago, before UST broke the buck (de-pegged from the actual dollar), Tether, USDC, and TerraUSD were the first, second and third top stablecoins in the cryptosphere by market cap (truly inaccurate and horrendous way of describing coin size, however, I again digress). Currently, with UST's collapse, Binance's BUSD has taken its place as the number three.

Please note that the fact that Circle's entire business model is built off of what we believe to be unlicensed patented technology, and that Circle's USDC product is "allegedly" regulated should not be lost on the fact that bearer of this message has been alleged by regulators to be a "self-proclaimed" financial guru (despite publicly calling - with full online documentation - Bear Stearns, mortgage/real estate crisis, Lehman, The Pan-European Sovereign Debt Crisis, among many others). That same message bearer was also alleged to have fraudulently marketed international patent applications that they knew were stalled and would not get issued (referencing now-issued patents **US11196566** and **JP6813477** covering stablecoins, Bitcoin, Ethereum, ODL [On Demand Liquidity], Solana, etc.). This is being mentioned to highlight that it is more than possible that being "regulated" is far and away from being right, safe or accurate – for a variety of reasons, most of which would be imprudent to review here.

Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	
Tether USDT	$0.9988	0.01%	0.04%	$66,337,667,700	$43,503,068,164 43,553,848,784 USDT	66,415,102,879 USDT	
USD Coin USDC	$1.00	0.00%	0.04%	$55,818,924,202	$5,028,424,574 5,026,954,476 USDC	55,802,605,113 USDC	
Binance USD BUSD	$0.9996	0.05%	0.13%	$17,571,337,985	$6,130,893,421 6,122,479,836 BUSD	17,547,224,379 BUSD	

Circle's USD is almost exactly 40% of the stablecoin market, and the stablecoin market is currently what the freely traded cryptocurrency market rests upon. Eight days after a published audit, there's a billion-dollar deficit in USDC reserves, but the disclaimers posted can potentially justify that. So far, so good, no?

GRANT THORNTON LLP
757 Third Ave., 9th Floor
New York, NY 10017

D +1 212 599 0100
F +1 212 370 4520

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

Board of Directors and Management
Circle Internet Financial, LLC

We have examined management of Circle Internet Financial, LLC's assertion that the following information (hereafter, the "Reserve Account Information") in the accompanying Reserve Account Report as of May 31, 2022 at 11:59 PM Pacific Time ("PT") ("Report Date") is fairly stated, based on the criteria set forth in the Reserve Account Report.

- USD Coin ("USDC") in Circulation[1] = 54,005,995,420 USDC
- The total fair value of US dollar denominated assets held in segregated accounts are at least equal to the USDC in Circulation at the Report Date

Circle Internet Financial, LLC's management is responsible for its assertion. Our responsibility is to express an opinion on the Reserve Account Information in the accompanying Reserve Account Report based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether the Reserve Account Information in the accompanying Reserve Account Report is fairly stated, based on the criteria set forth in the Reserve Account Report, in all material respects. An examination involves performing procedures to obtain evidence about the Reserve Account Information. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of the Reserve Account Information, whether due to fraud or error. In making an assessment of the risks of material misstatement, we considered and obtained an understanding of internal control relevant to the preparation of, and the Reserve Account Information in, the accompanying Reserve Account Report in order to design procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of such internal control. Accordingly, no such opinion is expressed. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

[1] Total USDC in circulation is the total USDC supply on USDC approved blockchains less (i) tokens allowed but not issued and (ii) access denied tokens outstanding at the Report Date as reported on USDC approved public blockchains. USDC approved blockchains currently comprise the Algorand, Avalanche, Ethereum, Flow, Hedera, Solana, Stellar and TRON blockchains and are used by Circle Internet Financial, LLC to issue and redeem USDC. USDC approved blockchains do not include any other protocols, frameworks or derivative blockchains.

GT.COM

Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd (GTIL). GTIL and each of its member firms are separate legal entities and are not a worldwide partnership.

According to Circle's website:

> Known as a fully-reserved stablecoin, every digital dollar of USDC on the internet is *100% backed by cash and short-dated U.S. treasuries, so that it's always redeemable 1:1 for U.S. dollars.*
>
> *USDC reserves are held in the custody and management of leading U.S. financial institutions, including BlackRock and BNY Mellon. Each month, Grant Thornton LLP, one of America's largest audit, tax and advisory firms, provides third-party assurance as to the size and composition of the USDC reserves.*

How Safe Are Circle's USDC Stablecoins?

Question du jour? **Are USDC assets held off the balance sheet of Circle, and/or can Circle's creditors gain access to said assets in the case of bankruptcy and/or liquidation?** We have only

spent a day looking into Circle, but stakeholders should be asking these questions and seeking real answers. Luckily, for anyone reading this missive, we've done the work for you…

In relation to the access to the assets in event of bankruptcy/liquidation, the creditors have the priority over the claims of public stockholders. (Kindly refer page No. 98 & 99 of the report).
Source : https://www.sec.gov/Archives/edgar/data/1876042/000110465922056979/tm2124445-8_s4a.htm#fCACS

share in connection with any redemption of their Public Shares. None of Concord's officers or directors will indemnify Concord for claims by third parties including, without limitation, claims by vendors and prospective target businesses.

If, after Concord distributes the proceeds in the trust account to our Public Stockholders, Concord files a bankruptcy petition or an involuntary bankruptcy petition is filed against us that is not dismissed, a bankruptcy court may seek to recover such proceeds, and we and our board of directors may be exposed to claims of punitive damages.

If, after Concord distributes the proceeds in the trust account to our Public Stockholders, they file a bankruptcy petition or an involuntary bankruptcy petition is filed against Concord that is not dismissed,

98

TABLE OF CONTENTS

any distributions received by shareholders could be viewed under applicable debtor/creditor and/or bankruptcy laws as either a "preferential transfer" or a "fraudulent conveyance." As a result, a bankruptcy court could seek to recover all amounts received by Public Stockholders. In addition, the Concord board of directors may be viewed as having breached its fiduciary duty to Concord's creditors and/or having acted in bad faith, thereby exposing it and Concord to claims of punitive damages, by paying Public Stockholders from the trust account prior to addressing the claims of creditors. Concord cannot assure you that claims will not be brought against us for these reasons.

If, before distributing the proceeds in the trust account to our Public Stockholders, Concord files a bankruptcy petition or an involuntary bankruptcy petition is filed against us that is not dismissed, the claims of creditors in such proceeding may have priority over the claims of our shareholders and the per share amount that would otherwise be received by Public Stockholders in connection with our liquidation may be reduced.

If, before distributing the proceeds in the trust account to Public Stockholders, Concord files a bankruptcy petition or an involuntary bankruptcy petition is filed against Concord that is not dismissed, the proceeds held in the trust account could be subject to applicable bankruptcy law, and may be included in our bankruptcy estate and subject to the claims of third parties with priority over the claims of Public Stockholders. To the extent any bankruptcy claims deplete the trust account, the per share amount that would otherwise be received by Public Stockholders in connection with our liquidation may be reduced.

Concord's directors may decide not to enforce indemnification obligations against the Sponsor, resulting in a

UNAUDITED PRO FORMA CONDENSED

COMBINED BALANCE SHEET

DECEMBER 31, 2021

($ in thousands, except share and per share amounts)	Concord Historical	Circle Historical	Assuming No Redemptions: Transaction Accounting Adjustments	Note	Assuming No Redemptions: Pro Forma	Assuming Maximum Redemptions: Additional Transaction Accounting Adjustments	Note	Assuming Maximum Redemptions: Pro Forma
Assets								
Current assets								
Cash and cash equivalents	$ 192	$ 161,564	$ 276,051	3a	$ 787,702	$ —		$ 511,651
			400,000	3b		—		
			(30,095)	3c		—		
			(20,010)	3d		—		
			—			(276,051)	3n	
Cash and cash equivalents segregated for benefits of customers and USDC holders	—	42,470,603	—		42,470,603	—		42,470,603
Accounts receivable	—	22,703	—		22,703	—		22,703
USDC receivable	—	154,837	—		154,837	—		154,837
Digital assets safeguarded on behalf of customers	—	738,365	—		738,365	—		738,365
Divestment consideration receivable, current	—	1,000	—		1,000	—		1,000
Prepaid expenses and other current assets	216	23,163	(10,945)	3e	12,434	—		12,434
Total current assets	**408**	**43,572,235**	**615,001**		**44,187,644**	**(276,051)**		**43,911,593**
Securities held in Trust Account	276,051	—	(276,051)	3a	—	—		—
Restricted cash for operations	—	20,959	—		20,959	—		20,959
Divestment consideration receivable, non-current	—	1,000	—		1,000	—		1,000
Long-term investments	—	28,233	—		28,233	—		28,233
Fixed assets, net	—	1,225	—		1,225	—		1,225
Digital assets, net	—	242,073	—		242,073	—		242,073
Goodwill	—	24,014	—		24,014	—		24,014
Intangible assets, net	—	6,606	—		6,606	—		6,606
Total assets	**$276,459**	**$43,896,345**	**$ 338,950**		**$44,511,754**	**$(276,051)**		**$44,235,703**

The **USDC assets sits on the Circle's balance sheet.** (Refer Page No. 110 of the report)

Liabilities, Redeemable Convertible Preferred Stock and Shareholders' Equity								
Current liabilities								
Accounts payable and accrued expenses	$ 194	$ 53,343	$ 90,000	3c	$ 143,537	—		$ 143,537
Deferred revenue	—	415	—		415	—		415
Loans payable, net of debt discount	—	24,039	—		24,039	—		24,039
USDC borrowed	—	154,837	—		154,837	—		154,837
Digital assets held as collateral	—	191,810	—		191,810	—		191,810
Digital assets safeguarding obligations to customers	—	738,365	—		738,365	—		738,365
Deposits from customers and USDC holders	—	42,316,946	—		42,316,946	—		42,316,946
Total current liabilities	**194**	**43,479,755**	**90,000**		**43,569,949**	—		**43,569,949**
Long-term liabilities								
Deferred rent	—	301	—		301	—		301
Convertible debt, net of debt discount	—	904,122	(853,356)	3f	50,766	—		50,766
Warrant liability	38,335	1,349	—		39,684	—		39,684
Earnout shares liability	—	—	1,472,390	3g	1,472,390	(37,053)	3g	1,435,337
Total long-term liabilities	**38,335**	**905,772**	**619,034**		**1,563,141**	**(37,053)**		**1,526,088**
Total liabilities	**38,529**	**44,385,527**	**709,034**		**45,133,090**	**(37,053)**		**45,096,037**
Commitments and contingencies								

Contact us via WhatsApp, SMS or phone – 1-212-300-5600

Source : https://www.sec.gov/Archives/edgar/data/1876042/000110465922056979/tm2124445-

Can Circle's consistent and increasing losses infect the stablecoins held on balance sheet?

It is not far-fetched to presume that those CBDC assets will be fought over by creditors bickering over the carcass of fallen Circle, if such an event were to come to pass – and both Circle and Veritaseum don't view that as a remote possibility.

A quick summary timeline revealing the balance of this report…

- **Up until 2019**: Money losing operations…
- **December 2020:** Circle reports doubt of ability to remain an ongoing concern
- **May 2021**: $400M+ cash injection by BlackRock, Inc., Fidelity Management and Research, Marshall Wace LLP and Fin Capita. Keep in mind that, backed by American investment bank Goldman Sachs, Circle is a major stablecoin partner of payments giant Visa. Big players don't want Circle to go down!
- **December 2021**: >$400M M2M loss. Throwing Good Money After Bad!
- **Now 2022**: Even further, and even more dramatic, erosion of core digital asset values

> *Circle is regulated as a licensed money transmitter under U.S. state law just like PayPal, Stripe, and Apple Pay. Circle's financial statements are audited annually and subject to review by the SEC.*

Within the next couple of days, we will be publishing a ~100-page forensic analysis of Coinbase (Circle's partner in Centre, the governance arm for USDC), much more in depth and involved than this anecdotal research. Until then, please continue to read to find out the reasoning behind our stated opinion.

Income Statement as of December 31

All figures are in USD ('000)

	The year ended December 31			
	2021	**2020**	**Variance**	**% Change**
Revenue and USDC interest income				
Transaction and Treasury Services	47,547	2,589	44,958	1,736.5%
USDC interest income	28,464	4,435	24,029	541.8%
Seed Invest revenue	8,866	8,417	449	5.3%
Total revenue and USDC interest income	**84,877**	**15,441**	**69,436**	**449.7%**
Third-party transaction costs				
Transaction and Treasury Services costs	30,731	785	29,946	n.m
USDC income sharing and transaction costs	11,890	2,826	9,064	320.7%
Total third-party transaction costs	**42,621**	**3,611**	**39,010**	**1,080.3%**
Operating expenses				
Compensation expenses	68,170	18,932	49,238	260.1%
General and administrative expenses	31,125	13,916	17,209	123.7%
Depreciation and amortization expense	3,945	4,500	(555)	(12.3)%
IT infrastructure costs	5,379	3,716	1,663	44.8%
Marketing and advertising expenses	13,697	400	13,297	n.m
Digital assets impairment, net	6,038	1,256	4,782	n.m
Total operating expenses	**128,354**	**42,720**	**85,634**	**200.5%**
Operating loss from continuing operations	**(86,098)**	**(30,890)**	**(55,208)**	**178.7%**

Contact us via WhatsApp, SMS or phone – 1-212-300-5600

Other income (expense), net	(417,761)	13,692	(431,453)	n.m.
Net loss before income taxes	(503,859)	(17,198)	(486,661)	2,829.8%
Income tax expense	4,854	115	4,739	n.m
Net loss from continuing operations	**(508,713)**	**(17,313)**	**(491,400)**	**(2,838.3)%**
Discontinued operations, net of taxes				
Gain (loss) from operations of discontinued Circle Trade business	1,650	(58)	1,708	2,944.8%
Gain from operations of discontinued Circle Invest business (including gain on disposal of $0.6 million for the year ended December 31, 2020)	28	730	(702)	(96.2)%
Gain (loss) from operations of discontinued Poloniex business	**(1,171)**	20,431	(21,602)	(105.7)%
Net income (loss)	**(508,206)**	**3,790**	**(511,996)**	**(13,509.1)%**

Other income (expense), net

The following table presents major categories of other income (expense), net. It appears as if a very convenient Level 3 style calculation saved the day in the red marker:

Contact us via WhatsApp, SMS or phone – 1-212-300-5600

Other Income *All figures are in USD ('000)*		**The year ended December 31**	
Particulars		**2021**	**2020**
Realized gains on investments		18,010	—
Unrealized gains (losses) on investments		(13,107)	13,221
Change in fair value of embedded derivatives Are these bear hedges? If not, looks fishy. What are liquidity, construction, slippage and tracking looking like? What is the modelling accuracy and input assumptions.		48,032	—
Change in fair value of convertible debt Circle issued >~$400m in convertible notes and lost more than that the same reporting period. There's a malaise going in those books. Stakeholders should REALLY PAY ATTENTION!		(436,803)	(3,489)
Change in fair value of warrant liability		(1,137)	(212)
Gain on treasury stock		—	2,877
Gain on sale of digital assets		5,956	298
Transaction advisory expenses related to convertible note issuance $31.4M fee for a ~$421M note while 100% of issued value was lost? Smells fishy AF!		(31,379)	—
Interest expense and amortization of discount		(4,772)	(3,363)
Income generated from winding down platforms		1,139	2,371
Transitional support income		—	1,061
Loss on equity method investments		(537)	(769)
Rental sublease income		1,320	942
Other, net		(4,483)	755
Total Other income (expense), net		**(417,761)**	**13,692**

As excerpted from last year's report:

> *Last year **there was substantial doubt of the Company's ability to continue as a going concern**, but that substantial doubt has since been resolved through the issuance of convertible notes. The Company has received significant financing in the form of a convertible note for a total of $441.0 million as of May 2021. The Company believes proceeds received from the financing subsequent to year-end is sufficient to meet the*

Company's cash needs and support their operations for at least the next twelve months from the issuance date of the financial statements.

Note, it's highly likely that Circle would've needed a new cash infusion under the extant circumstances as of the time of that statement. The crypto markets have deteriorated significantly since then, so whatever problems they have had have almost invariably been materially exacerbated.

With the benefit of hindsight, we can now attest to the change in fair value of said convertible debt, issued when there was "substantial doubt" of the Company's survival.

The fair value of convertible debt decreased by USD433.3 million for the year ended December 31, 2021, compared to the year ended December 31, 2020, primarily due to mark-to-market adjustments on convertible debt issued during 2021.

The Company has recognized USD436.8 million of expenses related to the change in the fair value of convertible notes in 2021. This is **based on the historical performance of loans facilitated through its platform**, as well as the consideration of market participant requirements. See below for consolidated financial statements for the fair value measurements of convertible debt.

All values are in USD ('000)	December 31, 2021			December 31, 2020		
Particulars	**Level 1**	**Level 2**	**Level 3**	**Level 1**	**Level 2**	**Level 3**
Assets						
Digital assets safeguarded on behalf of customers	738,365	—	—	67,598	—	—
Digital assets held as collateral(1)	—	—	28,705	—	—	—
Equity securities	—	—	—	13,631	—	1,076
Prepaid expenses and other assets – embedded derivative	—	—	2,979	—	—	—
Divestment consideration receivable	—	—	2,000	—	—	5,000
Total Assets	**738,365**	**—**	**33,684**	**81,229**	**—**	**6,076**
Liabilities						
Convertible debt, net of debt discount	—	—	904,122	—	—	30,614
Digital assets safeguarding obligations to customers	738,365	—	—	67,598	—	—
Acquisition payables	—	—	—	—	—	12,276
Warrant liability	—	—	1,349	—	—	212
Loans payable, net of debt discount	—	—	887	—	—	—
Total Liabilities	**738,365**	**—**	**906,358**	**67,598**	**—**	**43,102**

In 2019, the Company issued convertible notes in connection with the acquisition of SeedInvest. The first note had a par value of USD24.0 million, matures in seven years, and is convertible into Series E preferred shares with a 2.9% interest rate.

The second note had a par value of USD10.0 million and matured in two years with a 6.0% interest rate.

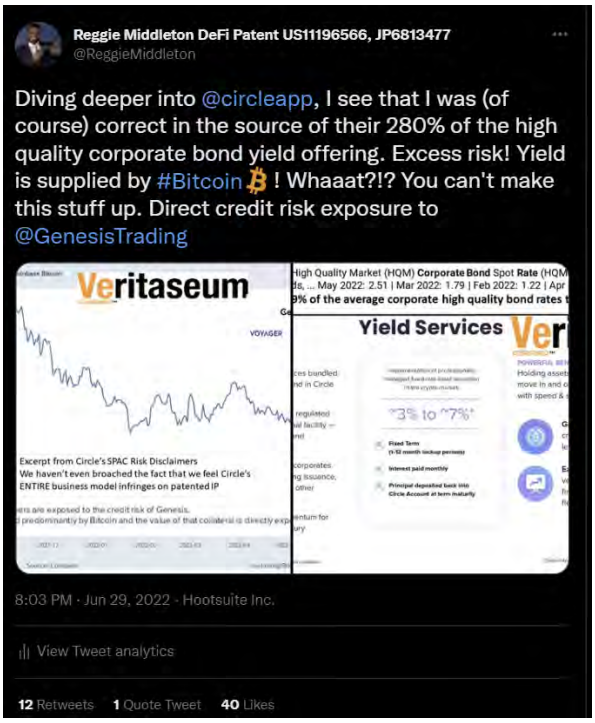
As of July 2021, the Company has raised an additional USD451.0 million from multiple lenders. The Company elected the fair value option for recording these notes, which were recorded at a net discount on the acquisition date. Their fair value was USD904.1 million as of December 31, 2021.

	In USD'000
Balance as of December 31, 2020	30,614
Issuance of convertible notes	451,025
Net discount on convertible notes	514
Capitalized interest	868
Fair value adjustment	436,803
Fair value adjustment – credit risk	(4,972)
Principal payments	(10,730)
Balance as of December 31, 2021	**904,122**

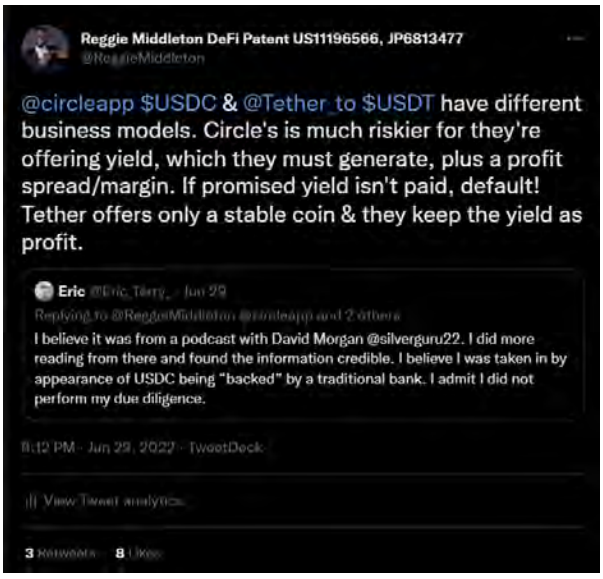
The following significant unobservable inputs were used in the valuation:

	December 31, 2021	**December 31, 2020**
Discount rate	11.5% – 13.0%	13.0%
Volatility	34.8% – 54.2%	42.3%
Risk-free rate	1.0% – 1.9%	0.4%

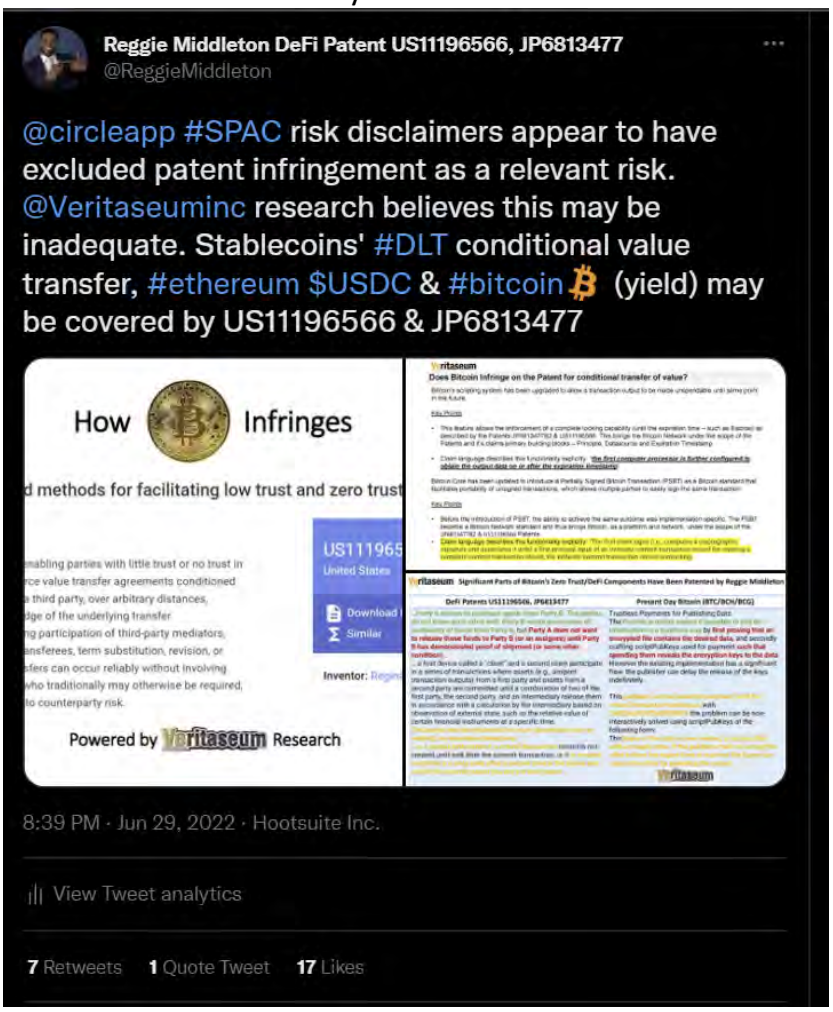
Various tweets of relevance



Join the conversation
https://twitter.com/ReggieMiddleton/status/1542297860577890304?s=20&t=8y9boEkVa1ftLlCj-tFPQg



Join the conversation
https://twitter.com/ReggieMiddleton/status/1542299949462966272?s=20&t=ki321TYVXjeafu_Ze3bzMw



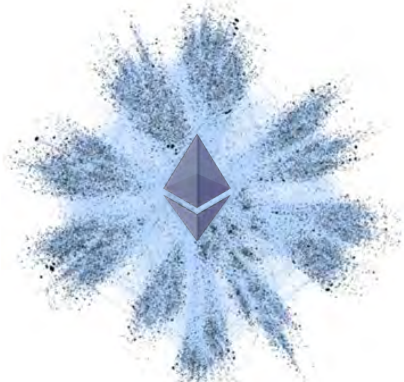
Join the conversation
https://twitter.com/ReggieMiddleton/status/1542306885231341568?s=20&t=qxbPbXEsPyqCDywVaGz2kQ

Summary Research Note on Circle Internet Financial Ltd.

Assessng IP covering chains that USDC are offered through…

Ethereum

Ethereum as a World Computer
Value Transfer through Smart Contracts
Interaction with the Ethereum EVM to transfer value via Smart Contracts.



POS Transaction Fee
Payment of a transaction fee from the user to the block producer (and attesting validator nodes) for using the Ethereum Network.

POW Transaction Fee
Payment of a transaction fee from the user to the block producer for using the Ethereum Network.

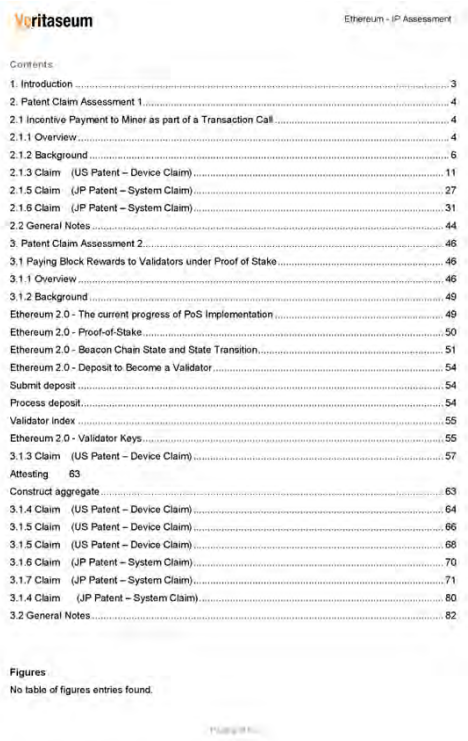
What Do the Foundational TechDeFi Patents US11196566 & JP6813477 Mean for Users of Ethereum? Twitter Discussion: @reggiemiddleton @veritaseuminc

Veritaseum Ethereum - IP Assessment

Ethereum IP Assessment:
Analyzing and Assessing Middleton Patents JP6813477B2 and US11196566B2

4th January 2022

Page 1 of 82


Veritaseum Ethereum - IP Assessment

Contents

1. Introduction 3
2. Patent Claim Assessment 1 4
2.1 Incentive Payment to Miner as part of a Transaction Call 4
2.1.1 Overview 4
2.1.2 Background 6
2.1.3 Claim (US Patent – Device Claim) 11
2.1.5 Claim (JP Patent – System Claim) 27
2.1.6 Claim (JP Patent – System Claim) 31
2.2 General Notes 44
3. Patent Claim Assessment 2 46
3.1 Paying Block Rewards to Validators under Proof of Stake 46
3.1.1 Overview 46
3.1.2 Background 49
Ethereum 2.0 - The current progress of PoS implementation 49
Ethereum 2.0 - Proof-of-Stake 50
Ethereum 2.0 - Beacon Chain State and State Transition 51
Ethereum 2.0 - Deposit to Become a Validator 54
Submit deposit 54
Process deposit 54
Validator index 55
Ethereum 2.0 - Validator Keys 55
3.1.3 Claim (US Patent – Device Claim) 57
Attesting 63
Construct aggregate 63
3.1.4 Claim (US Patent – Device Claim) 64
3.1.5 Claim (US Patent – Device Claim) 66
3.1.5 Claim (US Patent – Device Claim) 68
3.1.6 Claim (JP Patent – System Claim) 70
3.1.7 Claim (JP Patent – System Claim) 71
3.1.4 Claim (JP Patent – System Claim) 80
3.2 General Notes 82

Figures
No table of figures entries found.

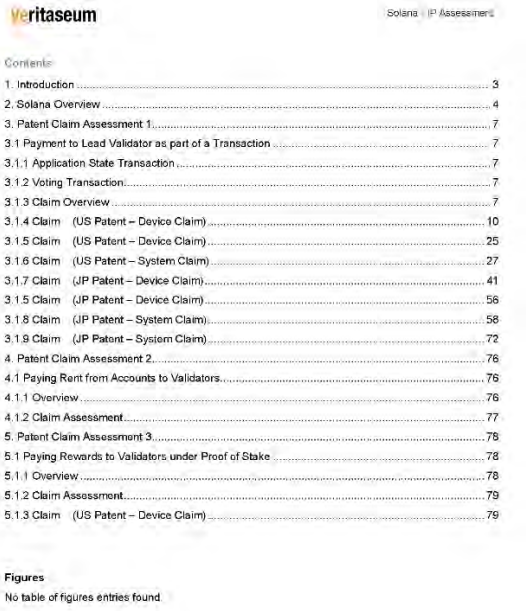
Solana

Veritaseum Solana - IP Assessment

Solana IP Assessment:
Assessing Infringement of Middleton Patents
JP6813477B2 and US11196566B2

4th January 2022

Page 1 of 79


Veritaseum Solana - IP Assessment

Contents

1. Introduction ... 3
2. Solana Overview ... 4
3. Patent Claim Assessment 1 ... 7
3.1 Payment to Lead Validator as part of a Transaction ... 7
3.1.1 Application State Transaction ... 7
3.1.2 Voting Transaction ... 7
3.1.3 Claim Overview ... 7
3.1.4 Claim (US Patent – Device Claim) ... 10
3.1.5 Claim (US Patent – Device Claim) ... 25
3.1.6 Claim (US Patent – System Claim) ... 27
3.1.7 Claim (JP Patent – Device Claim) ... 41
3.1.5 Claim (JP Patent – Device Claim) ... 56
3.1.8 Claim (JP Patent – System Claim) ... 58
3.1.9 Claim (JP Patent – System Claim) ... 72
4. Patent Claim Assessment 2 ... 76
4.1 Paying Rent from Accounts to Validators ... 76
4.1.1 Overview ... 76
4.1.2 Claim Assessment ... 77
5. Patent Claim Assessment 3 ... 78
5.1 Paying Rewards to Validators under Proof of Stake ... 78
5.1.1 Overview ... 78
5.1.2 Claim Assessment ... 79
5.1.3 Claim (US Patent – Device Claim) ... 79

Figures

No table of figures entries found.

Bitcoin as a yield generator and as an asset traded through Circle

Veritaseum

Does Bitcoin Infringe on the Patent for conditional transfer of value?

Bitcoin's scripting system has been upgraded to allow a transaction output to be made unspendable until some point in the future.

Key Points

- This feature allows the enforcement of a complete locking capability (until the expiration time – such as Escrow) as described by the Patents JP6813477B2 & US11196566. This brings the Bitcoin Network under the scope of the Patents and it's claims primary building blocks – Principle, Datasource and Expiration Timestamp
- Claim language describes this functionality explicitly: " ***the first computer processor is further configured to obtain the output data on or after the expiration timestamp*** "

Bitcoin Core has been updated to introduce a Partially Signed Bitcoin Transaction (PSBT) as a Bitcoin standard that facilitates portability of unsigned transactions, which allows multiple parties to easily sign the same transaction.

Key Points

- Before the introduction of PSBT, the ability to achieve the same outcome was implementation specific. The PSBT became a Bitcoin Network standard and thus brings Bitcoin, as a platform and network, under the scope of the JP6813477B2 & US11196566 Patents.
- Claim language describes this functionality explicitly: " The first client signs (i.e., computes a cryptographic signature and associates it with) a first principal input of an inchoate commit transaction record for creating a complete commit transaction record, the inchoate commit transaction record comprising:

Significant Parts of Bitcoin's Zero Trust/DeFi Components Have Been Patented by Reggie Middleto

DeFi Patents US11196566, JP6813477	Present Day Bitcoin (BTC/BCH/BCG)
…Party A wishes to purchase goods from Party B. The parties do not know each other well Party B wants assurances of availability of funds from Party A, but **Party A does not want to release those funds to Party B (or an assignee) until Party B has demonstrated proof of shipment (or some other condition)**… … a first device called a "client" and a second client participate in a series of transactions where assets (e.g., unspent transaction outputs) from a first party and assets from a second party are committed until a combination of two of the first party, the second party, and an intermediary release them in accordance with a calculation by the intermediary based on observation of external state, such as the relative value of certain financial instruments at a specific time. **The assets may be refunded if no such observation can be made by an expiration timestamp** …**In a typical embodiment, a refund transaction** record is not created until well after the commit transaction, or it **is created such that it is only valid after a certain time in the future and only if the commit output has not yet been spent**.	Trustless Payments for Publishing Data The **PayPub protocol makes it possible to pay for information in a trustless way** by **first proving that an encrypted file contains the desired data**, and secondly crafting scriptPubKeys used for payment **such that spending them reveals the encryption keys to the data**. However the existing implementation has a significant flaw: the publisher can delay the release of the keys indefinitely. This **problem can be solved interactively with the refund transaction technique**, with **CHECKLOCKTIMEVERIFY** the problem can be non-interactively solved using scriptPubKeys of the following form: The **buyer of the data is now making a secure offer with an expiry time. If the publisher fails to accept the offer before the expiry time is reached the buyer can cancel the offer by spending the output.**

Bitcoin Network Partially Signed Bitcoin Transaction (PSBT)

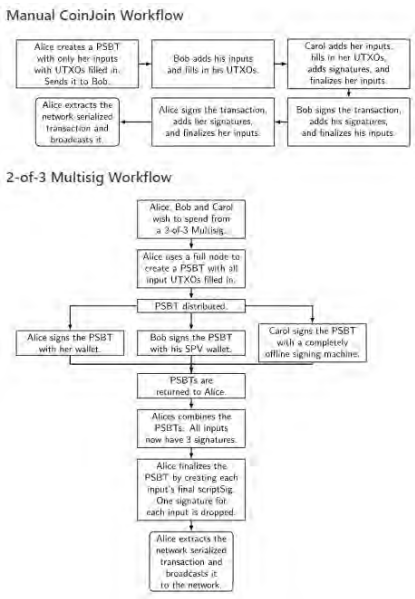
A Partially Signed Bitcoin Transaction (PSBT) is a Bitcoin standard that facilitates portability of unsigned transactions, which allows multiple parties to easily sign the same transaction.

Motivation

Creating unsigned or partially signed transactions to be passed around to multiple signers was implementation dependent, making it hard for people who use different wallet software from being able to easily do so. The goal of the PSBT incorporation was to create a standard and extensible format that can be used between clients to allow people to pass around the same transaction to sign and combine their signatures. The format is also designed to be easily extended for future use which is harder to do with what was the extant transaction formats.

Signing transactions also requires users to have access to the UTXOs being spent. This transaction format allows offline signers such as air-gapped wallets and hardware wallets to be able to sign transactions without needing direct access to the UTXO set and without risk of being defrauded.

```
BIP: 174
Layer: Applications
Title: Partially Signed Bitcoin Transaction Format
Author: Andrew Chow <achow101@gmail.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0174
Status: Final
Type: Standards Track
Created: 2017-07-12
License: BSD-2-Clause
```



0

Veritaseum Bitcoin Network – Partially Signed Bitcoin Transaction (PSBT) Roles & Patent Assessment

Role	Bitcoin Core	JP6813477B2, US11196566 Patent Assessment
Creator --- **Updater**	The Creator creates a new PSBT. It must create an unsigned transaction and place it in the PSBT. The Creator must create empty input and output fields. --- The Updater must only accept a PSBT. The Updater adds information to the PSBT that it has access to. If it has the UTXO for an input, it should add it to the PSBT. The Updater should also add redeemScripts , witnessScripts , and BIP 32 derivation paths to the input and output data if it knows them. A single entity is likely to be both a Creator and Updater.	Client 1 - Inchoate Transaction: The Inchoate Transaction is created by the Client performing the 'Creator' role.
Input Finalizer --- **Transaction Extractor**	The Input Finalizer must only accept a PSBT. For each input, the Input Finalizer determines if the input has enough data to pass validation. If it does, it must construct the 0x07 Finalized scriptSig and 0x08 Finalized scriptWitness and place them into the input key -value map. If scriptSig is empty for an input, 0x07 should remain unset rather than assigned an empty array. Likewise, if no scriptWitness exists for an input, 0x08 should remain unset rather than assigned an empty array. All other data except the UTXO and unknown fields in the input key -value map should be cleared from the PSBT. The UTXO should be kept to allow Transaction Extractors to verify the final network serialized transaction. --- The Transaction Extractor must only accept a PSBT. It checks whether all inputs have complete scriptSigs and scriptWitnesses by checking for the presence of 0x07 Finalized scriptSig and 0x08 Finalized scriptWitness typed records. If they do, the Transaction Extractor should construct complete scriptSigs and scriptWitnesses and encode them into network serialized transactions. Otherwise the Extractor must not modify the PSBT. The Extractor should produce a fully valid, network serialized transaction if all inputs are complete. https://github.com/bitcoin/bips/blob/master/bip -0174.mediawiki#roles	Complete Transaction: The Complete Transaction is created by the Client performing the 'Input Finalizer' and 'Transaction Extractor' roles. Note that all signatories will have signed the inputs which will be in the 'finalized sigScript ' field. *Note:* *The Transaction Extractor does not need to know how to interpret scripts in order to extract the network serialized transaction. However it may be able to in order to validate the network serialized transaction at the same time.* *A single entity is likely to be both a Transaction Extractor and an Input Finalizer*
Signer	The Signer must only accept a PSBT. The Signer must only use the UTXOs provided in the PSBT to produce signatures for inputs. Before signing a non -witness input, the Signer must verify that the TXID of the non -witness UTXO matches the TXID specified in the unsigned transaction. Before signing a witness input, the Signer must verify that the witnessScript (if provided) matches the hash specified in the UTXO or the redeemScript, and the redeemScript (if provided) matches the hash in the UTXO. The Signer may choose to fail to sign a segwit input if a non-witness UTXO is not provided. [7] The Signer should not need any additional data sources, as all necessary information is provided in the PSBT format. The Signer must only add data to a PSBT. Any signatures created by the Signer must be added as a "Partial Signature" key -value pair for the respective input it relates to. If a Signer cannot sign a transaction, it must not add a Partial Signature. The Signer can additionally compute the addresses and values being sent, and the transaction fee, optionally showing this data to the user as a confirmation of intent and the consequences of signing the PSBT.	Device/Facilitator: The Bitcoin Network (i.e., Bitcoin Blockchain as a state machine) that facilitates the sharing and manipulation of the PSBT for ultimate serialisation and submission to the blockchain. As per the patent definitions: "facilitator" (**100**)—A device for facilitating a value transfer between a first party utilizing a first client (**120**, **160**) and a second party utilizing a second client (**120**, **170**) via a transfer mechanism (**110**) according to the invention, the device comprising a computer processor (**160**), a memory (**170**) comprising a transaction record sector and a key pair sector (**200**) for storing an asymmetric key pair, and a network interface (**190**).
Combiner	The Combiner can accept 1 or many PSBTs. The Combiner must merge them into one PSBT (if possible), or fail. The resulting PSBT must contain all of the key -value pairs from each of the PSBTs. The Combiner must remove any duplicate key-value pairs, in accordance with the specification. It can pick arbitrarily when conflicts occur. A Combiner must not combine two different PSBTs. PSBTs can be uniquely identified by 0x00 global transaction typed key -value pair. For every type that a Combiner understands, it may refuse to combine PSBTs if it detects that there will be inconsistencies or conflicts for that type in the combined PSBT.	Transfer Mechanism: The Bitcoin Network includes miners and nodes for receiving complete transactions for inclusion in the mined block.

Disclaimer

Veritaseum LLC and Boom Bust Blog analysis and conclusions in this presentation are based on publicly available information. Veritaseum LLC recognizes that there may be confidential information in the possession of the Companies discussed in the presentation that could lead these Companies to disagree with Veritaseum LLC's conclusions. The analyses provided may include certain statements, estimates and projections prepared with respect to, among other things, the historical and anticipated operating performance of the Companies. Such statements, estimates, and projections reflect various assumptions by Veritaseum LLC concerning anticipated results that are inherently subject to significant economic, competitive, and other uncertainties and contingencies and have been included solely for illustrative purposes. No representations express or implied, are made as to the accuracy or completeness of such statements, estimates or projections or with respect to any other materials herein. Actual results may vary materially from the estimates and projected results contained herein. Veritaseum LLC and its affiliates may own investments that are bullish or bearish on the subject entity in this material. These investments may include credit-default swaps, equity put or call options, warrants and short sales of common stock. Veritaseum LLC is in the business of creating and trading –bringing into existence, buying, licensing and selling -public and private assets and properties, including intellectual properties. It is possible that there will be developments in the future that cause Veritaseum LLC to change its position regarding the Companies and possibly increase, reduce, dispose of, or change the form of its investment or positions in (or relative to) the Companies.

Nothing in this communication shall bear any warranty of fitness, whether express or implied.

This is not financial, investment or legal advice and should not be considered as such. It is only the opinion of the author(s),

This information and work is copyrighted.