Hi Professors,

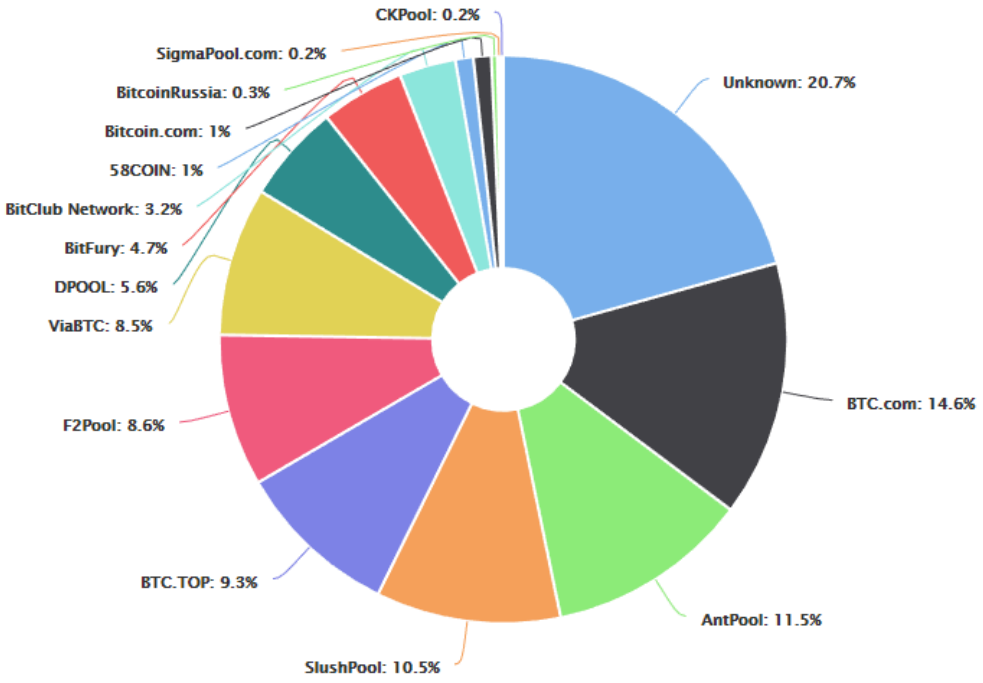
During the presentation from Dr. Athey there were multiple misstatements that were concerning to me. I understand that she is a respected professor at Stanford and that these may have been accidental; however I also believe that it is in the best interest of our academic environment that we ensure high caliber discussion and peer review.

My concerns revolve around misstatements around Bitcoin in comparison to Ripple's token called XRP. I would also like to raise concerns about potential conflicts of interest in a professor making false statements while simultaneously promoting a product that claims to solve these problems and being paid by that company.

1. Conflating mining nodes and full validating nodes on the Bitcoin network and thus claiming that Bitcoin is "controlled by a small group of miners in China".

In her talk, Prof. Athey claimed that mining has become centralized and Chinese miners are able to control the Bitcoin network. This claim was made to promote the Ripple network as a better alternative to Bitcoin. This is factually incorrect on several levels. First, mining nodes do not determine which transactions are valid, each node on the network fully validates the cryptographic signatures of a transaction before propagating that to other nodes. Therefore even if a miner with many computers attempted to send an invalid transaction to a node, that block would be automatically rejected as cryptographically incorrect. If a computer attempts to send multiple invalid transactions, then the Bitcoin network will block that miner from sending more transactions. For a nice visualization and more in-depth analysis of this concept, here is a great article on the topic. The point here is that regardless of how much computing power a single entity possesses, they will not be able to submit a transaction that is invalid. Therefore, Bitcoin can never be "controlled by miners" based on the design of the network. It is protected through full nodes across the world. A chart for all public full nodes can be found here.

Second, mining is not centralized in the hands of a few miners. Miners are able to pool their resources together in order to get a more consistent payout. Here is a current look at the distribution of those pools (below). Each of those pools are further divided into hundreds or thousands of individual miners from across the globe. Recent research has put this number into the hundreds of thousands of individual miners that are using these pools. Far from the picture of one massive controlling entity.



2. Claiming that Bitcoin accounts are "secured economically and not cryptographically".

Prof. Athey claimed that the funds in Bitcoin are not secured cryptographically, but economically due to mining. She argued that mining means your funds are only secured by profits of miners. She went on to claim that Ripple has solved this problem by removing miners from the picture. This is false. She is conflating two different things 1) stealing funds by cracking the encryption of the wallet 2) using mining power to 51% attack a network.

When holding funds in a Bitcoin wallet, that wallet is secured though SHA256 encryption and ECDSA cryptography. As long as you do not tell anyone what your private key is, this key is physically impossible to crack in order to steal your funds. In order to do so would require a computer larger than the milky way galaxy running for the history of the universe. For more resources on how mind-boggling secure Bitcoin is, see this article and this video. The security on this encryption has nothing to do with the "economics of the protocol".

When referencing "economics of the network" she may have been referring to the fact that mining power can be used in an attempt at an attack. However, this is a long debunked threat. Here is a great video from a distributed computing expert Andreas Antonopolous that concisely explains why this is not a threat. Essentially this only involves those who are attempting to spend their coins more than once in two different places and cheat the network. This is next to impossible practically speaking and **does not involve stealing a users funds**.

3. Claiming that "Bitcoin wastes electricity by stealing from rivers to solve useless math problems".

This is another claim that is based on inaccurate factual narratives promoted by alternatives to Bitcoin. Prof. Athey levied this argument against Bitcoin in order to claim Ripple as a "greener" solution. The specifics of this debate are quite detailed. Although I think that this can also be addressed pretty simply. Bitcoin is proven to actually be **creating renewable energy sources**, far from "stealing from rivers". As outlined in this research paper. Bitcoin miners are using nearly 77% renewable energy to power their mining operations. The reason behind this is that Bitcoin mining creates strong incentives to create new renewable energy and use the surplus for mining. For a great breakdown of this report and the myth of Bitcoin "stealing from rivers", this article here is a good start. This has been debunked for several years now.

For a more detailed review of Bitcoin's implications for energy production, this article by researcher Dan Held does a great job of explaining how Bitcoin can create the proper incentives for large scale development of more green and efficient energy sources.

4. Claiming that Mexican financial institutions are using Ripple technology.

In her presentation, Prof Athey gave the example of Mexican banks that are using XRP technology to exchange funds between dollars and pesos. She also showed a slide with an image of a Mexican bank exchanging pesos into dollars using XRP. This comes from a statement by Ripple in 2018 " Cuallix became the first worldwide institution to use xRapid to reduce the cost of sending cross-border payments from the U.S. to Mexico."

However, looking a little bit deeper, this does not appear to be the case. The company reportedly using the technology is called "Caullix" however, there is no record of this company actually existing. The only evidence of the company is a website that was created one year ago. They list multiple addresses on their website but those addresses are not owned by any company and are currently up for lease.

I called the company that Ripple has publicly stated uses the technology and asked them if they use "xRapid" or any services provided by Ripple, their response was "No." I've attached the audio clip below. This is really concerning, the one company that they advertise as using their blockchain technology is denying that claim. They even have a "quote" on their website from Cuallix, this brings that quote into question as well. You can see that statement here.

5. Claiming that Ripple does not sell XRP, they only "routinely disperse" the token.

During her presentation I asked Prof Athey why their company sells this token to retail investors if this is supposed to be for bank liquidity. Athey denied my comment and said they merely "routinely disburse the token"; but this is the same thing as selling it. In fact, Ripple holds over

80% of their token and sells millions of dollars of the token every month to investors. Ripple's latest report is that they sold 535 million to retail investors in the past year.

Additionally, there have been concerns that Ripple is engaging in millions of dollars of wash trading in order to overstate their market cap. A report was released just two days ago calling attention to this. That report can be found here https://messari.io

Other Concerns

There were other elements of her presentation that, while not direct misstatements, were still quite misleading.

- Showing Bitcoin wallets from 2013 without explaining that wallet infrastructure has changed and can now be accessed through a variety of user friendly mobile apps (i.e. Zap as a desktop application and a mobile wallet, bluewallet for mobile payments, and Joule for a google chrome extension)
- Claiming that Bitcoin has slow transactions without mentioning how Lightning technology has upgraded the Bitcoin network to allow instant, free, and cryptographically secure transactions. Despite failing to mention this, one of her slides explicitly cited the Lightning network Whitepaper by Joseph Poon.
- Claiming that if you enter the incorrect Bitcoin address, the funds disappear. This is incorrect because you do not enter the number of the address you would like to send it to, modern wallets use QR codes to prevent this.

I understand that no one is perfect, but these are pretty basic concerns about fairness of information and the quality of discussion that we have here at Stanford. I'm not sure about what to do about this, but I just wanted to bring these concerns to your attention.

Respectfully,
Conner Brown