agreements have reached 80%, the transaction would be packed into the ledger. For a node, the ledger will remain correct as long as the percentage of faulty nodes in UNL is less than 20%.

Tendermint (Kwon, 2014) is a byzantine consensus algorithm. A new block is determined in a round. A proposer would be selected to broadcast an unconfirmed block in this round. So all nodes need to be known for proposer selection. It could be divided into three steps: 1) *Prevote step*. Validators choose whether to broadcast a prevote for the proposed block. 2) *Precommit step*. If the node has received more than 2/3 of prevotes on the proposed block, it broadcasts a precommit for that block. If the node has received over 2/3 of precommits, it enters the commit step. 3) *Commit step*. The node validates the block and broadcasts a commit for that block. if the node has received 2/3 of the commits, it accepts the block. The process is quite similar to PBFT, but Tendermint nodes have to lock their coins to become validators. Once a validator is found to be dishonest, it would be punished.

3.2 Consensus algorithms comparison

Table 2 Typical Consensus Algorithms Comparison

Property	**PoW**	**PoS**	**PBFT**	**DPOS**	**Ripple**	**Tendermint**
Node identity management	open	open	permissioned	open	open	permissioned
Energy saving	no	partial	yes	partial	yes	yes
Tolerated power of adversary	$< 25\%$ computing power	$< 51\%$ stake	$< 33.3\%$ faulty replicas	$< 51\%$ validators	$< 20\%$ faulty nodes in UNL	$< 33.3\%$ byzantine voting power
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tendermint

Different consensus algorithms have different advantages and disadvantages. Table 2 gives a comparison between different consensus algorithms and we use the properties given by (Vukolić, 2015).

- *Node identity management*. PBFT needs to know the identity of each miner in order to select a primary in every round while Tendermint needs to know the validators in order to select a proposer in each round. For PoW, PoS, DPOS and Ripple, nodes could join the network freely.
- *Energy saving*. In PoW, miners hash the block header continuously to reach the target value. As a result, the amount of electricity required to process has reached an immense scale. As for PoS and DPOS, miners still have to hash the block header to search the target value but the work has been largely reduced as the search space is designed to be limited. As for PBFT, Ripple and Tendermint, there is no mining in consensus process. So it saves energy greatly.
- *Tolerated power of adversary*. Generally 51% of hash power is regarded as the threshold for one to gain control of the network. But selfish mining strategy (Eyal and Sirer,

2014) in PoW systems could help miners to gain more revenue by only 25% of the hashing power. PBFT and Tendermint is designed to handle up to 1/3 faulty nodes. Ripple is proved to maintain correctness if the faulty nodes in a UNL is less than 20%.

- *Example*. Bitcoin is based on PoW while Peercoin is a new peer-to-peer PoS cryptocurrency. Further, Hyperledger Fabric utilizes PBFT to reach consensus. Bitshares, a smart contract platform, adopts DPOS as their consensus algorithm. Ripple implements the Ripple protocol while Tendermint devises the Tendermint protocol.

PBFT and Tendermint are permissioned protocols. Node identities are expected to be known to the whole network, so they might be used in commercial mode rather than public. PoW and PoS are suitable for public blockchain. Consortium or private blockchain might has preference for PBFT, Tendermint, DPOS and Ripple.

3.3 Advances on consensus algorithms

A good consensus algorithm means efficiency, safty and convenience. Current common consensus algorithms still have many shortages. New consensus algorithms are devised aiming to solve some specific problems of blockchain. The main idea of PeerCensus (Decker et al., 2016) is to decouple block creation and transaction confirmation so that the consensus speed can be significantly increased. Besides, Kraft (Kraft, 2016) proposed a new consensus method to ensure that a block is generated in a relatively stable speed. It is known that high blocks generation rate compromise Bitcoin's security. So the Greedy Heaviest-Observed Sub-Tree (GHOST) chain selection rule (Sompolinsky and Zohar, 2013) is proposed to solve this problem. Instead of the longest branch scheme, GHOST weights the branches and miners could choose the better one to follow. Chepurnoy et al. (Chepurnoy et al., 2016) proposed a new consensus algorithm for peer-to-peer blockchain systems where anyone who provides non-interactive proofs of retrievability for the past state snapshots is agreed to generate the block. In such a protocol, miners only have to store old block headers instead of full blocks.

4 Applications of blockchain

There is a diverse of applications of blockchain technology. In this section, we summarize several typical applications of blockchain. We roughly categorize the applications of blockchain into finance in Section 4.1, IoT in Section 4.2, public and social services in Section 4.3, reputation system in Section 4.4 and security and privacy in Section 4.5. Figure 5 illustrates 5 representative application domains of blockchain.

4.1 Finance

- *Financial Services*. The emergency of blockchain systems such as Bitcoin (Nakamoto, 2008) and (hyperledger, 2015) has brought a huge impact on traditional financial and business services. Peters et al. (Peters and Panayi, 2015) discussed that blockchain has the potential to disrupt the world of banking. Blockchain technology could be applied into many areas including clearing and settlement of financial assets etc. Besides, Morini et al. (Morini, 2016) showed that there are real business cases like collateralization of financial derivatives that could leverage blockchain to reduce costs