accenture

Strategy | Consulting | Digital | Technology | Operations

EDITING THE UNEDITABLE BLOCKCHAIN

Why distributed ledger technology must adapt to an imperfect world

High performance. Delivered.

"Idealism is fine, but as it approaches reality, the costs become prohibitive."

William F. Buckley, Jr.

It's hard to believe today, with the annual economic benefit of the commercial Internet valued at $1.5 trillion,[1] that there was ever anyone opposed to internet commerce.

But some of the internet's earliest pioneers were die-hard purists, who felt that the "crassness of commerce" would compromise this "unique bastion of cooperation, sharing, information exchange and helpfulness."

These outspoken web purists didn't want commerce to impose itself on the nascent Internet. Little could they imagine that by 2016 ecommerce would be welcomed by more than two billion people every day.

Right now, the same basic story could be true for blockchain, a technology that stands on the cusp of broad acceptance and adoption. Blockchain could literally change the world of commerce in the way the Internet has done. But for that to happen, crucial debates within the inner circle of this technology need to be addressed, and the voices of pragmatism and practical ingenuity must be heard.

This paper looks at why distributed ledger technology—applied to enterprise and permissioned networks—will need to evolve to adapt to an imperfect world where human error, laws and mischief will require more flexibility. It looks at the mixed blessing of the indelible ledger in light of Europe's "right to be forgotten" laws, recent high-profile cybercurrency thefts and the age-old "fat finger" errors that have brought exponential harm to financial services.

If the industry is to embrace a new technology, it cannot be one in which human errors are immutable. As a solution for enabling permissioned networks to succeed, we propose an editable blockchain, which was developed by Accenture with leading academics.

Immutability

Immutability is currently one of the major issues at the heart of the blockchain conundrum. Blockchains are an "append-only" system, which means you can only add data to it, you cannot take it away. That means that all the information on a blockchain is essentially permanent and immutable. For example, each of the approximately 160 million transactions that have occurred on the Bitcoin blockchain since the currency launched in 2009 will remain on that ledger for as long as the currency exists.[2]

On one side of the debate are those who argue that immutability is precisely what makes the blockchain such a significant innovation. On the other side are pragmatists who increasingly see where and how in enterprise environments immutability may prohibit adoption due to human error, mischief and privacy laws.

Meanwhile, pressure is growing within the circles that are developing this technology to clarify a viable path forward. The World Economic Forum recently noted that success in this area will require "deep collaboration between incumbents, innovators and regulators."[3]

Mischief and Human Error

In 2013 it was discovered that illegal pornography had been embedded as metadata on Bitcoin's immutable blockchain. Three years later it is still there for all to see. As is a pixelated likeness of former Federal Reserve Chairman Ben Bernanke,[4] courtesy of another blockchain prankster.

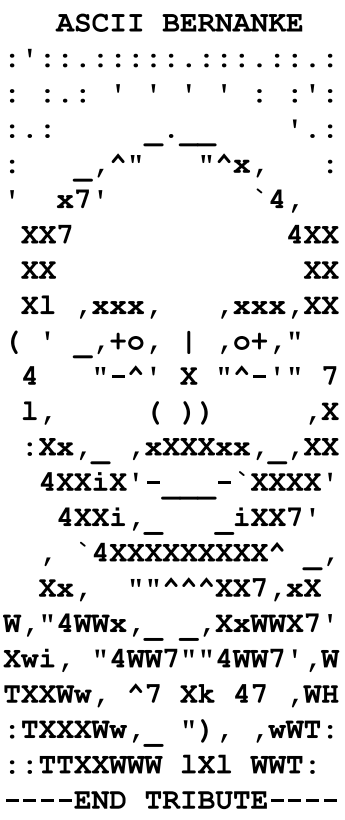
Even more distressing for the national security community, over 250,000 classified diplomatic cables released by Wikileaks in 2010 were immortalized on blockchain in a 2.5 megabyte file embedded across 130 separate bitcoin transactions.

This kind of mischief, some harmless and some potentially criminal, could be solved through a range of options. But for enterprise systems—often heavily regulated—and for used in permissioned environments with designated adminstrators it points to larger practical problems with the immutable blockchain, particularly in the traditional capital markets industry.

Compliance and risk managers are obligated to monitor and manage communications between trading counterparties across multiple messaging channels and to edit or even censor conduct where necessary.

If these channels and messaging protocols like FIX or SWIFT — which hold free-form fields — are tied to an immutable ledger, companies could struggle to redact prohibited messages or prevent rogue traders from leaking sensitive information onto a permanent ledger.

Also consider the innocent but not uncommon "wrong counterparty / wrong book" problem — trades that are mistakenly booked to the wrong trading account or apply the wrong symbols, marks or maturity. In the same way that banks need to ensure confidentiality between counterparties on correctly booked trades they also need to protect confidentiality when errors occur. If those errors cannot be corrected on a blockchain system, it becomes possible for one market participant to decipher another's trading strategy.



Source: money.cnn.com

Smart Contracts

Blockchain technology "has the potential to 'live-up to the hype' and reshape financial services," according to a recent report by the World Economic forum citing numerous use cases that involve smart contracts. Smart contracts are essentially a sequence of instructions residing on the blockchain that automatically execute according to those instructions when pre-agreed events take place. According to Autonomous Research, they could save investment banks approximately $16 billion in clearing and settlement costs by 2020.[5]

But what happens when there is a bug or weakness in the smart contract code? What happens when the complexity of translating real contracts, which by design are not always clear, into executable code leads to failures?

On an immutable blockchain that problem is resolved by adding an updated contract to the chain, which applies to all future transactions. But any exploitation of loopholes before then remains on the ledger, even when counterparties agree that it should be changed universally.

This situation occurred when hackers stole more than $60 million of "ether", a digital currency, from the high profile start-up fund known as The DAO. The theft was made possible by a glitch largely attributable to a human error in the programming of The DAO's smart contract code. Before that theft, the ether cybercurrency was generating a great deal of excitement as a way to apply smart contracts to blockchain systems.

But even the smartest contracts will be susceptible to human error. On an immutable blockchain, "patches" to a contract require the addition of new contracts to the chain. That is difficult to scale — especially as contracts become larger and more complex. Having the ability to edit, rather than append, smart contracts would preserve time and resources.

Even the smartest contracts are susceptible to human error.

If the financial services industry is to embrace a new technology for enterprise and permissioned networks, it cannot be one in which human errors are absolutely immutable.

Improving Through Failure?

The unknown culprit in The DAO theft has argued through their attorney that he or she is entitled to the assets under the terms of the erroneous code itself. And a surprising number of blockchain purists agree. One developer, who is an investor in The DAO, told The Wall Street Journal that he was opposed to a fix because the technology "must be allowed to fail to improve."[6]

Smart contracts allow complicated contractual arrangements to be written as computer programs, which are then immune to human intervention. "This immunity is a bad idea, especially for regulated enterprises" said Dr. Giuseppe Ateniese, a computer scientist who's worked with Accenture to create modified blockchain architectures. "It requires programmers to write perfect bug-free code the first time, everytime. Most of us have seen Dr. Strangelove or War Games. This is the Hollywood version of a smart contract failing spectacularly, but it points to a very real issue. People don't want computers with complete and unassailable autonomy, they want humans to be able to fix problems should they arise."

The DAO participants, who saw one-third of their development cash disappear in what they consider a misappropriation of assets, have taken the bold step of adding a "hard fork" to the blockchain at the moment before the theft occurred. One prong in the fork contains the original chain; the other starts a new chain omitting the $60 million loss and reconstructing all subsequent transactions to date.

While the new chain removes the theft, it leaves no trace, or version of the redaction. DAO users and developers have the option to adopt the fork and reverse the loss, or reject it and protect the software's original intent. It is left to the user to choose their version of the truth, as both are left equally viable.

Unfortunately for The DAO, their camp is divided and the hard fork has created a split in the network, with a large number of DAO participants continuing to transact on the original blockchain — either on ideological grounds or for financial gain (see figure).

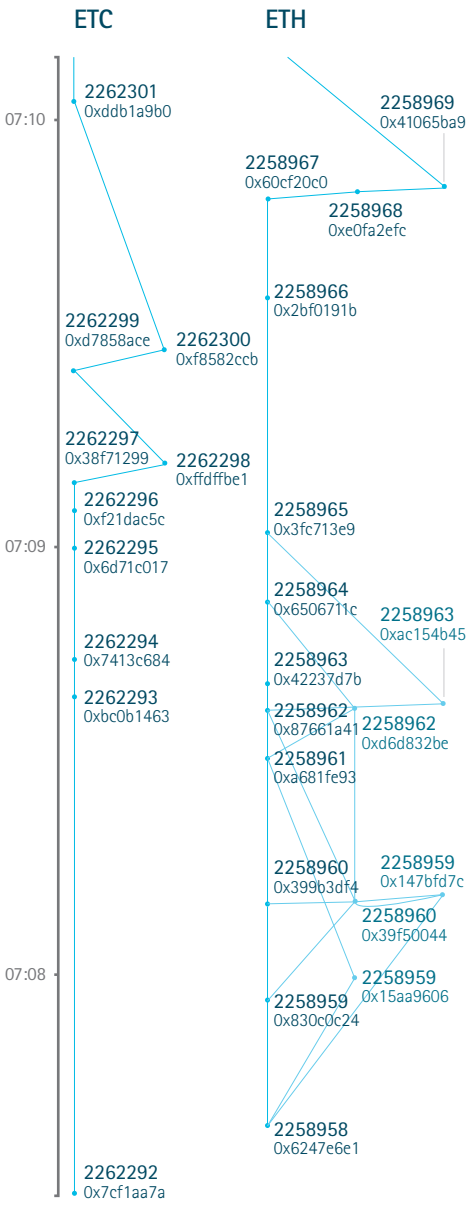
It must also be said that hard forks only make sense for recently mined blocks. Building the consensus required to actually create a hard fork at The DAO was difficult to begin with. But because only a month had passed since the incident, reconstructing subsequent blocks was relatively easy. If the theft had been uncovered much later, after a long period of growth in The DAO's blockchain — and the intertwining of its smart contracts — or if transaction volumes had been much higher, a hard fork would have been virtually impossible.

As Klint Finley observes in Wired, The DAO's experience has been a watershed moment for blockchain. "Machines will always be subject to the messy politics of the human world," he writes. "The heist has divided people and exposed the inevitability of human weakness. But it's also bringing people together to fix things. Humanity is making that possible, not mathematics."[7]

Certainly, The DAO theft has hurt the credibility of digital currency systems while increasing pressure for clarity around blockchain's strengths and weaknesses. One point is abundantly clear — if the financial services industry is to embrace a new technology, it cannot be one in which human errors are immutable and criminals are allowed to defend their actions on ideological grounds.

ETHEREUM CLASSIC VS. ETHEREUM

Price/USD	$1.30	$12.08
Price/BTC	0.00213119	0.01981240
Market Cap/USD	$109,050,675	$1,014,265,308
Market Cap/BTC	178,907	1,663,992
Hashrate/Gh/s	652 Gh/s	4610 Gh/s
Price (ETC/ETH)	14.25%	
Hashrate (ETC/ETH)	14.15%	



Sources: http://www.etc-eth.com as of 15/9/16 and http://fork.ethstats.net

The "Right to Be Forgotten"

"Individuals now have the ability to essentially go in with a virtual black marker and redact their names."

IAPP on Europe's new General Data Protection Regulation

In 2012 the European Commission introduced "right to be forgotten" protections under a new set of data regulations. Two years later, the European Court of Justice solidified the protections as a fundamental right. Since then over 300,000 requests for redactions of online content have been granted by Google alone.[8]

Now attention has turned to Europe's new and more robust General Data Protection Regulation (GDPR), signed into law in 2016. With a compliance deadline of 2018, there is an "adapt or die" dimension to the rules. Companies will face more requirements and scrutiny than ever before over how they use and control customer data. Serious infractions will lead to serious fines: 4 percent of a company's annual revenue or €20 million, whichever is larger.

Perhaps more importantly, the effects of these regulations will extend far beyond Europe. Every company with an operation in Europe or with customers there — every entity that holds or uses European personal data inside and outside Europe — will be impacted by the new rules.

One of the cornerstones of GDPR is the right of consumers to have all traces of their personal data erased from the records of companies with which they do business. Trevor Hughes, president and CEO of the International Association of Privacy Professionals, described GDPR as "groundbreaking." "Individuals now have the ability to essentially go in with a virtual black marker and redact their names." [9]

GDPR also requires "data portability" whereby companies must give customers a copy of their personal data to take with them upon request. These vast responsibilities for sharing and rescinding personal data on a case by case basis will have a huge impact on banks' back offices.

In many ways, blockchain technology and smart contracts are custom fit to automate the new workload. They could add granularity to personal data and encode permissions, conditions and restrictions for its use. They could also enable data portability and provide an easily auditable trail with proofs of consent.

But the technology could also be its own worst enemy under Europe's privacy rules. The requirement to hand consumers power over their personal information could clash with the blockchain's immutable record-keeping and make it extremely difficult to use the technology in compliance with the law.

GDPR won't take effect for nearly two years, but even today there are privacy regulations that could run at odds with blockchain's immutability. Under the Gramm-Leach-Bliley Act and the U.S. Security and Exchange Commission's (SEC) Regulation S-P, institutions must notify consumers of their information-sharing practices annually and inform customers of their right to opt out. If a customer opts in for one year and opts out for the next, how would the data be removed from a blockchain, and how would that process be managed for millions of customers in a given year?

Take also the U.S. Fair Credit Reporting Act (FCRA), under which consumer reporting agencies must correct or delete inaccurate, incomplete or unverifiable information, typically within 30 days. The U.S. Federal Trade Commission has estimated that 40 million Americans have inaccuracies in their credit reports under the current system.[10] The question begs asking — how do financial institutions comply with these new right to be forgotten regulations with a blockchain that always remembers? [11]

"The ability to prune data from the log, coupled with versioned edits and the ability to verify the integrity of these edits, is a powerful tool towards regulatory compliance."

Shaul Kfir, CTO Digital Asset

Progress We're Making

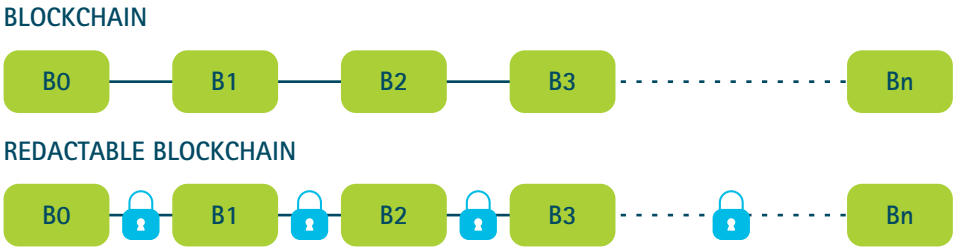
If permissioned blockchain applications are to go from lab experiments to real deployments, we need to rethink absolute immutability.

In an imperfect world there are many issues that an immutable blockchain will face. At Accenture, we believe that if the next generation of permissioned blockchain applications is to be turned from lab experiments into real deployments, we will need to rethink absolute immutability.

A variety of ideas are emerging. But the patent we recently filed with Dr. Giuseppe Ateniese for an editable blockchain should offer new room to maneuver, not only in financial services but across industries. The invention modifies existing blockchain technology to allow designated authorities to edit, rewrite or remove previous blocks of information without breaking the chain. One of its main features is that it is compatible with current blockchain designs, can be implemented now and requires only minimal changes to current application software.

The invention enables blockchain editing by using a new variation of the "chameleon" hash function, which can recreate matching algorithms through the use of secure private keys. After a change has been made to a block, the original blockchain remains fully intact and there is no need to create a hard fork and rebuild subsequent blocks. That means flawed smart contracts could be updated at the time the contract was issued and the changes would apply to subsequent smart contracts in the chain. Even where edits to one block impact subsequent blocks, the fix would be far easier than a hard fork.

The editable blockchain invention provides the means to build a virtual padlock on the link connecting two blocks (see figure). Redacting the blockchain is simple: the chameleon hash key is used to unlock the link between the block that must be changed and its successor. Thanks to the key, it is possible to substitute the block with a new one without breaking the hash chain.



The invention is designed to preserve the virtues of immutability as well. To positively identify blocks that have been changed, it is possible to architect blockchains so that any redaction leaves an inevitable "scar" that cannot be removed, even by trusted parties. This is accomplished by including both an editable chameleon hash to connect the blocks alongside a standard, uneditable hash. So while the editable blockchain capability will not force a node to purge data from their archives, users will now have the technical ability to comply with privacy laws.

A successful prototype of the invention was created by modifying the core technology of bitcoin, which is the most widely used blockchain technology. The modifications from the invention are possible in a range of existing blockchain technologies, requiring only minimal and inexpensive changes to the current blockchain, block or transaction-structures and to how local participant software interprets the information.

The editable blockchain invention is designed for permissioned systems, which have a designated administrator who manages the systems and grants permission to use it. This is in contrast to "permissionless" systems, where there is no single governing authority. An editable blockchain is effective only where the governance model and rules that control redactions are pre-agreed and controlled by known parties. Rules must be based on clearly stated principles and roles about when redactions are merited. The "versioning" effect of edits is crucial in maintaining the integrity of the chain.

According to the World Economic Forum, blockchain ventures have attracted more than US$1.4 billion in investment over the past three years. Financial institutions and technology firms are expected to spend more than $1 billion just in 2016[12] — a year when many ideas are expected to turn into real products. These applications promise to store files, notarize documents, manage health records, coordinate IoT devices and administer assets. But records will need to be expunged when they contain errors or sensitive information, or when it is required by law.

In short, we're on the cusp of a profound revolution in the way information is processed, stored and distributed across permissioned blockchain systems. But before that revolution can truly begin, the world must wait to see how fast this technology will be allowed to evolve for large-scale enterprise use.

If purists and pragmatists agree that blockchain's potential to change our world for the better is real, then the answer is obvious and the technology's moment is right now.

References

1. http://thehill.com/images/stories/blogs/interneteconomy25yrs.pdf
2. https://blockchain.info/charts/n-transactions-total
3. http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf
4. https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/
5. http://qz.com/656959/the-dtcc-and-4-top-banks-used-blockchain-tech-to-trade-credit-swaps/
6. http://online.wsj.com/public/resources/documents/print/WSJ_-C001-20160715.pdf
7. http://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/
8. https://www.google.com/transparencyreport/removals/europeprivacy/
9. http://www.usatoday.com/story/money/business/2014/05/13/google-search-european-court-of-justice/9027645/
10. https://www.ftc.gov/system/files/documents/reports/section-319-fair-accurate-credit-transactions-act-2003-sixth-interim-final-report-federal-trade/150121factareport.pdf
11. To protect data and manage storage on the blockchain, some solutions use only a hash of personally identifiable information (PII), which serves as a reference point and link to an off-chain PII database. But other solutions seeking to leverage the wider data management benefits of blockchain will look to store data on-chain.
12. https://www.greenwich.com/press-release/wall-street-blockchain-investments-top-1billion-annually-0

Authors

Richard Lumb

Group Chief Executive,
Financial Services

David Treat

Managing Director,
Capital Markets Blockchain Lead

Owen Jelf

Global Managing Director,
Capital Markets Lead

Acknowledgements

The Accenture-Ateniese invention would not have been possible without the Stevens Institute, which encourages professors, like computer scientist Dr. Giuseppe Ateniese, to engage in entrepreneurial activities. Accenture would also like to thank Digital Asset's Blythe Masters and Shaul Kfir for their practical input on the editable blockchain we've developed in cooperation with Dr. Ateniese. Thanks also to Accenture's Sean Conway, Chris Brodersen, Alissa Worley, John Velissarios, Giuseppe Giordano and Christine Leong for their supporting research and analysis.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 375,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

16-2668