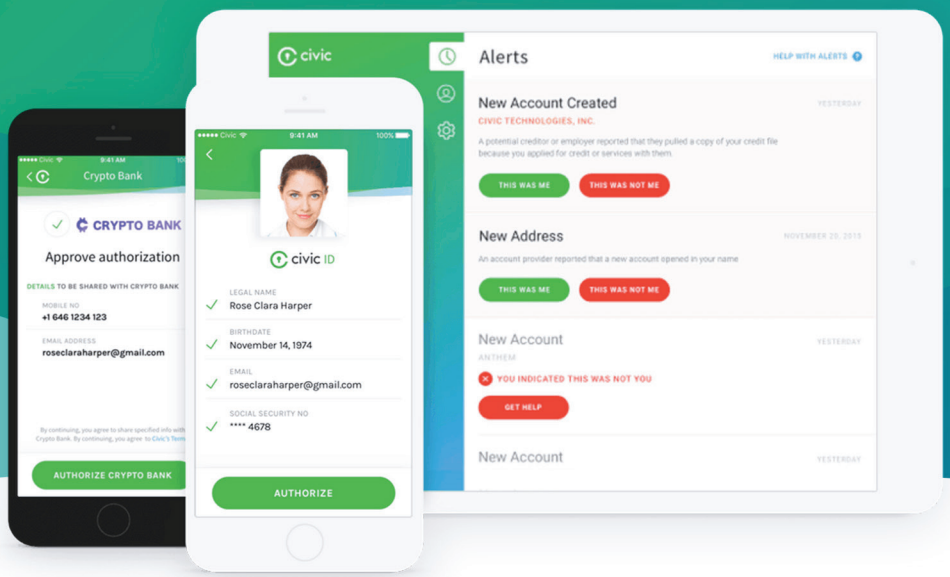
civic

WHITEPAPER



Contents

Abstract

The ability to store and share information digitally offers so many benefits that the digitization of data has become a consistent and growing trend. However, alongside the advantages of cost and convenience, a new set of concerns has developed. The ability to copy and share data has raised questions about the security of personal data. There have been countless high-profile hacks and leaks of personal information, as well as cases where unencrypted data has simply been lost or left vulnerable to theft.[1] Some services have been slow adopters of digital record-keeping, especially where data is particularly sensitive, such as in the government and healthcare sectors. The security risk in these sectors is higher, and the consequences potentially more severe, both for the individuals whose data is lost and for the organizations who have to deal with the legal and reputational implications.

"Switching to EHR (Electronic Health Records) implies a whole new set of responsibilities and challenges...With electronic records, there is a higher risk of compromising sensitive data because of the possibility of hacking attacks or unauthorized access..."

Center for Health Journalism[2]

Civic is building an ecosystem that is designed to facilitate on-demand, secure and low-cost access to identity verification ("IDV") services via the blockchain, such that background and personal information verification checks will no longer need to be undertaken from the ground up every time. Civic also intends to introduce a Civic token, or CVC, that participants in the ecosystem will use to transact in IDV-related services. Civic hopes this ecosystem can reduce the overall costs of IDV, remove inefficiencies, enhance security and privacy, greatly improve user experience and disrupt the current IDV supply chain.

Blockchain offers a compelling solution to the problem of combining accessibility with privacy and security. Records can be held securely, using end-to-end encryption, and yet openly authenticated, referenced and documented, so that data can still be trusted as reliable. This approach would not even have been possible just five years ago, but by using modern cryptographic techniques, coupled with the use of Blockchain technology and smart contracts, this ideal has now become a reality. This solves the problem of dealing with highly sensitive or classified information in a way that still enforces all the privacy and confidentiality rights that consumers and regulators expect.

1 http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
2 https://www.centerforhealthjournalism.org/2017/02/12/electronic-health-records-2017-adoption-and-barriers

Background

Financial Regulation

As the execution and administration of financial transactions has moved progressively into the electronic realm over the past 50 years, financial institutions, consumers, and law enforcement have been faced with new challenges. In the United States, the Bank Secrecy Act of 1970 (the "**BSA**") first required individuals and financial institutions to keep records that would enable authorities to detect and prevent money laundering by verifying the provenance of financial transactions. More extensive anti-money laundering ("**AML**") laws were introduced in the 1980s, followed in subsequent years by a series of laws designed to combat financial crime and certain activities associated with it, including drug trafficking and terrorism.

The trend was broadly followed in almost every country, with consumers and businesses growing accustomed to the need for financial institutions to conduct know your customer ("**KYC**") and IDV processes to verify the identity of a customer and the authenticity of the information provided by that customer when seeking access to a new product or service, for example, when opening a new account or applying for a loan.

Broader Market Context

Though largely born out of financial regulation, the trend quickly spilled over into other sectors, particularly in light of the rise in e-commerce and our increasingly digital lives. As a result of this trend towards ever-more extensive collection of personal information, the overall IDV sector is large and growing, as are security breaches and data theft.

- In 2016 alone, 15.4 million adults in the U.S. were victims of identity fraud, 16% more than in 2015. Victims suffered losses amounting to $16 billion, almost $1 billion more than 2015.[3]
- Globally, almost 1.1 billion identities were stolen in 2016 alone, nearly double the number stolen in 2015.[4]
- Personal Identity Information (or "PII") was the most common form of data stolen, accounting for 42.9% of data breaches, followed by Personal Financial Information ("PFI") at 39.2%, and Personal Health Information ("PHI") at 6.8%.
- In 2016, the services industry was most affected by data breaches, accounting for almost 45% of breaches, followed by the finance, insurance, and real estate sectors at 22%.
- The underground market price for an item of PII (e.g., a name, SSN, or date of birth) can be as little as $0.10 - $1.50. There is also a thriving market for scanned passports and other documents such as utility bills.

3 http://javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new
4 563.8m were stolen in 2015. See https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-APR24.pdf

Background

Frictions and inefficiencies in the IDV industry have both financial and social costs. Without proof of identity, an individual may be unable to exercise a range of legal rights, including the ability to vote, access to education or health care, and receiving social welfare.[5] As of January 2016, 1.5 billion people in the developing world lacked proof of legal identity, including 172 million children aged 4 and younger.[6]

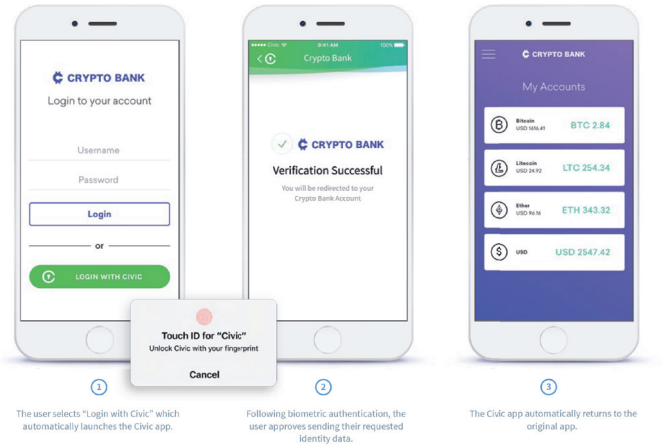
Due to a lack of identity documentation and the high costs of obtaining it, many individuals in the U.S. and globally are wholly or partially denied access to banking facilities, resulting in populations of "unbanked" or "underbanked" individuals. In the U.S., individuals with a limited financial history can face significant hurdles in gaining a foothold in traditional financial services. Minorities are disproportionately impacted by a lack of, or limited, financial history. For example, 29% of Hispanics and 25% of African Americans have been denied access to a service due to a mistaken or unverified identity, a significantly higher proportion than the corresponding figure for all U.S. consumers, at 19%.[7]

Approximately 9.0 million U.S. households, made up of 15.6 million adults and 7.6 million children, were unbanked in 2015… approximately 24.5 million U.S. households… were underbanked in 2015.' - FDIC [8]

Another widespread problem, particularly in many low-income countries, is that new births go unregistered because parents struggle to acquire the necessary documentation to have verified and recorded reliably by the relevant authorities.

As demonstrated above, there is a substantial and growing global market for IDV services. Due to the high costs and inefficiencies involved, and the clear and compelling interests at stake, the IDV industry presents a highly competitive landscape for newcomers who can offer innovative technical solutions. Driving down the costs of IDV-related services will increase access to, and thereby increase the size of the underlying market for, such services.

Simple Multi-factor Authentication



5 http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-4-25-web-English-final-ID4D-IdentificationPrinciples.pdf
6 ID4D Global Data Set http://data.worldbank.org/data-catalog/id4d-dataset
7 http://javelinstrategy.com/coverage-area/giving-consumers-identity-control
8 https://www.fdic.gov/householdsurvey/2015/2015execsumm.pdf

Background

The Costs of Data Acquisition

Not only are traditional IDV processes often seen as intrusive or time-consuming by consumers, but they come at a significant cost to the financial institutions required to carry them out as a matter of law and to avoid commercial losses due to fraud.

Due to the differences in regulation, the information required for different activities, and the varying efficiency of different institutions' IDV processes, it is impossible to derive a flat cost per customer. Anecdotally, it costs a financial institution such as a bank approximately $15-20 to on-board a single customer with full KYC, despite the process being similar (if not identical) for most organizations and being repeated every time the same customer attempts to access another product or service (e.g. to open another account or apply for a loan). These processes and their associated costs pose significant challenges for financial institutions.

'There's a high risk of getting KYC wrong… You need to carry out rigorous tests on major clients at least every 12 months, and that's very expensive. Many global banks are finding that their relationships with smaller regional banks and financial services firms are not worth the cost anymore, and they are exiting those relationships. Five years ago there was a strong correspondent banking network, and that is now being dismantled.'

Joachim von Hänisch, former director for Standard Chartered[9]

Moreover, the time taken to conduct a KYC audit is also increasing year-on-year, as more stringent regulations continue to be introduced. This has a detrimental effect on customer relations and invariably also impacts customer acquisition and conversion rates, since customers are forced to fill in lengthy application forms and provide extensive personal information. Additionally, institutions are being forced to collect sensitive data that they arguably do not need, such as a Social Security Number, in order to transact with a customer. As a result, the costs of KYC are spiraling for the financial industry, and are inevitably passed on to customers in one way or another.

"[G]lobal surveys revealed a single clear message: the costs and complexity of KYC are rising, and are having a negative impact on their businesses. While financial firms' average costs to meet their obligations are $60 million, some are spending up to $500 million on compliance with KYC and Customer Due Diligence (CDD)."[10]

Thomson Reuters

The same overheads and inefficiencies are present in other sectors where highly sensitive data may need to be verified, including in background checks for employment, working with vulnerable people, and driver checks for ridesharing. The sharing economy, which relies heavily on trust, grew an average of 32.4%[11] per annum from 2014 to 2016, and now comprises 27 million adults in the U.S.,[12] demonstrating the growth and scale driving demand for IDV services beyond the financial services sector.

9 http://www.bankingtech.com/195632/cost-of-kyc-too-high-says-swiss-start-up/
10 https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html
11 Compounded annual growth rate; in 2014 there were 15.4 million users
12 https://www.emarketer.com/Article/How-Popular-Sharing-Economy/1014135

Cultural factors

Compounding these data acquisition challenges are the cultural shifts that have taken place over recent decades. While it was once the norm to settle on a career early in life and to remain within the same organization for many years, if not permanently, it is now common for individuals to have many jobs and even different careers over the course of their lives. In the first five years after graduation, those who graduated between 2006 and 2010 had approximately 2.85 jobs, compared to just 1.6 jobs for those graduating between 1986 and 1990.[13]

A similar churn is seen in consumer markets, with customers more likely to switch banks, credit card companies, and energy or internet providers as new or more cost-efficient options become available. Greater transparency and access to information has led to greater competition in both the jobs and utilities markets, along with a growing demand for IDV, demonstrating that the existing rubber-stamp methods of bureaucracy that were established in the 1950s are no longer fit-for-purpose.

Internet-savvy Millennials and Generation Z will be good partners in this new IDV ecosystem. Millennials are often frustrated by the friction involved in the banking world, and they will happily swap providers to simply avoid it.[14] With this group estimated to spend over $10 trillion over their lifetimes,[15] organizations would be savvy to be more accommodating of seamless onboarding experiences. Generation Z, although not price-conscious, is reported to be financially cautious and supremely interested in value and authenticity, and may respect a more practical IDV ecosystem.[16]

Of course, the cultural revolution inherent in the digitization of information brings with it another broad trend and set of concerns in relation to personal privacy.

13 https://blog.linkedin.com/2016/04/12/will-this-year_s-college-grads-job-hop-more-than-previous-grads
14 https://techcrunch.com/2016/11/02/how-banks-can-tackle-millennial-skepticism/
15 http://adage.com/article/digitalnext/millennials-party-brand-terms/236444/
16 https://www.fastcompany.com/3062475/your-guide-to-generation-z-the-frugal-brand-wary-determined-anti-millen

Privacy and security

Privacy concerns arise whenever personal information is collected, processed, or stored. There have been many high-profile hacks, leaks, and thefts of personal data in recent years. The hack of Sony Pictures in November 2014 demonstrates the scale of the problem,[17] as well as the fact that hacks are no longer just perpetrated by individuals and small groups of hackers. Large amounts of employee data, including salary information and personnel records, as well as extensive email correspondence, movie scripts, and unreleased films were obtained.

In June 2015, the United States Office of Personnel Management admitted that its systems had been breached,[18] resulting in one of the largest ever breaches of government-held data, with the records of over 21 million people, including names, birth dates, addresses, Social Security Numbers, and even fingerprints, being stolen.

One of the unintended consequences of growing awareness and regulation around personal privacy is that organizations are now replicating the storage of personal data on an unprecedented scale,[19] and with varying levels of security. This approach has resulted in many high profile data breaches, costing billions of dollars in total. [20]

The IDV industry has grown up in response to this changing cultural and regulatory landscape concerning personal data, and a number of service providers now offer easy API access to multiple sources of consumer data for IDV purposes. The largely ad hoc approach has resulted in an outdated, costly, and inefficient system that serves neither customers nor the institutions tasked with undertaking IDV.

In many cases, companies are paying high fees to verify an individual who was already verified just hours ago by the same provider, but for a different company.

Any system that shares PII has to take personal privacy into account. With legacy KYC systems, maintaining the security of PII is a significant concern and regulations prevent such sharing from occurring in practice.[21] Some jurisdictions even have data localization laws that mandate the physical location of the servers storing this PII.[22]

A transformative solution would allow organizations to easily obtain proof that IDV information has been authenticated by a trusted institution without organizations sharing any PII between them, hence maintaining the user's privacy. Ideally the institution that initially paid a substantial cost to perform the initial IDV would be compensated with a small fee for providing this proof, thereby incentivizing both institutions to participate. This would lower the overall cost of KYC, thereby disrupting the entire IDV supply chain. Blockchain technology and in particular smart contract functionality is ideally suited to this application.

17 http://time.com/3639275/the-interview-sony-hack-north-korea/
18 https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/
19 https://digitalguardian.com/blog/27-data-security-experts-reveal-1-information-security-issue-most-companies-face-cloud
20 https://phys.org/news/2017-04-businesses-breaches.html#jCp
Gramm-Leach Bliley Act; Fair Credit Reporting Act -
21 https://www.ftc.gov
22 http://www.servers.global/meeting-the-challenge-of-data-localization-laws

Blockchain

The suite of technologies known as blockchain or distributed ledgers that have emerged in recent years offers a qualitatively different solution to the problems faced by organizations in the process of conducting IDV on their customers. In particular, smart contracts, or code executed on the blockchain, bring significant advantages over existing applications and frameworks of thinking. The following is an overview of those technologies. Open blockchains like Bitcoin have a number of properties that set them apart from the centralized databases typically used to record information. While they cannot be considered uniformly better or worse in general, their relative advantages include:

Low-cost

With no middlemen to impose uncompetitive fees and with a reward mechanism built into the protocol, transfers require only small transaction fees.

Immutability

The ledger is policed by every member of the network and its integrity checked and agreed by the network as a whole on an ongoing basis. Any changes that one or other party attempts to make to the blockchain are recognized and rejected by the majority.

Transparency

Everything that takes place on the ledger is visible to anyone. It is possible to see everything that has ever been recorded on the blockchain.

Irreversibility

Because the ledger is immutable, a transfer that has been accepted into the network cannot be reversed. With no trusted intermediary to act on behalf of users or control the movement of their funds, bitcoin transactions are immune to chargebacks and are like paying in physical cash, but online.

Pseudonymity

Blockchain addresses are effectively just strings of random characters that cannot intrinsically be associated with a specific individual. While it is easy for the owner to prove they control an address if they wish, and it is often possible to build up a picture of transaction relationships due to the transparent nature of the blockchain, the address itself does not contain the owner's PII. Assuming best practice, this enables a high degree of privacy when required.

Security

Because the blockchain is maintained by a large network of participants, no one actor can easily gain enough influence to submit a fraudulent transaction or successfully alter recorded data. Although possible in theory with enough resources, it would be prohibitively expensive in practice. The more valuable the token, the larger the network and the more resources would be required, meaning that the cost always outpaces the benefit.

Blockchain

Bitcoin

In its early years, blockchain was synonymous with bitcoin, the peer-to-peer currency launched in January of 2009 as blockchain's first application.[23] Bitcoin's innovation was solving the so-called 'double-spend' problem in online financial transfers: the issue that data is readily copied, and that it is therefore impossible to prevent the same funds from being sent to more than one recipient unless there is a trusted intermediary to keep accounts. This centralized model was used by all banks and payment processors who dealt with electronic funds transfers.

Such a centralized approach always involves trust, because there must be an authority whose job it is to organize the transfer of money from one account to another. In the physical world, money is handed over directly from person to person. Online, however, there must be intermediaries. Rather than transferring funds from their account directly to the recipient, the user instructs the intermediary to move funds on the user's behalf.

This centralized system has a number of potential drawbacks. The trusted intermediary may prove untrustworthy, has control over the end user's funds, and can unilaterally block or reverse transactions. The centralized nature of online banking and other online money transfer protocols leaves users vulnerable to intervention by these gatekeepers and comes with security risks, because there is always a single point of failure. Centralized databases can be hacked, and their administrators compromised or coerced by a range of actors.

Bitcoin's innovation was a system that allowed peer-to-peer online transfers of value for the first time ever. No trusted intermediary was necessary, thereby mitigating the single point of failure problem. Instead of the centralized accounting used by traditional payment processors, the blockchain is a shared ledger. While centralized systems are restricted and can only be accessed by trusted intermediaries, anyone can access the decentralized bitcoin blockchain directly. Similarly, it is maintained by the whole network, rather than security being tasked to the trusted authority.

This innovation was achieved by contriving a system in which it is difficult to add transactions to the ledger, but easy for anyone to check whether they are valid - that is, if the funds being transferred really belong to the transferor in the first place. The difficulty (from the standpoint of computational resources) means that there is a cost involved in attempting to process transactions and rewards (in the form of new bitcoins and transaction fees) for doing so legitimately.

Fraudulent transactions are quickly identified and discarded from the ledger. Attempting to add a fraudulent transaction is costly,[24] entails foregoing the financial incentives for acting honestly, and is highly unlikely to succeed in the first place because no single party in the overall network has more than a small proportion of the overall 'authority' to validate transactions. In practice, it is simpler and more profitable to act honestly and so there is little point attempting to double-spend funds.

Smart contracts

The bitcoin blockchain was designed for peer-to-peer online transfers of value, effectively acting as digital cash. It achieves this not by actually moving money from one address to another, but by maintaining and updating the ledger to reflect how much money is registered to each address. The same approach to recording data transparently, securely, and immutably by consensus of the entire network can be extended to many other applications (since the financial value in the bitcoin network is simply information about who owns what). For example, messages can be stored on the blockchain, either encrypted or in plain text. Additionally, secondary tokens representing assets, such as shares in a business, securities, commodities, and other currencies, can be secured on the original blockchain.

It is also possible to create a system that takes a similar approach to the execution of computer code. Smart contracts are code that is executed on the blockchain. Software is typically run on a single computer or centralized server, just as online money transfers are typically centralized, for the reasons explained above. However, it is now possible to extend the blockchain's functionality to software, creating decentralized applications or "**dApps**." Once uploaded to the blockchain, these are stored immutably and run when the required conditions are met.

The most famous smart contracts platform is Ethereum, which was launched in 2016 after a highly successful crowdfund in the summer of 2015.[25] Ethereum, which has become extremely well-known in the cryptocurrency world due to its soaring value, as well as some high-profile problems including The DAO and the ensuing controversial hard fork,[26] is a completely new platform, coded from scratch. Although other smart contracts and dApps platforms have been created, including Lisk,[27] none have had the popularity and prominence of Ethereum.

Blockchain

Rootstock

Early versions of the bitcoin software included more extensive functionality than simple payment, and the scripting language allowed for more complex operations, until these were removed in 2010 due to the potential vulnerabilities they introduced.

Since then, there have been numerous initiatives to bring '2.0' functionality to the bitcoin blockchain in various ways. Rather than these features being included in the core, they have been created as platforms operating as a layer built on top of the bitcoin network, for reasons that include:

Security

The bitcoin network is the largest and most secure cryptocurrency network. No other platform has the hashrate or history of bitcoin.

Popularity

Bitcoin has more users and community members than any other platform by an order of magnitude over competing networks.

Awareness

Bitcoin is better known than newer platforms that have not yet established the same profile.

Rootstock (or "RSK"), one such layer on top of the bitcoin network, is a secure and scalable smart contracts solution that supports the existing bitcoin ecosystem.

The bitcoin network requires that transaction fees are paid in the native currency of bitcoin (or "BTC"), including any smart contracts or other '2.0' activity secured on the bitcoin blockchain. Similarly, the Ethereum network requires the use of its native currency, Ethereum (or "ETH") as gas. Fees for executing smart contracts on Rootstock, however, are paid in smart BTC, which has a one-to-one peg with BTC.

RSK also allows for the creation of separate blockchain tokens. As noted above, these tokens are digital assets, cryptographically secured upon the blockchain, which can represent whatever the issuer wants and is prepared to back (if necessary), and which can play whatever role in the ecosystem that its rule-set determines. These tokens can be transferred on a peer-to-peer basis for a minimal transaction fee, just like native tokens (e.g., BTC in the bitcoin protocol and ETH on Ethereum). They can be incorporated into smart contracts as an integral part of the ecosystem.

'As RSK does not mint, nor has pre-mined coins, then it has no speculative value and does not compete with Bitcoin.' [29]

'RSK is the first open-source smart contract platform with a 2-way peg to Bitcoin that also rewards the Bitcoin miners via merge-mining, allowing them to actively participate in the Smart Contract revolution. RSK goal is to add value and functionality to the Bitcoin ecosystem by enabling smart-contracts, near instant payments and higher-scalability.' [28]

23 Bitcoin was first articulated in 2008, on the Cryptography Mailing List, see http://www.metzdowd.com/mailman/listinfo/cryptography and in a white paper published by Satoshi Nakamoto, see https://bitcoin.org/bitcoin.pdf. Satoshi Nakamoto is widely accepted to be a pseudonym for an individual or group of people who created bitcoin. Despite numerous theories and news headlines to the contrary, Nakamoto's true identity remains unknown to the public.

24 This is often expressed in terms of a '51% attack'. That is, an attacker would require over half of the computational resources of the entire bitcoin network in order to create a fraudulent transaction.

25 Ethereum's crowdfund collected 30,000 BTC, then worth around $16 million. At the time of writing, the platform has a market cap of over $17 billion.

26 The DAO (Distributed Autonomous Organization) took a smart contracts approach to investment. Decisions about which projects to fund were intended to be taken collectively by investors, and funds dispersed automatically. However, a hacker was able to exploit a loophole in The DAO's smart contracts and drain tens of millions of dollars from the pool of invested funds.

27 Lisk grossed $5.5 million in its crowdsale in 2016.

28 http://www.rsk.co/ for more information

29 See http://www.rsk.co/ for more information

Product Description

The IDV industry as it presently exists relies on each institution obtaining and keeping records of clients' PII. As discussed, there are both significant overheads and security risks to this approach. Civic, already a trusted player in the IDV space, intends to leverage the above-described innovations in blockchain and smart contracts technologies to build on its success to date to introduce a "2.0" version of its own ecosystem. The key innovation enabled by this blockchain-based approach is the efficient and secure verification of previously-audited PII by third parties without the need to share the underlying PII between those parties, retaining User control over the data.

The following is a description of Civic's existing identity products and services, which will act as foundational elements of, and reference implementation for, the new product that Civic now intends to introduce.

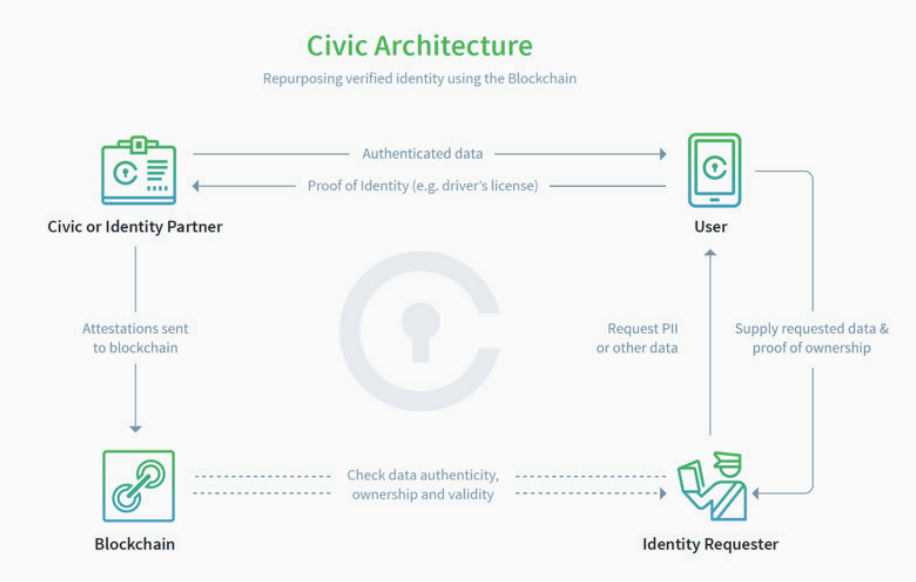
Civic's existing identity products and services

At present, Civic provides a digital identity platform known as the Civic Secure Identity Platform (the "**SIP**"), which individuals can access by downloading the Civic Secure Identity App (the "**Civic App**"), setting up their digital identity on the their device, and verifying their identity to become a Civic user. The Civic App stores a user's PII securely on the user's phone using high-level encryption and biometric locks (such as a fingerprint ID). By keeping this data in the user's control, the Civic App makes it harder for hackers and other malicious groups to gain access to a user's information.

Through its decentralized architecture with the blockchain and biometrics on the mobile device, the Civic App enables users to share and manage their fully verified identity data. Initially the user captures their PII as requested into the Civic App which then goes through a thorough verification process by Civic. Once fully verified, the attestations to this data are written by Civic to the blockchain which can then be used by recipients of the data to verify the PII's authenticity and ownership.

Civic's identity partners can request a user's information through custom QR codes to be scanned by the user with the Civic App. Once a user has unlocked the Civic App with his or her biometrics, the user can scan these codes, review exactly which information is being requested, and choose whether to approve or deny the request.

Thus, the SIP allows for a voluntary information exchange between the user and the identity requestor, according to requirements set by the requestor. In this way, the SIP allows for real-time authentication of identity data verified by Civic or a Civic identity partner and secure sharing of that data.



Civic's planned identity ecosystem

In its next phase of development, facilitated by a token sale, Civic intends to go beyond its existing products and services to develop a fully decentralized Civic ecosystem for IDV services (the "**Ecosystem**"). The Ecosystem will consist of three new components: (1) a variety of smart contracts; (2) an indigenous utility token known as the Civic token or "**CVC**"; and (3) new software applications, introduced by Civic and others, that allow participants to interact within the Ecosystem.

Civic's Ecosystem will be designed to incentivize participation by trustworthy IDV providers known as "**Validators**," who may include financial institutions, government entities, and utility companies, among others.[30] Just as Civic currently validates the identity information of users of the Civic App, Validators will be able to verify the identity of an individual or business, known as a "**User,**" and 'stamp' this approval on the blockchain in the form of a record known as an "**attestation**." Such attestation is effectively the hash of an underlying element of PII, plus certain metadata relating to that hashed element (as further described below). Parties known as "**Service Providers**" who are seeking to verify the same information about a given User, and who may include other Validators, would no longer need to independently verify that information and could instead leverage the work already performed by trusted Validators.

Civic intends for this kind of robust and decentralized IDV Ecosystem to emerge through the use of smart contracts, which will ideally be built on RSK to give the Ecosystem the same security as the bitcoin network, while enabling smart contracts, a high degree of scalability, and near instant transactions.[31] The ecosystem is intended to ensure that Users remain in complete control over their PII, by requiring the User's consent before the IDV transaction between the Validator and the Service Provider can be completed.

The smart contracts will enable Validators to offer their attestations for sale to Service Providers (subject to obtaining the User's approval), and Service Providers to determine which Validators are offering attestations and at what price. Each Validator can publish a price at which it is prepared to sell its attestation of a User's PII. Prices can be updated by Validators at any time, but any such updates will take a minimum of the time taken for the validation of a transaction on Rootstock (typically about 10 seconds) to appear. Prices can be offered for existing attestations and new attestations to be made.

Once the Validator, Service Provider and User all sign-off on the transaction via the smart contract system, the Service Provider will pay the Validator in CVC. The smart contract will then allocate a set portion of the paid CVC to the User to incentivize User participation in the Ecosystem. Users will be able to use their CVC to purchase identity-related products and services from Civic, including some or all of the products and services currently available (as described below). Civic envisions that other service providers will also make their identity-related products and services available through the Ecosystem, and that Users will use their CVC to obtain those third-party offerings.

In addition to the RSK or other smart contracts, the Civic ecosystem will also include Civic's existing Civic App (through which Users will share their PII with chosen Validators and consent to transactions by interacting with the smart contracts), and additional software to be developed by Civic (and others) through which Validators and Service Providers will themselves be able to interact with the smart contracts. While Civic intends to develop the initial smart contracts and software, the Ecosystem is intentionally open to third-party providers.

The Users will store their data on a personal device using the Civic App,[32] and optionally backed up to a personal account on a cloud-based or distributed storage platform.[33] Civic will not handle the storage of the data in this form, not least due to the regulatory implications of being responsible for this information; different jurisdictions have varying approaches to data storage, and some require that PII is stored in the same country as the User (where storage is dealt with by a third party such as a financial institution). For Civic's contemplated Ecosystem, it is enough that Validators have access to the data they require, with the permission of the User. This approach has the additional benefit of decentralizing data storage, shifting the responsibility onto the User who has to prove ownership, which is ultimately through each User's device.[34]

30 In the financial services sector, this typically means banks and other financial organizations carrying out Know Your Customer ('KYC') processes, but Identity Verification is a broader trend that takes many forms, according to need. These entities will be able to verify the identity of an individual or business (a 'User') and 'stamp' this approval on a blockchain. Through the use of smart contracts, built on RSK (Rootstock) and the bitcoin blockchain, a robust and decentralized identity verification ecosystem will emerge, in which PII and other sensitive data can be exchanged securely and privately. 31 Subject to the availability of all necessary features on the Rootstock platform. 32 Or any subsequently developed app available in the Ecosystem for this purpose. 33 This will be subject to the availability of the cloud services and to the requirements of the country laws applicable to the Users 34 Depending on the regulatory environment for Users, there is also the option of storing data using InterPlanetary File System ("IPFS"), which will be explored in future iterations of the project and has many benefits outside of just backing up the data. This is however outside the scope of this paper. IPFS is a protocol designed to create a permanent and decentralized method of storing and sharing files. It is a content-addressable, peer-to-peer hypermedia distribution protocol. Nodes in the IPFS network form a distributed file system, see https://en.wikipedia.org/wiki/InterPlanetary_File_System.

Civic's planned identity ecosystem

The mechanics of attestation

The PII that is stored on a User's device can be attested to by Validators. The user can share the PII and any attestations with any other participants in the Ecosystem that trust a given Validator. An attestation gives a participant confidence in the adequacy of the process used to verify specific fields of PII with potentially greater efficiency and lower costs.

A User's PII is structured in a hierarchy, with elements like SSN, address, city, country, and date of birth, among others. This data follows a defined model and Civic's intention is to follow industry standards where they exist, and even contribute to further standardization in the industry.

The provability of an attestation is achieved by organizing the data into a Merkle tree,[35] where each node representing an element of PII (e.g., name) contains a hash of its content and a hash of the hashes of its child nodes (e.g., first name and last name). This results in a "**root hash**" (also known as the Merkle Root) that can be used as a fingerprint for the data being attested to. This root hash is recorded in the blockchain and signed by the Validator making the attestation as to that specific PII. Arbitrary numbers known as "nonces" are used to randomize hashes on structured data that have a relatively small universe of possible values to minimize the risk of any hash being reversed. Should the User not wish to reveal all of the underlying PII that was attested to, portions of the Merkle tree can selectively be revealed, and hashes provided for any elements the User prefers not to reveal.

This structure has two advantages: (1) it enhances User control by allowing the User to selectively reveal pieces of personal information in different circumstances; and (2) promotes security by using properties of the blockchain to prove that the data have not been tampered with after an attestation has been made.

The only way for a participant to reproduce the hash is to create it from the original data. This allows the User to share the data with another participant in the Ecosystem and to prove that it is the same data that was previously attested to by the Validator. Should the Validator revoke its attestation for any reason, this can be reflected on the associated blockchain transaction, but the details of the attestation can never otherwise be changed. The blockchain on which these transactions are recorded is currently the bitcoin blockchain, because of its proven integrity and wide adoption, but the same design could equally be used on any other blockchain platform.

The method used for recording these attestations is to create derived addresses where small amounts of cryptocurrency can be spent. The root hash is converted to a valid blockchain address using the additive property of Elliptic Curve Cryptography (ECC):

$$k_{priv} + h = k_{attest}$$

designed in a way that makes it unfeasible to determine the User and Validator associated with the address. This is essential to protecting the privacy of participants.

Allowing entities to sell their attestations but not the underlying data, would turn the IDV market on its head. Entities who have invested heavily in IDV and KYC processes and built large, verified customer bases would be able to transform these once costly activities (i.e., customer IDV and KYC) into revenue generators, all without selling or transferring any customer PII.

Through this design, Civic aims to address the needs of:

Service Providers, by lowering their costs of verifying the identity of an individual or entity from scratch.

Validators, by enabling them to recoup the costs of the identity verifications they perform and the attestations they provide.

Users, by granting them rights to view or amend, and control who has access to, their data directly. The CVC that Users receive for participation will be reusable within the Civic ecosystem to obtain other identity-related services from Civic or ecosystem participants.

Governments, by allowing departments or agencies to rely upon each other's attestations of identity with the express consent of a User.

35 https://en.wikipedia.org/wiki/Merkle_tree

Ecosystem token (CVC)

Civic intends to introduce a Civic token, or CVC, which will be used as a form of settlement between participants to an identity-related transaction within the Ecosystem. The CVC paid in a transaction is distributed to the Validator and the User as a reward for sharing information. The proportion in which they share the CVC is defined by the smart contract and can be adjusted by consensus of the Ecosystem participants.

CVC will also provide a means to incentivize all participants, including Users, to contribute to the Ecosystem. Moreover, Civic anticipates that the Ecosystem will develop such that Civic and third-party providers of identity-related products and services will offer those products and services to Ecosystem participants in exchange for CVC.

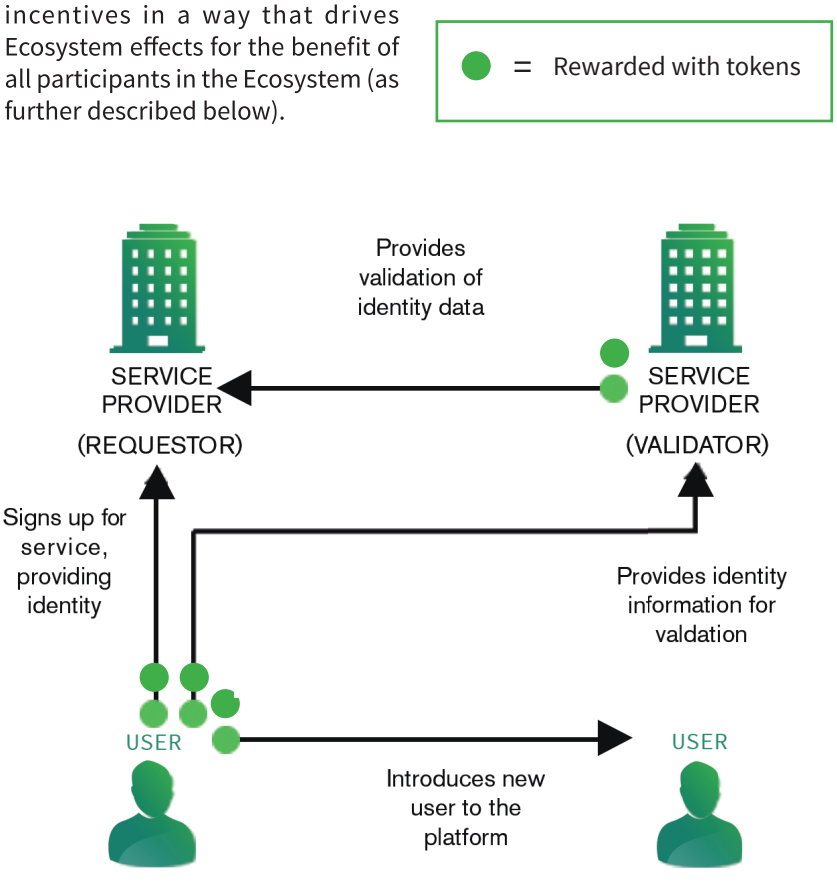
Civic Users who own CVC may be able to use their CVC to purchase existing services directly from Civic. Civic may also build additional identity-focused services that can be exchanged for tokens, including:

- Services to run personal background checks;
- Blockchain notary services which would allow identity and document authenticity to be provable;
- Dark web monitoring and searches;
- Access to individual credit reports; and
- Peer-to-peer identity services.

A fixed supply of CVC will be created during a token sale, with no mechanism for supply to be increased. A ledger will be maintained for CVC[36] and will follow the ERC20 standard. The ledger will provide a secure mechanism for owners to transfer CVC to other participants.

Using a dedicated token, the CVC, to facilitate transactions in the Civic Ecosystem provides a number of advantages over the use of existing tokens, including that:

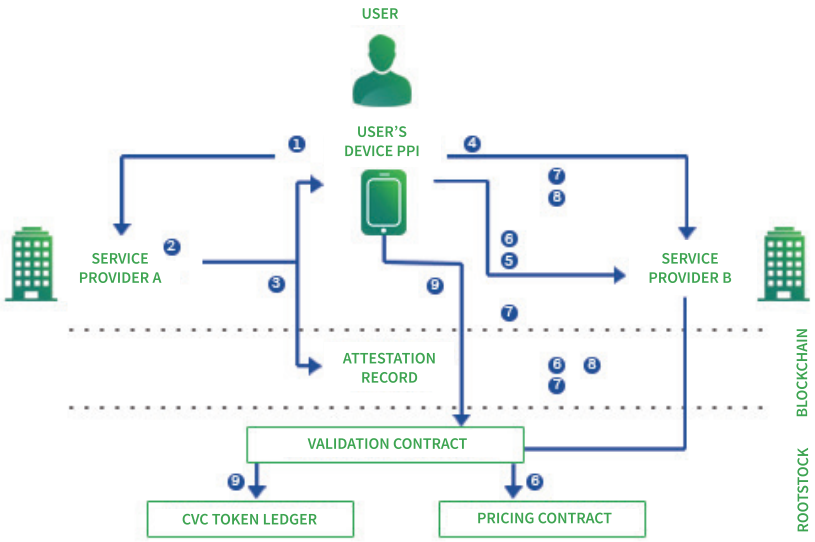
- It can be used across any number of jurisdictions, retaining a single uniform method of settlement;
- Using a blockchain-based token makes it possible to perform settlements automatically and irrefutably within a smart contract;
- Having a unique, specialized token for accessing identity services provides stability and shields the Ecosystem from extraneous considerations that can make other cryptocurrencies volatile;
- It makes it possible to manage incentives in a way that drives Ecosystem effects for the benefit of all participants in the Ecosystem (as further described below).



36 Ideally on Rootstock, subject to the availability of all necessary features on the Rootstock platform per footnote

A market for efficient attestation of User data

Building on the distributed data model, the attestation model, and the CVC token, Civic will provide a platform for attestations to be shared between IDV service providers in order to radically reduce costs, compensate participants in the Ecosystem, and keep Users in full control of their data. The following diagram and process map gives an example of an initial attestation by a Validator, in this case Service Provider A, and the purchase of this attestation by a second service provider, Service Provider B, who is seeking to rely upon Service Provider A's attestation. For purposes of this reference implementation, we assume that the User is using the Civic App.37



1 The User applies for a product or service from Service Provider A and sends them the required PII from the Civic App.

2 Service Provider A verifies the User's PII using its existing verification methods.

3 By reference to the PII stored on the User's device, Service Provider A calculates the hashes of that PII and records an attestation to that PII on the blockchain. The attestation may also include supporting metadata, such as its verification level, details related to Service Provider A's process of verification, or any applicable industry standards (e.g., NIST, FIPS, or PIV standards). The blockchain transaction details of this attestation are then provided to the User.

4 At a later date, the User applies for a product or service from Service Provider B.

5 Service Provider B requests access to all or certain portions of PII from the User, including the rules and requirements around what data Service Provider B is willing to accept. The Civic App will then determine whether these requirements are met.

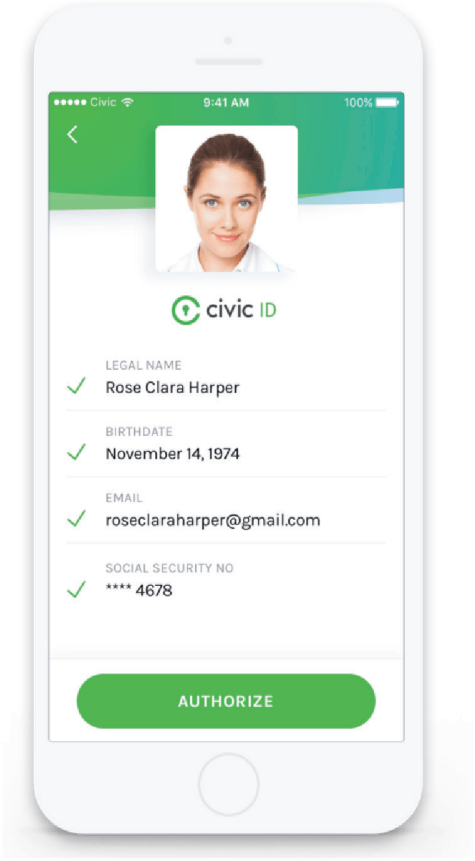
6 Assuming the User has and is willing to share the requested data, Service Provider B and the User agree on a mutually acceptable Validator that has previously attested to the data and the rules and requirements around that data. In this case, we will assume that the mutually acceptable Validator is Service Provider A, who offers a price (in CVC) for its attestation, and that Service Provider B accepts that price. 38

7 The User then sends Service Provider B an outline of the types of data that are in the attestation by Service Provider A, as well as the necessary information to enable Service Provider B to locate and view the blockchain transaction details relating to Service Provider A's attestation on the blockchain. Service Provider B would then be able to recreate the hashes for that PII and compare them to the transaction on the blockchain, thus confirming the availability of the requested data. If Service Provider B is satisfied with the resulting hashes, Service Provider B can then purchase the attestation, and pay the amount of CVC corresponding to the price of that attestation, into escrow (via the smart contract).

8 Once Service Provider B has paid CVC into escrow, the User, through his/her Civic App,39 can send Service Provider B the PII with the requested content in plain text.

9 To complete the transaction, the User triggers the release of CVC from escrow, which is shared between the User and Service Provider A (the original Validator) at a ratio defined by the smart contract.

Data backup vs. decentralized data source



To maintain the highest level of privacy, PII must be controlled by the User at all times and be stored locally on their device. This physical separation creates a particularly difficult path to data theft as individual devices need to be targeted on a person by person basis in order to steal PII, and prevents the types of mass data breaches to which we have become accustomed. It also allows early adopters of the Civic Ecosystem to store a much more limited amount of sensitive data and still have a high level of certainty about the authenticity of the actors they are dealing with. Moreover, when a User's PII is shared with other parties, it is always shared directly by the User via a peer-to-peer protocol for this sharing, promoting compliance with privacy and data protection regulations in even the strictest jurisdictions.[40]

However, as adoption grows, the value of specific identity attributes on the black market should decline as entities move away from mere data points being used to transact and move towards verification of ownership before a transaction takes place. For example, credit card details have black market value because transactions can take place simply with knowledge of the data. Once a credit card number has to be presented with blockchain-based proof that the user indeed owns that number, the value of simply having those details progressively deteriorates with adoption of the Ecosystem.

At this juncture it is less important where the data is stored and rather that the ownership proofs are protected. It currently makes sense for distributed data models to be easily adopted in a more sensitive environment. The benefit here is that large organizations can leverage the efficiencies of permissioned distributed data storage for things like PII, which has the added benefit of always having the latest data that the User has permissioned the organization to access.[41]

40 Once supplied to another party, the use and storage of User PII by that party is governed by the specific contractual agreement (e.g., applicable terms and conditions or terms of service) by which the User provides his/her PII, and not by the Civic Ecosystem.

41 If this is the case, IPFS can become the data storage layer for identity data, and not just the backup for the users device. See supra note 39.

Conclusion

Civic is proposing the creation of a new Ecosystem that will improve efficiencies and reduce the costs of the existing IDV industry. Organizations that have invested heavily in IDV services will have the opportunity to monetize their processes both inside and outside their core business areas. These reduced costs and ease of access to verifiable Users will likely encourage organizations to improve their processes to help combat fraud and deliver better services.

For end Users, the longer term impact of this disruption should be greater privacy and control of their PII and other sensitive data. Access to services will be faster and more seamless and Users will be able trust more readily the services they are using. Simply through participation in the Ecosystem Users will earn tokens which will allow them access to a vast array of useful services that will ultimately help them protect and control their identity.

At scale it will no longer be enough to simply have PII to commit identity fraud, but proof of data ownership will be required as well. Organizations will be able to trust Users without the need to retrieve and store unnecessary data. This new paradigm will ultimately reduce the risk of data breaches and dramatically increase the cost of committing fraud.

For more information, visit www.civic.com, or email tokensale@civic.com.