Blockwell's Reponse to the Questions from posed in   83 FR 64563

Foreword: We as a business believe that the only way that this industry will move forward and indeed allow our nation to benefit from the massive technological innovations that are to come is by educating groups like yours on what it is you're actually dealing with (from a technological perspective).

A short background: I am an experienced technologist having worked in emerging technologies pretty much my entire professional life. The majority of that was in a leadership role. My clients include Disney, Ubisoft, WB Games, Jon Huntsman for President, Smoothie King, and many others.

I am a smart contract auditor for a well regarded Japanese exchange that is regulated by the JFSA and have been in talks with those close to regulatory bodies in Singapore, HK, and Japan over the past few months. What I am not, is a financial industry person. With this response we're hoping to help you understand what this technology really is and can be so that you can make the best decisions possible.

For the purpose of clarity we mirrored your questions and put our own with bold Blockwell prefaces. I tried to be as thorough as I could but am certain I missed something. If you have any questions on the below, please feel free to reach out.

1. What was the impetus for developing Ether and the Ethereum Network, especially relative to Bitcoin?

Blockwell: To understand that you would need to talk to Vitalik directly. To answer the underlying question though: The primary benefits of developing the Ethereum network is the ability to create programs and ecosystems around them which are in essence unbreakable so long as the network itself stands.

While the majority of the industry has been talking about the financial equivalency, it's important that you understand the power of tokens beyond just as fundraising mechanisms or digital asset representations of stocks, commodities and other security based items.

Tokens are the missing link for incentivizing and rewarding the construction and organization of self-sustaning businesses. Tokens, when implemented correctly, provide a direct and meaningful share of the value that a participant creates for a network. If the network is valuable, others will want to join it and as such their contributions to the network are rewarded by the demand it brings.

2. What are the current functionalities and capabilities of Ether and the Ethereum Network as compared to the functionalities and capabilities of Bitcoin?

Blockwell: The Ethereum network's functionality differences are around the implementation of smart contracts. While Bitcoin later developed a system know as Rootstock or RSK for short, RSK itself was represented on Ethereum. With Ethereum for instance we can build a bridge to IoT devices that are powered by tokens that users earn based on tagging the data collected.

This allows users to gain a share of the value that they create and programmatic systems and advancements in AI to gain significantly from a competent source of training data with a vested interest in accuracy. Afterall, if their work produces an inferior product the tokens that power access to their network are going to have a lesser value.

3. How is the developer community currently utilizing the Ethereum Network? More specifically, what are prominent use cases or examples that demonstrate the functionalities and capabilities of the Ethereum Network?

Blockwell: To be honest the regulatory chill had a noticable impact on the users willing to experiment. The collective environment have moved people from exploring what this new technology can be to only working with it when they have 6 figures for legal fees and are using it as a fundraising tool. I think that is something that needs to be direly rectified.

There are plenty of interesting concepts both on the mainnet and on the Ethereum testnet known as Rinkeby. As it becomes safer for the good entrepreneurs to experiment, and as the guidelines become clearer on what innovations are safe to explore in America, you'll see all manner of interesting concepts. From Token Curated Registries (curated directories that power themselves with tokens), to more intelligent Business Incentive programs, Community engagement programs, and more.

4. Are there any existing or developing commercial enterprises that are using Ether to power economic transactions? If so, how is Ether recorded for accounting purposes in a comprehensive set of financial statements?

Blockwell: While we can't speak to which enterprises are using Ether directly, the ledger itself is fully transparent and the entire record of an organizations transactions are available. If anything it makes accounting easier as every single use is tracked

5. What data sources, analyses, calculations, variables, or other factors could be used to determine Ether's market size, liquidity, trade volume, types of traders, ownership concentration, and/or principal ways in which the Ethereum Network is currently being used by market participants?

Blockwell: Perhaps this video: https://www.youtube.com/watch?v=XcFIAUdFii0&feature=youtu.be will help you to better understand the possibilities for yourself. You can get a wealth of data from the chain like never before. I've also included a sheet from one of our tools at the bottom of this document for further elaboration. This technology can remove immense amounts of friction in the markets if properly implemented.

Despite their bad wrap, DEXes are actually a regulator's best friend. I track hackers for exchanges and token startups from time to time and the trail stops cold when it hits a centralized exchange. I can find out where the money went if something is sold on a DEX because there's an endless trail. With a centralized exchange I need subpoena powers to do that.

6. How many confirmations on the Ethereum blockchain are sufficient to wait to ensure that the transaction will not end up on an invalid block?

Blockwell: Coinbase uses 60, personally once I see 20 confirmations I'm more than confident about a small ticket transaction. Larger transactions are more likely to be hit by a direct hack or compromising their keys than they are by brute forcing the chain with a "51% attack".

Technology

7. How is the technology underlying Ethereum similar to and different from the technology underlying Bitcoin?

Blockwell: They're both blockchains and they've both been through significant tests and survived. Ethereum's biggest difference is that it was designed to be a platform from the beginning (not a currency) with the token itself powering the platform.

If you build a smart contract driven app on Ethereum for instance and the whole of the system is on Ethereum, you have a 100% margin product. The user pays the gas fees, your token powers your network, and your returns paid their operating costs prior to reaching you. That is for a fully automated product though.

8. Does the Ethereum Network face scalability challenges? If so, please describe such challenges and any potential solutions. What analyses or data sources could be used to assess concerns regarding the scalability of the underlying Ethereum Network, and in particular, concerns about the network's ability to support the growth and adoption of additional smart contracts?

Blockwell: Ethereum mainnet has scalability challenges but the sidechain solutions are infinitely scalable and can be anchored to proof of work systems, create their own POW networks through universities and other organizations (quorums) and validated through a "paper ballot" style system of auditing alongside anchoring.

Candidly speaking we've spent the last 11 months building a system for just these types of situations at Blockwell. As the network grows you will start to see chains of chains, validation between networks with the "calculations of truth" being made onchain in a verified way and offchain systems simply taking in and sending out data between them (whether two businesses or two parts of an app).

9. Has a proof of stake consensus mechanism been tested or validated at scale? If so, what lessons or insights can be learned from the experience?

Blockwell: I have yet to see a viable proof of stake mechanism that I am happy with. It leads to an entrenched wealth power dynamic that actually has a deleterious effect on critical mass. This negates the economies of scale that blockchain and tokens can bring to business systems through providing direct, results based digital asset rewards.

10. Relative to a proof of work consensus mechanism does proof of stake have particular vulnerabilities, challenges, or features that make it prone to manipulation? In responding consider, for example, that under a proof of stake consensus mechanism, the chance of validating a block may be proportional to staked wealth.

Blockwell: A lot of people have put a lot of thought into this but for our purposes proof of stake still needs to prove itself.

11. There are reports of disagreements within the Ether community over the proposed transition to a proof of stake consensus model. Could this transition from a proof of work to a proof of stake verification process result in a fragmented or diminished Ether market if the disagreements are not resolved?

Blockwell: Whether it does or it doesn't, so long as there are sufficient network effects and a wide enough spread of vested interests fragmentation will not cause significant damage to the network as a whole.

12. What capability does the Ethereum Network have to support the continued development and increasing use of smart contracts?

Blockwell: Blockwell currently has several different ethereum blockchains that are using smart contracts. One very valuable thing about Ethereum chains is that your wallet is your wallet, regardless of the chain. Whether you're on the mainnet (what we know as Ethereum), or on Rinkeby (Ethereum testnet), or on our own Caelum or Fornax business app servers, your wallet is infinitely yours and no other party can unlock it if kept secure.

This coupled with the solid track record as an actual platform tells me as an experienced technologist that Ethereum will be able to support smart contracts for as long as a network exists. Many think of the Parity multi-sig issue as a weakness but in reality it proved a real strength to the network:

The creator of the language, who everyone agrees messed up his own contract, could not get $300M worth of assets back. He wasn't above playing dirty to try, he had a vote cast where his death Ether was counted and lost. If there were a way to unravel the chain and restore things he would have. He couldn't. That moment was what led me to doubling down on the Ethereum network as a technology stack.

Governance

14. In light of Ether's origins as an outgrowth from the Ethereum Classic blockchain, are there potential issues that could make Ether's underlying blockchain vulnerable to future hard forks or splintering? Markets, Oversight and Regulation

Blockwell: Sure. But I'm not sure that's an issue for you as an organization. It's no different than infighting amongst board members or the split of startup founders. If Ethereum splinters and forks those forks will have proven to be superior or Ethereum will regain the network it needs to be successful. This is not a negative thing nor is it a process to try to artificially stave off.

15. Are there protections or impediments that would prevent market participants or other actors from intentionally disrupting the normal function of the Ethereum Network in an attempt to distort or disrupt the Ether market?

Blockwell: Yes, but it is not the answer you're expecting. If you find a way to allow safe innovation inside the network wherein retail customers can actually participate, the network effects will help to shield more entrenched powers from disrupting the network.

The industry as a whole has moved past the idea of using Ether as a long term store of value and are constantly talking about "Treasury Management" and other philosophies of risk management in cryptoassets. What this means principally is businesses that raise in ETH will no longer be holding large piles of it as cash reserves.

As the market matures and more people use it as fuel for their actual decentralized applications the price will start to normalize. That doesn't mean you shouldn't be vigilant of disruption and manipulation of other cryptoassets some of which may be built on Ethereum. My view is this space needs two things:

1) Less risk for the good entrepreneurs and innovators to actually play with it and see what it is.
2) More watchful eyes, education and mechanisms to catch fraud, and educate ignorant but well meaning participants about what they can and can't do.

22. Are there any emerging best practices for monitoring the Ethereum Network and public blockchains more broadly?

Blockwell: Everyone has an opinion. Feel free to reach out, we have some tools that may help in certain cases. Overall the best practices are still being developed. I would invest more heavily in learning how to use the blockchain itself for your needs than in inflexible enterprise toolsets that barely scratch the surface.

Cyber Security and Custody

23. Are there security issues peculiar to the Ethereum Network or Ethereum supported smart contracts that need to be addressed?

Blockwell: Just bad code or total destruction of the network at present. The biggest security issue I've seen as a smart contract auditor for exchanges is the prevalence of copy / paste code from businesses. Often times the developer themselves doesn't actually know how their contract works..

24. Are there any best practices for the construction and security of Ethereum wallets, including, but not limited to, the number of keys required to sign a transaction and how access to the keys should be segregated?

Blockwell: More than anything there needs to be risk management amongst your wallets and the parties in your organization. If you require 3 keys, CEO, COO, and CFO and the CEO and COO die in a plane crash with all your asssets held in one set of cold wallets it doesn't leave you in a positive position.

Diversification of your wallets, their storage locations, and the parties with access will limit the damage that any one person or accident can do to you or your business.

25. Are there any best practices for conducting an independent audit of Ether deposits?

Blockwell: Depends on what you're auditing for. You can pull records in seconds and there are ways you can track down everything you want to know. Discussing those way publicly seems to be a surefire way to teach the crooks how to avoid your gaze. That said, see appendix below.

--

And lastly, I want to thank you for opening the floor to this type of comment. Hopefully in the near future there can be an actual open forum of sorts between the business community and the regulatory one. Nobody wants another great depression and the community at large has learned first hand why your job is so important with the "crypto winter".

I think the more effort you as an organization put into learning, educating yourself, and working with the good actors to lay groundwork the better off the country as a whole will be as this innovative technology continues to take wing.

Best,
Josh Smith
Founder
Blockwell.ai

Appendix

PDF Example of the Ethereum Network at life:

https://drive.google.com/file/d/1hnszlGi6mz5We43_6q0JsZb9HWZYqXvc/view?usp=sharing

Sample Ethereum Functions called Today:

trade	amountGet	0.0001884 ETH|0.02 USD	LTO Network|LTO,ether|ETH	ether|ETH,LTO Network|LTO	
transfer	_value	25000000 GBPT	3458999 DROP|1743.35 USD	151 BITT	
cancelOrder	amountGet	10 LPT	99948966060 LTCC	1428469.395 ETA	
approve	_value	1.1579208923731619542357098500868790785326998466564056403945758400791 3129639935e+59 WETH	1.1579208923731619542357098500868790785326998466564056403945758400791 3129639935e+59 CASH	20 KPX	
deposit					
depositToken	amount	20 KPX	347405.734534940637026789 ATMI|169.69 USD	6480 FDZ	
withdraw					
withdrawToken	amount	5500 UMT	3106150.094156941339 KIN|76.65 USD	40 HAK	
adminWithdraw	amount	243.9763 CEL	15949.492474394236355589 FTM	4301.71630163 UBT|105.95 USD	
approveAndCall	_value				
buy					
transferFrom	_to				
__callback	result				
mine					
transferOwnership					

claimTokens				
register				
confirmTransaction				
tradeWithHint	srcAmount			
sell				
burn				
buyTokens				
mint	amount			
updatePrice				
swapTokenToToken	srcAmount			
depositToMiningBalance				
bidOnSiringAuction	_matronId			
delegatedTransfer	_value			
burnTokens				
giveBirth				
changeRate				
breedWithAuto	_sireId			
activate				
createSaleAuction	_startingPrice			
createSiringAuction	_startingPrice			
setReferralCode				
pause				
swapEtherToToken	minConversionRate	333265143.32984882 WBTC	334914739.67001232 WBTC	1032.023193 664125758599 ELF	
setReferral				
withdrawFromMiningBalance				
createGen0Auctio				

n					
safeTransferFrom	_to				
finalize					
checkIn					
multiMint	values				
distribute	amounts				
lock					
batchFillOrders					
unfreeze					
renameMonster					
withdrawEther					
swapTokenToEther					
transferAndCall					