digital currency initiative

Digital fiat currency (DFC). A key part of our vision for a decentralised financial system is the ability for people to transact familiar currencies using blockchain technology. These fiat currencies present a different challenge to existing digital currencies as there are already other versions of the currency in existence, both physical and digital. One of the main issues is how to ensure all versions of the currency can trade at par with one another. This requires an entity or entities to provide a guarantee that a unit of fiat currency on the blockchain will always exchange 1:1 with other manifestations of the currency. It is this characteristic - rather than any intrinsic value derived from usage - that determines the value of the tokens on the blockchain.

The entity that provides this backing could be the central bank or in the private sector. The precise balance of responsibilities between the public and private sectors will be different, depending on policy choices made in different countries. Supporting many different potential implementations will require technology flexible enough to accommodate this. We are working with central banks to create the technological tools they need to implement a DFC.

Meeting the technical challenge. Existing blockchain software has been created for a specific purpose. For example the Bitcoin Core software was created to run Bitcoin. People have used to to launch other coins but these are structurally similar to Bitcoin. Creating a DFC requires a toolkit and this is why the DCI has created Cryptokernel (CK). CK is flexible enough to accommodate different configurations and can be tailored to the challenge of creating a DFC in different jurisdictions with different policy preferences.

We have created an experimental digital currency called K320 with the purpose of testing the CK software in a real world environment. This related project is important to the DFC work as central banks and policymakers want to see how software performs in a real world environment before trusting their currencies to it.

Intrinsic and extrinsic blockchains. Implementing a digital fiat currency has a broader application for the financial system. A DFC is one example of an extrinsic blockchain, this means the slots in the ledger are tokens representing assets elsewhere. However once the problem has been solved for a DFC then the solution can be applied to other assets. This asset could be intangible (e.g. a share in a company) or tangible (e.g. a barrel of oil, or an ounce of gold). The main difference between an intrinsic and extrinsic blockchain is that the latter requires a trusted party which will guarantee the link between the asset and the ledger. The incentives and consensus mechanism may also need to be different because, for example, on a blockchain representing crude oil creating a new token does not bring a new barrel of oil into existence.

An intrinsic blockchain by contrast is entirely self-contained. Bitcoin is an intrinsic blockchain, as are all the altcoins derived from it. If you buy a bitcoin, you are buying a slot in the ledger – it does not represent or derive value from another asset separate from the blockchain itself.