FCAM

Decentralised Digital Investing

What Drives Decentralised Finance

February 2021

The innovation of blockchain technology is entering a period of broad market acceptance. The idea of highly reliable infrastructure impervious to bias and manipulation is particularly valuable for creating and exchanging new forms of digital money and entering into financial contracts. An alternative decentralized financial (DeFi) system is being built using this new innovative technology that is set to revolutionalise how society forms commercial agreements and exchanges value. There are three key pieces of unique technology, that when combined create the computing infrastructure required for DeFi to operate.

1. Blockchains

the physical network that performs the validation, data storage and safe keep.

2. Smart Contracts

a self-executing contract with the terms of the agreement written directly into lines of computer code.

3. Oracles

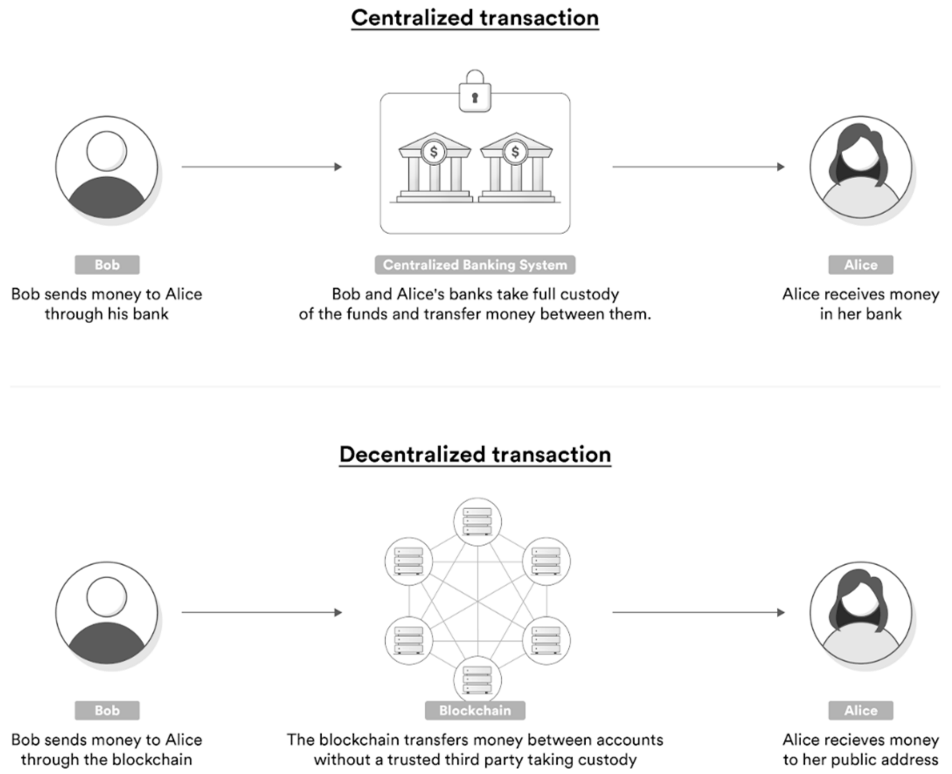
third party services that provide smart contracts with external information. Blockchains and smart contracts cannot access data that is outside of their network, as such oracles serve as bridges between blockchains and the outside world.

We will go through and break down each of these unique technologies.

Blockchain
Decentralised Computer Networks

The first component necessary is the physical computing network responsible for processing the instructions sent to it and facilitating the actual exchange of value between counterparties. This is where the blockchain comes into play. The blockchain serves as a global computer network responsible for physically exchanging of value between two or more parties in a non-custodial manner and documenting the results as data stored in an immutable ledger that anyone can verify as being valid. Blockchains achieve this by operating as a decentralized network of independent computers, which all run the same open-source software set to the same specification, redundantly validate the same transactions, and maintain an ongoing copy of the same ledger.

The shared ledger consists of public key addresses (akin to user bank accounts) that prove ownership of digital assets and can only be accessed by users in possession of the corresponding private key addresses (akin to the user's password), with only one unique private key for each public key.



Bob sends money to Alice through his bank

Bob and Alice's banks take full custody of the funds and transfer money between them.

Alice receives money in her bank

Bob sends money to Alice through the blockchain

The blockchain transfers money between accounts without a trusted third party taking custody

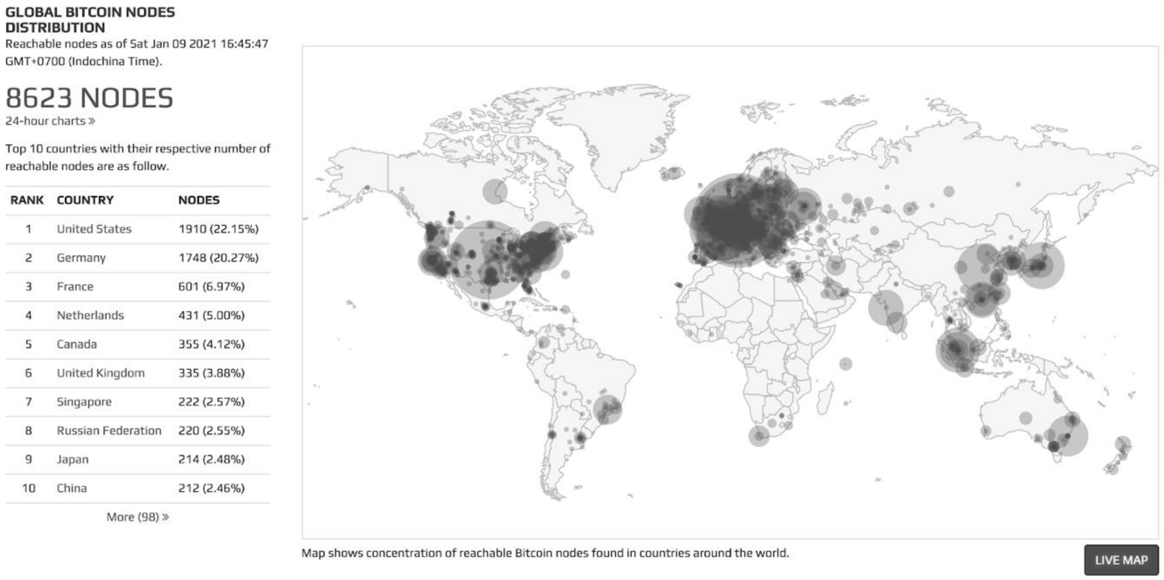
Alice recieves money to her public address

Source: Chainlink

Blockchains use a decentralized network to facilitate the exchange of value between parties without ever taking custody of the asset, whereas a bank takes custody conducting payments.

The question is, how does a network of computers reach a consistent agreement (consensus) about the state of a shared ledger despite malicious attempts to corrupt it? The answer: financial incentives and decentralization. In a Proof of Work (PoW) blockchain, each blockchain node (miner) batches together a series of pending transactions sent by users (called a block) and competes to get their block approved by being the first miner to generate a specific cryptographic hash through brute force (i.e., guessing random numbers until correct). The first node to generate a valid hash wins the block reward (newly minted cryptocurrency + transaction fees), and their block of transactions is confirmed by all other nodes on the network and added to the ledger.

The process is designed this way in order to make it difficult for a single miner or small group of miners to consistently generate a valid hash, keeping the network decentralized. A decentralized network of financially incentivized nodes is inherently resistant to the actions of a few malicious nodes as long as they don't get control over a sufficient amount of the computing power of the PoW-based blockchain (which in most cases is 51%). Additionally, each block contains a unique hash of the previous block, creating a continuous chain of blocks dating back to the first "genesis" block. If any historical block was tampered with, it would become immediately apparent to all network participants as the hashes from one block to another would no longer match.



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Jan 09 2021 16:45:47 GMT+0700 (Indochina Time).

8623 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	1910 (22.15%)
2	Germany	1748 (20.27%)
3	France	601 (6.97%)
4	Netherlands	431 (5.00%)
5	Canada	355 (4.12%)
6	United Kingdom	335 (3.88%)
7	Singapore	222 (2.57%)
8	Russian Federation	220 (2.55%)
9	Japan	214 (2.48%)
10	China	212 (2.46%)

More (98) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

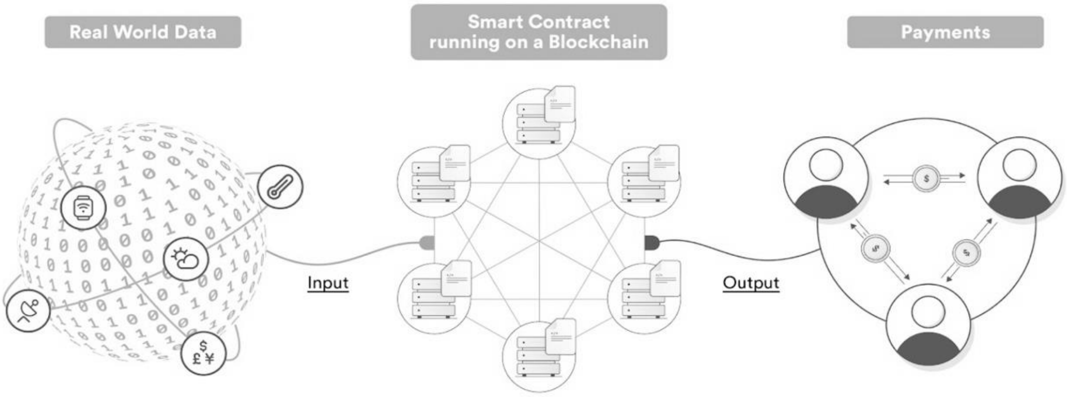
The Bitcoin blockchain consists of thousands of independent nodes operating around the world.

While there are different ways to achieve consensus in a decentralized network (e.g., Proof of Work, Proof of Stake, Proof of Authority, Avalanche) and some blockchains employ different permissions about who can participate in the network's consensus (e.g., Permissionless, Permissioned), this is generally how the two most widely used blockchains, Bitcoin and Ethereum, currently work. The value in such blockchain network designs is that it is extremely expensive and highly impractical to achieve 51% control over the network, meaning users can trust to a very high degree that the data stored and computation performed on the network is secure, reliable, and accurate without any realistic possibility of manipulation or tampering of the ledger. Also, since blockchains are decentralized, run on open-source software, operate in a permissionless manner, and keep track of previous state, the network is always online for anyone with an Internet connection to access, ensuring that any user at any time is able to independently verify the validity of transactions.

Smart Contracts
Decentralised Applications

A smart contract is a self-executing contract with the terms of the agreement directly written into lines of computer code. Smart contracts self-execute predefined actions when specific conditions associated with a given transaction are met. An easy way to understand smart contract is to view it as "programmable money." The most interesting properties of a smart contract are that they are automated, immutable and enforceable. In other words, they execute without human involvement, cannot be tampered with and are legally enforceable.

When paired with a blockchain, smart contracts potentially offer a transparent, automated, and efficient way to facilitate various contractual processes, especially monitoring the performance of agreements with less reliance on third parties. Smart contracts attempt to minimize reliance on existing institutions, such as third-party enforcement mechanisms and financial institutions that historically facilitate economic exchange. The simplest model for understanding conditional logic is "if x event happens, then execute y action." For example, if Team A wins the sporting event then make a payout to Bob; if Team B wins then make a payout to Steve. Instead of manually entering the results of the sporting event, the smart contract is triggered directly by a piece of data informing it on the outcome. Upon receiving the data, the smart contract automatically executes an action often in the form of a payment.

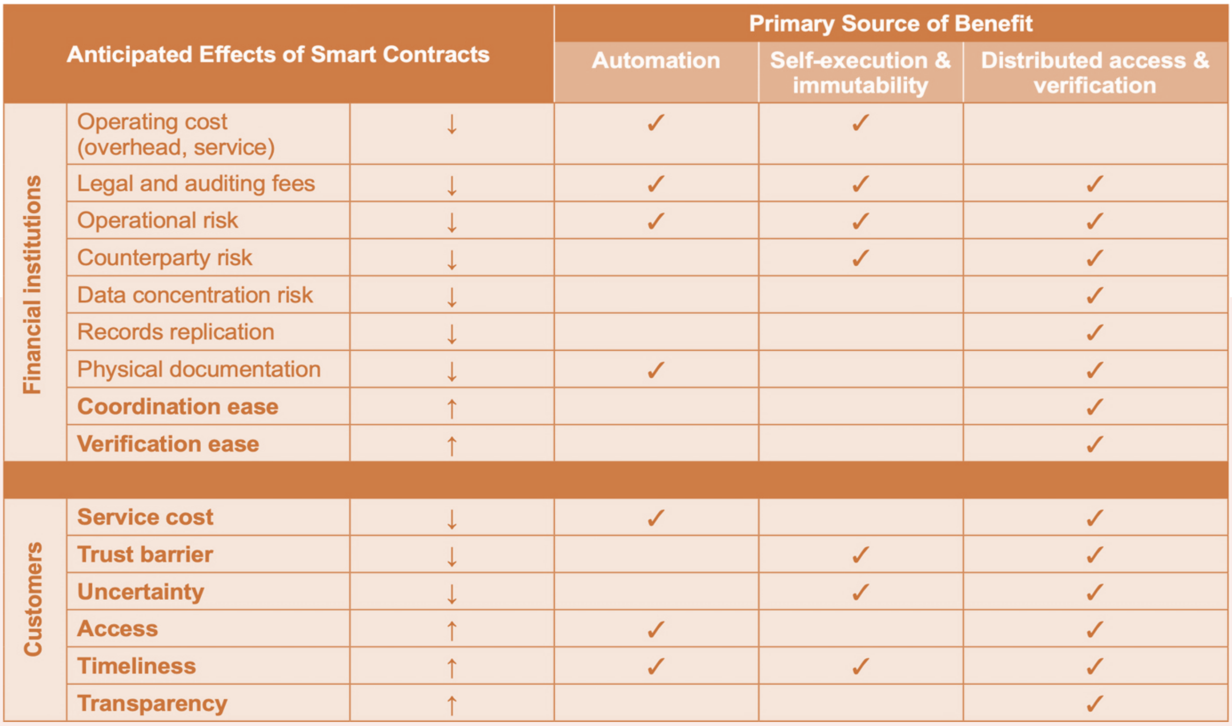


Source: Chainlink

Smart contracts can be best used to capture contractual elements that are mathematical or algorithmic in nature, hence the push towards financial services application. There are multiple other industry applications for this technology: record storing, insurance, supply chains, real estate and mortgage markets, employment agreements, healthcare services, government voting and the internet of things.

Purists envision smart contracts facilitating self-enforcing peer-to-peer (P2P) economic interactions, with little involvement from financial intermediaries, lawyers and courts. To the extent that smart contracts and blockchain facilitate more P2P transactions with reduced reliance on third-parties, direct costs associated with third-parties, such as financial intermediaries and enforcement mechanisms, would disappear.

Smart contracts seek to directly reduce enforcement costs in three ways. First, they increase the cost of breach through self-execution and immutability, thereby reducing uncertainty, the likelihood of contract defection, and, ultimately, the need to maintain and use costly third-party enforcement mechanisms. Second, smart contracts' use of automated control protocols reduce the cost and increase the speed and accuracy of monitoring and verification. Finally, smart contracts' use of blockchain establishes transparent monitoring that is accessible to all parties, without the need for costly replication. On a more macro-level, economists argue these properties will increase the universe of feasible contracts.



Anticipated Effects of Smart Contracts			Primary Source of Benefit		
			Automation	Self-execution & immutability	Distributed access & verification
Financial institutions	Operating cost (overhead, service)	↓	✓	✓	
	Legal and auditing fees	↓	✓	✓	✓
	Operational risk	↓	✓	✓	✓
	Counterparty risk	↓		✓	✓
	Data concentration risk	↓			✓
	Records replication	↓			✓
	Physical documentation	↓	✓		✓
	Coordination ease	↑			✓
	Verification ease	↑			✓
Customers	**Service cost**	↓	✓		✓
	Trust barrier	↓		✓	✓
	Uncertainty	↓		✓	✓
	Access	↑	✓		✓
	Timeliness	↑	✓	✓	✓
	Transparency	↑			✓

Table 1: How smart contracts can potentially unlock value in financial services. Source: World Bank

The development of smart contracts has not been without its problems. The legal enforceability and jurisdiction of smart contracts creates problems for international transactions that span multiple geographies and the complicated legal status of blockchains themselves.

Issues around smart contract coding remain, as new contracts are developed daily. The open-source nature of the code and having a large number of people working on it can mean a better chance of finding and fixing vulnerabilities or bugs quicker.

The issues of confidentiality and privacy are often raised with smart contracts, as all transactions executed are propagated across all of the nodes on the executing network. The benefit of this disclosure is that it provides regulatory disclosure and ultimately compliance.

In practice, smart contracts are being used across a number of public blockchains, the largest being Ethereum. Smart contracts are a type of Ethereum account that are not owned by a particular user, instead they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Deploying a smart contract is technically a transaction, so you need to pay for the transaction in the same way that you need to pay gas for a simple ETH transfer.

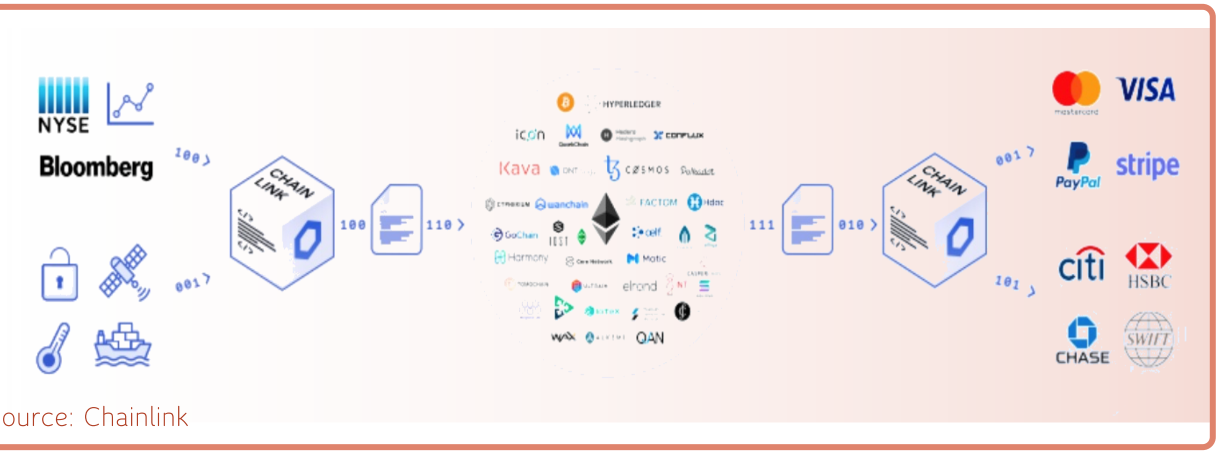
The development of smart contracts has contributed to the explosion of DeFi over the past 12months. Smart contracts form the contractual backbone of the borrowing, lending and exchange protocols that operate on the Ethereum blockchain. Smart contracts enable developers to build far more sophisticated functionality than simply sending and receiving cryptocurrency. These programs are what we now call decentralized apps, or dapps. More on those in a later write up.

Oracles
Decentralised Internet

The third component required to operate DeFi is for smart contracts to become aware of events and interact with systems existing outside the native blockchain they run on. External connectivity entails two functions: 1) consuming data originating outside the blockchain and 2) passing instructional commands to external systems for them to perform

Blockchains are inherently closed and deterministic systems, meaning they have no built-in capabilities to talk to and exchange data between external systems (as doing so could break network consensus). While this generates the valuable security and reliability properties that users seek when using a blockchain, it also severely limits the types of data inputs that smart contracts can ingest and the types of output actions they can trigger on external systems. Most valuable datasets like financial asset prices, weather conditions, sports scores, and Internet of Things sensors, as well as the currently preferred fiat settlement methods like credit cards and bank wires, exist outside the blockchain (off-chain). Given the importance of these resources to real-world business processes, blockchains need a secure bridge to the outside world in order to support a vast majority of smart contract application use cases.

Providing smart contracts connection to the outside world requires an additional piece of infrastructure known as an oracle. An oracle is an external entity that operates on behalf of a smart contract by performing actions not possible or practical by the blockchain itself. This usually involves retrieving and delivering off-chain data to the smart contract to trigger its execution or passing data from the smart contract to an external system to trigger an off-chain event. It can also involve various types of off-chain computations in advanced oracle networks (discussed more below), such as aggregating data from multiple sources or generating a provably fair source of randomness.



Source: Chainlink

An oracle provider (Chainlink) providing data on chain to operate smart contracts.

Similar to blockchains, the oracle mechanism cannot be operated by a single entity, as that would give the centralized oracle sole control over the inputs the contract consumes, thus control over the outputs it produces. Even if the blockchain is highly secure and the smart contract logic is perfectly written, the oracle will put at risk the entire value proposition of the smart contract if it is not built to the same security and reliability standards as the underlying blockchain network, often referred to as the oracle problem.

In summary, the development of smart contracts on public blockchains has the potential to create a more efficient, cost effective, transparent and automated financial system available to anyone with an internet connection. The potential size and scale for this new system is enormous, but it is crucial that the technologists developing the code interact with governments and regulators to ensure a better more democratic financial system exists for future generations to embrace.

Sources:

- Completing the God Protocols: A Comprehensive Overview of Chainlink in 2021- SmartContent – 2021
- World Bank - Smart Contract Technology and Financial Inclusion – 2020
- blog.chain.link/what-is-a-smart-contract-and-why-it-is-a-superior-form-of-digital-agreement/