Back to Guides

Smart Contracts: The Blockchain Technology That Will Replace Lawyers

A Beginner's Guide to Smart Contracts

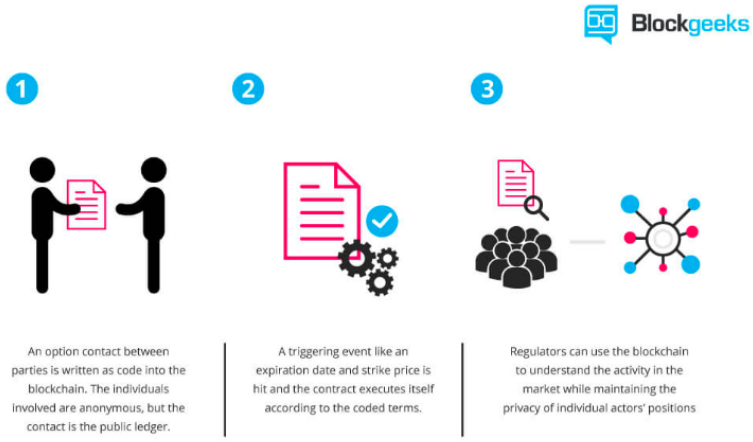
One of the best things about the blockchain is that, because it is a decentralized system that exists between all permitted parties, there's no need to pay intermediaries (Middlemen) and it saves you time and conflict. Blockchains have their problems, but they are rated, undeniably, faster, cheaper, and more secure than traditional systems, which is why banks and governments are turning to them.

In 1994, Nick Szabo, a legal scholar, and cryptographer, realized that the decentralized ledger could be used for smart contracts, otherwise called self-executing contracts, blockchain contracts, or digital contracts. In this format, contracts could be converted to computer code, stored and replicated on the system and supervised by the network of computers that run the blockchain. This would also result in ledger feedback such as transferring money and receiving the product or service.

What are Smart Contracts?

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

The best way to describe smart contracts is to compare the technology to a vending machine. Ordinarily, you would go to a lawyer or a notary, pay them, and wait while you get the document. With smart contracts, you simply drop a bitcoin into the vending machine (i.e. ledger), and your escrow, driver's license, or whatever drops into your account. More so, smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations.



As Vitalik Buterin, the 22-year-old programmer of Ethereum, explained it at a recent DC Blockchain Summit, in a smart contract approach, an asset or currency is transferred into a program "and the program runs this code and at some point it automatically validates a condition and it automatically determines whether the asset should go to one person or back to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof."In the meantime, the decentralized ledger also stores and replicates the document which gives it a certain security and immutability.

Example

Suppose you rent an apartment from me. You can do this through the blockchain by paying in cryptocurrency. You get a receipt which is held in our virtual contract; I give you the digital entry key which comes to you by a specified date. If the key doesn't come on time, the blockchain releases a refund. If I send the key before the rental date, the function holds it releasing both the fee and key to you and me respectively when the date arrives. The system works on the If-Then premise and is witnessed by hundreds of people, so you can expect a faultless delivery. If I give you the key, I'm sure to be paid. If you send a certain amount in bitcoins, you receive the key. The document is automatically canceled after the time, and the code cannot be interfered by either of us without the other knowing since all participants are simultaneously alerted.

You can use smart contracts for all sort of situations that range from financial derivatives to insurance premiums, breach contracts, property law, credit enforcement, financial services, legal processes and crowdfunding agreements.

A Smart Contract Example

Here is the code for a basic smart contract that was written on the Ethereum blockchain. Contracts can be encoded on any blockchain, but Ethereum is mostly used since it gives unlimited processing capability.

```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
```

```
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

An example smart contract on Ethereum. Source: https://www.ethereum.org/token

The contract stipulates that the creator of the contract be given 10,000 BTCS (i.e. bitcoins); it allows anyone with enough balance to distribute these BTCs to others.

Here's How You Can Use Smart Contracts

Jerry Cuomo**, vice president for blockchain technologies at IBM, believes smart contracts can be used all across the chain from financial services to healthcare to insurance. Here are some examples:**

Government

Insiders vouch that it is extremely hard for our voting system to be rigged, but nonetheless, smart contracts would allay all concerns by providing an infinitely more secure system. Ledger-protected votes would need to be decoded and require excessive computing power to access. No one has that much computing power, so it would need God to hack the system! Secondly, smart contracts could hike low voter turnout. Much of the inertia comes from a fumbling system that includes lining up, showing your identity, and completing forms. With smart contracts, volunteers can transfer voting online and millennials will turn out en masse to vote for their Potus.

Management

The blockchain not only provides a single ledger as a source of trust, but also shaves possible snarls in communication and workflow because of its accuracy, transparency, and automated system. Ordinarily, business operations have to endure a back-and-forth, while waiting for approvals and for internal or external issues to sort themselves out. A blockchain ledger streamlines this. It also cuts out discrepancies that typically occur with independent processing and that may lead to costly lawsuits and settlement delays.

Case history

In 2015, the Depository Trust & Clearing Corp. (DTCC) used a blockchain ledger to process more than $1.5 quadrillion worth of securities, representing 345 million

process more than $10 quadrillion worth of securities, representing 3.5 billion transactions.

Supply Chain

Smart contracts work on the If-Then premise so, to put in Jeff Garzik's words,

"UPS can execute contracts that say, 'If I receive cash on delivery at this location in a developing, emerging market, then this other [product], many, many links up the supply chain, will trigger a supplier creating a new item since the existing item was just delivered in that developing market.'" All too often, supply chains are hampered by paper-based systems, where forms have to pass through numerous channels for approval, which increases exposure to loss and fraud. The blockchain nullifies this by providing a secure, accessible digital version to all parties on the chain and automates tasks and payment.

Case history

Barclays Corporate Bank uses smart contracts to log change of ownership and automatically transfer payments to other financial institutions upon arrival

Automobile

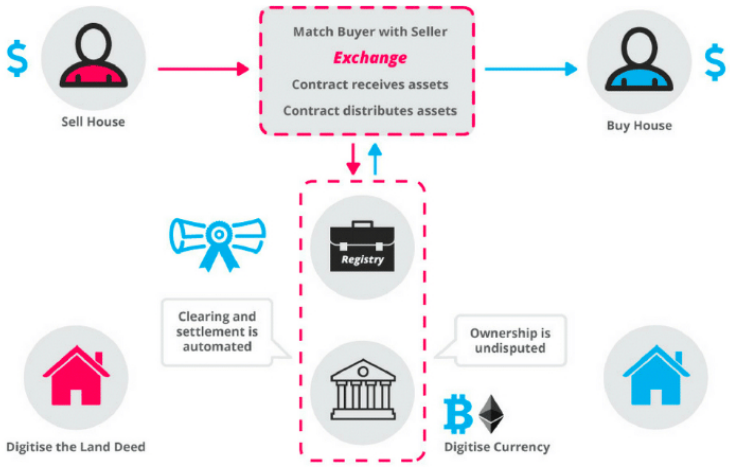
There's no doubt that we're progressing from slothful pre-human vertebrates to super-smart robots. Think of a future where everything is automated. Google's getting there with smartphones, smart glasses, and even smart cars. That's where smart contracts help. One example is the self-autonomous or self-parking vehicles, where smart contracts could put into play a sort of 'oracle' that could detect who was at fault in a crash; the sensor or the driver, as well as countless other variables. Using smart contracts, an automobile insurance company could charge rates differently based on where, and under which, conditions customers are operating their vehicles.

Real Estate

You can get more money through smart contracts. Ordinarily, if you wanted to rent your apartment to someone, you'd need to pay a middleman such as Craigslist or a newspaper to advertise and then again you'd need to pay someone to confirm that the person paid rent and followed through. The ledger cuts your costs. All you do is pay via bitcoin and encode your contract on the ledger. Everyone sees, and you accomplish automatic fulfillment. Brokers, real estate agents, hard money lenders, and anyone associated with the property game can profit.

Healthcare

Personal health records could be encoded and stored on the blockchain with a private key which would grant access only to specific individuals. The same strategy could be used to ensure that research is conducted via HIPAA laws (in a secure and confidential way). Receipts of surgeries could be stored on a blockchain and automatically sent to insurance providers as proof-of-delivery. The ledger, too, could be used for general healthcare management, such as supervising drugs, regulation compliance, testing results, and managing healthcare supplies.



Smart Contracts are Awesome!

Here's what smart contracts give you:

Autonomy – You're the one making the agreement; there's no need to rely on a broker, lawyer or other intermediaries to confirm. Incidentally, this also knocks out the danger of manipulation by a third party, since execution is managed automatically by the network, rather than by one or more, possibly biased, individuals who may err.

Trust – Your documents are encrypted on a shared ledger. There's no way that someone can say they lost it.

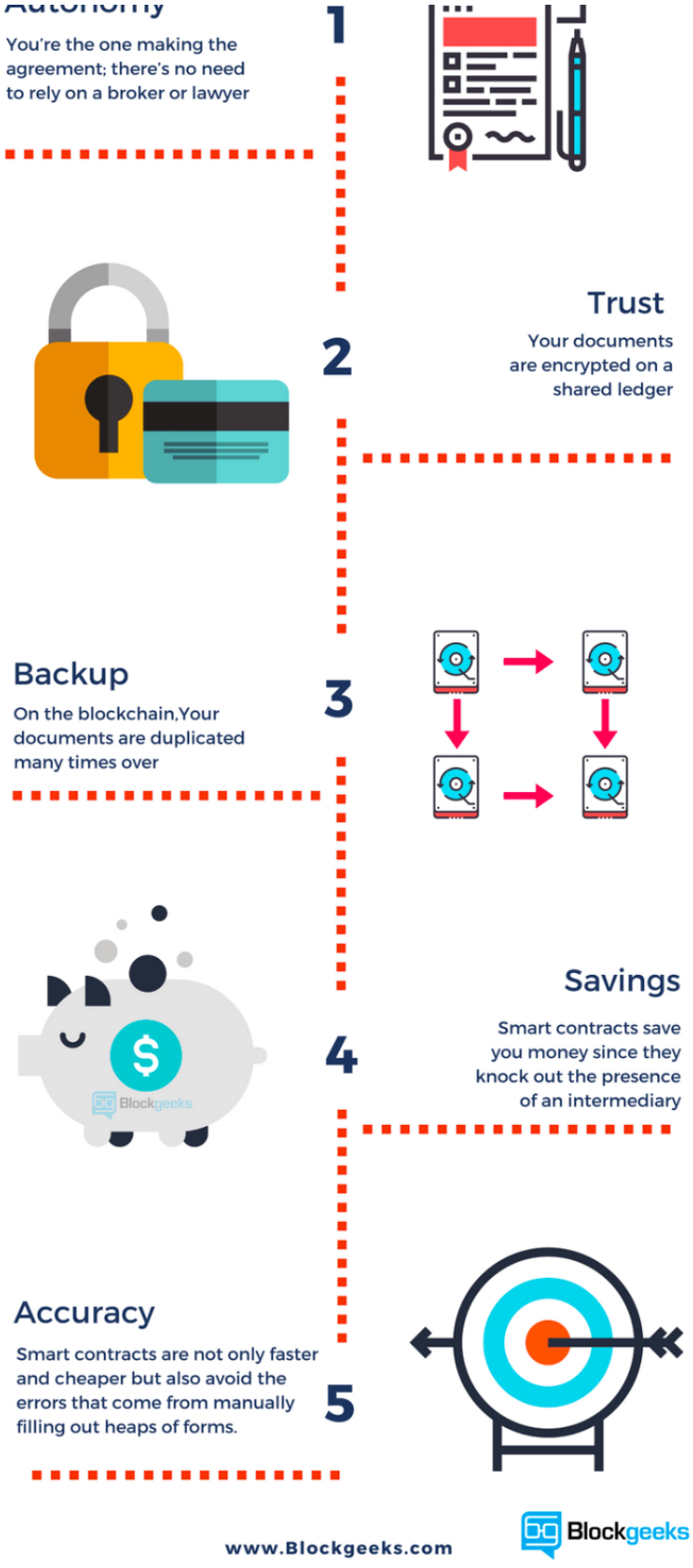
Backup – Imagine if your bank lost your savings account. On the blockchain, each and every one of your friends has your back. Your documents are duplicated many times over.

Safety – Cryptography, the encryption of websites, keeps your documents safe. There is no hacking. In fact, it would take an abnormally smart hacker to crack the code and infiltrate.

Speed – You'd ordinarily have to spend chunks of time and paperwork to manually process documents. Smart contracts use software code to automate tasks, thereby shaving hours off a range of business processes.

Savings – Smart contracts save you money since they knock out the presence of an intermediary. You would, for instance, have to pay a notary to witness your transaction.

Accuracy – Automated contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.



Here's how Jeff Garzik, owner of blockchain services Bloq, described smart contracts:

> "Smart contracts … guarantee a very, very specific set of outcomes. There's never any confusion and there's never any need for litigation."

"Smart Contracts are where the rubber meets the road for businesses and blockchain technology. While a few highly specialized distributed financial services use cases for blockchain have appeared—for example, payment ledger services for the Yangon Stock Exchange in Myanmar. Its services on top of blockchain that are really interesting. In the Yangon Exchange, it solves the problem of distributed settlement in a trading system that only synchronizes trades twice a day. But the autonomous execution capacities of smart contracts extends the transactional security assurance of blockchain into situations where complex, evolving context transitions are required. And it's this possibility that has Amazon, Microsoft Azure and IBM Bluemix rolling out Blockchain-as-a-Service (Baas) from the cloud." – Patrick Hubbard**, Head Geek, SolarWinds**

Now for Problems

Smart contracts are far from perfect. What if bugs get in the code? Or how should governments regulate such contracts? Or, how would governments tax these smart contract transactions? As a case in point, remember my rental situation?

What happens if I send the wrong code, or, as lawyer Bill Marino points out, I send the right code, but my apartment is condemned (i.e., taken for public use without my consent) before the rental date arrives? If this were the traditional contract, I could rescind it in court, but the blockchain is a different situation. The contract performs, no matter what.

The list of challenges goes on and on. Experts are trying to unravel them, but these critical issues do dissuade potential adopters from signing on.

And here's To the Future of Smart Contracts…

Part of the future of smart contracts lies in entangling these issues. In Cornell Tech, for instance, lawyers, who insist that smart contracts will enter our everyday life, have dedicated themselves to researching these concerns.

Actually, when it comes to smart contracts, we're stepping into a sci-fi screen. The IT resource center, Search Compliance suggests that smart contracts may impact changes in certain industries, such as law. In that case, lawyers will transfer from writing traditional contracts to producing standardized smart contract templates, similar to the standardized traditional contracts that you'll find on LegalZoom. Other industries such as merchant acquirers, credit companies, and accountants may also employ smart contracts for tasks, such as real-time auditing and risk assessments. Actually, the website Blockchain Technologies sees smart contracts merging into a hybrid of paper and digital content where contracts are verified via blockchain and substantiated by physical copy.

Blockchains Where You Can Process Smart Contracts

Bitcoin: Bitcoin is great for processing Bitcoin transactions, but has limited ability for processing documents.

Side Chains: This is another name for blockchains that run adjacent to Bitcoin and offer more scope for processing contracts.

NXT: NXT is a public blockchain platform that contains a limited selection of templates for smart contracts. You have to use what is given; you're unable to code your own.

Ethereum: Ethereum is a public blockchain platform and the most advanced for coding and processing smart contracts. You can code whatever you wish but would have to pay for computing power with "ETH" tokens.

As to the potential of smart contracts itself, there's no end to the range of industries it can impact, from healthcare to automobiles to real estate and law. The list goes on and on. Says, Ethereum CTO, Gavin Wood

"The potential for [smart contracts] to alter aspects of society is of significant magnitude. This is something that would provide a technical basis for all sorts of social changes, and I find that exciting."

Comments

Dmitry Buterin 2 years ago

What are the biggest challenges and limitations of smart contracts as of today?

1

Alex Todd 2 years ago

@Dmitry Buterin

Today, the biggest challenge is the misconception of what the term "smart contract" really means, as it is not a contract in the conventional sense of the word – so the term can be misleading. However, once that gets cleared up, there are many other limitations that will need to be addressed, such as how do you trust them to do what they promise to do, and what recourse do you have if they don't?

5

George Nguyen 7 months ago

@Alex Todd

I would say it's more like a individual deal and agreement. Contract is more of legal enforcement

0

david teruzzi 2 years ago

@Dmitry Buterin

To be or not to be? Code is Law or Code is not Law ?

Just think what happened to TheDAO. To be part of the DAO people accepted "terms and conditions" in English while services in the platform run pieces of Ethereum code. Obviously "terms and conditions" cannot include BUGS and cannot provide a perfect match between english and solidity code (for instance)

So we have 3 big challenges :

4