Understanding Blockchain

There has been a fair amount written about blockchain by now, and I will reference a number of papers to add clarity and depth to the conversation, while also attempting to give a relatively simple laypersons view of the topic.

The underpinning for blockchain is a peer to peer network of “nodes”, that collaborate to store information and transact the data. The blockchain is a list of records, linked using cryptography. This creates a chain of information that is relatively immutable, and secure. Every block added contains a cryptographic hash of the previous block, along with a time stamp and transaction data generally represented as a merkle tree root hash. As you can deduce from this, you end up with an information trail that is difficult to tamper with. This security is further improved, as any addition to the blockchain must be approved by the peer nodes on the network.

Satoshi Nakamoto invented blockchain in 2008 as the foundation for the crypto currency BitCoin, and it has expanded significantly from there with types of blockchains expanding and correspondingly, as the capabilities expand, so have the use cases.

> The idea emerged that the Bitcoin blockchain could be in fact used for any kind of value transaction or any kind of agreement such as P2P insurance, P2P energy trading, P2P ride sharing, etc. Colored Coins and Mastercoin tried to solve that problem based on the Bitcoin Blockchain Protocol. The Ethereum project decided to create their own blockchain, with very different properties than Bitcoin, decoupling the smart contract layer from the core blockchain protocol, offering a radical new way to create online markets and programmable transactions known as Smart Contracts.
> Private institutions like banks realized that they could use the core idea of blockchain as a distributed ledger technology (DLT), and create a permissioned blockchain (private or federated), where the validator is a member of a consortium or separate legal entities of the same organization. The term blockchain in the context of permissioned private ledger is highly controversial and disputed. This is why the term distributed ledger technologies emerged as a more general term.
>
> HTTPS://BLOCKCHAINHUB.NET/BLOCKCHAINS-AND-DISTRIBUTED-LEDGER-TECHNOLOGIES-IN-GENERAL/

Blockchain what and why- from **gavofyork**

As blockchain thinking matured, additional approaches and types of blockchains emerged. As you can see from the included slide share by Dr. Gavin Wood, Ethereum became a platform based on blockchain, allowing for the use of smart contracts. Dr. Wood describes blockchain as: “A Byzantine-Fault-Tolerant decentralized singleton fixed-function state-transition system.” Essentially, he is describing it as a type of computer or computing machine.

Whereas the foundational application of BitCoin is compared to an adding machine, we see the Ethereum implementation as analogous to a computer that is multi-user and highly accessible, while still retaining the security of the blockchain approach. This is extremely exciting as it opens the door to the idea of Smart Contracts! Smart Contracts are guaranteed to have:

1. Atomicity: The entire operation runs or nothing does
2. Synchrony: No two operations can interfere with each other
3. Provenance: All messages (Method calls) can be inspected to determine caller address
4. Permanence: Objects data are permanent
5. Immortality: Object can never be externally deleted – can only voluntarily commit suicide
6. Immutability: Objects code can never be changed

From this description, you can infer some powerful concepts with profound implications to how we might do business going forward. Contracts that are managed with this approach can be fully visible to all parties, eliminating fraud. These approaches can be seen as the foundation for fully trusted, automated transactions, replacing significant man hours, lawyers interventions and cost. The ideas of Smart Contracts and the multiplicity of uses for blockchain is outside the scope of this post, but I would encourage you to continue to read more on the topic, and reference the short post and linked slide share I have here, from the Pistoia Alliance presentation on this topic.