Draft Thoughts on Blockchain Questions

1. **What considerations should public or private organizations undertake regarding the security requirements of a proposed implementation of blockchain?**

In considering blockchain security, there are at least three things to think about: (1) whether the blockchain system is robust against faults/attacks, (2) how to avoid social engineering and fraud, and (3) how to avoid unintended transactions via improperly programmed smart contracts.

Robustness. Distributed ledgers rely on their distributed nature for non-repudiation. While each block is cryptographically tied to the next block, on a single ledger it would still be possible to alter the ledger, as there wouldn't be any alternative record to compare the cryptographic linkage to. Fundamentally, one needs to ensure that there are enough nodes to ensure Byzantine fault tolerance – that is, enough nodes to detect and override faulty nodes. In general, this number is 3f+1, where f is the number of potentially faulty nodes. So in any blockchain system, it is important to have enough nodes to make sure that a simultaneous attack cannot succeed.

Social Engineering/Fraud. We've seen a number of cases of social engineering/fraud that attack users of blockchain systems. In a number of cases, people have been convinced to invest in cryptocurrency systems that don't exist, and the fraudsters abscond with their money. In other cases, the cryptocurrency may exist, but the individuals keep their "wallets" in an exchange which then makes fraudulent transactions siphoning off value. And if people do keep their wallets on their own devices and lose their private key, they may lose the ability to transact altogether.

Cryptocurrency Regulatory Issues

As you might imagine, cryptocurrency raises a whole host of issues. To start with, how do we ensure Bitcoin isn't used to buy heroin. And whose responsibility is that. In a distributed ledger, there may not be a single entity in control of the system. So who owns the compliance responsibility. Does anyone have to file Financial Crimes Enforcement Network (FinCEN) reports. What about Know Your Customer rules. There have been efforts to regulate cryptocurrencies under money transmission laws, or to establish so-called BitLicenses. And FinCEN has said that initial issuers of cryptocurrencies are subject to its money transmitter regulations and must comply with its anti-money laundering and Know Your Customer rules. But the overall regime remains murky.

And even where Bitcoin is used legitimately, how do we regulate exchanges? We've already seen two significant cryptocurrency exchanges collapse: Mt. Gox and

QuadrigaCX. In both cases, theft and/or fraud appears to be the cause. As long as exchanges remain unregulated, those who use them to transact in Bitcoin and transfer it into money that can be used more readily in the real world—which is pretty much everyone—will be at risk of bad actors.

Then there is a question of whether trading of cryptocurrencies should be regulated, and who should do it. Court cases have held that cryptocurrencies are commodities regulated by the Commodities Futures Trading Commission, or CFTC. But the CFTC's authority is limited in cash markets, as opposed to options market, and most cryptocurrencies are sold in spot markets. As a result, little regulation is extant.

Another recent phenomenon is initial coin offerings, or ICOs. Instead of issuing shares, blockchain companies issue tokens, which investors (or speculators) purchase in hopes that the value of the tokens will increase. Because tokens don't necessarily qualify as securities as such, there have been lots of questions regarding the necessary disclosures (if any) and how ICOs should be regulated. Many tokens do more than represent an interest in something; they have a utilitarian value on the blockchain of enabling transactions. In other words, the coin represents future access to a product or service, rather than an investment generating a return. If true, this takes the token out of securities regulatory frameworks, even if the blockchain would operate just fine without the token. For example, one could imagine a payment (token) being required to confirm an identity-related claim on a blockchain. That has a utilitarian value in that you can't confirm the identity without transferring the token. But there is no inherent reason why that is the case, other than the creator of the blockchain set it up that way. Neil Tiwari, in his note The Commodification of Cryptocurrency in the Michigan Law Review last year, argues just for such increased scrutiny of the "utility" provided by utility tokens, to ensure that there isn't a backdoor for escaping securities regulation. As it turns out, many utility tokens are in fact securities, because they represent an external tradeable asset.

Improperly Programmed Smart Contracts. Many blockchains enable smart contracts to be executed on top of them, transferring value in response to certain pre-programmed actions. If these programs have an error in them, people may be able to take advantage to have them operate not as intended. The best example of this is the DAO, which operated on the Ethereum blockchain. Someone figured out how to manipulate it to siphon off money intended to fund new ventures. The net result was that the blockchain needed to be forked to undo the transaction.

Smart Contracts

And what of smart contracts? The name is really a misnomer. They are merely self-executing code. That doesn't make them a contract—there still needs to be offer and acceptance, established by a set of rules that humans agree to. Generally, applications

of smart contracts are seen in permissioned blockchains, where who can write to the blockchain and who can set up a node is controlled. The consortium sets the rules of the blockchain, and then self-executing code can be placed on the blockchain. But the ultimate enforceability if there is a dispute is set by those underlying rules agreed to in advance, and takes place outside of the blockchain, in arbitration or in court.

There are smart contracts that are executed on permissionless blockchains. Ethereum, which you may have heard of, is designed to enable execution of code on its blockchain. But what happens if the code doesn't operate as expected, or if there is a bug?

There is increasing coding of decentralized autonomous organizations, or DAOs. The idea is just as a blockchain can be a decentralized ledger without a single entity in control, a DAO can encode rules on a blockchain without a need for a centralized authority to govern them. One of these, confusingly named The DAO, was built on the Ethereum blockchain, to be a crowdfunding source: you could contribute ether to The DAO in return for tokens, which gave holders the ability to vote on plans and a reward if the project funded was profitable. Except there was a bug, and a hacker was able to drain The DAO of funds.

Now, The DAO operated as programmed; it simply wasn't programmed correctly. And without a central authority to reverse transactions, the hacker would now own the ether he drained from The DAO. The only way to address this was a hard fork of the Ethereum blockchain itself, entering transactions returning the money to the original holders. Enough Ethereum nodes embraced the hard fork for it to work, but you can see how this runs counter to the non-repudiation principle that theoretically underlies blockchain technology. And if that wasn't enough, the SEC ruled in 2017 that The DAO tokens were securities and subject to Federal securities laws, because, after all, they represented a share in the profits from the ventures funded by The DAO.

2. Which stakeholders should be involved in such discussions? Should different blockchain systems be associated with different application contexts?

There are a mixture of stakeholders that matter. Certainly, those entities offering services using the blockchain, as well as their customers who make use of the blockchain, should be involved. There is also a difference between permissioned and non-permissioned blockchains. With permissioned blockchains, there is an agreement that sets forth the rights and obligations of node operators and who can write to the blockchain is limited. In this case, the consortium establishing the blockchain is able to negotiate governance. For non-permissioned blockchains, there is a set of rules but governance isn't as established; it requires agreement among the community on how to operate.

In both cases, there is also a role for governments. While government shouldn't regulate the underlying technology, it has a role to play in regulating specific harms that may arise. I have discussed this more in depth previously in a blog I wrote while working at Microsoft entitled What's Next for Blockchain: Technology, Economics and Regulation. Technology is inherently difficult to regulate effectively at an early stage, because its evolution is unpredictable. Just see these magazine articles: "How Yahoo! Won the Search Wars" (Fortune March 1998). "Will MySpace ever lose its monopoly" (The Guardian February 2007). "Nokia: Can Anyone Catch the Cell Phone King?" (Forbes March 2007). What is important is that we regulate uses of technology, rather than the underlying technology itself. We do this in the law all the time. There are lots of potential harms related to cryptocurrencies, but it wouldn't make sense to regulate blockchain to address those, given the broad variety of other uses for it.

3. **What components of blockchain should be highlighted? Can the immutability of blockchain architecture be reconciled with requirements of emerging privacy policies, such as GDPR in the EU and CCPA in California? How should these components be incorporated into a decision-making and assessment process to determine its appropriateness for any use case?**

Yes, blockchain implementations can be reconciled with privacy laws. The CNIL, the French data protection commissioner's office, has published a helpful paper on blockchain and privacy issues titled Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. Fundamentally, blockchains are used to store public keys that identify individuals, but these can effectively be rendered anonymous by the individual by deleting his/her private key, or via other measures

As the CNIL guidance states, "…*blockchain can contain two main categories of personal data*: *Identifiers of Participants* and Miners [and Additional or "Payload" Data]. *Each participant has an identifier, called a public key*, consisting of a series of alphanumeric characters that seem random. This public key refers to a private key that is only known by one person.…"

Guidance thus far recognizes that it is not technically possible to "delete" information stored on the blockchain. Although definitive guidance would be helpful, alternative measures which obfuscate the information on the blockchain likely are "similar to effective erasure of data" according to the CNIL.

- **Deletion of the Private Key.** The CNIL also stated that the deletion of the private key would make it impossible to prove what payload data had been associated with the public key and as such "would no longer pose a risk to confidentiality." The

self-help approach where the user has control over their information through a portal or other technology is also supported by regulators.

- **Deletion of Underlying Data.** Presumably, deletion of all the data on the centralized server that is linked to by the blockchain (so that the public key is merely a number without purpose) would satisfy the right to be forgotten.

- **Hashing or Encrypting Payload Data.** While it does not go into specifics, the CNIL acknowledges that proper hashing or encryption techniques of payload data would be an acceptable method of erasure for blockchain technology.

- **Other Options.** Additionally, over time, there may evolve approaches that are also recognized as acceptable, but were not mentioned in the guidance (e.g., scrambling payload data, multiple public keys corresponding to specific personal data (like a new metadata approach) and other approaches.

4. **How can we ensure that we forge an adaptive path forward for blockchain implementation in California, one that is neither too permissive nor too constrained? Consider implications beyond this legislation.**

Blockchain and the Future of the Internet

Josh Rogin, a Washington Post columnist and CNN commentator, recently published a piece suggesting that China has moved ahead of the U.S. on blockchain and this posed geostrategic risks. Remember, the immutability of blockchain means everything is recorded, in theory in perpetuity. This means that a repressive government could use it to track and control its citizens' transactions. Rogin fears this is exactly what China plans to do. He notes that China has been investing heavily in blockchain development while cracking down on blockchain systems it doesn't control, such as outlawing cryptocurrencies and requiring blockchain operators to collect personal data on their customers. Ultimately, if its vision for blockchain is realized, China could control the system by which everyone in the country (and anyone outside who wishes to do business with Chinese entities) engages in transactions, giving it a large degree of visibility and control.

Add to this that China controls 74% of Bitcoin's computing power (that is, Bitcoin miners), according to a recent report by researchers at Princeton and Florida International University. Given that Bitcoin operates on a consensus mechanism, that means China potentially has the power to alter the Bitcoin blockchain by forcing through changes and using the fact that the majority of computing power is under its control to make those ledgers the ones accepted.

This fear may be overblown. But it dovetails with calls for the U.S. to promote the use of blockchain via open technologies, just like those that power the Internet, which was designed from the outset to be open. As blockchain becomes more central to the technology economy, expect to see more attempts to use it to drive national economic interests