Mark Seery's Summary of Blockchain advantages / disadvantages		
What happens	**Upside**	**Downside**
Hundreds to millions of computers perform the same blockchain approval calculation	**Accuracy:** A single calculation error unlikely to be retained by the block chain.	**Inefficiency / cost:** Significant compute and energy resources are used to add a single block to the block chain. In aggregate, the resources used can be staggering. Even at an individual node level, the cost can be significant.
Hundreds to millions of computers have a copy of the blockchain	**Tamper resistant:** Difficult to tamper with all copies of the blockchain. Both a computational error or a deliberate tampering would require that 51% of all participating nodes be impacted. As the number of blockchain participants increases, the probability of this decreases. As the amount of processing performed by one entity increases, the value of the blockchain decreases, which becomes a deterrent to 51% control of the blockchain. Some researchers do claim though that now criminals can rent computational resources, rather than having to purchase them, it may become easier to get 51% control. It still requires enormous computing resources to change blocks that have been on the chain for a long time, so experts believe only the most recent blocks would be exposed and that the blockchain would adapt to the threat. 51% attacks are an area of mostly theory with little real-world experience to judge them by. **No single point of failure:** A traditional database may be more vulnerable to technical failures in one or a few servers.	**Inefficiency / cost:** Significant storage and energy resources are used to store all copies of the blockchain, with the potential for a blockchain exceeding the storage capacity of some participating nodes.
Peer to peer elimination of a centralized entity	**Reduced Fees:** The potential for "middle-man" fees to be reduced. **Security / privacy:** No centralized entity monitoring.	**Potential information loss:** The potential for private information to be lost forever, if a private key is lost. In the case of a cryptocurrency, this could also mean loss of currency.
A block can be added any time or day the verification process can be completed.	**Continuous update:** No waiting for weekend or overnight blackout periods to end.	**Low-velocity updates**: The number of transactions per second is commonly many orders of magnitude less than traditional transaction systems
Transactions are not anonymous, they are confidential	**Privacy:** Private/personal information remains confidential.	**Identity & Illegal activity** Public key is obtainable identity information Privacy is considered to also create the right conditions for illegal activity.
Each block in the block chain contains a unique hash of the block, and a hash of the preceding block	**Immutability/security:** Once a block is added to the blockchain it is difficult to change, because all the blocks that come after it have to also be changed. The longer the blockchain, the more computationally intensive this becomes. This is a good characteristic for records that are not meant to change, and for anything that requires an audit trail.	**Immutability:** While this is a good characteristic, if data or code does need to change, it can require abandoning one chain and taking up a new chain
Open Source	**Transparency:** While personal information remains private, how the code works is transparent and public.	
Private-public cryptographic signature verification	**Robust verification:** Every node verifies the authenticity of the user.	**Complexity:** Every node using an algorithm like ECDSA (Elliptic Curve Digital Signature Algorithm) to ensure that the transaction happens between the correct nodes, is asserted by some, to be tricky and complex.
New paradigm	**New benefits**	**Integration challenges with existing approaches** **Regulation gaps and scams** **Lack of inhouse skills for Enterprises** **Lack of understanding by consumers**
Publicly viewable transaction ledgers	**Transparency**	**Lack of privacy** Especially for enterprises (which is leading to improvements in private transaction options and use-specific authentication, see permissioned blockchain, example Hyperledger and Corda).