BeL2 Launch
FAQ

What is Elastos announcing today?
The Elastos Foundation is announcing support for 'Bitcoin Elastos Layer2,' codenamed 'BeL2,' a Layer 2 solution for Bitcoin. This means that instead of relying on the public Internet (Layer 3 or the Network Layer) to transmit data, Bitcoin transactions can now be conveyed across Layer 2 (or the Data Link Layer) enabling the data to be where data is encoded, transferred, and decoded on a node-to-node basis. Layer 2 is effectively a point-to-point proprietary network guaranteeing data speeds, packet delivery irrespective of traffic levels across the network, which – in addition – offers enhanced levels of security.

In practical terms, Elastos is implementing technical upgrades to the Elastos Smart Chain (ESC) to support BeL2 and the Bitcoin ecosystem. This represents a huge endorsement of Layer2 Bitcoin and both parties' belief and commitment to its future.

Beyond speed, efficiency and security, Layer 2 now offers the possibility to conduct more sophisticated transactions with Bitcoin beyond simple transfer; these include the implementation of smart contracts – irreversible digital agreements between two parties that can be defined, managed, tracked, (mutually) modified, and reconciled with complete integrity through a Blockchain, with no reference to (or requirement for) a third-party intermediary.

The world of smart contracts is effectively infinite, enabling two parties to securely, transparently and anonymously automate and conduct any transaction of their choosing; from the exchange of goods and services, to the receipt of royalties or commission. Now, this world will be available to the World's largest Blockchain community, using the Bitcoin digital currency that they know and trust.

TECHNICAL

But what's new? I can already conduct smart contracts on Bitcoin using a host of Layer2 alternatives such as the Lightening Network or other side chains?
Correct, solutions such as RSK, DriveChain, Liquid, Rollkit, RGB and, most famously, the Lightening Network offer Layer2 'work-arounds', enabling smart contracts to be denominated in Bitcoin.

However, they don't represent genuine staking; the opportunity to put Bitcoins to work (in the same way as with tokens such as Ethereum and Tezos).

In addition, among the existing BTC Layer 2 projects, they all lack a core capability, that is, the Bitcoin network and the second-layer network cannot mutually perceive the transactions on each other's chains. The traditional solution is to use multi-signature by validators. Passing transactions from both sides to each other inevitably introduces the two problems of collective evil behavior by validators and how to punish evil behavior.

How does BeL2 work exactly?
Zero-knowledge proof technology (ZKP) is fundamental to this process. ZKP is a technology that can generate mathematical proofs for certain complex calculation processes. By verifying the proof results, it can be confirmed that the corresponding calculation process is valid, expected, credible and unforgeable.

The main process of this solution is to first generate a zero-knowledge proof for the BTC main network transaction, and then verify it by the second-layer network, so that the second-layer network can perceive the transaction content of the first-layer network, and based on zero-knowledge proof technology, the second-layer network The network can trust that the transaction is genuine and valid.

On this basis, we can not only transfer information from the first-tier network to the second-tier network, but also transfer information from the second-tier network to the first-tier network through the relayer.

In order to avoid the relayer cheating, we can supervise the second-tier network transaction content passed by relayer. Combined with the deposit mechanism (all relayers must deposit an amount greater than the transaction value in the smart contract of the Layer 2 network before they can become relayers), if the relayer cannot prove that his behavior is true and effective, his deposit will face penalties.

Compared with the previous solution, this solution can be run completely in a self-hosted state. Even the relayer can serve without authorization and permission, as long as it stakes sufficient deposit. The criteria for penalties are also straightforward, as long as the relayer is proved to have cheated, or it cannot prove that he completed the delivery of the relevant transaction.

What precisely is the role of ELA (and Elastos) in this process?
Because the first step will be implemented in ESC, and the relayer will pledge margin in ESC, then we will use ELA as an acceptable margin asset type. In the future, ELA's LSD assets may also be accepted.

If I'm a node manager, what does BeL2 mean for me?
It offers the possibility of staking; the chance to earn 'interest' (or a return) from the Bitcoin tokens under management. While Blockchains such as Tezos, Cosmos, Solana, Cardano and, most famously, Ethereum have traditionally enabled 'dormant' tokens to be put to work (verifying transactions and the status of tokens, according to the corresponding smart contracts), this has never been possible with Bitcoin. In effect, 'saved' Bitcoin tokens remained 'dormant'; apart of trading on price fluctuations, there was previously no other manner to create value from them.

BeL2 makes staking possible; node managers will have the opportunity to earn from their Bitcoin reserves, in the same way as owners of Ethereum and other 'stakable' tokens.

The emergence of Bitcoin-denominated smart contracts also means that there will be exponentially more activity across the Blockchain, more transactions to verify, and more gas fees to earn.

How will gas fees be allocated between ELA and Bitcoin tokens?
There is no problem of allocating handling fees between ELA and BTC. Only the Relayer role is "redundant" during the transaction process. All handling fees are paid to the Relayer and distributed on the BTC main network. When the transaction is completed, the transaction that withdraws BTC will allocate a portion of BTC to the Relayer as a handling fee.

What does BeL2 mean to me if I hold ELA?
For ELA holders, you can pledge ELA to join BeL2 and become a relayer. The inspection and judgment of all transactions have been completed in the BeL2 contract. The relayer only needs to sign and broadcast the transactions approved by the contract to the BTC network. This task is simple and easy. , and can earn BTC service fees.

If I'm a Bitcoin miner, what does BeL2 mean for me?
BeL2 opens up the programming capabilities of BTC. The BTC on the main network is not just transfer transactions or the issuance of BRC20 assets. BeL2 can bring more transaction types and more business scenarios to BTC and BRC20, which means more BTC mainnet transactions, and of course more fee income. These fees will subsidize the income of miners after the BTC halving.

Bitcoin miners can merge mine ELA and stake it to earn more BTC; in effect, more BTC can be earned at no extra cost.

What differences and new features will BeL2 mean for the Essentials wallet?
Ideally, we hope that users can get one-stop service in Essentials, trade here, act as a relayer here, and let ELA and BTC intersect here.

Simply put, BTC is the foundation of the crypto world, and the programming capabilities of ETH's Solidity contracts are impressive. BeL2 hopes to combine the two to achieve: support BTC and assets issued on BTC, and program transactions of these assets in Solidity contracts.

But I can already build and impose smart contracts direct in native Ethereum; why is BeL2 such big news?
Correct, building and administering decentralized smart contracts is at the heart of the Ethereum Blockchain; it's 'Turing-complete' scripting language enables developers to write more complex smart contracts and distributed applications.

However, the World has already made its choice – Bitcoin accounts for nearly 40% of the entire cryptocurrency world's value, so it is reasonable to say that the Bitcoin Blockchain is the most popular. It is certainly the one that has the most value locked up in it.

In addition, Bitcoin is considered far more secure that it's Ethereum counterpart. In part, this is due to the number of miners validating Bitcoin transitions (1 million) compared to an ever-declining volume of Ethereum counterparts due to the decline in returns.

There are even reports of the US Department of defense considering Bitcoin as a development of national strategic interest given its security credentials. In December '23, U.S. Space Force Major Jason Lowery urged the U.S. military to prioritize the investigation of proof-of-work systems like Bitcoin for the country's defense.

Bitcoin has been notoriously difficult scale due to capacity limitations. How will BeL2 mitigate these?
Bitcoin's programmability has traditionally (by design?) been relatively limited, which is mainly reflected in the functional limitations of its scripting language. Bitcoin's scripting language is a stacked programming language that is used to define the input and output conditions of transactions.

However, this scripting language is not Turing complete, which means it cannot solve all computing problems. In contrast, Ethereum uses a Turing-complete scripting language that allows developers to write more complex smart contracts and distributed applications.

BeL2 innovatively applies zero-knowledge proof technology to BTC. By generating proofs for BTC transactions and checking and verifying the proofs in the ETH contract, ETH can understand what is happening on BTC and act accordingly.

This is the basis of BeL2. Based on this, we can let BTC transactions "trigger" the ETH contract to perform operations, such as transferring assets. You can also set a timeout to force BTC users to perform a certain operation, otherwise they may face penalties from the ETH contract (such as deducting his pledged assets in the contract). The community can also be allowed to supervise BTC transactions. If an evil transaction occurs that does not comply with the transaction content, anyone can submit the proof of the transaction to the smart contract, so that the evil transaction party can be punished.

When transactions can be guaranteed to be executed, we can use BeL2 to complete more complex transaction types and business scenarios, allowing BTC to participate in daily commercial activities, just like DeFi on ETH.

A technology based on zero-knowledge proofs: the two parties involved in the transaction are Alice and Bob. Three possible transaction outcomes: normal completion, refusal to complete, and evildoing.

As Laozi said: Tao gives birth to one, two gives birth to three, and three gives birth to all things. BeL2 does exactly that.

Specifically, what have been Bitcoin‘s traditional challenges with scale?
At the beginning of the birth of Bitcoin, geeks were discussing how to expand its applications and performance, which is the issue of Bitcoin expansion, which includes three aspects

1. Transaction speed, Lightning Network is a great project, it perfectly solves the problem of transaction speed
2. Issue assets, such as Omni USDT, Taproot assets, BRC20, and RGB protocols, but they all rely on relatively centralized services.
3. Programming capabilities. BitVM attempts to use Merkle trees to implement chip circuits on Bitcoin. This is an amazing idea and deserves attention. Apart from this, there are currently no other options.

Currently, the Bitcoin network can only process about 7 transactions per second. This limitation significantly reduces Bitcoin's efficiency and usefulness compared to traditional financial systems such as Visa, which can process thousands of transactions per second.

The root of this scalability problem lies in Bitcoin's blockchain structure. The size of each block is limited to 1MB, and each block is generated approximately every 10 minutes. This limits the number of transactions each block can contain, thereby limiting the processing power of the entire network. Additionally, Bitcoin’s consensus mechanism also takes time to verify transactions, further limiting transaction speed. For example, during peak transaction periods, users may have to wait for hours or even days for transaction confirmation, and the transaction fee may exceed $10 in gas.

This makes Bitcoin unable to meet user needs in many cases. For users and merchants looking for instant payments, this delay may be unacceptable.

Specifically, how will these issues now be addressed with the arrival of BeL2?
Based on the zero-knowledge proof technology mentioned earlier,

1. Expand the transaction programming capabilities of BTC. As mentioned above, we can write the content of the transaction as a smart contract and execute it in the EVM of ETH. Through the game between the two parties of

the transaction and the participation of Relayer, the transaction can be under supervision. Complete, this allows BTC to be programmed for more complex scenarios.

2. Using zero-knowledge proof technology, we can also submit transaction information on BTC to smart contracts. If these transactions carry BRC20, or RGB, or TapRoot asset information/Sats, then these can also be recorded in the contract. , allowing smart contracts to become their trusted ledgers, thus solving the centralization problem of indexers.

Does BeL2 leverage Ethereum's EVM to facilitate the roll up? What are the implications for Ethereum's relationship with Bitcoin; what does Ethereum gain from the relationship?

As mentioned earlier, BTC is the cornerstone of the entire crypto world, and smart contracts open up space for expansion of the programmability of crypto assets. It makes it easier to integrate crypto assets with the Internet and reconstruct the existing and future Internet ecology.

BeL2 connects the advantages and features of both, allowing them to play to their respective strengths. We no longer have to debate whether to fork BTC and whether to add more instructions to it. There is no need to worry about whether the POS mode of ETH is safe enough.

Through BeL2, all EVM-compatible networks, and even all networks that support smart contracts, can be used as a trading network for BTC mainnet assets. Issuing assets on BTC and running assets in smart contracts is the most appropriate division of labor and collaboration. BeL2 makes it possible.

Is BeL2 dependent on the EVM Could the Ethereum Foundation ever veto or block this integration which so clearly benefits Bitcoin?

Of course not. Our ultimate goal is to implement verification and checking of BTC transaction proofs on the standard version of Solidity. If any EVM wanted to prevent it, it would have to modify the Solidity standard, which would be extremely costly and risky, and we don't think the Ethereum Foundation will do that. And even if it does, this is a decentralized network, and we can execute smart contracts for transactions on other, more friendly networks.

If I have Bitcoins locked up in other networks such as Lightening, will I be able to stake these also, via BeL2?

This is currently not possible, only on the mainnet, and currently we only support the traditional BTC address format, and currently do not support the Taproot address format, or any address format generated by the Schnorr algorithm.

VISION

Elastos founder, Rong Chen, recently spoke about the SmartWeb. What does this mean, and how does BeL2 fit into this vision?

In Elastos' vision for Web3, Rong Chen birthed the term 'SmartWeb', a category which transforms the Internet into a user-driven, interactive ecosystem. It's about merging decentralised technology and security, transitioning from centralised control to a more democratic space where users own and control their data.

In SmartWeb's previous vision, BTC helped ELA obtain stronger computing power protection through joint mining, making it safe. Now with BeL2 technology, we can issue assets directly on BTC, and the security of these assets is directly protected by the BTC consensus. At the same time, trade these assets on ELA and program these assets. Instead of putting everything on ELA. I think this can better realize Rong's vision for SmartWeb.

Rong's vision for a truly 'smart' Web is based on the following criteria:

- **Decentralised Structure**: SmartWeb utilises Elastos' decentralised structure, operating across a network of distributed nodes rather than central servers, enhancing security and preventing singular entity control.
- **Security Through Sandboxing and Blockchain**: Security in SmartWeb is multifaceted. It employs sandboxing technology to isolate applications, preventing malicious software from affecting the system or accessing user data without permission. The integration of blockchain technology provides an immutable ledger for transactions, fostering trust and transparency.
- **User Empowerment and Control**: SmartWeb is designed to return control to users. Through decentralised applications (DApps) and digital identities, users gain autonomy over their digital interactions, managing their data, and controlling how it's shared.
- **Peer-to-Peer Interactions**: A vital component of SmartWeb is its peer-to-peer communication model. Unlike the traditional internet, where data often goes through centralised servers, SmartWeb enables direct communication and data exchange between users' devices and personal nodes, boosting privacy and efficiency.
- **Integrated Digital Economy**: SmartWeb isn't just about secure communication; it also fosters a decentralised digital economy. Blockchain and smart contracts facilitate secure, transparent financial transactions without traditional intermediaries.

BeL2 will enable such decentralized services to flourish through a digital currency that users are both familiar with and trust, Bitcoin. Such services could cover the provision and exchange of any asset type, from intellectual property (IP) to financial instruments; all delivered and assured directly between parties concerned.

This means that both parties will now be at liberty to define their own terms of business, with no reference of requirement of a third party, and to assure the integrity of the same through the Bitcoin-validated smart contracts.

The arrival of BeL2 means that Bitcoin has 'just got smart'?
It means that native Bitcoin users can now directly assure any form value exchange through an accompanying smart contract; an inviolable, permanent record against which any agreement can be based.

So, in terms of the ease with which smart contracts can now be developed in Bitcoin, yes – in this sense, BeL2 will make Bitcoin smart.

But the concept of smart has a deeper meaning and relevance:

- Smart Web; as defined by Elastos founder Rong Chen is the culmination of disintermediated services provided with complete integrity, privacy and security (see above). In fact, the antithesis of how the current Web2 has evolved; based on and subject to the interests of a defined set of intermediaries.
- These principles underpin Elastos' own smart chain (ESC)

What does the opportunity of 'being your own bank' mean in practice?
Historically, financial services have been provisioned by third parties; intermediaries who don't necessarily stake their own assets, but those 'loaned' to them by depositors. While we are not questioning the integrity of the entire banking system, two realities are now becoming evident:

- Banks' interests are not necessarily/always aligned with its customers (depositors/loanees), particularly consumers. Interests may range from profitability to maintaining good relationships with regulators; all of which are perfectly legitimate, but which don't necessarily serve the end user to his/her best advantage.
- For instance, the Bank of England's key interest rate (the rate at which banks can themselves earn interest) reached 5% in June this year, at a time when Barclays was offering just 0.85% on its easy access Everyday Saver; HSBC 1.35% on its easy access Flexible Saver; and NatWest 1.11% on its Flexible Saver account for savings under £25,000. The above is a simple example of commercial banks' multiple objectives not necessarily prioritizing those of its customers.
- Banks have long held a form of 'soft' monopoly on financial instruments; while such products are available from unlicensed financial institutions (fin techs, for instance), daily life is virtually impossible without a functioning bank account.
- Being your own bank is about eliminating the intermediary (or, at least having the option to), to obtain financial products and services that better correspond to your needs. This direct relationship would increase the volume and range of supply available; and the opportunity to arbitrage (negotiate a better deal for yourself).
- It is also becoming a financial services provider yourself; even on a modest level. Assets – from property to savings – could be make available to potential customers, direct; with terms negotiated mutually.
- BeL2 brings disintermediated banking closer to reality:

    - Based on the World's most popular, liquid and universally accepted digital currency
    - Now supporting and supported by sophisticated smart contracts that can define, enforce and automate every aspect of the transaction
- Whether you are a business or a consumer, being your own bank is about offering or receiving financial services on your terms direct, without any intermediary.

What is the concept of 'social banking' about?

- The metaphor reflects the impact social media exerted on the traditional publishing industry. In common with the banking sector, prior to the Web, publishing's incumbents (particularly largescale distribution and broadcast) enjoyed a virtual monopoly. The capital cost and complexity of establishing a newspaper and competing for readers and subscribers proved a virtually insurmountable barrier to competition.
- Social media enabled even individuals to compete for readers, viewers and subscribers direct with their respective audiences; the intermediary (journalists, editors etc) had been removed, and content providers could publish direct, on their own terms.
- Social banking reflects the same possibility, businesses and individuals going to the market direct to sell/receive financial services. Just like social media, providers' reputation (and brand) would be defined by the volume and nature of the endorsements they generate, while purchasers of said instruments could also be rated accordingly.
- Just as in the case of social media, the mechanics and protocols of these relationships will be defined over time (and in accordance with relevant legislation) but the precedents are established.

What are the regulatory and compliance implications of the above?

- Principles and protocols of financial law and fiscal regulations would have to be established according to jurisdiction. There are no reasons to expect that such regulation can't be defined and imposed for mutual benefit, as has been the case for other disruptions such as on-banking fintech services and online commerce etc.

Is BeL2 going to put banks out of business?

- Again, the social media metaphor is perfectly illustrative. Traditional media companies have adapted and prospered; many adding complementary social media services to their more traditional offering. In some cases, the former are subscription-based, in others, a free 'teaser' designed to entice readers and viewers to the full offering.
- Social banking could evolve in a similar manner; the key is – thanks to the arrival of BeL2 – such disintermediated, direct financial services are now a possibility.

With all the emphasis on banking, what other opportunities with so-called 'Smart Bitcoin'?
Absolutely, BeL2 facilitates the provision and assurance of any service, financial ir otherwise, as long as in includes an exchange of value. The latter could range from royalties or access, to real world assets such as property or, even, the generation, administration and exchange of carbon credits.

Isn't the above a departure from the original mission and principles behind Bitcoin?
Bitcoin was originally designed to be a simple, secure digital currency focused on enabling decentralized value transfer.

Therefore, by design, the goal of Bitcoin is to provide a simple and efficient currency exchange system, rather than a fully programmable platform. This design choice strengthens Bitcoin's security, but also limits its applicability to more complex applications.

BeL2's objective is to simply extend the usefulness and range of applications for World's most popular decentralized digital currency, without compromising its inherent security.