$H O L \bigcirc C H A | N$



Holochain & Holo 101

Reorientation for Blockchain Audiences

November 2018

Strategic Partnerships, Holochain

About this document

- Introduces Holochain and Holo:
 - Purpose
 - Design and Architecture
 - Pros and Cons
- Written to orient blockchain audiences to Holochain
- Light technical content: e.g. audience expected to know basics e.g. how a blockchain works, consensus mechanisms
- About the product and network, not the Holo organisation

dApps can be built with blockchain...

- Blockchain is a ledger originally optimised for tracking assets:
 - Every node stores and executes everything
 - Data consensus required
- Smart contract functionality allows for logic during execution
- Accounting data can be replaced with arbitrary data (e.g. text, images, code)
- Arbitrary logic + arbitrary data = application on the blockchain

...but blockchain is not optimised for this

- Storing all transactions requires lots of data. Bitcoin blockchain is 185GB+
- Every node executing every smart contract is expensive
- Authority to write to data decentralised but data construct itself
 remains pseudo-centralised
 - All activity must be uploaded to the blockchain to be accepted.
 Sub-networks cannot resolve actions among themselves
- Incentive towards centralisation since more control of consensus = more power and wealth

Bolt-on solutions only partially address this

- Sharding improves TPS, execution, and data storage efficiency by reducing duplication
- Side chains also help scaling and may enable smaller sub-networks to act asynchronously
- Cross-chain protocols are being built to try to deal with network interoperability
- dApps like Vault12 trying to solve DPKI

Holochain does all of this natively and often in a better way

Introducing HOLOCHAIN

What is HOLOCHAIN?

Framework for Distributed Applications

- Connected apps that only use users' devices (no servers)
- Overcomes Cost, Speed & Scale challenges of blockchain approaches
- Each Holochain dApp (hApp) creates its own network
- hApp networks are natively interoperable with the right permissions (c.f. an "internet of blockchains")

Hash Chains + Distributed Hash Tables + Digital Signatures







How H O L O C H A I N works

- Each Holochain application (hApp) has its own shared set of rules (DNA)
- All hApp data is validated and signed before being saved to local storage
- Each user has their own tamper-resistant local storage (hash chain) per hApp
- Public data is published to the hApp's shared storage (distributed hash table)
- Shared hApp data is validated by many random peers
- Invalid data results in publishing a warrant that triggers a response from the hApp e.g. rejecting data, node blacklisting (immune system)

How HOLOCHAIN works



Resulting structure: a DAG formed on a DHT



Peer Validation-Based Consensus

- Source chains are stored on a randomised set of peer nodes (DHT)
- All actions require both parties to validate and sign/countersign them
 - Actions that do not involve others do not require consensus
- The action is further validated by peers holding a copy of the source chain
- To make a fraudulent transaction a node needs to collude with all their validators. This likely requires control over a significant majority of nodes
- It is up to the hApp designer to make it non-trivial to create a new node/agent (e.g. identity verification, asset deposit)

Holochain is a full framework not a data structure

		\$	ΙΟΤΑ	0
Function	Accounting Ledger	Virtual Machine	Virtual Machine	Any (Framework)
Data Structure	Blockchain	Blockchain	Unstructured DAG ¹	DHT and DAG of source chains
Consensus	Proof-of-Work	Proof-of-Work ²	"Witness" ³ node validation	Counterpart + witness ³ node validation
Redundancy	Every node does everything	Every node does everything	Nodes handle own activity + some others	Nodes handle own activity + some others
Error Handling	Data rejected	Data rejected	Data rejected	Custom e.g. data rejection, node blacklisting

In constrast, Nano (and Holochain) are DAGs comprised of individual node blockchains;
 Moving to proof-of-stake;
 Witness node validation means that nodes not involved in the transaction validate the transaction

This means it's meta to blockchain

A currency built on	
Holochain	

...has its own network and consensus rules like Bitcoin or Nano... ...not a simple token e.g. ERC20

A dApp built on Holochain

...is an independent, full-scale network...

...not a local or centralised app + smart contracts

A smart contract virtual machine

...could be built on Holochain ...and would look a little like Hashgraph

Holochain apps are natively interoperable, creating an "internet of Holochains"

Validate TPS Online / offline? membranes?

Holochain has huge advantages

 Transactions per day (*capacities)

 NETWORK
 ESTIMATE

 BLOCKCHAINS
 10 000 000

 HOLOCHAIN*
 200 000 000

 VISA
 150 000 000

 PAYPAL
 15 000 000

 BITCOIN
 200 000

Highly scalable: Due to parallel nature of DAGs and limited global consensus

Flexible, node-oriented violation response: E.g. Fake messages could be blocked while fraudulent transactions might lead to permanent blacklisting

Lightweight: Nodes only execute code and store data related to their activities. Holochain applications/nodes can run on a Raspberry Pi

More forgiving: DPKI enables recovery of lost keys, and countersigned transactions mean that transactions to mistyped addresses will time out

Natively Interoperable: Between each hApp network

Potential applications

- Social Networks, Social Media & VRM: You want to run a social network without a company like Facebook in the middle. You want to share, post, publish, or tweet to shared space, while automatically keeping a copy of these things on your own device.
- **Supply Chains & Open Value Networks:** You want to have information that crosses the boundaries of companies, organizations, countries, which is collaboratively shared and managed, but not under the central control of any one of those organizations.
- **Cooperatives and New Commons:** You want to create something which is truly held collectively and not by any particular individual. This is especially good for digital assets.
- **P2P Platforms:** Peer-to-Peer applications where every person has similar capabilities, access, responsibilities, and value is produced collectively.
- **Collective Intelligence:** Governance, decision-making frameworks, feedback systems, ratings, currencies, annotations, or work flow systems.
- Collaborative Applications: Chats, Discussion Boards, Scheduling Apps, Wikis, Documentation, etc.
- **Reputational or Mutual Credit Cryptocurrencies:** Currencies where issuance can be accounted for by actions of peers (like ratings), or through double-entry accounting are well-suited for holochains. Fiat currencies where tokens are thought to exist independent of accountability by agents are more challenging to implement on holochains.

Holo and Holo Fuel

What is Holo?

Holo provides users on the the traditional web access to Holochain Apps

- Each hApp is a full node, connected to the network
- Access via web browser vs local hApps with constantly syncing data
 - Mobile & IOT users
 - Users behind firewalls or other network restrictions
- Holo is a distributed cloud hosting hApp allows people or organisations to rent hApp hosting from people with hosting capacity

Holo recognises that the client-server model remains optimal for some users

What is Holo Fuel?

An accounting system to record value flows and facilitate Holo hosting payments

- An accounting ledger hApp in the same way that Bitcoin is an accounting ledger dApp
- Dynamic circulating supply tied to Holo network activity and redeemable against it
- Showcases mutual credit currency design principles
- Value stable, but not a stablecoin

Holo Fuel Design

- A mutual credit currency where all newly created fuel is backed by a corresponding debt
- All debt (and thus all Fuel) is backed by some form of collateral / wealth
 - Hosts \rightarrow Fuel earnings potential from hosting
 - Reserve accounts \rightarrow currencies held by reserve (e.g. USD, EUR, BTC)
 - Holo $Org \rightarrow Transaction$ fees
- Holo Fuel circulating supply shrinks as Fuel is used for hosting and repaid
- Reserves create passive system stability and resilience
 - Sells new Fuel at prices algorithmically based on aggregated host settings
 - Hosts can then redeem Fuel for currency held by reserve (c.f. escrow)
 - Prevents hyperdeflation if hosts individually reluctant to sell new Fuel
 - Price signals also act as dampener on short term volatility

Holo Fuel Supply and Circulation



*Holo org and all users have a credit limit. For Holo's credit limit, we will be transparent and clarify under what conditions we will spend on credit.

Getting Started

Our next 12 months commitments

- HoloToken (HOT) will be redeemable for HoloFuel
 - Represents IOU's for web hosting (storage and processing)
- Develop Holochain to a secure and stable state
- Launch Holo on Holochain
 - Deliver distributed computing services at most 1/10,000 of the cost on ETH
- Create a vibrant Holochain app ecosystem

Getting started

Rust Developer Preview: https://github.com/holochain/holochain-rust

Go Pre-Alpha: https://developer.holochain.org/

Devcamp: TBD

Social Media / Telegram / Mattermost