

Good morning Chairman Rothfuss and Members of the Select Committee on Blockchain, Financial Technology and Digital Innovation

Technology. My name is Mary Beth Buchanan, and I offer testimony this morning in support of Wyoming's proposed legislation to prohibit the compelled production of private cryptographic keys. This bill would strengthen protections against disclosure of a digital asset's private keys in a range of proceedings, while balancing those protections with the need for discovery related to digital assets in certain legal actions.

By way of background, I am the Chief Legal Officer and Company Secretary at the Bitstamp Group. Founded in 2011, Bitstamp is a leading digital asset exchange platform. As an early entrant to the digital asset space, Bitstamp has had a unique vantage point to watch the growth of digital assets. This includes adoption by consumers, increasingly sophisticated security challenges, and a changing regulatory landscape. With the formation of Bitstamp USA in 2018, Bitstamp has continued its expansion as a market-leading regulated exchange, dedicated to the

transparent and secure exchange of digital assets for our customers, and committed to the safety of customer funds.

Prior to joining Bitstamp, I was the General Counsel at Kraken, another digital asset exchange platform. I have also been a partner with an international law firm, where I chaired the firm's Digital Asset Team, and represented digital asset exchanges, coin developers, and other participants in the digital asset ecosystem. Finally, before entering the private sector, I spent more than 20 years as a federal prosecutor, most recently serving for 8 years as the United States Attorney for the Western District of Pennsylvania.

Digital assets have enormous potential to revolutionize our financial systems. They can be traded across borders, and they can reduce or eliminate the need for third parties, through transparent wallets and programmable smart contracts. In fact, nearly instant 24 hour settlement is the norm for on-chain transactions. Fundamental, however, to any development in this space, is the ability to safely store and maintain the security of these assets.

Digital assets rely upon private keys for secure storage. Custodians and custodial products across the digital asset space continue to innovate to protect those private keys. These protections include generating private keys offline, in so called “cold-storage;” dividing or “sharding” the key into different segments to control how the key can be used; and hardware security modules, requiring physical interaction with a device, in order to access a private key.

Thoughtful and layered methods to securely store a private key are paramount, because anyone with access to a private key has control over those assets, including the ability to irreversibly move them. Similarly, a lost private key takes with it the ability to access the associated digital assets. Because of this, a common phrase in the digital asset world is “not your key, not your coin.”

Essentially, turning over a private key is akin to turning over a password, with the potential for irrevocably losing the ability to identify and access those funds. Given the dangers of a lost or publicly exposed

private key, placing limits on legal process to compel disclosure of a private key, except where necessary and appropriate, is sound policy.

Therefore, given the severe and irreversible risks, I would urge consideration of further protections in the event that digital assets must be turned over. In the event that a private key is ever shared, any party taking possession of that information must consider how to safely preserve it and protect it from bad actors.

Such controls could include third-party custodians, bonding requirements, hardware security modules, or any number or combination of tested custodial innovations in the digital asset space. The use of a custodial service would also assure that there is a limitation on the amount of assets held, as opposed to the entire contents of an individual's wallet being held. As you may be aware, assets held in a digital wallet may be enhanced over time by third-party events, including the forking of digital assets and airdrops of new digital assets by token developers.

To allow any forced disclosure of private keys, without protections to prevent loss or theft, creates an unacceptable risk of loss for the disclosing party.

Sincerely,

Mary Beth Buchanan

Chief Legal Officer and Company Secretary, Bitstamp