Illinois Department of Financial & Professional Regulation
100 W Randolph St, Floor 9
Chicago, IL 60601

January 18, 2017
Re: IDFPR Requests Comment on “Digital Currency Regulatory Guidance”

To whom it may concern at the IDFPR:

Thank you for this opportunity to comment on the Digital Currency Regulatory Guidance and acknowledging this innovative technology, along with many of its possible use cases. We are Blockchain Consulting Group, founded by Mr. Taylor Gerring, a blockchain expert who has been involved in the cryptocurrency space for numerous years and has worked on projects such as Hive Wallet and The Ethereum Foundation. He now travels around the world giving educational talks on blockchain technology.

We feel that the State's approach to this oncoming technological wave is the appropriate stance; asking questions and obtaining knowledge on the subject allows for reasonably unrestricting innovation. Blockchain technology has the possibility to bridge a gap between the way government and citizens interact. Through the use of distributed ledgers and smart contracts, agencies in the State of Illinois could have the an interoperable system that will them allow to verify and share data in real time, without expensive infrastructure.

As the state seems to have a firm grasp on blockchain technology and its main components, we’d like to highlight a few specific areas where near-term innovation may lead to a divergence in understanding how these mechanisms work. Two specific areas of note came to mind:

First, on the issue of “mining”, it’s important to understand that continued efforts to broaden differing models in which consensus can be agreed upon will likely create further confusion about this process, what it is for, and why it is necessary. More generally, this process can be seen as “validation” since the participants (“miners”) are working to finalize the information as quickly as possible, which each subsequent validation provides increased assurances the information will not be reverted. In the proof-of-work model, there is a lottery model in which participating validators compete to produce a valid block. Contrast this to proof-of-stake consensus models, in which validators cooperate to agree upon a valid block, similar to voting.

In both consensus models, incentivization for doing this validation task is a key component for decentralized ledgers where the participants may not be known. Traditionally, the incentives come from two specific areas: transaction fees and block subsidy (“mining reward”). Each network has its own set of parameters for calculating how these should be allocated and on which schedule they should be released. Although Bitcoin is famous for its limit of 21 million bitcoins released at a rate that halves every approximate 4 years, it is not a strict requirement that new units of currency are generated this way. Nor is it a strict requirement that this or another economic component, such as transaction fees, must be allocated to the validators. In the case of Dash, additional network services are provided by nodes which are not validators/miners, and receive a set percentage of the block rewards for doing so.

Finally, some clarification around use of wallet software and operation thereof. “Wallet” software never stores or holds any unit of value. Rather, it is a node within a heterogenous network of peer-to-peer accounting software. At its core, the wallet serves to perform the cryptographic calculations allowing for valid network messages to be broadcast to its peers. In some cases, an intermediate service may relay these messages over traditional protocols with the intent of facilitating communication on resource-constrained devices (such as mobile phones). In none of these examples does value move from software to software, rather the owner who controls some units broadcasts a cryptographically-secure message assigning a new owner, which may be any destination within our outside the originating wallet. Therefore, transfers of digital currency are not “made directly from wallet to wallet”, instead, the value is tracked solely on the decentralized ledger where the user of a particular wallet address can prove ownership, thereby granting them ability to reassign ownership.

Below we will touch on subjects ranging from the smart contracts and security, to saving on expenses and technological readiness.

Smart Contracts: Smart contracts allow two parties to execute a contract without the requirement of a trusted third party. Essentially, building a smart trust between the parties knowing the protocol is self-executing and self-enforcing. The capabilities and cost saving of smart contracts may be vast when coupled with the Internet of Things (IoT). This ability to trade value and services by all types of automated devices will likely give rise to a new M2M (“machine-to-machine”) economy.

Security: Through the use of cryptography, blockchain technology is almost incorruptible due to the resources needed to revert the entire history. An attacking party would have to control over 51 percent of the public system computational power to forge records of truth, which provides strong guarantees against censorship or interference by third parties. The information being shared amongst the network is safe and accurate, since even if their was an attack on the network, the mesh-like properties of peer-to-peer networks enable quick re-synchronization to a consistent state, even through partial connectivity.

Escrow: By use of smart contracts, the state will have the ability to set up smart contracts with applicants, recipients, or vendors. If eligible, applicants and recipients will have a direct channel to send or receive funds or have access to programs. The State can put funds in a smart contract acting as escrow, and once a vendor has completed their service the smart contract can disburse funds upon completion of specific goals.

Public Records: Citizens would be able to own their own data and stay in control of who has access to their information. The information would be registered on the blockchain, allowing them to easily permission those who they deemed fit. Some use cases may include: Medical records, birth certificates, education certificates, licenses, etc. Redundant and expensive paperwork can be replaced with digital signatures, which are harder to forge than most physical documents.

Cost Savings: The State of Illinois will have an opportunity to cut expenses with this technology, by ridding itself of third parties, data centers and associated costs ranging from paper, storage, to security. Third parties who merely extract rent and add no additional value to a transaction can be reduced, eliminating their costs. Since blockchain technology is peer-to-peer, there is a lessened need for data and archive centers to connect disparate information stores.

Readiness to Implement: Blockchain technology is still in a nascent stage, with plenty of room to evolve. The benefits of this technology range from interoperability between government agencies, back office efficiency, sovereign identity, green initiatives and tracking of records and assets. Ideal usage of this new technology will likely require communication and experimentation to master, but once mastered, there are many promising possibilities. Financial institutions around the world are already developing and testing their own permissions ledgers, with variations of all sorts. As additional industries, such as insurance and energy are starting to look to blockchain, we feel this technology is ready for use in pilot projects at the government level.

Thank you for the public comment period on Digital Currency Regulatory Guidance, and the State of Illinois' interest in blockchain technology. This technology is still in its infancy and needs guidance and room to grow. Although stumbling blocks are expected along any maturing technology, blockchain carries exceptional benefits that may lead to help bridge the growing gap between government agencies and its citizens.

Sincerely,

Taylor Gerring
Blockchain Consulting Group
4660 N Winthrop Ave
Chicago, IL 60640