Bitcoin in Research.

It's curious to see that in the past someone used 10.000 bitcoins to buy a pizza…, probably he is regretting right now about this purchase… The key points of Bitcoin relies on block chain, that nodes of the Bitcoin network must agree on the content of this ledger, ensure the privacy of users and the rewards obtained. A consequence of Bitcoin decentralized structure is that there is no organization nor government in control and therefore no central entity able to apply monetary policy. Initial adoption has been slow, but there are some exchange offices where you can change local currency for bitcoins as well as some ATMs that exchange bitcoins for cash. Also, in some countries Bitcoin transactions are taxed and there are some regulations. In order to reduce the influence of any third party in a transaction between two participants, Bitcoin design replaces the centralized intermediary with many weaker entities that maintain the ledger. Unlike a distributed design, Bitcoin nodes don't partition the workload, data is replicated, and each participant repeats all verification work.

The mechanism of Bitcoin protocol relies on two main rules: (i) block creation is difficult where valid blocks are required to contain a proof-of-work, and (ii) adopt the longest chain, where when there are conflicting blocks, nodes adopts the longer consistent chain abandon blocks in their shorter chain. It's important to mention that mining nodes don't have to hold the entire history of transactions, since some of the contents of the block chain can be safely erased. One problem to the original design is that the Bitcoin protocol decentralization is at risk, because the current system is controlled in many aspects by small groups of miners and wallet providers. Unlike most of the software, protocol updates in Bitcoin are difficult, because a bug in Bitcoin core may cause inconsistencies between versions of the code leading to an split in a block chain. A consequence of Bitcoin open source code is that is used to create many alternative currencies (altcoins) with minor changes like Litecoin, o bigger changes like Namecoin.

There is a large gap between Bitcoin and the scalability of other payment processors like Visa, so the main question is whether the decentralized block chains can be scaled up to match the performance of such a payment methods. To analyze the scalability of Bitcoin it's important to analyze: (i) maximum throughput, (ii) latency, (iii) bootstrap time, and (iv) cost per confirmed transaction. Not only scalability, other important aspect of Bitcoin is its stability, that is related to the stability of: (i) the transaction validity rules, (ii) the consensus protocol, (iii) mining pools, and (iv) the peer-to-peer layer.

Another fact to take into account is to design/use alternative consensus protocols. Important factors to consider are: (i) parameter changes, every altcoin has varied at least some of the consensus protocol parameters, (ii) alternative computational puzzles like ASIC-resistant puzzles or non-outsourceable puzzles, (iii) virtual mining and proof-of-shake, and (iv) designate a small number of authorities to receive, sequentially order, and sign transactions.