



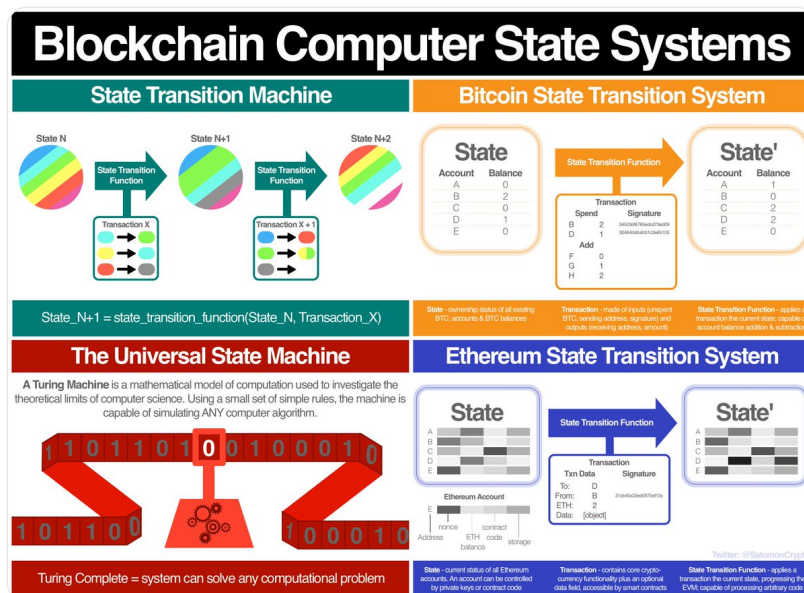
Haym Salomon @SalomonCrypto

Aug 5 · 20 tweets · [SalomonCrypto/status/1555684780921892864](https://twitter.com/SalomonCrypto/status/1555684780921892864)

## (1/19) Computer Science Fundamentals: Blockchain Computers, [@Bitcoin](#) and [@ethereum](#)

What is a blockchain computer and what makes it special?  
How did [@VitalikButerin](#) build on top of Bitcoin to create  
Ethereum? Why is Ethereum The World Computer?

This thread has answers!



(2/19) [@ethereum](#) calls us all in different ways. Some are called by the decentralization, others to become unrealistically wealthy; everyone has their reasons.

Personally, I've heard the siren's song of The World Computer and am drawn the future we will build on top of it.

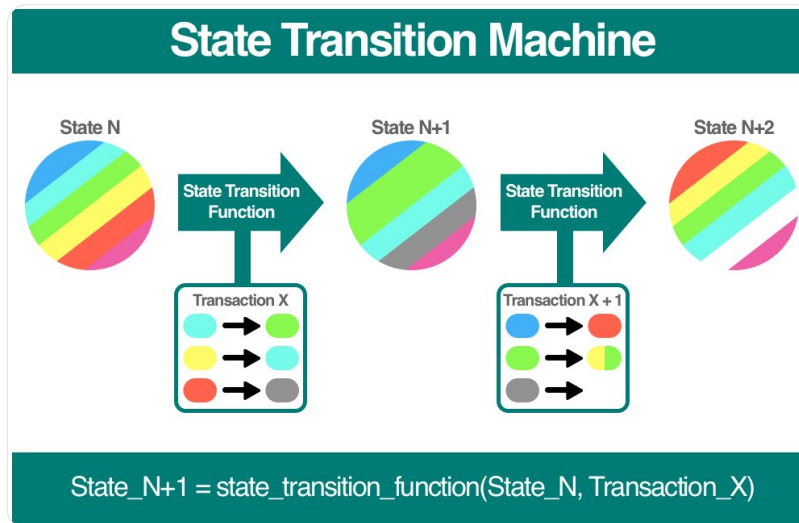


(3/19) But not all understand The World Computer metaphor. Crypto is so incredibly fast paced (and is inherently muddled with delusional visions of generational wealth) that it is easy to miss what makes [@ethereum](#) so special.

Let's go back to computer science basics.

(4/19) A state machine is a mathematical model of computation with two major components:

- the state, the configuration of the system at a moment in time
- a transaction, the set of instructions to change the state



(5/19) The machine operates by applying a state transition function:

INPUTS: current state and the pending txn

OUTPUT: the new machine state.

In the example above, the txn describes which colors to change while the state transition function does the actual changing.

(6/19) The state transition machine model provides a simple framework for breaking down computation into a step-by-step process.

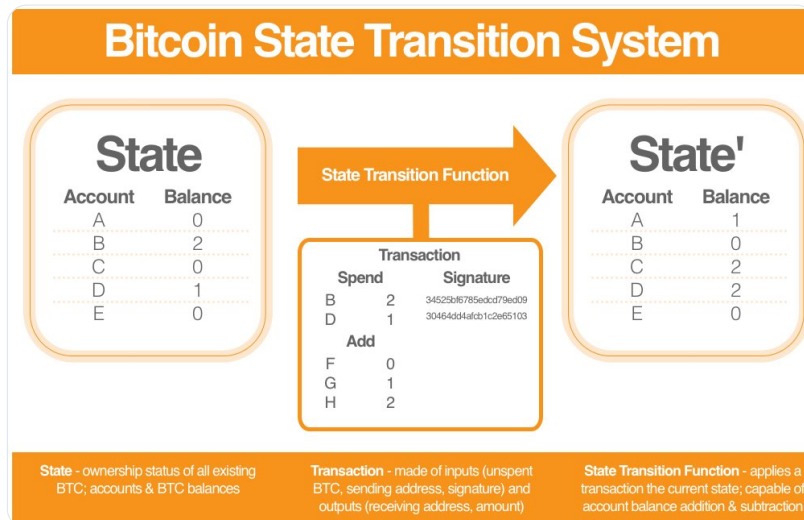
Now let us apply the concept to [@Bitcoin](#).

(7/19) At its core, [@Bitcoin](#) can be described as a state transition system that functions similarly to a simple banking system.

State - balance sheet

Transaction - request to move \$X from A to \$B

State Transition Function - reduce \$X from A's account, add \$X to B's account



(8/19) While [@Bitcoin](#) can natively facilitate simple scripts, the language has some critical limitations. In practice, the vast majority of activity is the addition, subtraction and management of account balances.

(9/19) Put simply, [@Bitcoin](#) can be thought of as a specialized computer only capable of balance management.

When described as a state transition system, this specialization (limitation) can be seen in the basic and inflexible capabilities of the state transition function.


(10/19) In 2009, Satoshi Nakamoto combined research in public key cryptography with innovations in consensus algorithms to produce [@Bitcoin](#).

We've discussed the computational capabilities of Bitcoin - meh.


The impressive part is that it happens on a trust-less network.

(11/19) We'll avoid the temptation to veer deeply into consensus in this thread - below is a resource for those with curiosity.

For now, consensus systems substitute a formal barrier of participation with an economic one. The result: a decentralized, transparent & fair platform.



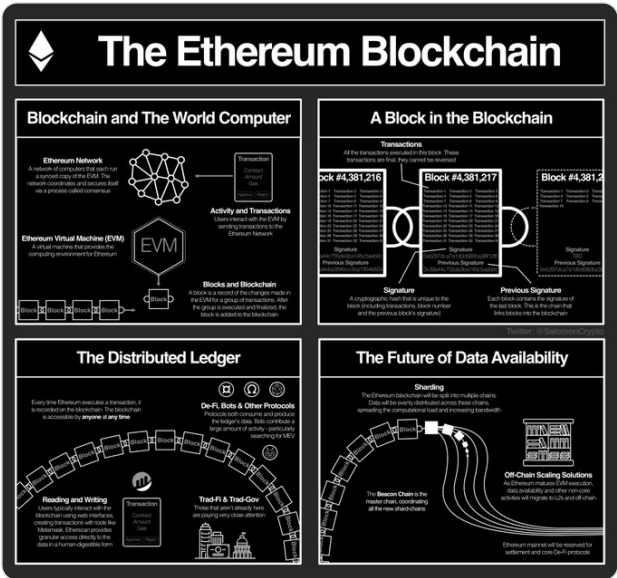
**Haym Salomon**  
@SalomonCrypto · Follow



(1/10) The **@ethereum** Blockchain: Your guide to the distributed ledger technology that powers The World Computer.

What is the blockchain? What role does it play in the Ethereum protocol? What does the future hold for this core tech?

Read on for these answers, and more!



**The Ethereum Blockchain**

**Blockchain and The World Computer**

**Ethereum Network**  
A network of computers that each act as a node in the network. The network coordinates and validates transactions in a peer-to-peer consensus system.

**Ethereum Virtual Machine (EVM)**  
A virtual machine that provides the computing environment for Ethereum.

**Activity and Transactions**  
Transactions are sent to the EVM by sending transactions to the Ethereum network.

**Blocks and Blockchain**  
A block is a record of the changes made in the Ethereum system. After the group of transactions is validated, the group is added to the blockchain.

**A Block in the Blockchain**

**Transactions**  
All the transactions included in the block. These transactions are hashed and timestamped.

**Block #4,381,216** **Block #4,381,217** **Block #4,381,218**

**Signature**  
A cryptographic code unique to the block including transactions, block number and the previous block's signature.

**Previous Signature**  
Each block contains the signature of the previous block. This is the chain that links blocks in the blockchain.

**The Distributed Ledger**

Every time Ethereum sends a transaction, it is recorded on the blockchain. The blockchain is accessible by anyone at any time.

**De-Fi, Bots & Other Protocols**  
Private data can be shared and produced in the ledger's data. This continues a management of data, providing a secure way to search for data.

**Reading and Writing**  
Blockchain uses a distributed ledger. Every transaction is recorded in the ledger. The ledger is accessible by anyone at any time.


**TradeFi & Trade-Gov**  
Blockchain is a distributed ledger. It is a secure way to store and manage data. It is a secure way to store and manage data.

**The Future of Data Availability**

**Sharding**  
The Ethereum blockchain will be split into multiple chains. Data will be stored in multiple chains. This will allow for more data to be stored in the blockchain.

**Off-Chain Scaling Solutions**  
As Ethereum matures, it will need to scale. Off-chain scaling solutions will be used to store data. This will allow for more data to be stored in the blockchain.

5:31 AM · Aug 2, 2022

[Read the full conversation on Twitter](#)

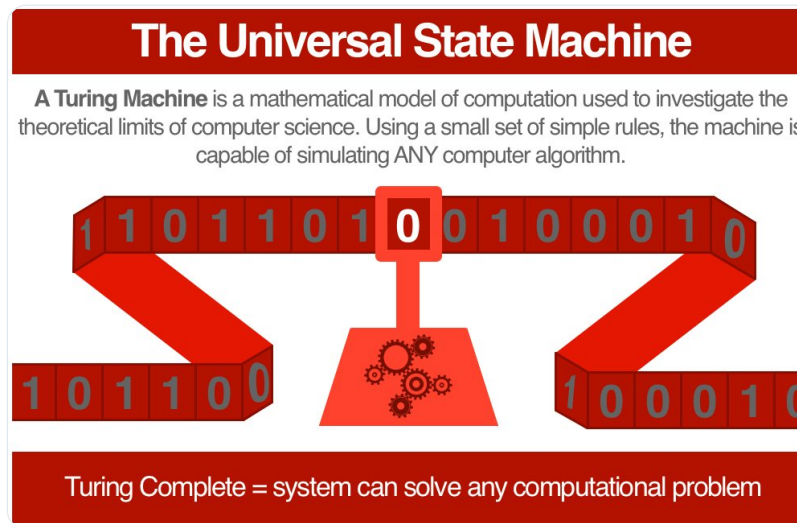
(12/19) Think about it this way: blockchain computer are a state machine operated by a decentralized network of un-trusted computers.

[@Bitcoin](#)'s state transition function is very basic: balance sheet management. The obvious question...

Can a state transition function do more?

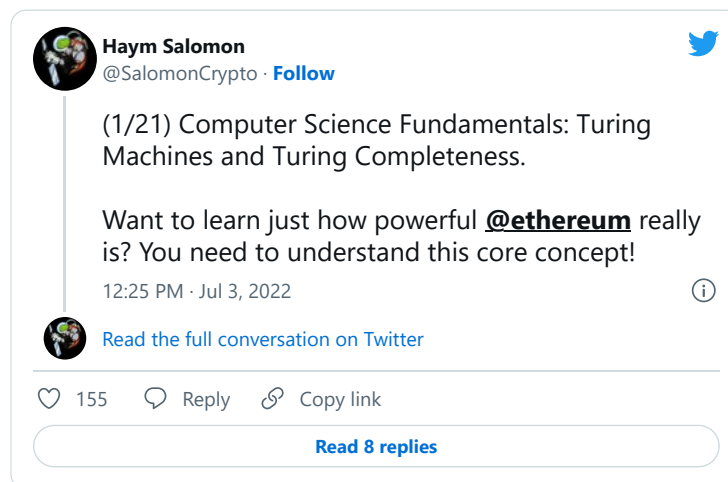
(13/19) The answer is an emphatic YES! In fact, the right state transition function is capable of generalized computing!

The Turing Machine, named from mathematician Alan Turing, is a state machine capable (mathematically proven) of simulating any computer algorithm.



(14/19) Any computational system can be described via a state machine. A careful analysis of that state machine will check to see if the system can be used to simulate a Turing Machine.

If so, we call the system Turing-complete; it is capable of generalized computation.



(15/19) [@Bitcoin](#) is the state machine for a decentralized banking system. Its scope and capabilities are limited by the language of the state transition function.

If Bitcoin is specialized, then [@ethereum](#) is generalized.

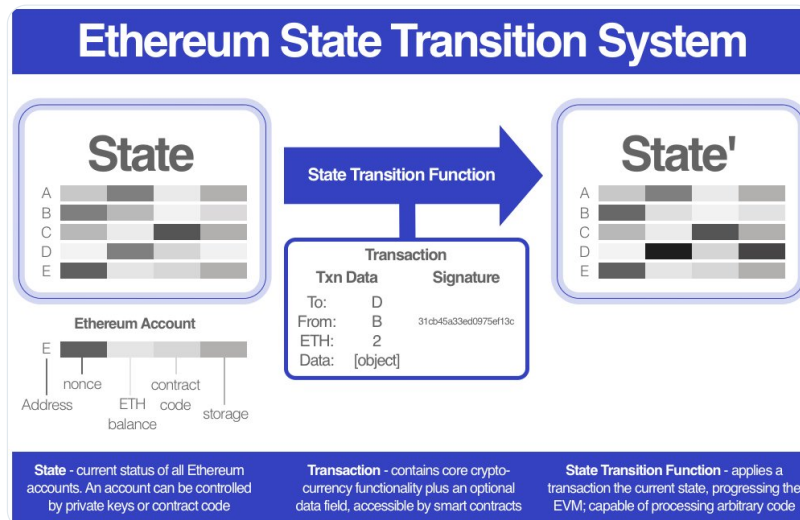
Solidity, the language of Ethereum, is Turing-complete.

(16/19) [@ethereum](#) State Machine

State - status of all Ethereum accounts

Transaction - typical cryptocurrency transaction with an optional data field, accessed programmatically by smart contracts

State Transition Function - the code executed by the EVM



(17/19) [@ethereum](#) is much more complex than [@Bitcoin](#), you can see it even in these simplified diagrams.

But take a step back and the picture is more clear: both Ethereum and Bitcoin are blockchain computers; Bitcoin is like a calculator, Ethereum like a Macbook.

(18/19) In summary, [@Bitcoin](#) and [@ethereum](#) should be understood as the next iteration in computing technology.

First we had personal computing. Then we had cloud computing.

Bitcoin is the first, specialized example of shared computing.

Ethereum is The World Computer.

(19/19) Still having trouble wrapping your head around it? Maybe you're an audio learner!

Check out this clip from my interview with [@flywheelpod](#), I'll walk you through the same ideas.





Follow me for more explainers and as much alpha as I can possibly serve.

...