

Privacy-First CBDCs

Leveraging ZKPs and Ethereum
for Next-Gen Digital Currencies

**Andre
Omietanski**

General Counsel, Aztec Labs

Joe Andrews

Co-Founder, Aztec Labs



What we will cover

- Overview of CBDC Projects
- Privacy-First CBDC Designs
 - Comparison of Privacy Enhancing Technologies
 - Applicability of ZKPs to CBDCs
 - Advantages of Launching a Privacy-First CBDC on Ethereum
- Summary of Key Takeaways
- Q&A

Disclaimer and Note

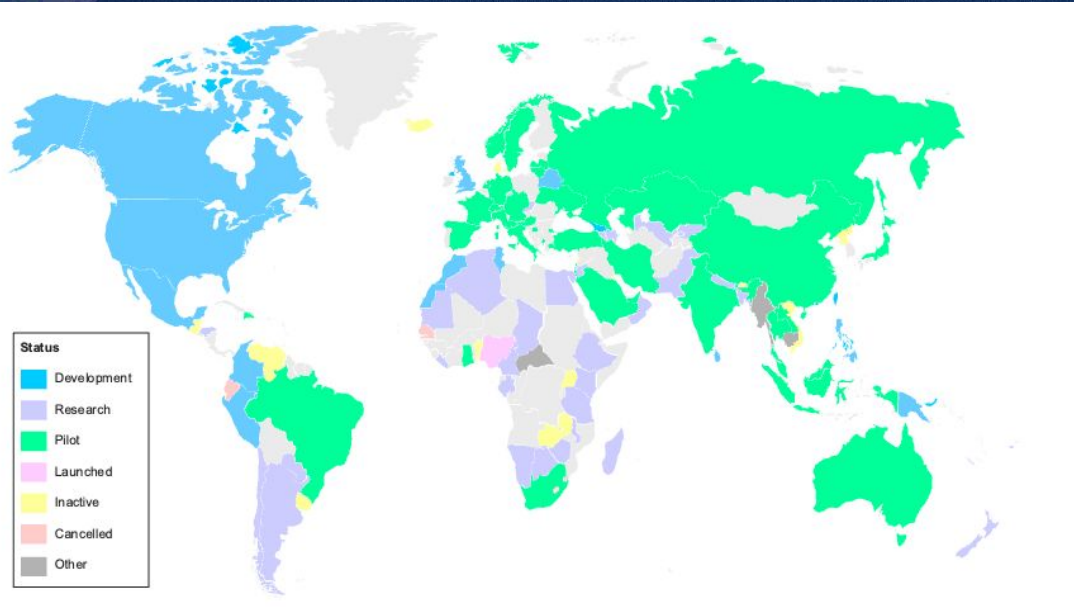
- This presentation is for discussion / educational purposes only; we **do not** endorse, support and/or encourage/discourse the creation of CBDCs.
- **We do**, however, **endorse**, support and encourage the use of **the best privacy enhancing technology and Ethereum**, for any CBDCs or base layer government systems.
- **On Thursday 21 November**, we will release our **Privacy-First CBDCs Report**.



Overview of CBDC Projects

CBDC Snapshot

As of September 2024, **134 countries** are exploring or developing CBDCs

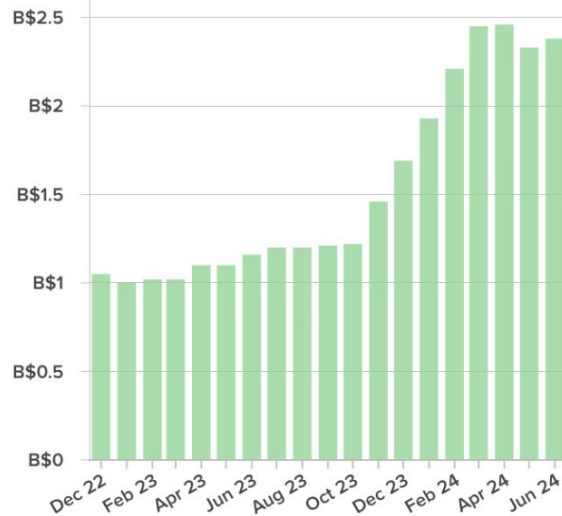


- Every G20 country is **exploring** a CBDC
- All original BRICS members are **piloting** a CBDC
- All advanced retail CBDC projects **are intermediated** through banks, financial institutions
- Three countries have **fully launched a CBDC** —the **Bahamas, Jamaica** and **Nigeria**
- **Digital yuan (e-CNY)** is still the **largest CBDC** pilot in the world

Rise of CBDCs

Total SandDollar in circulation

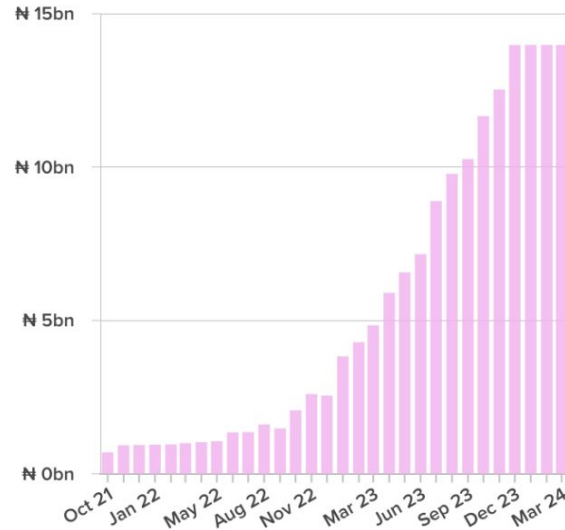
From 2022-2024 (in millions)



Source: [Central Bank of Bahamas](#)

Total eNaira in circulation

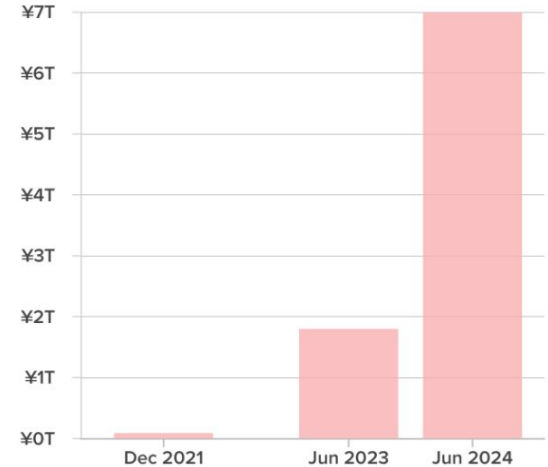
From 2021-2024 (in billions)



Source: [Central Bank of Nigeria](#)

e-CNY transaction volume quadruples since 2023

Total transaction volumes to date



Source: [People's Bank of China](#) • PBoC did not release official data in 2022

CBDCs in the US?



"Dangerous threat to freedom" - Trump on the creation of a digital dollar

Analysis of Existing CBDC Designs

Existing designs are just **not good enough**; most are:

- **Intermediated** - rely on existing banks to facilitate transactions
- **Lack privacy** - rely on existing banks to store sensitive personal financial information
- **Lack interoperability** - not interoperable with Ethereum

We can and should do better
(and maybe *Trump* will change his mind)





A CBDC without privacy is a dystopia

Privacy-First CBDC Designs

Thesis (1/2)

- Fiat needs a fundamental redesign to preserve its status in the advent of crypto
- Next-gen digital fiat currencies (CBDCs) need privacy by design architecture and ought to be launched on Ethereum

Thesis (2/2)

Smaller nations are best suited to experiment with novel CBDC designs, which could benefit from:

- Strategic Geopolitical Leverage, Enhanced Global Presence and Economic Influence
- Financial Transparency, Inclusion and Remittance Efficiency,
- The chance to become a digital reserve currency by linking on chain assets to a central banks balance sheet

potentially leapfrogging larger nations in geopolitical significance

Comparison of Privacy Enhancing Technologies

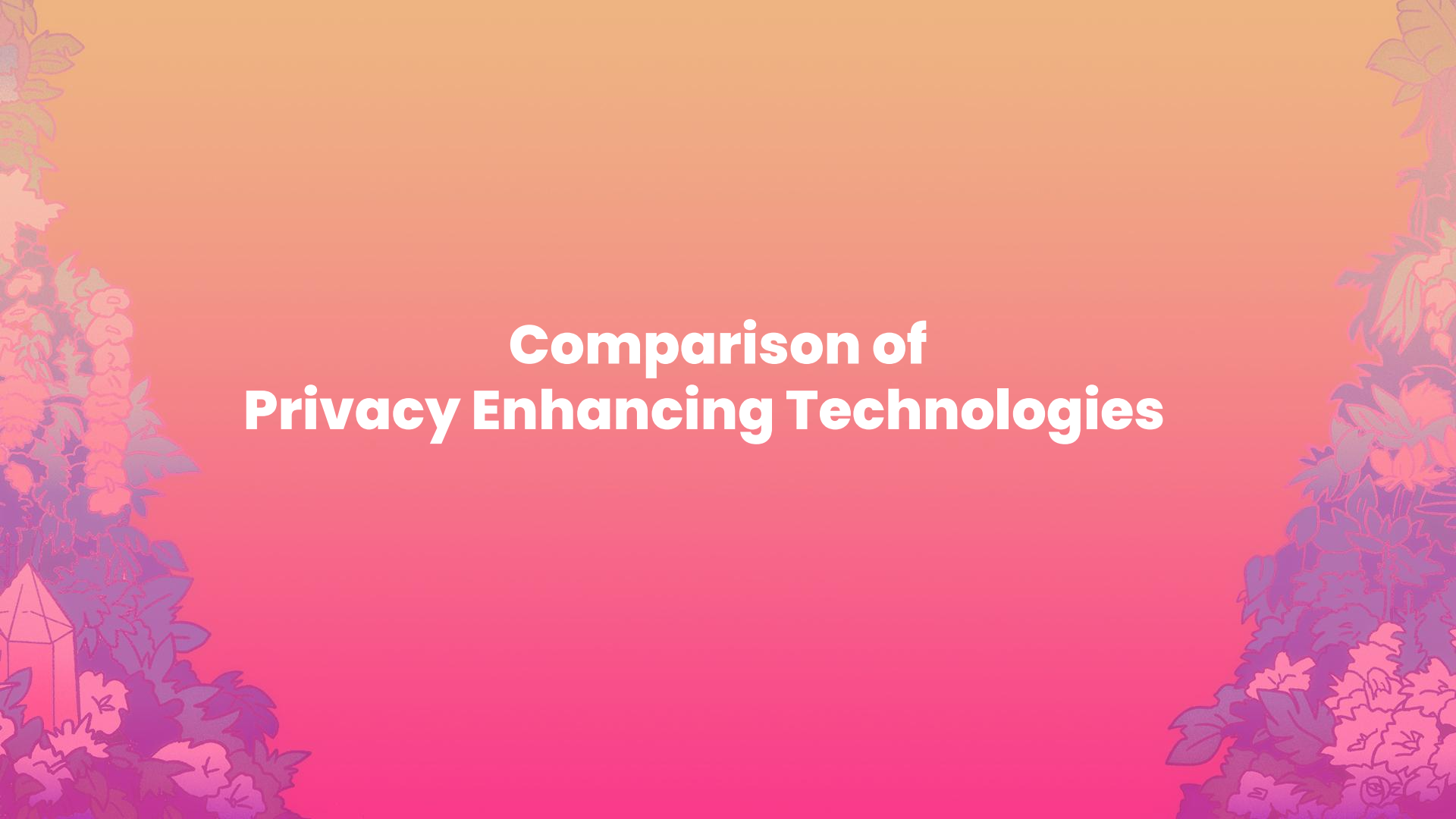


TABLE 1 – COMPARISON OF PRIVACY-ENHANCING TECHNOLOGIES^{14,15}

	Zero knowledge proofs (ZKP)	Pseudonymisation	Private information retrieval (PIR)	Attribute-based encryption (ABE)	Differential privacy	Interactive multi-party computation (MPC)	Federated learning	Homomorphic encryption	Trusted execution environment (TEE)
Description	A cryptographic technique where one party (the prover) can prove to another party (the verifier) that a given statement is true without revealing all / any inputs that build up the statement.	High level design approach of replacing information that identifies an individual with a pseudonym.	A cryptographic technique that enables information retrieval from a server / database without revealing which item is retrieved.	A generalisation of encryption schemes where decryption of a ciphertext is only possible if the user key's attributes match the attributes of the ciphertext (e.g., account ID, email address).	A cryptographic technique that shares information about a dataset without revealing information about individuals in the dataset.	A cryptographic technique that enables different parties to jointly compute a function over certain inputs while keeping the inputs private.	A distributed machine learning approach enabling multiple parties to collaboratively train a model without sharing their data with each other.	A cryptographic technique that enables computation over encrypted private data, which decryption returns a result identical to if the computation was performed over plaintext.	A secure area of a computation processor that guarantees code and data loaded inside are protected with respect to confidentiality and integrity.
Example Projects Developing / Utilising PET for Privacy	Aztec , Miden , Aleo	Equifax and most traditional finance institutions	Google and Meta	IBM and big tech generally	Apple, Google and big tech generally	Taco , dWallet Labs	NVIDIA, Google, Apple	Zama , Phenix , Inco , Sunscreens , Apple	Flashbots , Secret Network , Marlin
Used in production	✓ First proposed in the 1980s, the technology is securing >\$1b of assets on DLTs combined.	✓ Common way to comply with the GDPR in traditional web development.	✗ Most PIR protocols are still in research and development.	✓ First proposed in the 1980s and growingly adopted in businesses.	✓ Adopted across different companies.	✓ Applied in different large-scale projects.	✓ Adopted across different companies.	✗ Homomorphic encryption schemes are mostly in research and development.	✓ Adopted across different fields.

¹⁴ **Note:** The actual trade-offs heavily depend on implementations of each PET of choice (e.g., different MPC implementations can have different scalability and trustlessness trade-offs). The table is intended to serve as a general frame of reference, rather than an exhaustive description of each PET.

¹⁵ **Note:** ZKPs could be combined with one or more PETs to also enable the various benefits of the alternative PETs.

	Zero knowledge proofs (ZKP)	Pseudonymisation	Private information retrieval (PIR)	Attribute-based encryption (ABE)	Differential privacy	Interactive multi-party computation (MPC)	Federated learning	Homomorphic encryption	Trusted execution environment (TEE)
Interoperable between existing banking infrastructure and DLTs	✓ Proofs are easily verifiable both offline and with DLTs.	✗ Prone to privacy leaks with fully transparent DLTs.	✗ Applications with DLTs are mostly in research and development.	✓ Encrypted private data can be stored in both databases and/or on DLTs.	✗ Applications with DLTs are mostly in research and development.	✓ Applied across both general computing and DLTs.	✗ Applications with DLTs are mostly in research and development.	✗ Applications with DLTs are mostly in research and development.	✓ Applied across both general computing and DLTs.
Privacy-respecting AML compliance	✓ AML analysis can be programmed into the statement being proved without revealing any information that is desirable to remain private.	✓ AML analysis can be performed on pseudonymised data.	✗ AML analysis can't be performed within PIR itself. It has to be added before or after the retrieval outside PIR if needed.	✗ AML analysis can only be performed on decrypted data.	✗ AML analysis would be ineffective, as it can be performed on grouped datasets but not on individuals.	✓ AML analysis can be confidentially performed on private data.	✗ AML analysis can be performed, but by the payment service provider with full knowledge of the data that is being analysed.	✗ Analysis of encrypted private data cannot be performed with the technology, just computation over them.	✓ AML analysis can be confidentially performed on private data.
Computation over private data	✓ Computation can be performed over private data fed as private inputs to the ZKP program.	✓ Minimal added limitations on computations over data.	✗ PIR could support computations over data during the data retrieval process, but in an inefficient manner.	✗ ABE does not support computations over encrypted private data.	✓ Computation can be performed over differential privacy datasets.	✓ Computation can be performed over private data.	✗ Computation is learnt from distributed local data using the technology, but not on those data.	✓ Computation can be performed over encrypted private data.	✓ Computation can be performed over private data.
Scalable	✓ Verification	✓ Minimal added	✓ Overhead scales	✓ Encryption and	✓ Mature	✓ Computation	✓ Various large-	✓	✓ Computation

	Zero knowledge proofs (ZKP)	Pseudonymisation	Private information retrieval (PIR)	Attribute-based encryption (ABE)	Differential privacy	Interactive multi-party computation (MPC)	Federated learning	Homomorphic encryption	Trusted execution environment (TEE)
	effort stays near constant for arbitrarily large computations proved. Simple programs are possible on user devices in seconds. Larger programs proving efforts; distributed and aggregated with recursion.	effects on scalability.	sub-linearly with the amount of data involved.	decryption overhead is insignificant.	techniques were developed for application over large datasets.	and communication complexity can scale sub-linearly with the right designs.	scale systems based on the technology are in production.	Large computation overhead. These computations can be outsourced to data centres without compromising data privacy, but with a cost.	overhead is insignificant.
Trustless / ensures data protection	✓	✗	✓	✓	✓	✗	✗	✓	✗
	Implementations are cryptographically secured and should be open sourced.	Privacy integrity largely depends on whether the service provider is managing data storage and transit correctly.	Implementations are cryptographically secured and should be open sourced.	Implementations are cryptographically secured and should be open sourced.	Implementations are cryptographically secured and should be open sourced.	Privacy integrity depends on the number of colluding parties not exceeding a certain threshold.	Local federated learning nodes (e.g., payment service providers) are trusted to respect and upkeep its users' privacy.	Implementations are cryptographically secured and should be open sourced.	Existing chip manufacturers need to be trusted to construct safe TEEs free from privacy-exposing loopholes, backdoors, and attacks. A number of vulnerabilities of TEEs already disclosed to date, in particular related to SGX

PETs Summary

	ZKPs	FHE	TEE
Used in production	✓	✗	✓
Interoperable between existing banking infra / DLTs	✓	✗	✓
Privacy preserving AML compliance	✓	✗	✓
Trustless / ensures data protection	✓	✓	✗



**ZKPs are the ultimate d/acc
solution for CBDCs**

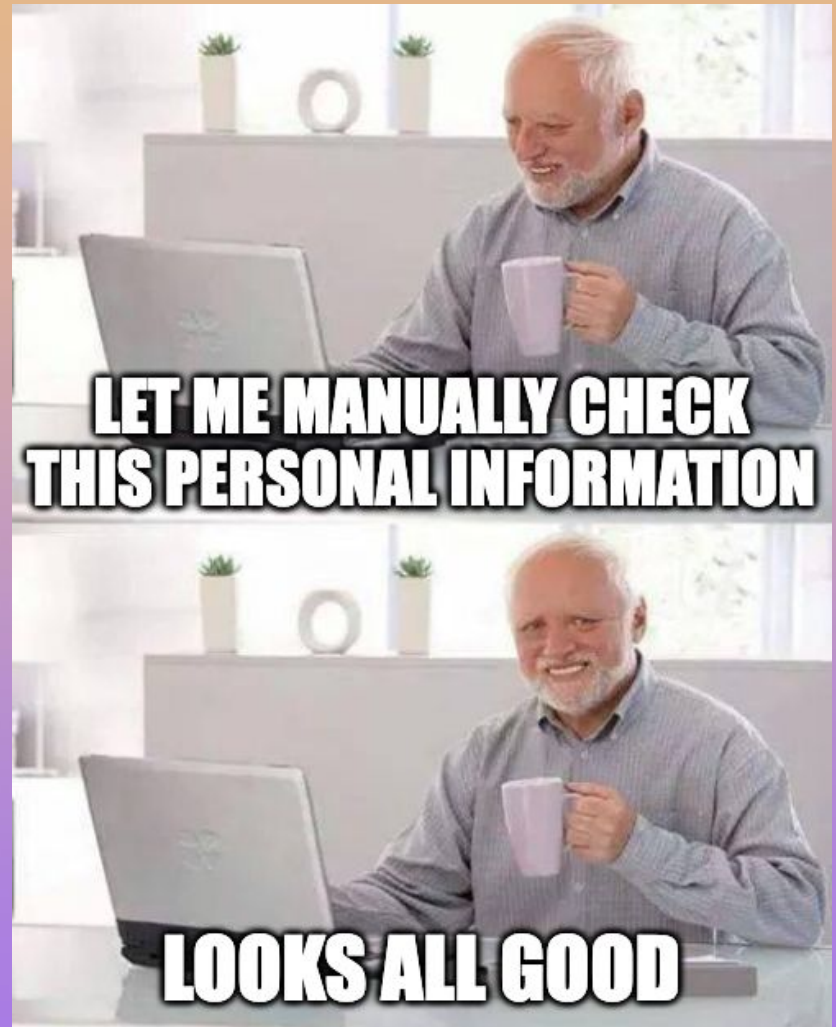
Applicability of ZKPs to CBDCs

Current AML / CFT Model

Current AML / CFT models are inefficient, ineffective and expensive:

- **Manual Labour.** A significant cost component of AML compliance spend for financial institutions is labour resources
- ***Expensive / Ineffective:**
 - anti-money laundering policy intervention has **less than 0.1 percent impact on criminal finances**
 - **compliance costs exceed recovered criminal funds** more than a hundred times over
 - banks, **taxpayers and ordinary citizens are penalised** more than criminal enterprises
 - It is estimated that **in Europe, AML requirements necessitate compliance costs higher than the amount actually recovered from criminals by authorities.**
- **Cryptographic Compliance > Harold:** In speeding up and minimising the number of interactions required, ZKPs offer an alternate, more efficient and more secure way to satisfy AML/CFT.

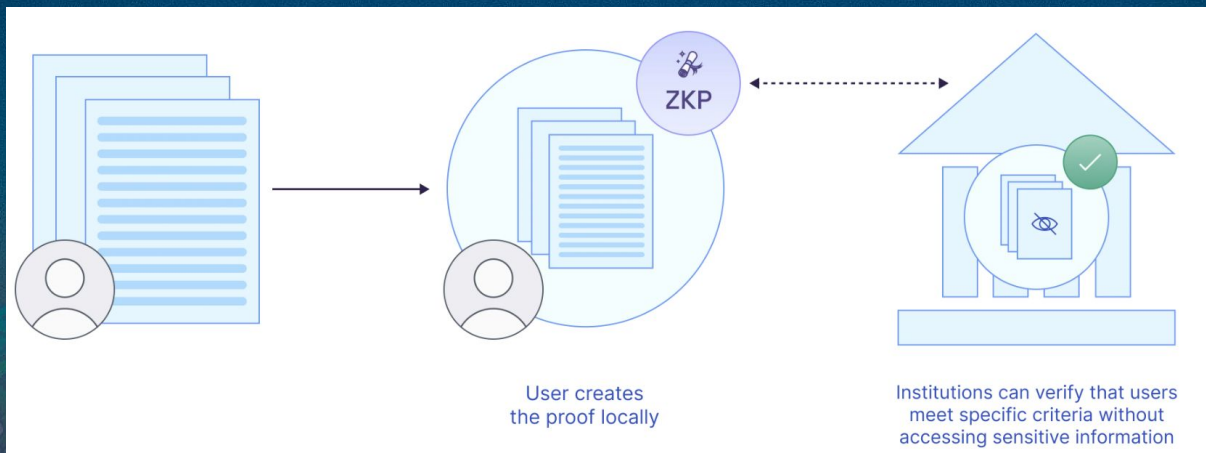
* "Anti-money laundering: The world's least effective policy experiment? Together, we can fix it" 2020 - Ronald Pol, La Trobe University, Melbourne, Australia



ZKP Model

A central bank could define a program, written as a ZKP, that checked if the following statements are true before a state update to the relevant balance ledger is made:

- each end user who is a party to the transaction is validly registered, and the transaction comes with a valid proof of a KYC check as produced by the ZKP
- neither party is on a sanctions list defined by the central bank or regulatory body
- any other checks that can be represented as code

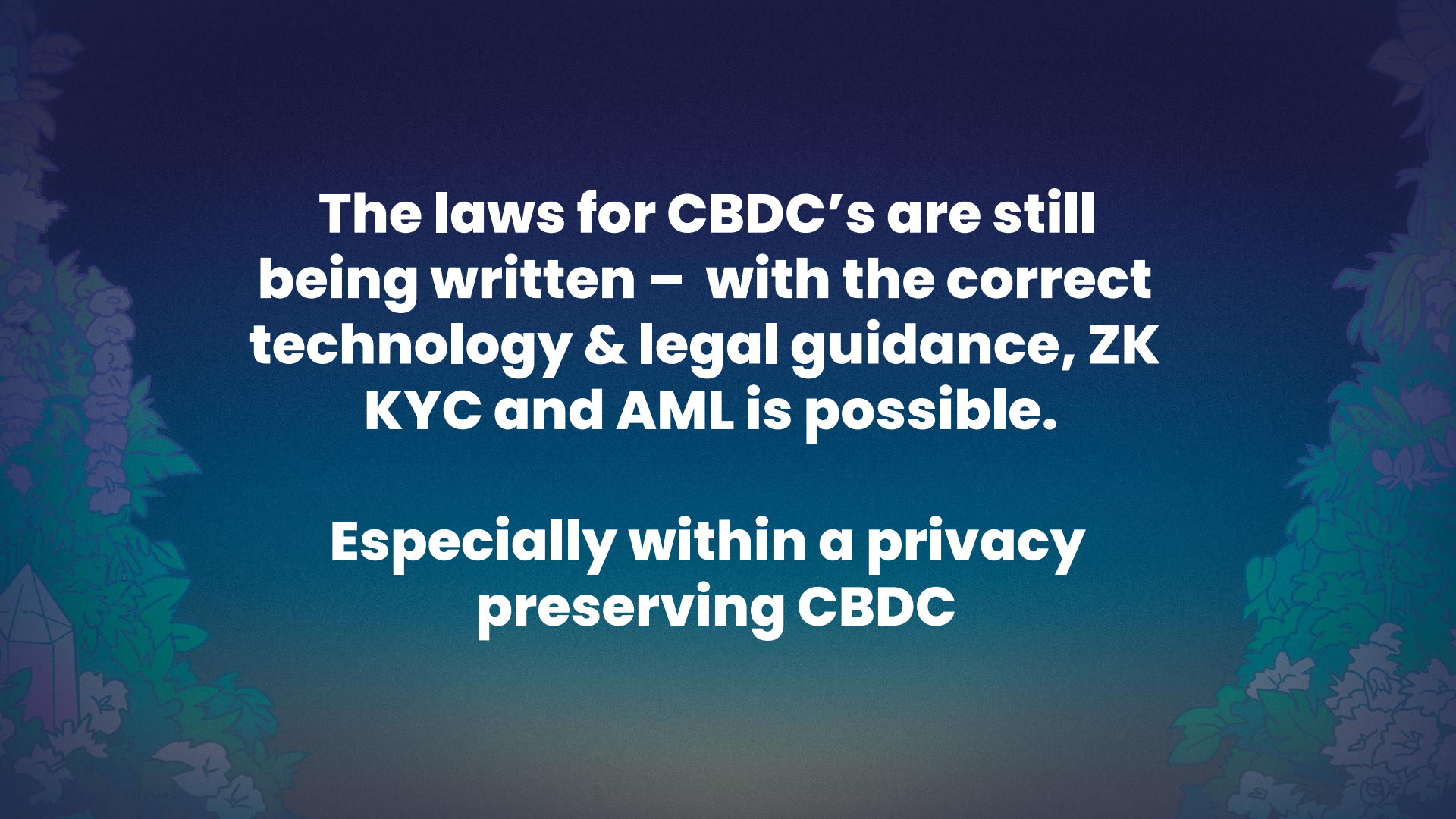


But how do we comply with laws?

ZKPs can be used to comply with standard AML/ CFT laws, including:

- Customer Due Diligence
- Enhanced Due Diligence
- Ongoing Transaction Monitoring
- Suspicious Activity Reporting
- Sanctions Screening

Our upcoming Privacy-First CBDC Report, will contain an analysis on how each of these laws in the UK, Thailand, Montenegro and Switzerland can be satisfied using ZKPs.



**The laws for CBDC's are still
being written – with the correct
technology & legal guidance, ZK
KYC and AML is possible.**

**Especially within a privacy
preserving CBDC**

TABLE 3 – JURISDICTIONAL ANALYSIS

Jurisdiction	Existing Laws and Regulations	Description of Law / Rule	Example ZKP Solution(s) ²⁴
<i>Customer Due Diligence (“CDD”)</i>			
United Kingdom	Relevant persons are obliged to comply with CDD requirements under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017/692 (“ MLRs ”) in order to identify the user and verify their identity. This includes undertaking an assessment of the purpose and nature of the business relationship or occasional transaction and obtaining further information on this where appropriate.	<p>CDD must be carried out where a relevant person ‘establishes a business relationship’, meaning a relationship between a relevant person and a user which is expected to have an element of duration. It is also required where customers of relevant persons carry out occasional transactions that exceed €1,000, where money laundering or terrorist financing are suspected, or if there are any doubts as to the veracity or adequacy of any documents or information provided for identification or verification.</p> <p>The MLRs permit simplified customer due diligence, following a risk assessment, and require enhanced due diligence in specified circumstances, as set out below.</p> <p>The MLRs and Part I of the Joint Money Laundering Steering Group (“JMLSG”) guidance permit relevant persons to use electronic identification processes to satisfy CDD requirements – which they may perform themselves or via third-party organisations – provided the relevant person is satisfied that the relevant process is sufficiently extensive, reliable, accurate, independent of the customer, and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person. The JMLSG guidance indicates that while, in general, an electronic check that accesses data from a single source is not normally enough on its own to verify identity, it may be sufficient where,</p>	<p>To perform an occasional transaction above the relevant threshold or access certain wallet functions, a user, using the CBDC ZKP supported infrastructure, would have to prove in zero knowledge²⁵ that they have all requisite documentation, and can pass any related required corroborating checks (e.g. ‘liveness’ checks), in order to meet CDD identification and verification requirements.</p> <p>ZKPs could thereby be used to attest to completion of CDD checks, as only the resultant proof would need to be disclosed to the central bank or other ecosystem participants (e.g. PIPs, if incorporated into the CBDC model), which would confirm that these obligations have been complied with, rather than sharing any form of the underlying CDD data.</p> <p>As noted, certain regulatory frameworks already envisage the use of electronic identification processes to satisfy CDD requirements, provided the relevant process is capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person, and recognise the potential strength of an identity source issued by a relevant authority that contains cryptographic security features. In principle, this provides the legal and regulatory basis for the incorporation of identity verification in a CBDC system using ZKPs, although it may be necessary for changes to applicable regulatory frameworks to be made in certain jurisdictions</p>

²⁴ **Note:** These solutions are illustrative examples proposed on the basis of the capabilities of ZKPs and their ability to achieve conceptually the objectives of the legal and regulatory requirements set out in the table, rather than being presented as examples that would necessarily satisfy the relevant requirements today, acknowledging that changes to the applicable existing legal and regulatory frameworks may be necessary in certain jurisdictions to facilitate this.

²⁵ **Note:** The way a user (the prover) accomplishes this is by first encoding the statement to be proved as a series of polynomials (the sum of a series of algebraic terms) that are identically zero if and only if the statement is true. This encoding – often called the “arithmetization” of the statement – is the step that makes zero-knowledge proofs possible. The user (the prover) then convinces the relevant person (the verifier) that the polynomials are indeed identically zero.

Jurisdiction	Existing Laws and Regulations	Description of Law / Rule	Example ZKP Solution(s) ²⁴
		for example, the source has been issued by a government authority and contains cryptographic security features.	to allow for this, or for further authoritative guidance to be issued in relation to the use of ZKP programs meeting certain criteria as a particular form of permitted electronic identification process to facilitate practical implementation.
Montenegro	<p>Entities regulated under the Money Laundering and Terrorism Financing Prevention Act (in Montenegrin: <i>Zakon o sprečavanju pranja, uvoza i finansiranja terorizma</i>) ("Official Gazette of Montenegro" nos. 110/2023 and 65/2024) ("MLPA") include, among others, financial institutions, payment service providers and electronic money institutions. These regulated entities are required to adhere to CDD measures (in Montenegrin: <i>niske poznavanja i praćenja poslovanja klijenta</i>) to, among other obligations, (i) verify the customer's identity, (ii) identify the ultimate beneficial owner, and (iii) collect and document information regarding the purpose of the business relationship and the relevant transaction.</p> <p>Considering the broad scope of the MLPA, institutions providing services related to CBDC are expected to fall within the definition of regulated entities and, as a result, will be subject to the provisions of this act.</p>	<p>CDD must be conducted in several circumstances, including: (i) when a regulated entity establishes a business relationship with a customer; (ii) when executing occasional transactions exceeding €15,000, either as a single transaction or a series of related transactions; (iii) for any occasional transaction of €1,000 or more that constitutes a transfer of funds under the MLPA; (iv) when there are doubts regarding the accuracy or adequacy of the customer's identity or the information obtained; and (v) when there are grounds to suspect that assets or transactions may be linked to money laundering or terrorist financing, irrespective of the transaction amount.</p> <p>The MLPA allows for the use of simplified CDD measures (in Montenegrin: <i>pojednostavljene niske poznavanja i praćenja poslovanja klijenta</i>) in situations where, based on a risk assessment, the risk of money laundering or terrorist financing is determined to be lower.</p> <p>Recent amendments of the MLPA introduced the possibility of customer identification electronically or via video-electronic identification. The Rulebook on Detailed Conditions, Methods of Implementation, and Training for Conducting Video-Electronic Identification of Customers (in Montenegrin: <i>Pravilnik o bližim uslovima, načinu sprovođenja i obuci za sprovođenje video-elektronske identifikacije klijenta</i>) ("Official Gazette of Montenegro", no. 22/2024) was published in March 2024, while other relevant bylaws and CBM guidance on implementation of this type of customer identification are still pending.</p>	
Thailand	Before engaging with any customer, financial service providers ("FSPs") must conduct CDD.	CDD must be carried out when a customer establishes a continuous or fixed-duration business relationship with an FSP. CDD is also required for specific occasional	

Jurisdiction	Existing Laws and Regulations	Description of Law / Rule	Example ZKP Solution(s) ²⁴
		<p>transactions, including (i) electronic money transfer exceeding THB 50,000 and other transactions that, either individually or cumulatively, exceed THB 100,000, (ii) when money laundering or terrorist financing activities are suspected, and (iii) when there are any doubts about the customer's identity information.</p> <p>During CDD, FSPs must verify the customer's identity, the beneficial owner of the transaction, and cross-check these identities against lists of specified persons under counter-terrorism financing laws. In conducting CDD/EDD, FSPs may obtain information of the customer from other reliable sources (e.g. database of the Department of Provincial Administration).</p> <p>FSPs must not engage in transactions with customers for whom they cannot obtain sufficient information for the CDD process, and they must consider reporting such transactions to the Anti-Money Laundering Office (AMLO).</p> <p>To improve the efficiency of compliance processes, relevant anti-money laundering regulations have been updated to allow for the use of electronic data obtained by the FSPs in accordance with the electronic transaction laws for KYC/CDD purposes.</p>	
	FPs must require that the identity of their customer or persons using their services be verified before allowing them to engage in certain transactions.	A KYC process is required when a customer establishes a continuous or fixed-duration business relationship with an FSP. The KYC process is also mandatory for specific occasional transactions, such as electronic money transfer exceeding THB 50,000 and other transactions that, either individually or cumulatively, exceed THB 100,000.	
Switzerland	Financial intermediaries ("FIs") under the Swiss Anti-Money Laundering Act ("AMLA") are required to verify the identity of their clients.	<p>FIs must verify the identity of the client upon:</p> <p>a) entering into a business relationship (e.g., opening an account);</p>	

Jurisdiction	Existing Laws and Regulations	Description of Law / Rule	Example ZKP Solution(s) ²⁴
Ongoing Transaction Monitoring			
United Kingdom	Ongoing transaction monitoring is a separate but related obligation from the requirement to apply CDD and EDD measures.	<p>Relevant persons will be required to conduct ongoing monitoring of the business relationship (including scrutinising transactions) throughout the course of the relationship, in order to ensure the continued legality of the relationship and assist law enforcement if required.</p> <p>The information that should be monitored and the frequency of the review will be ascertained in accordance with the determination of money laundering and terrorist financing risk and, in circumstances where EDD is required, firms will also need to conduct enhanced monitoring of the business relationship.</p>	<p>The CBDC system could be designed to require certain additional checks to be performed if specific objective criteria are met. Those criteria could, for example, be that an account has made numerous and consecutive under-threshold payments (with respect to the threshold for occasional transactions), or received multiple refunds or a single substantial refund, requiring higher levels of disclosure from the user.</p> <p>In these circumstances, access to the CBDC or the account might be suspended until the relevant person provides proof of further checks to the central bank (or a PIP, if incorporated into the CBDC model) by way of a specific ZKP proved by the user, such as proving in zero knowledge that multiple refunds to an account were in relation to legitimate transactions.</p> <p>A ZKP could be coded in relation to each trigger which requires proof of appropriate additional checks by the relevant person, which may include CDD or other objective checks relating to the nature of the transaction.</p>
Montenegro	Although ongoing transaction monitoring is closely linked to CDD and EDD measures, it constitutes a distinct obligation under the MLPA.	<p>Entities regulated under MLPA are obligated to continuously monitor identified risks of money laundering and terrorist financing. Specifically, these entities must regularly assess business relationships and transactions to ensure they are consistent with the customer's business profile, risk level, and operational activities.</p> <p>Additionally, the MLPA mandates that <u>CDD</u> and ongoing monitoring must be conducted periodically, even after the business relationship has been established, depending on the assessed risk of money laundering or terrorist financing. This obligation, for instance, arises when there is a change in certain circumstances of the customer.</p>	
Thailand	FSPs must continuously monitor the business relationship throughout the duration of such relationship. This monitoring ensures that activities remain consistent with the objectives of the business relationship, the customer's business information, the assessed risk level of the customer, and information regarding the sources of income, as well as other available customer information.	The information to be monitored and the frequency of reviews will depend on the risk level of the customer. In cases where EDD is required, FSPs must consider conducting enhanced transaction monitoring by increasing the frequency, procedures or methods for monitoring transactions and business relationships, as well as the frequency of verifying customer identification	

Launching on Ethereum

The issuance of at least part of a CBDC supply on Ethereum would have a transformative impact on the development of such CBDC and the issuing country:

- Interoperability with DeFi
- Decentralised, Secure and Cost-Effective Infrastructure
- Programmability and Smart Contracts
- Global Liquidity and Accessibility
- Transparency and Trust



Summary of Key Takeaways

- Existing CBDC designs point to **dystopian financial voyeurism** rather than **utopia**
- A **privacy-first CBDC** is possible on **Ethereum** today. By utilising **ZKPs**, we can design the future of money
- The **first nation** that executes this, will **reap** asymmetric economic and geopolitical rewards

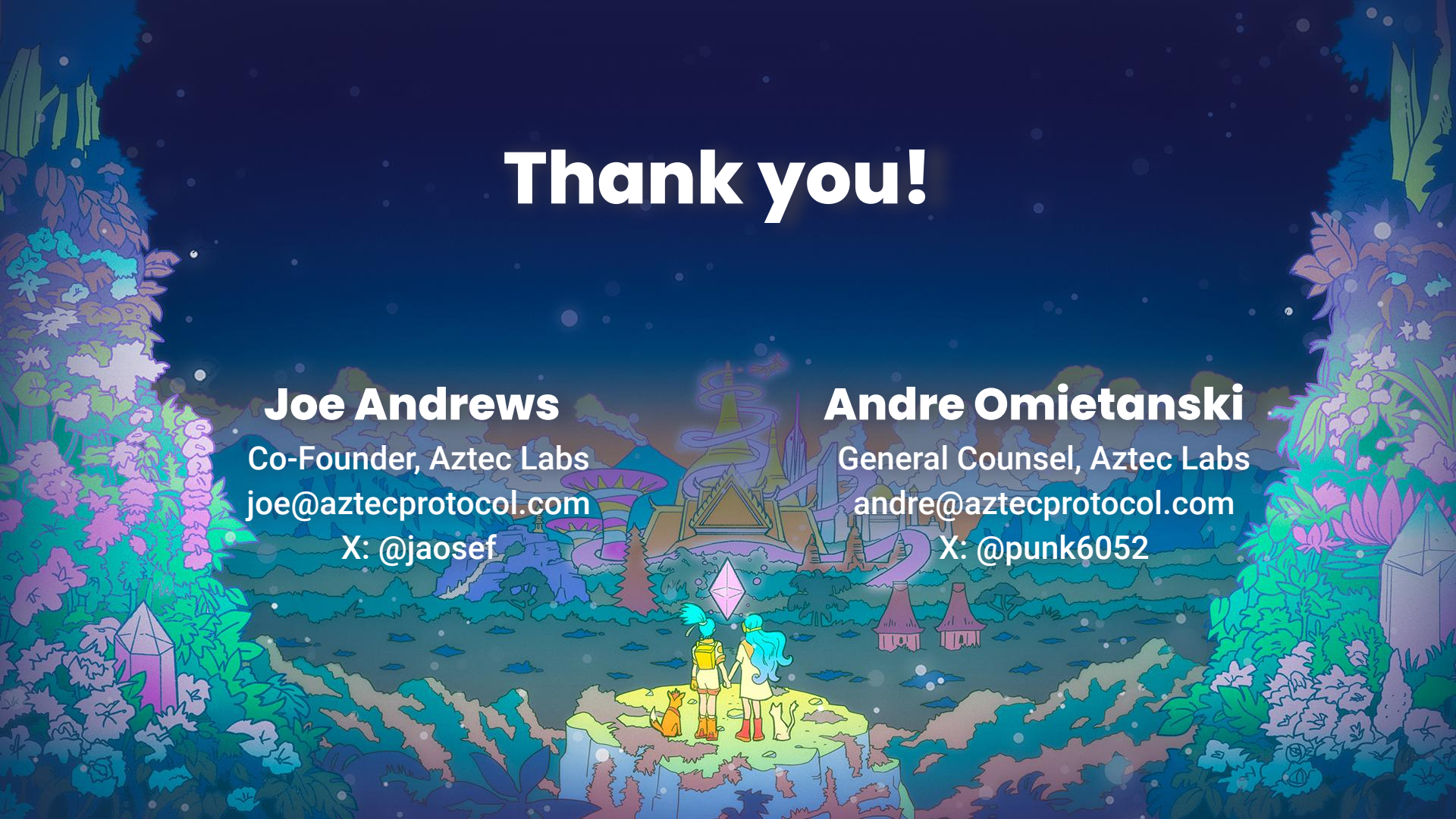
Thank you!

Joe Andrews

Co-Founder, Aztec Labs
joe@aztecprotocol.com
X: @jaosef

Andre Omietanski

General Counsel, Aztec Labs
andre@aztecprotocol.com
X: @punk6052



Comparison of ZKP Tooling



Let's Compare ZKP tooling

	Noir	Circom	ZoKrates	Halo2	Leo
Description	open-source, Rust-based DSL	novel DSL for defining arithmetic circuits	toolbox for zkSNARKs on Ethereum	proving system packaged as a Rust crate	Aleo programming language
Offline / DLT Interop	✓	✓	✓	✓	✗
Simple Syntax	✓	✗	✓	✗	✓
Multiple proving systems	✓	✓	✗	✗	✗

Noir advantages

Noir allows simple integration with new proving systems and is compatible with any SNARK/STARK-based proving system, which facilitates:

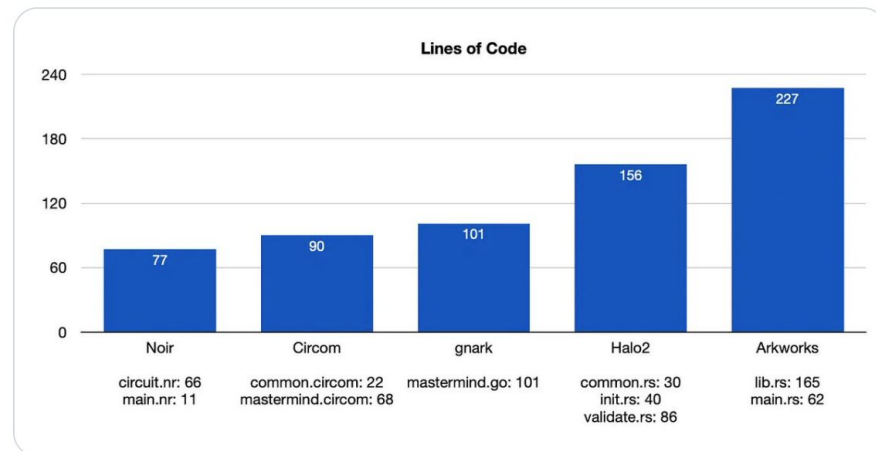
- **Better Scalability:** cryptographic advancements on proving technology, better user experience and lower energy costs
- **Increased Security:** flexibility to choose more secure implementations of proving technology
- **Lower Maintenance Costs:** minimal changes to the ZKP program source code needed to perform a proving system upgrade.



Veridise
@VeridiseInc

The lines of code varied greatly between different frameworks/languages. @NoirLang implementation was the most succinct with 77 lines of code, while Arkworks was nearly three times longer with 227 lines of code.

2/5



12:39 PM · Oct 15, 2024 · 1,586 Views