



Wolfram Cross-Chain

Introduction to Cross-Chain

The market of cryptocurrencies is numbered in the thousands, and people want to exchange them. One way to exchange tokens is using a middleman (centralized exchange) to handle your tokens and someone else's, and swap them, for a fee. However, what if you didn't want to *exchange* your token, you wanted to *retain* it and use it on another blockchain?

This is more complicated than it sounds. If blockchains are considered like nations, with their own languages, that's like saying: I want to go to China and speak Chinese in English. The only way to accomplish this is a translator app, where you are speaking English into it and Chinese comes out.

Asset-wise, there are non-US businesses that will accept USD as payment, but usually you have to exchange it for another country's currency. What if you didn't want to exchange it because you didn't believe their currency was as stable as USD? This could be similar to the case with someone holding Bitcoin, who wants to use its value in dApps on Ethereum (e.g. wrapped BTC), but doesn't want to trade it all for ETH. Broadly speaking, bridging and cross-chain communication is the "Oracle Problem".¹

"Blockchains are traditionally blind to the real world. This implies reliance on third parties called oracles when extrinsic data are needed for smart contracts. Oracle implementation, however, is still controversial and debated due to the reintroduction of trust and a single point of failure."²

Unlike ancient Greek oracles, blockchain oracles don't predict the future, instead they are trying to bring information from the past or present (such as clock time) to smart contracts.³ Such a simple concept in the rest of the internet, passing data around, becomes very non-trivial on blockchains. The nature of the oracle problem is bringing trusted data into a trustless system. Oracles face their own *trilemma*, which is similar to the blockchain trilemma.

⁴

¹ <https://cointelegraph.com/magazine/2021/12/30/can-blockchain-solve-its-oracle-problem>

² Caldarelli, Giulio. "Wrapping Trust for Interoperability: A Preliminary Study of Wrapped Tokens." Information 13.1 (2021): 6.

³ <https://encyclopedia.pub/entry/2959>

⁴ <https://github.com/unghuuduc/NeuRacle#oracle-trilemma>

If you want asset prices in fiat terms, rainfall measurements, football scores, or anything “real world”, you need a trusted oracle. Many groups are working on making data available for smart contracts on-chain. They have to make systems that are very expensive to attack. For example, manipulating data feeds gives you the ability to steal from a smart contract that secures \$10 million, your oracle should cost at least \$10 million to break.⁵ That’s assuming a purely economically rational hacker. In reality, governments and competitors might attack something for other reasons.

There are other reasons that make chain-to-chain communication hard. Different blockchain’s “languages” can drastically differ. Bitcoin uses a model called *UTxO* (unspent transaction outputs), which is used to keep track of who owns what. For currencies that were a re-invention of Bitcoin, like Ethereum, some chose an *account-based* model. Whereas *UTxO* is a chain of who spent what, going all the way back to the genesis block, account models are more like banks updating your checking balance with a series of debits and credits. This is just to say that blockchains can differ drastically in their core transaction features and methods that make them ledgers.⁶

The code that runs and validates chains could be written in entirely different languages and programming paradigms (like *functional* vs. *object-oriented*). It takes domain expertise in each blockchain to build something that *makes it seem* like the networks are talking to each other. It’s easier to make a bridge from one Ethereum Virtual Machine (EVM) using Solidity to another versus Ethereum to Solana (EVM to *Rust-based* VM). Blockchains can also have different types of finality (how a transaction gets finalized), like Bitcoin’s probabilistic finality vs. Tendermint’s deterministic or absolute finality.⁷

But the internet’s applications could all be written in different languages, why can they communicate freely? The answer is that they’re all on the same protocols (TCP, HTTP, SSL, FTP). Their data can pass back and forth, be intercepted, etc. because essentially they’re on an open network. Interoperability of web apps was also drastically improved by them sharing APIs (application programming interfaces) in a RESTful model using JSON. Each blockchain is its own protocol, a closed network with its own messaging needs, but people are working to mesh them together so we can have a cross-chain future. Overtime, we’ll see blockchain messaging standards emerge in the way they did with web apps.

In cross-chain communication, you often get someone trying to mess up the messages or insert their own. The majority of hacks draining the most money from protocols have been

⁵ <https://cointelegraph.com/magazine/2021/12/30/can-blockchain-solve-its-oracle-problem>

⁶ <https://medium.com/coinmonks/understanding-cardano-extended-utxo-950ae19829cf>

⁷ <https://medium.com/mechanism-labs/finality-in-blockchain-consensus-d1f83c120a9a>

bridge exploits.⁸ These are often the result of a hacker finding a bug in the bridge code, or a flaw in the design, or some kind of economic exploit, that allows them to drain the tokens that were supposed to be locked.⁹

Back to the translator analogy, you need trust. You need a third-party, trusted translator. If the conversation you are having is about how much money to send each other, you better trust that translator a lot. He could easily change the information you're passing from one language to another in order to steal from you. The financial nature of token transfers makes it a constant target.

Adding trust defeats the whole initial idea of blockchain, which was intended to be a trustless peer-to-peer network. You can decentralize a bridge to decrease the trust of the "translator", with the goal of making it *trust-minimized*, but you can't yet make it trustless. And there's still essentially a middleman.

This is an extremely important point: A trustless system, as an idea, was conceived because people and institutions inherently cannot trust each other for everything. That's why society puts so much emphasis on financial laws, regulations, law enforcement, and government oversight. And as a result, these sorts of regulations have the potential to centralize powers, which can then become maliciously used by those in power for their own benefit. Trustless systems, whether in transactions and storage of value like Bitcoin, or in financial primitives like Uniswap, allow us to take trust out of the equation, mostly. That is mostly trustless, because you still have to trust that the code of Bitcoin, Uniswap, etc. doesn't contain bugs.

It has been said that "Cross-chain communication is impossible without a trusted third party."

¹⁰ They also said that people can't go to Mars, but we are going to try. This may be mathematically accurate, but statements containing the word "impossible" don't always stand the test of time. In fact, stemming from recent research into ZK-STARKs (Zero-Knowledge Scalable Transparent ARguments of Knowledge) cryptography, some groups claim that they have trustless cross-chain interoperability.^{11, 12}

For now, let's say we do believe that cross chain communication is impossible and two independent blockchains will never trustlessly interact. That's unfortunate because now we essentially need to create a strong "legal" framework to make the parties behave. A potential solution could involve decentralized nodes that validate a bridge, whose stake in a token gets

⁸ <https://rekt.news/leaderboard/>

⁹ <https://aktarytech.com/exploits-hacks-and-theft-take-their-toll-on-crypto-adoption/>

¹⁰ Zamyatin, Alexei, et al. "Sok: Communication across distributed ledgers." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2021. <https://eprint.iacr.org/2019/1128.pdf>

¹¹ <https://toposware.com/>

¹² <https://arxiv.org/pdf/2206.03481.pdf>

slashed for unwanted behavior. Essentially a “blockchain-based filter” in between two blockchains. This concept of fines on smart contracts is a way to bring psychology and game theory into the actions that programmers take for example.

Imagine again the English to Chinese translator. If you decentralized the translation, as in you had many different translators taking your message in English and passing it on in Chinese, and 2/3rds of them had to say the same thing, then you have made it more trust-minimized. Most of them would have to work together in collusion to fudge your message. You can further prevent collusion by “churning” them, or randomizing their identities so they don’t even know who is who. An additional security step would be to fine (*slash*) individual translators for trying to pass false messages.

But for the variety of cross-chain solutions working now, there’s a graveyard of those that have failed. Surely that graveyard makes the running ones nervous, but that could lead to better understanding of the problem since the stakes are so high. The dead in this graveyard are bridges and protocols that were robbed by highway bandits, black hat hackers, or state-sponsored groups. Billions of dollars have been drained (in 2022 alone), and it is a major focus of government regulation of this industry. The biggest bank robberies and art heists never even saw these numbers.

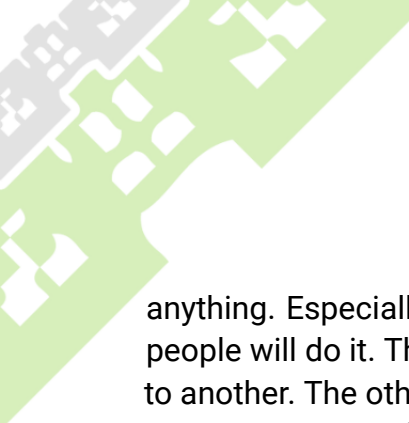
Bridge hacks are such a serious issue that they directly lead to the first US sanctions on a smart contract. The United States Department of the Treasury, under the Office of Foreign Assets Control (OFAC), sanctioned the smart contract addresses that referenced the Tornado Cash protocol.¹³ In March of 2022, the FBI concluded that the Ronin Bridge hack (\$624,000,000 drained) was carried out by the Lazarus Group, a North Korean collective. This was on top of several of their other hacks, which used Tornado Cash as a *mixer* service to launder the stolen funds and anonymize their destination.¹⁴ By August of 2022, OFAC put sanctions on the Tornado Cash addresses, making it illegal for US citizens to interact with them. A first of its kind sanction, which shook up the crypto industry because of its pure technology / code nature, as opposed to being an entity or individual.

This is all to say that cross-chain communication is a technology with potentially huge consequences if done insecurely. Bridge builders should be extremely familiar with the tradeoffs and security concerns in their design. Until a solution emerges, bridges will need extensive and ongoing audits by smart contract auditors and bug bounty programs to catch threats before they happen.

Given all of the risks associated with cross-chain, why do it? For one, because people will try

¹³ <https://home.treasury.gov/news/press-releases/jy0916>

¹⁴ <https://www.trmlabs.com/post/u-s-treasury-sanctions-widely-used-crypto-mixer-tornado-cash>



anything. Especially with crypto's high risk-tolerance, you can guarantee that if it can be built, people will do it. There is demand to go cross-chain because it moves value from one system to another. The other system might have lower gas fees, faster transactions, new dApps, DeFi, or games. From a financial perspective, there might be arbitrage opportunities going from one token representation with high liquidity to another of low liquidity. There could be centralized exchange off-ramps present on one chain and not the other. Bridging is a business; the platform charges a toll for users to go across.

In this paper, we're going to explore the litany of ways blockchains communicate, with a focus on communication with Cardano and its sidechains.

DRAFT



Cross-Chain Architecture Primer

There is no formal definition of cross chain architecture. In general, the aim is to make a channel in the middle of two or more blockchains that is secure.¹⁵ On the *trusted* end of the spectrum, wBTC (wrapped Bitcoin) uses multiple institutions and KYC (Know Your Customer) and AML (Anti-Money Laundering) legal practices to ensure security. You have to trust the institutions and their internal security. Then there are a variety of *trust-minimized* solutions, like RenVM which aims for permissionless custody (no identity / KYC needed).^{16,17}

Bridges have diverse architectures, but some simple classifications are starting to emerge. A *single-organization* bridge is where a single party has custody of the funds locked in the bridge contract. A *multi-organization* bridge has a fixed set of independent parties (K of N) has custody of locked funds. Then there's a *crypto-economic* model bridge where a dynamic set of parties, determined by their weight in assets, have custody of the funds. In crypto-economic bridges, community members can pick up and run nodes, adding security to the bridge and receiving fees. When building a bridge, the decisions you make will have different tradeoffs around security, capital efficiency, decentralization, network congestion, cost of overhead, settlement time, dApp integrations, etc.

The biggest looming question is whether bridges can ever really be secure enough to trust large sums on. Vitalik Buterin, founder of Ethereum, has argued no, because their locked funds create huge incentives for 51% attacks.¹⁸ That is when more than half of the validating power is taken over by a single organization. Thus even if the bridge code is secure, or as he says, "perfect ZK-SNARK-based bridge that fully validates consensus," it is still vulnerable to 51% attacks. Some very experienced bridge building groups have argued that Vitalik's argument simply states the need for overcollateralized cross-chain bridges.¹⁹

A perfect bridge still comes with limitations. It's important to note that bridging will allow liquidity to flow across chains, but that liquidity becomes broken. The more bridges are made, the more fracturing of total crypto liquidity there will be. Part of Ethereum's competitive

¹⁵ https://layerzero.network/pdf/LayerZero_Whitepaper_Release.pdf

¹⁶ <https://medium.com/renproject/introducing-ren-2-0-43025b3d5d6>

¹⁷ <https://newsletter.thedefiant.io/p/it-was-almost-impossible-to-keep-26b>

¹⁸

https://old.reddit.com/r/ethereum/comments/rwojtk/ama_we_are_the_efs_research_team_pt_7_07_january/hrngyk8/

¹⁹

<https://www.altcoinbuzz.io/reviews/crypto-education/vitalik-forgot-one-thing-this-is-why-crosschain-bridges-can-be-safe/>

advantage is that

it is a single network that holds so much DeFi TVL (total value locked), and dApps remain atomically composable. *Atomicity* is the ability to compose many different transactions in a single block, like a flash loan. As soon as you add side chains and bridges to other chains,

atomicity between them is broken. A core philosophy of DeFi is interoperability in a single block; these multi-step transactions lead to the metaphor “Money Legos.”²⁰

Cardano Cross-Chain Initiatives and What Use Cases they Fulfill

Cardano’s governance and funding initiative, Catalyst, has devoted significant resources to cross-chain solutions. In fund 9, out of \$12.8M total, there is \$900,000 set aside for work on cross-chain.²¹ The challenge is to enhance existing collaborations with other chains, and to create new connections. There are several existing solutions which we will talk about here.

First, a little about execution in Cardano. Given the heterogeneity of blockchains (sometimes called Layer 1s) need to develop their own unique smart contract language that runs on their engine. Ethereum’s EVM reads and executes Solidity (a language similar to JavaScript). Many other blockchains, like Avalanche, use Solidity because they also run the EVM. The Rust programming language has become popular in blockchains like Solana, NEAR and Cosmos because of its secure compiler. Reflecting its focus on research and mathematics, Cardano uses Plutus, a functional programming language.

“Plutus Core is the scripting language used by Cardano to implement the EUTxO model. It is a simple, functional language similar to Haskell, and a large subset of Haskell can be used to write Plutus Core scripts.”²²

A notable feature of Cardano making it different from others is it had a unique path to a smart contract system.²³ Cardano research enabled the Extended Unspent Transaction Output (EUTxO) accounting model. It is extended, as Bitcoin UTXOs don’t allow smart contracts as complex as Ethereum’s account-based model. Cardano researchers accomplished this EUTxO model by using state machines called Constraint Emitting Machines (CEMs). This allows them to maintain the graph-based nature of UTXOs that provides security and avoids some issues

²⁰ <https://boxmining.com/defi-money-legos/>

²¹ <https://cardano.ideascale.com/c/campaigns/26598/stage/stage-assessqa429167/ideas/unspecified>

²² <https://docs.cardano.org/plutus/learn-about-plutus>

²³ <https://www.essentialcardano.io/article/overview-of-the-research-enabling-smart-contract-support-on-cardano>

like *re-entrancy* that account-based methods have.²⁴

One benefit of EUTXO as opposed to the EVM method is that it has deterministic fees; you can accurately predict the fees ahead of the smart contract transaction. In the account model, your transaction could fail and you still pay fees. Here's a good explanation of UTxO from Cardano Docs:

"The users' wallets manage these UTXOs and initiate transactions involving the UTXOs owned by the user. Every blockchain node maintains a record of the subset of all UTXOs at all times. This is called the UTXO set. In technical terms, this is the chainstate, which is stored in the data directory of every node. When a new block is added to the chain, the chainstate is updated accordingly. This new block contains the list of latest transactions (including, of course, a record of spent UTXOs, and new ones created since the chainstate was last updated). Every node maintains an exact copy of the chainstate."²⁵

Since cross-chain solutions are made of smart contracts on each side, builders will have to be knowledgeable about Plutus and something else (Rust, Solidity, etc.) for an integration. This is one reason why bridge code can be complex. Imagine the planning needed for building an IRL bridge where one side of the river is granite and the other side is sandstone.

The choices Cardano has made largely reflect their desire for the highest security through *formal proof*, using a functional programming language to prove that the blockchain and smart contracts will behave as they are specified. Their other stated goal is massive decentralization, which they've achieved with so many stake pool operators validating the blockchain. However, areas like interoperability and scalability still need work, hence the focus on cross-chain and sidechain integrations.

Cardano Sidechains and EVM

Sidechains are a scaling and interoperability solution for when you want to add new features or get around the limitations of a main chain.²⁶ They require a bridge, like Ethereum to Polygon. Cardano has several in the works.

Many people thought they could do better than the EVM, and rightfully so. Just because it was the first smart contract platform doesn't make it the best. There are many proposed solutions that enable better scalability, easier code-readability and onboarding of new devs, and existing languages like JavaScript, Python, Rust and Haskell.

²⁴ <https://iohk.io/en/research/library/papers/the-extended-utxo-model/>

²⁵ <https://docs.cardano.org/plutus/eutxo-explainer>

²⁶ <https://www.web3.university/article/sidechains-vs-layer2s>

But time-to-market is just too powerful of a force and Solidity / EVM keeps winning. The tooling (like testing suites, deployment packages, existing contract libraries, etc.) and familiarity of the EVM still make it a go-to for many people learning to build decentralized applications. This means that any new chains that want developers and dApps will need to plug in an EVM. Cardano has several ways to do this. There is already an EVM sidechain (Milkomeda), and IOG (Input Output Global) itself is working on its own EVM sidechain, codenamed Mamba.²⁷²⁸

Milkomeda

As stated by their docs, Milkomeda's focus is to enhance dApp development, developer productivity and blockchain adoption by making seamless sidechain and cross-chain solutions. They recognize that there will likely be a handful of blockchains that will remain dominant over the course of this industry, and they believe that Cardano is one of them. They have some interesting things to say about account vs. UTXO models:

"The Account-based model is used by Ethereum and the majority of current smart contract platforms, primarily due to the fact that it is simpler to comprehend when designing and launching the smart contract layer of the blockchain as it exposes global state to every contract at any time. As any programmer knows, global state is dangerous and severely limits the ability of programs to parallelize/scale, and this similarly maps onto the blockchain context as well.

This global-access paradigm of Account-based is going to be severely limited with the introduction of sharding (coming up for Ethereum) where each shard will be distinct and separate from one another, meaning much of the original benefits will be swept away in pursuit of building a system that actually scales. This means that the way that protocols are designed will begin moving towards how the UTXO-model works, yet carrying along all of the previous baggage from choosing Account-based in the first place."²⁹

Milkomeda's first EVM sidechain is called C1. When ADA is brought over through the bridge, it creates milkADA, which can then be used in the EVM dApps.

Milkomeda's key innovation is what they call *wrapped smart contracts*. These allow Cardano

²⁷ <https://iohk.io/en/blog/posts/2022/07/06/introducing-the-cardano-evm-sidechain/>

²⁸ <https://iohk.io/en/blog/posts/2022/01/14/how-we-re-scaling-cardano-in-2022/>

²⁹ <https://dcsparc.gitbook.io/milkomeda/why-cardano-first>

users to perform an action on the main chain and have it executed on the sidechain and returned, without them even knowing. A single message can take your data and assets from the main chain, do something on C1 (perhaps a swap on an EVM dApp), and bring the data and assets back to your main wallet. This has been a goal of many cross-chain solutions, to abstract away the multiple steps involved.

“Thanks to our new innovation called wrapped smart contracts, it will be possible for users on the Cardano mainnet to call and use contracts on the sidechain without having to leave mainnet at all. Users will submit a single Cardano transaction with the data and assets required to interact with the sidechain dApp and the sidechain bridge layer takes care of the rest. The assets/data are transferred over to the sidechain, the requested action is executed on the target dApp, and the results are deposited back to the user’s wallet in the end.”³⁰

“There are several potential sidechains that can be deployed on top of the Milkmeda protocol using existing VMs today including the EVM (Solidity), WASM, IELE, Facebook’s Move VM, Solana VM, Flow/Cadence, Hyperledger Fabric, Quorum, NEAR VM, among others.”³¹

You will start seeing more EVM dApps running on sidechains and Layer 2s of Cardano. It would be a goal of the sidechains to have brand-name EVM dApps like UniSwap, Curve, AAVE to launch on their chain. The momentum of EVM is too big to ignore.

Aneta BTC

Bitcoin still has most of the liquidity. But there’s interesting reasons to use its value across other chains, that’s why wrapped Bitcoin was created.

“The creation of wBTC by BitGo, Kyber Network, and Ren, formerly known as Republic Protocol was revolutionary in its own right, but wBTC is entirely centralized due to BitGo being the sole custodian for wBTC and this entity, partly owned by Goldman Sachs, has full legal control of all locked Bitcoin wrapped in wBTC.”³²

This custodial aspect worries people because of centralization, censorship and relying on the trust of individuals and institutions. Other wrapped Bitcoin methods attempt to be trust-minimized and non-custodial by using smart contracts and nodes that do the safekeeping and transfer of assets.

³⁰ <https://dcspark.gitbook.io/milkmeda/our-solution-1/the-m-1-sidechain>

³¹ <https://dcspark.gitbook.io/milkmeda/our-solution-1/milkmeda-protocol>

³² <https://medium.com/@anetaBTC/anetabtc-litepaper-v1-0-171f29b3276a>

AnetaBTC is an option for wrapped Bitcoin on Cardano and Ergo blockchains. Like most wBTC implementations, users send BTC to a Vault that assures its safekeeping so they can mint anetaBTC on the destination chain. The main security feature of this bridge is the Vault and the BTC Relay, which is an overcollateralized Bitcoin SPV client (Simplified Payment Verification). If the Vault tries to steal BTC, it is recognized and the vault loses its collateral. The Vault also watches the BTC blockchain to make sure it is up to date with the latest block headers. The Relay automatically detects and recovers from Bitcoin network forks.

In addition to the BTC they want to bridge, users also have to provide a security deposit, which is what makes the Vaults overcollateralized.

One interesting feature of bridges is that there are often databases involved (individual blockchain protocols hold their own data, and don't use relational DBs). When users request to create or redeem their anetaBTC, a transaction is logged in a database and that request is relayed to the bridge. The bridge code also writes to the database. The actual blockchain events are used to confirm items in a database. Use of databases in bridge nodes is typical, and they are often made so they can be resynced directly from the on-ledger immutable data.

"The user will request to issue or redeem anetaBTC and the anetaBTC database will relay which function the user is trying to perform and send that request to the anetaBTC bridge. From there, the anetaBTC bridge will send that information to anetaBTC-stats where the events will be written to the official anetaBTC events database and read the information back to anetaBTC-stats."³³

Akamon Bridge by MELD Labs

Akamon is a robust bridge between Cardano and Polygon (MATIC). It recently announced that it will be bridging a very crucial asset into the Cardano ecosystem, a stablecoin.³⁴ Cardano currently needs more stablecoin options, and through Akamon and other bridges, USDT may soon be available. Stablecoins (tokens with a price pegged to a fiat currency) are necessary for a thriving DeFi ecosystem, as traders need somewhere to park funds to avoid volatility.

Akamon stakes the ADA tokens that you lock in, providing revenue that is used to lower your bridge fees. Since there are idle tokens in the bridge, certainly using them to participate in staking or DeFi is an attractive option for bridge builders. However, if the tokens are lost while

³³ <https://docs.anetabtc.io/docs/protocol-overview/Wrapping-Assets>

³⁴ <https://medium.com/meld-labs/akamon-a-solution-for-stablecoins-on-cardano-f4e7470e98af>

in custody, the value of the bridged asset goes to zero.

Another way Akamon lowers fees is when users pay their bridge fee (the price they charge for using the bridge, on top of gas for the network) in MELD, or when the user is an Akamon NFT holder.

The bridge fee is normally paid in the native token of the source network. So you pay an ADA fee to go to Polygon and a MATIC fee to go back to Cardano. The bridge fee is quoted by a validator node and accepted by a user. The fees are sent to a contract that distributes the funds among the validator nodes.

Like many bridges, Akamon has a PostgreSQL database component. There are two blockchain indexers (one for Cardano side and one for Polygon side) that watch and synchronize data to the DB. The validator node then reads new requests to handle. Since the database is built from on-chain immutable data, it has the ability to re-sync at any time. Whether starting up a new node, or due to a failure / deletion of the data.

On the Cardano side, Akamon built its own indexer to watch for new deposits in the bridge contract. They did this with a Node-to-Client connection in Ouroboros' ChainSync. On the Polygon side, they use The Graph as the industry standard indexer.

The Akamon Node reads the database and decides what actions should be performed on-chain, like signing, fulfilling, or disapproving requests.

Wanchain Bridge

Building bridges has become a specialty of blockchain engineering groups like Wanchain. They had some of the earliest implementations, and devoted a lot of time to research and communication of bridging paradigms.³⁵ They have their own consensus model for interoperability called Galaxy.³⁶

"Wanchain bridge nodes are permissionless and use multiparty computation and staking to prevent collusion."³⁷

Their bridge nodes are permissionless so anyone can set them up. They offer several different kinds of cross-chain bridges: direct bridges, layer 2 bridges and NFT bridges.

³⁵ <https://www.explorewanchain.org/#/>

³⁶ https://www.wanchain.org/_files/ugd/9296c5_5205d584ee594e879d4b8b58048b6fac.pdf

³⁷ <https://iohk.io/en/blog/posts/2022/07/08/bridges-and-sidechains-wanchain-making-cardano-interoperable/>

Wanchain is very experienced in bridges, having done them on EVMs, Polkadot and UTxO chains.

“Wanchain’s expertise is in connecting fully heterogeneous blockchains. The current cross chain infrastructure already includes blockchains that use EVM (like Ethereum and Wanchain), WebAssembly (like Polkadot), and even blockchains that have no virtual machines at all (like Bitcoin, XRP Ledger, and Litecoin). When possible, we solve this issue by developing native smart contracts on both the source and target chains. Otherwise, if a network does not support smart contracts, Wanchain bridge nodes jointly manage a dedicated lock account using sMPC. Wanchain’s ever-changing selection of permissionless bridge nodes then communicate with smart contracts (or lock accounts) on each chain, as needed.”³⁸

Like Milkomeda and others, Wanchain will serve as an EVM compatible sidechain to Cardano. The first Wanchain bridge to Cardano will be deployed to mainnet following the Vasil hardfork. The delay until the hard fork is likely due to the improvements Vasil makes both to the Plutus language, the ability of Plutus V2 primitives to better interact with the EUTXO model, and other smart contract optimizations.³⁹

SingularityNET AGIX Converter Bridge

Bridges can be very limited in scope too, such as only being used for a single token of a specific protocol that is migrating away from one chain and onto another.

A group working on decentralized artificial intelligence called SingularityNET first launched their AGIX token on Ethereum as an ERC-20. It’s not surprising that their focus on AI and machine learning research made them a fit for the Cardano ecosystem due to its mathematical backgrounds. SingularityNET built a bridge to convert their AGIX token into a Cardano representation.⁴⁰

Proposed Bridge: Rosen Cardano to Ergo

Ergo is another blockchain built on the UTxO model. They’ve extended it, like Cardano has, to an EUTXO, to allow for smart contracts. Cardano’s founder, Charles Hoskinson, had a lot of

³⁸ <https://iohk.io/en/blog/posts/2022/07/08/bridges-and-sidechains-wanchain-making-cardano-interoperable/>

³⁹ <https://academy.bit2me.com/en/what-is-vasil-the-new-cardano-hard-fork/>

⁴⁰ <https://blog.singularitynet.io/the-agix-erc-20-converter-bridge-is-live-fa90ccba061a>

nice things to say about Ergo, its focus on research, and community.⁴¹

“During the episode, Hoskinson pointed out that he has ‘always loved Ergo’ and considers the blockchain to be ‘the spiritual successor of Bitcoin.’ ... He pointed out how Ergo’s Sigma Protocols and UTXO model “are consistent with an evolution of Bitcoin’s tech,” and that Cardano even looked to Ergo’s eUTXO research because development had been a little further along at the time. Ultimately, Hoskinson suggested that Ergo deserves much more “attention, respect, and liquidity,” and that the industry would be a lot further ahead if more blockchains took a page out of Ergo’s book.”⁴²

Ergo has been developing the Rosen Bridge (named after Einstein-Rosen bridges, a.k.a. space-time wormholes) for a cross-chain solution to Cardano.⁴³ This bridge only utilizes the smart contracts of Ergo, eliminating the need to audit on multiple chains. This is a very interesting direction to explore for the improvement of bridge security.

“This bridge utilizes a two-layer architecture. In the first layer, watchers are monitoring and report the events on the networks. Upon reaching a consensus on a particular event, the second layer is being notified. In the second layer, Guards will verify the event and create/sign the required transaction for ergo or chainX.”⁴⁴

Rosen bridge is in active development as of Sept. 2022.⁴⁵ It already has a wrapped bitcoin solution, and they continue to add more chains.

Proposed bridge: Ardana and Nervos Force Bridge

Nervos is another UTxO chain, and Cardano announced in 2021 that they would be partnering on a bridge.⁴⁶ The Cardano stablecoin platform Ardana also announced that they would be partnering with Nervos through their Force Bridge.⁴⁷ It’s yet to be determined when this bridge will be launched. Nervos also plans to use this bridge to connect EOS, TRON and Polkadot. The more connections that are made, the more liquidity can flow across the entire crypto ecosystem.

⁴¹ <https://ergoplatform.org/en/blog/2022-04-13-ergo-pulse-with-charles-hoskinson/>

⁴² <https://ergoplatform.org/en/blog/2022-04-13-ergo-pulse-with-charles-hoskinson/>

⁴³ <https://github.com/mhssamadani/RosenBridge>

⁴⁴ <https://github.com/rosen-bridge>

⁴⁵ https://twitter.com/mhs_sam/status/1563517338405597186

⁴⁶ <https://iohk.io/en/blog/posts/2021/06/02/nervos-partnership-to-build-the-first-cross-chain-bridge-with-cardano/>

⁴⁷ <https://medium.com/ardana-hub/nervos-network-to-utilize-cross-chain-bridge-93be6604a2c2>

Proposed Bridge: Sifchain Peggy2 Cardano to Cosmos

This has been proposed for Catalyst Fund 9.^{48,49} Sifchain intends to be the premier Omni-Chain Decentralized Exchange (DEX) for the Cosmos Ecosystem. They are already running EVM bridges to Cosmos that have gone through several audits. Sifchain itself is a Cosmos SDK blockchain using the Tendermint consensus algorithm.

Sifchain has had success in connecting EVM chains and their dApps to the Cosmos Hub ecosystem and its other blockchains, called “Zones” and their dApps.

Cardano & Chainlink CCIP

Most of what Chainlink is used for is to provide access to real-world data to smart contracts in the form of Oracles. Cardano has partnerships with Chainlink for price feed Oracles.⁵⁰ Chainlink’s position in the industry makes it a potential solution for many cross-chain endeavors. Here’s an excellent explanation of how Chainlink goes from decentralized oracles to cross-chain frameworks:

“Chainlink 2.0 is a framework that aims at solving the oracle problem [Ora] by introducing the Decentralized Oracle Network (DON). Historically, oracle services introduce trust. However, Chainlink tackles this problem by filtering the off-chain data source through a BFT (Byzantine Fault Tolerance) layer. The committee of Oracles that composes the DON sign their reports with a multi-signature scheme. By doing so, Chainlink is increasing decentralization and minimizing trust in oracle services. Furthermore, Chainlink proposes an interoperability feature with its Cross Chain Interoperability Protocol (CCIP). The global consistency of cross-chain communication in CCIP is reduced to the security of their Anti-Fraud Network which is a dedicated DON actively watching for misbehavior across other DONs.”⁵¹

It was mentioned in the post announcing their partnership that cross-chain with Cardano could be a possibility.

“Chainlink’s recently announced Cross-Chain Interoperability Protocol (CCIP) creates additional opportunities to collaborate with Cardano in building a multi-chain world. He underscored the “tremendous amount of respect between the Chainlink and

⁴⁸ <https://cardano.ideascale.com/c/idea/422010>

⁴⁹ <https://twitter.com/sifchain/status/1545022253506744322>

⁵⁰ <https://iohk.io/en/blog/posts/2021/09/25/cardano-to-integrate-chainlink-oracles-for-real-time-market-data/>

⁵¹ <https://arxiv.org/pdf/2206.03481.pdf>

Cardano ecosystems” as well as the “collaborative nature” of the Cardano community.”⁵²

Cardano ZK-Rollups and Layer 2s

Cardano, given its mathematical prowess, is embracing a new math-based technology called ZK-Rollups (so named for their Zero-Knowledge Proofs). ZK is a cryptography advancement that first gained popularity in blockchain by allowing Zcash to have a privacy guarantee that shields transaction data.

“Zero-knowledge proofs allow one party (the prover) to prove to another (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself.”⁵³

Rollups gain 100% of their security from the main chain, as opposed to side chains that need to rely on their own network’s security. Their transactions are technically happening off-chain from the main chain, but their validity is guaranteed on the main chain with proofs. It’s an area of cryptography that has recently made strides into production ready systems like Toposware.⁵⁴ Rollups provide a secure way to validate off-chain transactions, but they don’t change the fundamentals of moving assets cross-chain—you still need a bridge.

In rollups, a bridge has a much bigger job to do, but the benefit of this extra work is that it’s possible to make the bridge more cryptographically secure.

“A set of parties (sequencers) are responsible for providing evidence about the state of the other network to the bridge contract. It is up to the bridge contract to validate the evidence’s correctness and to independently verify the other network is not compromised.”⁵⁵

Rollups (like Arbitrum, Optimism, dYdX, Loopring, zkSync) have become so essential to Ethereum scaling that the Ethereum Foundation has prioritized them in its roadmap. Ethereum plans to lower fees for rollups and make them more officially supported.⁵⁶ Three specific types of rollups are taking the stage so far: Optimistic rollups, Zero-Knowledge (ZK) rollups, and

⁵² <https://chainlinktoday.com/cardano-announces-strategic-collaboration-to-integrate-chainlinks-oracles/>

⁵³ <https://z.cash/technology/zksnarks/>

⁵⁴ <https://www.alchemy.com/overviews/zk-rollup-projects>

⁵⁵ <https://blog.infura.io/post/offchain-protocols-sidechains-and-rollups>

⁵⁶ <https://medium.com/neworderdao/the-l2-landscape-d3bcb8b0f422>

Validiums.⁵⁷

Orbis is built on Cardano with ZK-Rollups to create Layer 2 and Layer 3 scaling solutions. You move your ADA to Orbis (which is essentially “Cardano ON Cardano”, it runs Plutus) but with much higher transaction speed and lower fees.⁵⁸ This is achieved by having many transactions bundled together on Orbis, and then a formal proof is submitted to Cardano on what is called a verifier contract. For example, do 100 transactions on Orbis, bundle them together, and Cardano only has to process, store and verify a single proof. Hence it rolls up to the main chain. This can be thought of as a form of blockchain compression.

Rollups can also be built on top of Orbis, which would be Layer 3s. Theoretically their security is still on the main chain. This is another unique way to scale. It could be used for games, private institutional blockchains, EVMs, and other siloed systems that want high speed and security.

Like many bridges and blockchains themselves do, Orbis intends to expand from more centralized to decentralized as time goes on. To do this, they will be allowing anyone in the community to operate their off-chain prover node. Currently they operate it, next it will be operated by a permissioned group, then eventually anyone could operate a prover node.⁵⁹

Wallets for Interacting with Cardano Bridges

A wallet’s interface and capabilities are important for doing anything in crypto. Whether this wallet is mobile, browser-based or just in a command-line interface, it’s important that the user knows what is happening to their assets. Complex transactions, like bridging from one blockchain to another, are extra important for communicating to the user what is happening.

Is it possible that a wallet could help users go cross-chain? A multi-chain wallet that did this would be a great benefit to user experience.

We’ll highlight a few wallets that interact with Cardano dApps: Yoroi, Nami and Daedalus.

“Yoroi is a mobile and hardware-enabled wallet that makes it easy to store ADA, developed by the commercial arm of Cardano. Users can set up an ADA wallet in

⁵⁷

<https://www.defipulse.com/blog/rollups-validiums-and-volitions-learn-about-the-hottest-ethereum-scaling-solutions>

⁵⁸ <https://cardanofeed.com/cardano-s-scaling-zk-rollups-solution-will-support-defi-innovation-52469.html>

⁵⁹ <https://youtu.be/GOR8dVxO7Sw?t=1295>

seconds, and it is compatible with hardware wallets like Ledger and Trezor.”⁶⁰

“Nami is a browser based wallet extension to interact with the Cardano blockchain and is non-custodial. The main difference to current wallets is that Nami can be injected into the browser context and be connected to any website in order to interact with dApps.”⁶¹

“Daedalus is the official Cardano wallet developed by IOHK, the foundation behind Cardano. It is the most secure but also the hardest to install and requires 10GB data on your hard drive to download the entire Cardano blockchain and sync it.”⁶²

Oracle: Charli3

A prominent group building a decentralized oracle on Cardano is Charli3.⁶³ Through winning Catalyst funds, Charli3 intends to help bootstrap the DeFi ecosystem on Cardano by providing free price feed data. Unless providing something like a random number, oracles will need data providers themselves. Charli3 has recently partnered with a leading financial data provider, dxFeed to bring off-chain price information to Cardano smart contracts.⁶⁴

The Flaws of What Exists Today

Bridge Code and Complexity

There are many tradeoffs in building a bridge, but the biggest glaring issue right now is security. Not just in the decentralization aspect or Sybil-resistance (defense against many fake identities), but in the smart contract code itself. Clearly there have been oversights when writing bridge contracts that experienced auditors may not even catch.

Bridges are complex machines. Adding the complexity of programming in a blockchain environment, there's bound to be flaws and bugs. As the industry evolves, and green coders become more experienced, the quality and testing of code is likely to increase. All code has bugs, but when there are funds to steal, seemingly minor bugs can become fatal for a bridge.

There is no standard way yet to build a bridge. In fact, many groups use completely different

⁶⁰ <https://phemex.com/academy/daedalus-vs-yoroi-vs-adalite-ada-wallets>

⁶¹ <https://namiwallet.io/>

⁶² <https://phemex.com/academy/daedalus-vs-yoroi-vs-adalite-ada-wallets>

⁶³ <https://charli3.io/#about>

⁶⁴ <https://oraclecharli3.medium.com/charli3-partnered-data-provider-dxfeed-d51f7d22444b>

language to describe similar things. Some just say “validators”, while others use terms like clients, guardians, watchdogs, etc. In the \$326M Solana Wormhole bridge hack, there was a key piece of authorization overlooked. The hacker was able to submit their own address to the contract that mints wormhole ETH on the Solana side, bypassing the guardians that were set up to verify bridge deposits on the ETH side.⁶⁵ The guardians were checking IDs at the front door, but the back door was left wide open. This was an oversight, but also attests to the difficulty of catching every bug with the current way bridges are built.

Bridges that are too Centralized

The Ronin bridge was hacked after employees who run validators on the bridge were ‘spear-phished.’⁶⁶ One employee may have downloaded a malicious PDF after a fake job offer was posted on LinkedIn.⁶⁷ This PDF had code on it that was executed on the employee’s computer, gaining access to the bridge’s private keys. Only 5/9 keys were needed to drain \$624 million. Clearly this was far too centralized. Having a network of validators does no good if the keys are all accessible from the same place. The Harmony Horizon bridge hack only took 2 of the 5 keys to be stolen.⁶⁸ Which begs the question—what number of nodes would be statistically “decentralized” in terms of lowering the risk associated with the effort to compromise private keys?

Bridge Private Keys Management

Private keys are still the lynchpin of many crypto projects. Like King Arthur’s Sword Excalibur, whoever holds it also holds the rightful sovereignty. Whatever you do, store them under your mattress, or inject them under your skin, there’s always the chance that they get stolen.

Worst case scenario, there could literally be an individual with a single private key holding the bridge’s assets. Slightly better than this is a federation of individuals (or companies) holding keys.⁶⁹ Better than that would be many decentralized nodes that validate the bridge’s transactions, with disincentives for collusion and false reporting of data.

Bridges often make use of the cryptography concepts like Multiparty Computation (MPC)

⁶⁵

<https://www.radixdlt.com/post/rekt-retweet-10-badges-why-the-326m-wormhole-hack-on-solana-could-never-happen-on-radix>

⁶⁶ <https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing>

⁶⁷ <https://www.nftgators.com/a-fake-linkedin-job-post-reportedly-led-to-axies-625m-ronin-bridge-hack/>

⁶⁸ <https://halborn.com/explained-the-harmony-horizon-bridge-hack/>

⁶⁹ <https://medium.com/wanchain-foundation/how-safe-are-todays-wrapped-btc-bridges-b0f35a7b15e2>

and Threshold Signature Schemes (TSS).

“Wanchain introduced its implementation of MPC / TSS in its first cross-chain bridge between BTC and Wanchain all the way back in 2017. Our implementation of it drew heavily from the 1996 Gennaro paper, while also introducing an innovative algorithm which reduces the number of interactions in the MPC calculation process.

An important concept in the application of MPC technology to cross-chain bridges is the relationship between the individual private key of each participating MPC node and the group private key of the whole node set.

The group private key is the key which is used to control the MPC-managed locked account where the BTC is held on the native Bitcoin blockchain. Any holder of this key has full control over all assets in that account.

However, no individual is ever meant to hold this key. Rather, a group of nodes work together to generate the group private key through the MPC mechanism described by Gennaro in 1996. This group private key is generated when each participating MPC node contributes their own individual private key. TSS is applied through this process to ensure that even if a few nodes are offline or deliberately choose not to participate, the process will complete as long as more than some threshold number of nodes participate. Therefore, the entire mechanism is highly fault-tolerant, and even if individual MPC nodes are malicious, it will not affect the protocol operation.”⁷⁰

This cryptographic strategy allows robustness and creates the basis for a multi-signature. However, it does not prevent collusion if a threshold of signatories decide to become malicious. One way to prevent collusion is through node “regrouping” or “churning.” This makes it harder for nodes to identify who each other are and decide to collude.

In their paper from 2020, a Wanchain engineer argues that renBTC did not (at the time, from the limited source code available) properly implement MPC, and thus their bridge could be a “honey pot” for some smart hackers or collusion of nodes.⁷¹ However, Ren has continued to be a winner in Bitcoin wrapping. Ren functions by using a network of decentralized nodes known as Darknodes. They use novel concepts in cryptography such as Shamir’s Secret Sharing and Secure Multiparty Computation.⁷²

⁷⁰ <https://medium.com/wanchain-foundation/how-safe-are-todays-wrapped-btc-bridges-b0f35a7b15e2>

⁷¹ <https://kriptomat.io/cryptocurrencies/ren/what-is-ren/>

⁷² <https://medium.com/@anetaBTC/anetabtc-litepaper-v1-0-171f29b3276a>

Trusted Setup “Ceremony” to go Trustless

Actually doing Multiparty Computation has been described as a sort of “Secret Ceremony.” Individual signatories get together around the same time and execute the process. People go to great lengths of privacy and decentralization of these ceremonies to ensure they are not infiltrated. The user of one of these systems has to place trust in the security of this ceremony.

“Systems that use zk-SNARKs require a trusted setup, an elaborate process that relies on multi-party computation to generate a crucial pair of cryptographic keys. Trusted setups are vulnerable to manipulation, but an attacker would have to compromise every participant in order to undermine the system's privacy guarantees. So, in theory, the greater number of participants, the more secure the process.

The most famous trusted setup ceremonies in the crypto space thus far have been Zcash's. In October 2016, Zcash generated its first-ever set of public parameters via a ceremony that involved six participants. Then, in 2018 it conducted another ceremony as part of its Sapling upgrade. That one involved 87 participants. The Tornado Cash team says its setup had a total of 1,114 contributions.”⁷³

Areas Needing More Research and Experimentation

Advanced Areas of Cryptography

Academic, industry, and government research into cryptography is what kicked off the whole field, enabling cryptocurrencies in the first place. There are a variety of cryptography choices to make when designing a system, which is another reason that blockchains have trouble with interoperability. For example, Bitcoin and Ethereum chose the Secp256k1 elliptic curve for signatures, while Cardano chose the curve25519 standard.⁷⁴ ⁷⁵ However, Cardano intends to support this other type of cryptography after the Vasil hardfork.⁷⁶

There are probably more areas of existing cryptography research that are waiting to be discovered as a solution for blockchain. Zero knowledge (ZK) technologies were developed in

⁷³ <https://www.theblock.co/linked/65115/ethereum-tornado-cash-trusted-setup-ceremony>

⁷⁴ <http://ethanfast.com/top-crypto.html>

⁷⁵ <https://iohk.io/en/blog/posts/2022/07/08/bridges-and-sidechains-wanchain-making-cardano-interoperable/>

⁷⁶ <https://iohk.io/en/blog/posts/2022/07/08/bridges-and-sidechains-wanchain-making-cardano-interoperable/>

the 1980s and are just gaining ground in blockchain technology 30-40 years later.⁷⁷

ZK technology and the privacy and verification it provides is already a game-changer for many crypto projects. Who knows what is happening in universities, governments and private research now that will lead to new cryptography breakthroughs in the future. Advancement in this area is essential, for one, because quantum cryptography-breaking research is also underway. Some day a quantum computer may be fast enough to guess private keys and then the whole system falls apart.

Game Theory

How people react to incentives, disincentives and opponents in games (which money could be considered as one) is a leading area of research for blockchain systems.⁷⁸

“Cryptography is used to prove past events — such as the authenticity of messages, while economic incentives are used to encourage desired future behavior. With backward looking security mechanisms, and forward looking incentivization, cryptoeconomics allows us to build robust decentralized protocols, opening up new ways to organize and govern ourselves.”⁷⁹

UMA Protocol’s optimistic oracle is an interesting take on game theory in distributed data systems.

“UMA’s dispute resolution system known as the Data Verification Mechanism (DVM). Anyone can earn a reward by proposing answers to a request. Proposed data will not be sent to the DVM unless it is disputed. Disputes are rare in practice. This is consistent with game theoretical principles, since users would lose money for making incorrect proposals that are disputed. The only winning move is to propose data that is correct.”⁸⁰

Bridge Auditors

A Google search for “Smart Contract Auditors” returns many advertisements from companies offering that service. A smart contract audit checks for known vulnerabilities in your code before you deploy it. The problem is, they don’t know the unknown ones. Many smart contract

⁷⁷ <https://cointelegraph.com/explained/zk-starks-vs-zk-snarks-explained>

⁷⁸ <https://www.calebdbrown.com/blog/the-game-theory-of-cryptocurrency>

⁷⁹ <https://matthewfinestone.medium.com/game-theory-and-blockchain-db46e67933d7>

⁸⁰ <https://umaproject.org/products/optimistic-oracle>

languages are Turing Complete, including Plutus and Solidity.^{81, 82} Decades of industry experience in computation have shown that any Turing-complete system will have some bugs that will be revealed only after some time.

Making a smart contract system into a Finite State Machine, where there is only a limited number of inputs and outputs guaranteed, can improve security.⁸³ The model of a finite state machine would be a good choice for implementing code for something as say, a nuclear reactor, where certain bad states you want to avoid would be impossible to do. There may be a method of making bridges using finite state machines, ensuring the billions of dollars of locked funds have fewer unknown attack vectors.

Bug Bounty Programs

What is a bug worth? A bug in a bridge might be exploited for hundreds of millions of dollars in locked funds. But law enforcement has caught blockchain hackers before, and you can bet that they are getting better at it. With sanctions and surveillance, it will continue to get harder for hackers to get away with theft of digital assets. They can use their skills, get paid, and not have to watch their back. There are platforms like ImmuneFi that have built a system for anonymous hackers to get paid legally for finding bugs in participating protocols.⁸⁴ Any dApp that is not participating in bug bounties is unnecessarily exposed.

Cardano and Thorchain

Thorchain has developed a method, albeit a high complexity one, to create a cross-chain swapping solution. It allows for swapping of native assets (not wrapped or synthetic) through middle chains. Thorchain has already integrated with other UTxO chains like Bitcoin, Litecoin and Dogecoin.⁸⁵ With enough Plutus expertise, this seems like a relevant possibility to bring liquidity of people's native holdings into ADA. Thorchain has a Discord channel devoted to Cardano integration, and some members are trying to plan that build out.

"THORChain has developed a cross-chain value exchange solution using rotating Threshold Signature Scheme (TSS) Vaults which secure wallets across multiple blockchains and allow swaps through continuous liquidity pools. THORChain has integrated UTxO chains like Bitcoin, Litecoin, and Dogecoin as well EVM chains such as Ethereum and Avalanche C-Chain. THORChain operates as a secondary consensus layer

⁸¹ <https://medium.com/@dr.orlovsky/turing-g%C3%B6del-and-chaos-in-smart-contracts-4221c08a7e0a>

⁸² <https://docs.cardano.org/plutus/learn-about-plutus>

⁸³ <https://www.radixdlt.com/post/is-scrypto-turing-complete>

⁸⁴ <https://immunefi.com/about/>

⁸⁵ <https://docs.thorchain.org/chain-clients/utxo-chains>

to each Layer 1 blockchain, eliminating the need for trusted solutions from an asset bridge.”⁸⁶

Options for an Experimental Prototype

Wolfram as a Blockchain Oracle

Since the oracle problem is about trust, it's helpful to have a group with an already well-trusted set of APIs and security practices delivering the off-chain data. Wolfram Alpha is already considered a source of truth for a variety of applications. It became integral to Siri in the iPhone 4s in 2011. The next step, with Wolfram Blockchain Labs, is to become a cryptographic source of truth, an oracle. Wolfram's immense amount of computational productivity and data services could be used to make smart contracts smarter.

A leading example of blockchain oracles being used to great potential is parametric insurance payouts backed by trusted rainfall data. Farmers can purchase policies to insure against inadequate rainfall, and receive instantaneous payouts because of smart contract automatic claims.^{87, 88} Wolfram has long been an aggregator of weather data, and this is an area that we can pursue.

Oracles in Parametric Insurance and Betting

The way peer-to-peer transactions cut out a lot of middlemen, smart contracts do as well. Insurance is a transfer of risk to someone who has pre-calculated the aggregated cost of that risk. An insurer is often a highly complicated organizational structure due to the need for underwriters, claims handlers, attorneys, and regulators. If some of this human element can be completed by algorithms, on a trusted blockchain, there could be great benefit for the industry and cheaper policies. Parametric insurance attempts to address this.

“Parametric policies do not require the insured to prove that a loss occurred or how much it is worth. Instead, they pay out according to an algorithm that relies on an independent index, or trigger, and/or the point when that index reaches a predetermined value. There are minimal requirements, if any, on the insured to declare a claim to the

⁸⁶ <https://discord.com/channels/838986635756044328/979423963216228363>

⁸⁷ <https://www.yahoo.com/now/instech-report-finds-parametric-insurance-120100912.html>

⁸⁸ <https://blog.chain.link/parametric-insurance-smart-contract/>

insurer.”⁸⁹

Smart contract parametric insurance provider, Arbol, transacted more than \$100m in gross written premiums (GWP) in the first half of 2022.⁹⁰ They rely on weather data from Chainlink providers. They’re also building their own decentralized data repository called dClimate.⁹¹ The major emphasis in smart contract parametric insurance will be around decentralization and security of the parameters that trigger the policies.

There are a variety of oracle solutions that can be built. Wolfram Alpha is also an aggregator of sports scores and statistics. Betting is a major use case for smart contracts, because they can pool funds in cryptocurrency from anyone with a Web3 wallet and an internet connection. Then the winning payouts can be triggered based on game results coming from a trusted oracle.

“Smart contracts can substantially expand the reach of existing sports markets while introducing completely novel value streams for the sports industry such as being able to easily launch your own market. Some of the initial use cases include: Prediction Markets – smart contracts can represent various two-sided prediction markets where users take positions on different sports-related outcomes with or without odds. Sports data from global or local leagues can be used to settle prediction markets based on match results, individual player stats, team standings, the coin toss, etc.”⁹²

Different Oracle Architecture

Typically, we’ve been thinking of oracles as third-party systems. They represent a decentralized layer in between some real-world data and the blockchain. However, one way to improve their security could be to make first-party oracle systems. That is, the data API provider is also the oracle.⁹³ This puts the trust on the API provider instead of a decentralized system that could be attacked. It’s a tradeoff to think about.

“The risk of an attack on or by third-party oracle nodes exists, even though it is reduced using decentralization. With first-party oracles, the middleman nodes don’t exist, so the issue is eliminated. You can drive your DeFi app with high-fidelity digital asset data from

⁸⁹

https://www.linkedin.com/posts/andrew-klaus-cpcu-5346b896_the-effective-weapon-that-is-parametric-insurance-activity-6940714105230028800-h-f0

⁹⁰ <https://www.reinsurancene.ws/arbol-transacts-over-100mn-in-gwp-in-h1-2022/>

⁹¹ <https://www.dclimate.net/>

⁹² <https://blog.chain.link/bringing-sports-markets-to-blockchains-using-chainlink/>

⁹³ <https://api3.org/>

Amberdata's first-party oracles with reduced risk."⁹⁴

Wolfram Alpha, a trusted and secure source in itself, might be a good candidate as a first-party oracle system for smart contracts.

Chainlink is a leader now for oracles, but some other players have shown promise with different structures. For example, the UMA oracle has a system that makes the proposers of data *bond* a certain amount of tokens. Then when a smart contract requests the data from the proposer, there is a time-period where disputes can happen. Someone can dispute the data provided, which if found to be a correct dispute, will cause the proposer to lose their bond.

"Proposers respond to price requests by referencing off-chain price feeds to submit the price of an asset. In return for their work they will receive a pre-defined proposal reward set by the Requestor. To propose prices, the Proposer is required to stake a proposal bond. In the event that the price information they proposed is disputed and deemed incorrect, the Proposer will lose their bond."⁹⁵

UMA is an example of Game Theory principles applied to making a decentralized oracle.

Cardano and Wolfram Language

In a video on Cardano's channel where Stephen Wolfram talks about *Wolfram Language*, its mission to make the world's knowledge computational, and how this could fit into a blockchain oracle.⁹⁶ Wolfram Language has access to physical knowledge about the world, represented in a computational form that could be used to build advanced smart contracts. To a blockchain, "knowledge about the world" could mean knowledge about *other* blockchains. Therefore, cross-chain solutions may be built using Wolfram Language. If Wolfram is considered a trusted source about events on-chain, then it could be used to build the indexers, relayers and nodes that allow for bridges to be built.

Wolfram Language is the leader in the paradigm of "Algorithmically Oriented Programming".⁹⁷ It has computing notebooks that can actually be connected to nodes for Cardano, Tezos, Ark,

⁹⁴ <https://www.amberdata.io/oracles>

⁹⁵ <https://docs.umaproject.org/protocol-overview/how-does-umas-oracle-work>

⁹⁶ <https://www.youtube.com/watch?v=h94VrSuPFJc>

⁹⁷ <https://www.wolfram.com/language/uses/>

Bitcoin and many others.^{98,99} With this interactive computing environment, we have done experiments where we query metadata from an NFT on Tezos, like its IPFS link, and then mint another NFT with that metadata on Cardano. This is all done within a page or two of a notebook, with cryptographic signatures included. To consider this an “interactive bridging of an NFT”, we would just need the ability to lock it on the source chain before minting on the destination chain. In essence, the job of bridge relayer becomes in your hands, and you can get a feel for how a basic cross-chain system would work.

Cross-Chain Messaging Example

You can build (or paste) smart contracts from each blockchain. The architecture works like this: Wolfram servers run nodes for a variety of blockchains like Ethereum, Bitcoin, Cardano, Tezos and more. Then there is an API interface from those nodes to the Wolfram Kernel. This is connected to external storage providers like IPFS (Interplanetary File System) and Amazon S3, and to Wolfram’s computing nodes. This creates a full computing environment for blockchain at your fingertips. For cross-chain messaging, essentially you and your notebook become an interactive relayer.

Wolfram has put a lot of research into random number generation.¹⁰⁰ Random numbers are a highly in-demand product from oracle providers like chainlink. When trying to do smart contracts, you often run into the need for something random. On a centralized server, you just call a random function and it's easy. In blockchain, this is very non-trivial. With many decentralized nodes verifying the transactions, how do you ensure that they’re all agreeing on the same random number? Wolfram’s random number generator computation can be considered a source of shared truth for this.

Computational notebooks, like Wolfram Language, Jupyter, or Google CoLab became really popular in places where interactive computing was useful. Machine learning and AI research benefitted drastically from them. Having a notebook with multiple blockchain nodes connected could be a spark for innovation in cross-chain. Eventually, the environment and private keys created with them could be audited, secured and decentralized before being used in mainnet. It provides an excellent platform for prototyping cross-chain messaging between testnets.

⁹⁸ <https://reference.wolfram.com/language/guide/Blockchain.html>

⁹⁹ <https://www.wolfram.com/broadcast/video.php?sx=blockchain&v=2405>

¹⁰⁰ <https://reference.wolfram.com/language/guide/RandomNumberGeneration.html>

Indexers and Outbound Oracles

We've established that getting data into the blockchain computing environment is an oracle. However, the reverse is also needed; getting blockchain data from on-chain to off-chain systems. These are often called *indexers*, or sometimes *outbound oracles*.¹⁰¹

“Outbound or output oracles send information from smart contracts to off-chain systems or the external world. An action by an outbound oracle could include telling a banking network to make a payment or instructing an IoT smart-lock to unlock a car once an on-chain rental payment has been made.”

Being an indexer involved running a blockchain node, as Wolfram Alpha already does. Then it is listening for information on events and saving those for external systems to use. This is another great possibility for tools like Wolfram Language to be used for interactive computing of blockchain information.

¹⁰¹ <https://www.amberdata.io/oracles>