**Research proposal checklist**

To be reviewed by the School of Law, a PhD proposal must be 1000-1500 words (excluding bibliography) and must contain the following:

* A research question or hypothesis (i.e. indicating the nature of what aspect of the topic are you investigating or what theoretical proposition you are endeavouring to establish);
* A justification for the likely significant original contribution the proposed research will make (note that this requires you to demonstrate an understanding of what literature is already out there and to explain the rationale for your research proposal);
* The proposed methodology to be adopted (for example, will you be relying purely on doctrinal, library-based research or do you propose to undertake empirical research?);
* A proposed chapter structure and indicative time-scale mapping out the research over 3 years;
* A bibliography of the sources you have consulted in preparing the research proposal.

**Project Title; Summary; Specific Aim(s); Agreement with Supervisor**

**QTUM** is an interesting Blockchain that is based on the Bitcoin core code and the UTXO model, but operates based on a Proof-of-Stake consensus algorithm. It emulates Ethereum’s smart contract capability, but so far, does not have a working Oracle system to allow smart contracts to access information from the outside world.

This project will examine work on Oracles – principally on the Ethereum blockchain – and try to improve upon this while adding this capability to the QTUM ecosystem.

* Read a reasonable cross-section of work including journal articles and monographs within the field.
* What the state of the literature is and what gaps there are that a PhD could address?
* If it is a new or emerging area where little academic literature exists (eg FinTech), then take steps to reviews other sources such as policy documents, newspapers and practitioner articles

QTUM is an open-source blockchain-based distributed computing platform which combines time-proven Unspent Transaction Outputs model of Bitcoin with novice virtual machines, including EVM and x86. Thanks to the EVM, QTUM can run Ethereum smart contracts without any changes in their source code, which simplifies the migration of software to the new blockchain.

In [cryptocurrencies](https://en.wikipedia.org/wiki/Cryptocurrencies), an **unspent transaction output** (**UTXO**) is an abstraction of [Electronic Money](https://en.wikipedia.org/wiki/Digital_currency). Each **UTXO** represents a chain of ownership implemented as a chain of [Digital Signatures](https://en.wikipedia.org/wiki/Digital_signature) where the owner signs a message (transaction) transferring ownership of their **UTXO** to the receiver's [Public Key](https://en.wikipedia.org/wiki/Public-key_cryptography).

The total **UTXOs** present in a blockchain represent a [set](https://en.wikipedia.org/wiki/Set_(mathematics)) , every transaction thus consumes elements from this set and creates new ones that are added to the set. The set thus represents all the coins in the system.

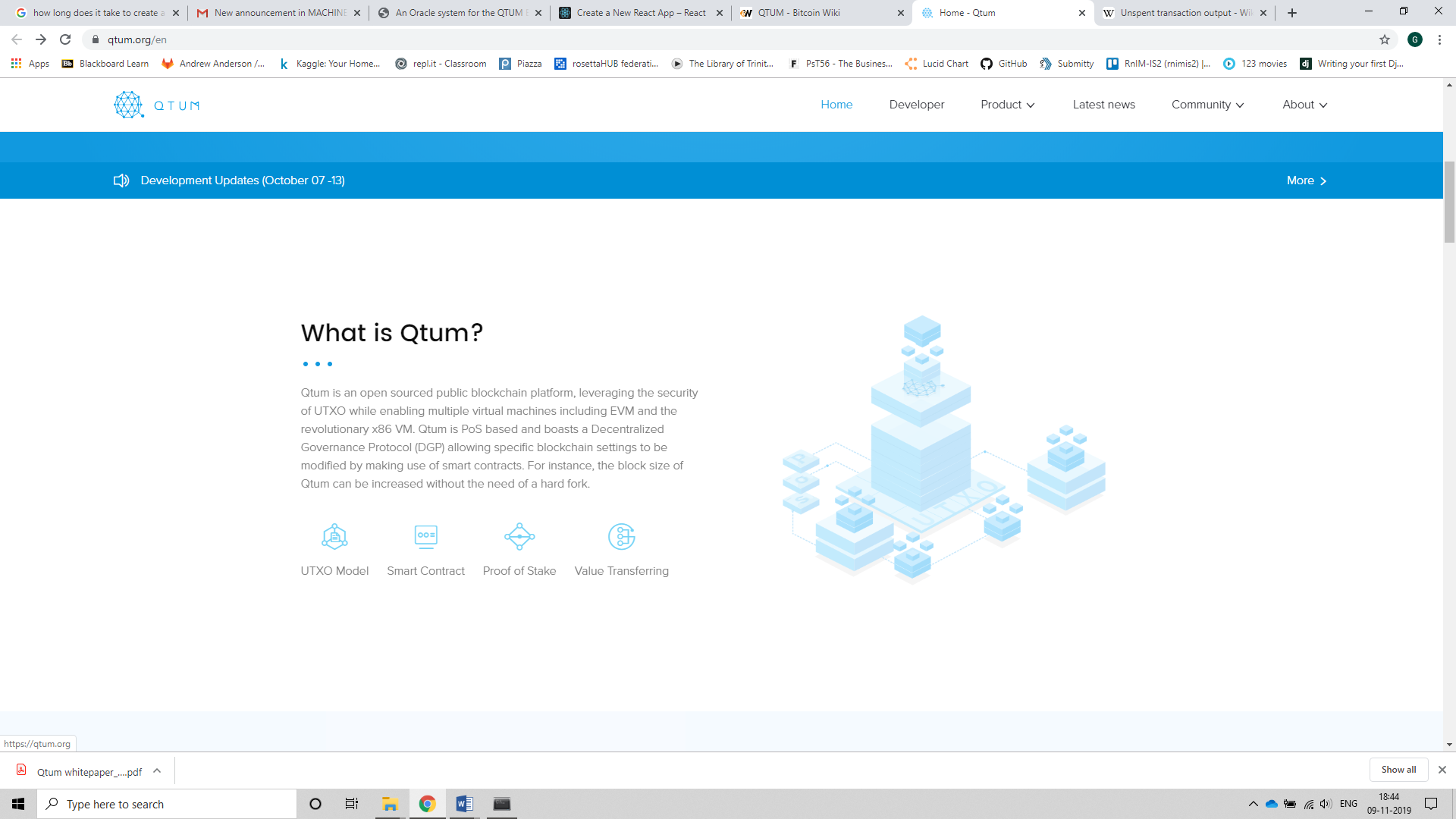
An **UTXO** defines an output of a [blockchain](https://en.wikipedia.org/wiki/Blockchain) transaction that has not been spent, i.e. used as an input in a new [transaction](https://en.wikipedia.org/wiki/Transaction_processing). [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) is the most famous example of a cryptocurrency that uses the UTXO model.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Outputs are a superset of UTXOs. Accordingly, UTXOs are a subset of the outputs superset. Bitcoin UTXO lifespans have been studied.[[1]](https://en.wikipedia.org/wiki/Unspent_transaction_output#cite_note-1)

In the case of a valid blockchain transaction, unspent outputs (and only unspent outputs) may be used to effect further transactions. The requirement that only unspent outputs may be used in further transactions is necessary to prevent [double spending](https://en.wikipedia.org/wiki/Double_spending) and fraud.

<https://qtum.org/en>

<https://qtum.org/en/developer>



**Proof of work and proof of stake:**

Both are called consensus mechanisms.

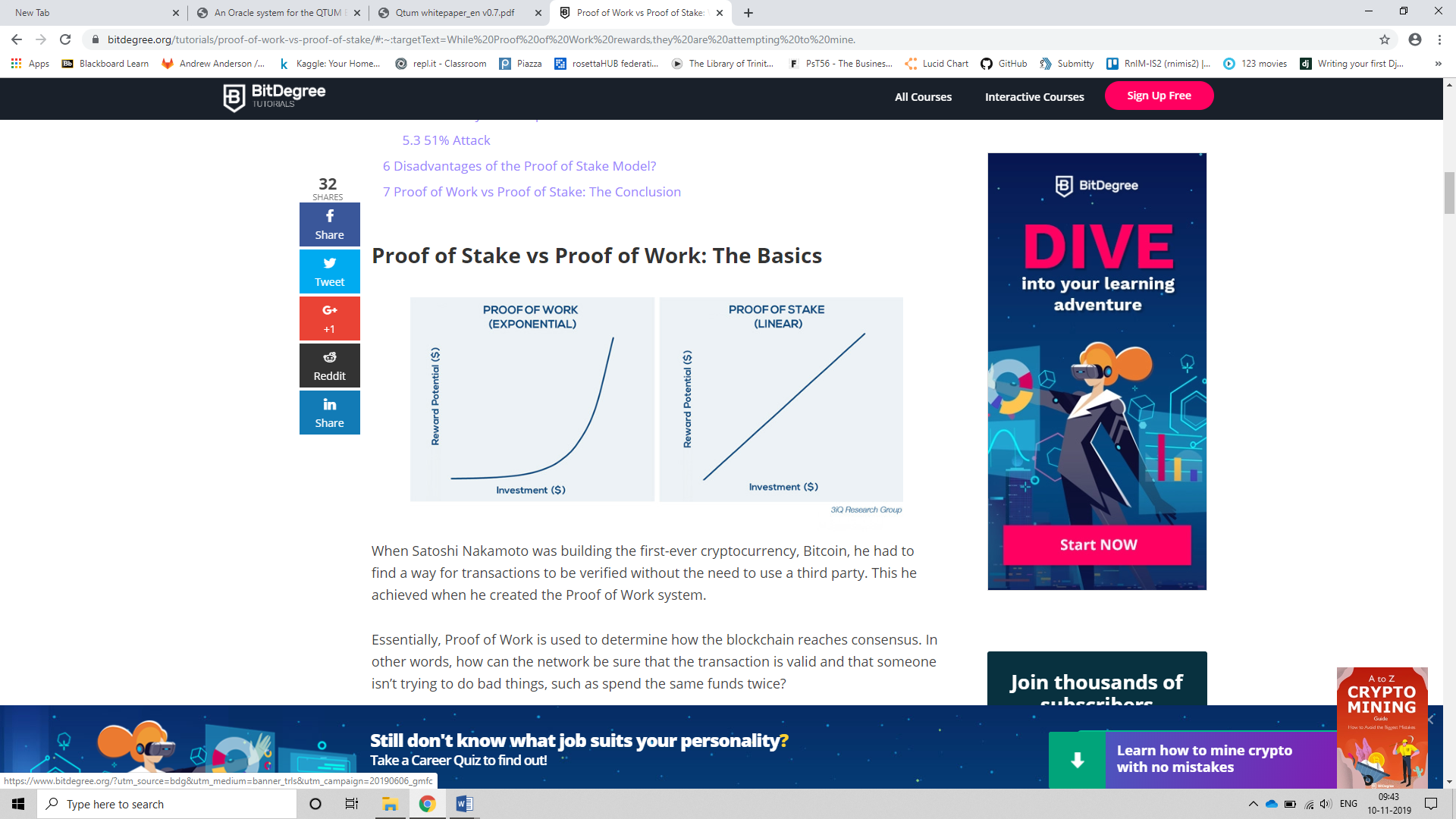
**Proof of Work** is based on an advanced form of mathematics called ‘cryptography’. Cryptography uses mathematical equations that are so difficult only powerful computers can solve them. No equation is ever the same, meaning that once it is solved, the network knows that the transaction is authentic.

**Drawbacks:**

Not only does it need significant amounts of electricity, but it is also very limited in the number of transactions it can process at the same time.

Founders of proof of stake argued that Bitcoin and its Proof of Work model required the equivalent of $150,000 in daily electricity costs.

Includes the amount of electricity it requires, the centralization of power that mining pools now have, and the threats of a 51% attack.



7/second | 15/sec (number of transactions processed)

**Bitcoin – Proof of Work**

Every block contains different transactions within it, which must each be independently verified. For the Bitcoin network to achieve this without a third party, somebody must use their **computational power to solve a cryptographic algorithm**, otherwise known as **Proof of Work**.

Thousands of individual devices all compete to become the first to solve the cryptographic algorithm. Whoever gets there first, wins the reward.

**The total amount of electricity required to keep the Bitcoin network functional is more than the amount used by more than 159 individual countries!**

**Proof of Stake**

Does not need highly complex sums to be solved, meaning that the electricity costs to verify transactions are substantially lower.

When using a Proof of Stake consensus mechanism, it would not make financial sense to attempt to perform a 51% attack. For this to be achieved, the bad actor would need to stake at least 51% of the total amount of cryptocurrency in circulation. The only way they could do this is to purchase the coins on the open market.

If they decided to buy an amount this substantial, then the real-world value of the coin would increase along the way. As a result, they would end up spending significantly more than they could gain from the attack. Not only this but once the rest of the network had realized what had happened, the bad actor would lose all of their stakes!