**7CCSMDLC TUTORIAL QUESTIONS**
**TOPIC 2: CRYPTOGRAPHY AND TRANSACTIONS**
**TUTORIALS WEEK 3 SOLUTIONS**

**Q1. What are the hash functions SHA256 and RIPEMD160?**

Information can be found on BitcoinWiki:

en.bitcoinwiki.org/wiki/SHA-256

en.bitcoinwiki.org/wiki/RIPEMD

**Q2. What is a cryptocurrency wallet? What is the difference between wallets held on personal machines or on dedicated personal hardware versus wallets held on an exchange?**

A wallet is a means to store the public key (or the cryptocurrency address) and the private key which are jointly associated with an account on a cryptocurrency platform, such as Bitcoin. The storage may in physical form (eg, written on paper and possibly encoded as a QR-code) or in electronic form. If in electronic form, the information may be stored as software code on a client's personal machine, or in a dedicated personal hardware container, such as a secure USB stick. An example of personal hardware wallets are the Nano USB sticks made by the French company Ledger:

shop.ledger.com/products/ledger-nano-s

A wallet held by a user on their personal machine or on dedicated hardware is under the user's control. A wallet held by an exchange on behalf of the user is never completely under the user's control, and therefore is much more likely to be subject to malfeasance, hacking theft, or loss.

It has become common practice for exchanges to shift the majority of the cryptocurrency belonging to their users from the user's own wallets held by the exchange to a wholesale back-office account, for greater security. But this practice can mean that malefactors only have to hack one account to steal the majority of the currency held by the exchange.

**Q3: The Script Programming Language is a stack-based language. What does this mean? What are the two main operations enabled by Script?**

A stack-based language stores data in a data-type called a stack, which may be thought of as a vertical store (like a chest of drawers). There are two elementary operations, which Script also has:

- Push, which adds an element to the top of the stack.
- Pop, which removes the most recently-added item from the top of the stack.

This is also called a Last-In, First-Out (or LIFO) queue.

**Q4. What are 10 main Cryptocurrency exchanges as measured by trading volume?**

A list can be found here:

https://coinmarketcap.com/rankings/exchanges/

The top-ranked exchange is currently Binance, with daily trading volume of around USD$ 21 billion.