HALBORN

BRIDGING LEGACY FINANCE AND DEFI: THE INTEROPERABILITY CHALLENGE

OCTOBER 2024

HALBORN.COM

INTRODUCTION

In recent years, "interoperability" has become a key topic in blockchain and decentralized finance (DeFi) discussions. But what does it really mean in the financial sector, and why is it attracting so much attention?

At its core, interoperability in finance allows different systems to exchange information and work together efficiently. While the concept is simple, traditional finance (TradFi) has struggled with it. Proprietary protocols and standards have made cross-system interaction difficult, revealing significant inefficiencies.

The rise of Web3 technologies, including blockchain, DeFi, smart contracts, tokenization, and Central Bank Digital Currencies (CBDCs), introduces powerful solutions capable of fostering a seamless, interoperable financial landscape. These innovations are increasingly part of global financial institutions' strategic plans, highlighting the need for ongoing research, collaboration, and dialogue to improve understanding and deployment.

This whitepaper examines TradFi's interoperability challenges, DeFi's potential solutions, and the hurdles related to privacy and standardization.

It also explores the importance of enhancing security and efficiency across public and multi-blockchain networks to achieve true interoperability, as well as promising Web3 innovations set to transform financial services in the years ahead.

INTEROPERABILITY CHALLENGES AND OPPORTUNITIES IN TRADFI

Despite advances in open banking, which have enabled consumers to connect their financial services more efficiently, a lack of genuine interoperability in TradFi systems remains a persistent pain point for many consumers and businesses.

For example, in the current financial system, if a bank wants to verify a customer's identity using another institution's records – a necessity for nearly all transactions – they would have to go through a lengthy process of requesting and verifying the information manually, thereby causing a delay that negatively impacts the customer.

This lack of interoperability not only slows down processes and hurts the user experience, but it also increases costs for financial institutions. As such, the resulting inflexibility can substantially limit the ability to innovate and collaborate with other systems, creating a barrier to entry for new players and much-needed solutions in the industry.

Clearing, **settlement**, and **trade finance** are three particularly notable areas in TradFi where significant pain points persist – and where **DeFi solutions** hold great promise.

TRADFI CLEARING AND SETTLEMENT: NOT SO SWIFT

In TradFi systems, clearing and settlement processes underpin nearly all financial transactions, ensuring that trades are executed securely and efficiently. Two critical components of this system are **SWIFT**, used for cross-border payments, and traditional **clearinghouses** like stock exchanges. Both are considered payment intermediaries, or 'middlemen.'

SWIFT (Society for Worldwide Interbank Financial Telecommunication) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized, and reliable environment.

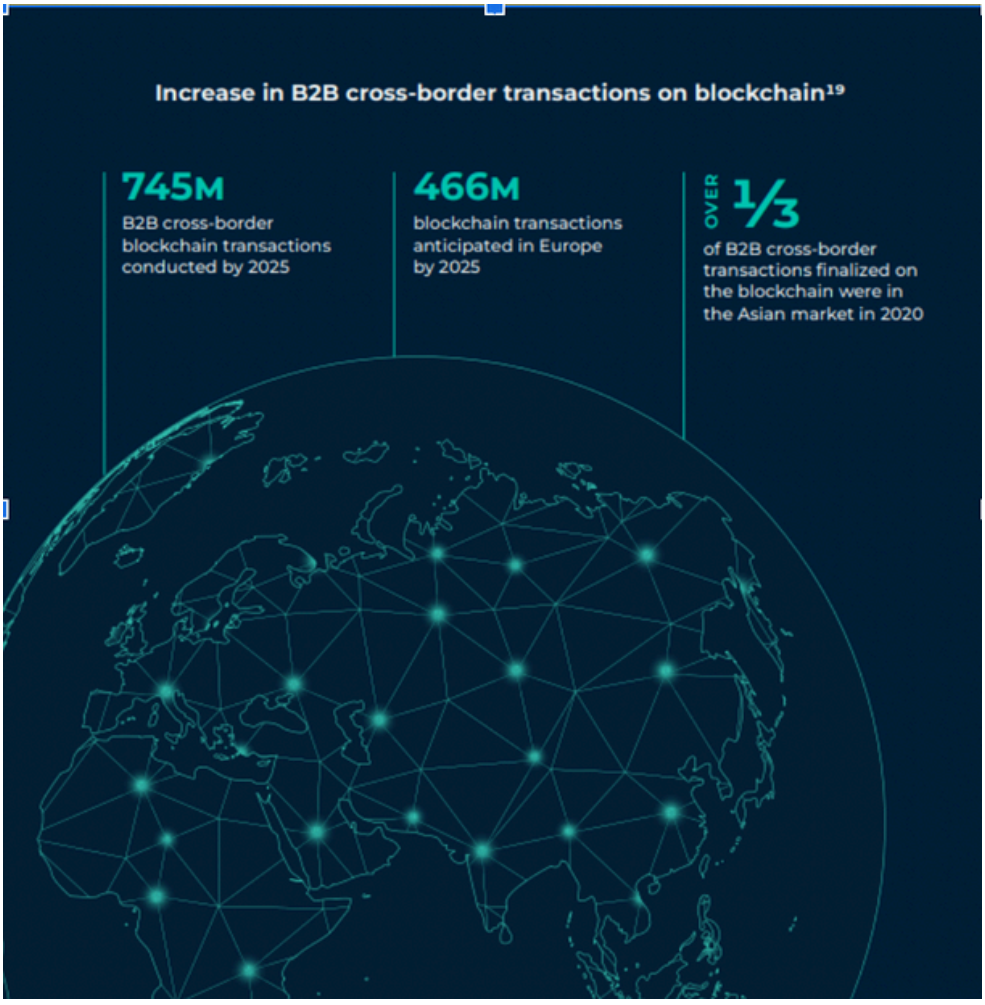
SWIFT transactions can be slow due to the involvement of multiple disparate intermediaries and banks, often taking between one to three days to settle due to a lack of interoperability and the need to operate across varying systems.

Recent innovations such as Swift's GPI service have improved transparency and speed, but still have not solved for round-the-clock clearing and settlement availability that many businesses desire. Additionally, SWIFT transactions can be expensive, with fees varying based on the transaction size, path, and number of banks involved.

"Blockchain - with programmability, with the smart contracts, with the always-on - kind of matches the speed of the internet (...) But payments money doesn't match the speed of commerce on the internet right now, and that's a mismatch. How do we get that more aligned and think about what the future network looks like?"
Ryan Rugg, Global Head of Digital Assets, Citibank

Clearing Houses act as intermediaries between buyers and sellers in financial markets, ensuring the correct settlement of trading accounts, clearing trades, reporting trading data, and ensuring that money or securities are available for transfer.

While they provide a layer of security and trust, the process can be cumbersome and lack transparency, leading to potential delays and inefficiencies. This is especially evident in B2B cross-border transactions, where blockchain technology is poised to make a significant im



Source: Convera, Fintech2025+: Trends, technology, and transformation in global commerce

FOREIGN EXCHANGE: DIGITAL WALLETS DRIVING LOWER FEES

Foreign exchange (FX) transactions frequently encounter issues such as delays and high fees due to the reliance on banks as intermediaries. These inefficiencies can adversely affect cross-border payments and trade, where timing issues and currency fluctuations can reduce business profits and operational efficiency if they are handled poorly.

Digital wallets that utilize blockchain technology and real-time payment systems (RTPs) can **eliminate intermediaries and facilitate instant FX conversions at reduced costs**. Insurance, healthcare, assisted living and many forms of media and entertainment are already actively using digital wallets for quick and easy global payday remittances, according to Bank of America.

This innovation has proven to be transformative in regions like Asia-Pacific, where global real-time payments are increasingly standard. In fact, according to commercial cross-border payment provider Convera's recent FinTech 2025+ report, RTP transactions are expected to reach $511.7 billion by 2027, marking a 21.3% annual growth rate.

Furthermore, the **transparency** afforded by blockchain allows businesses to see transaction details – from exchange rates to fees – in real time, enhancing control over finances and reducing overhead, which can lead to improved customer service.

TRADE FINANCE: PRIMED FOR INNOVATION

Trade finance represents the financial instruments and products that facilitate international trade and commerce by providing short-term finance, and is critical for managing cash flow and reducing the risks associated with global trade.

Traditional trade finance processes are largely **manual**, involving multiple parties sitting hundreds to thousands of miles apart, including buyers, sellers, banks, transporters, and inspectors. The end-to-end process of financing trade is not only time-consuming but also **prone to fraud and errors**, with documents like bills of lading, letters of credit, and other trade documents often handled in paper form.

Naturally, this environment is not conducive to interoperable data. Much noise has been made in recent years about the opportunity ahead in digitizing paper-based processes to improve speed and security, while reducing costs.

Recently, Citi's Ryan Rugg shared an example of the bank's work with the global shipping titan Maersk to illustrate how tokenized guarantees on a blockchain show incredible promise by removing intermediary delays and enhancing speed and transparency. In the test pilot, as its vessel passed through a canal, the smart contract, which Citi had pre-funded, automatically released payments once the ship received fuel.

INTEROPERABILITY IN DEFI AND BLOCKCHAIN FINANCIAL SERVICES

As is evidenced by experiments such as those conducted by Citi, DeFi solutions are emerging with some of the most promising use cases for TradFi's persistent interoperability challenges. By using blockchain technology and smart contracts, DeFi platforms create more of an **open financial system** that is accessible to anyone with an internet connection, potentially removing the need for 'middlemen' intermediaries (e.g. correspondent banks).

The resulting seamless transfer of data and value between different protocols and platforms is creating exciting new business opportunities.

Interoperability is integral to DeFi because it enables different protocols and decentralized applications (dApps) to communicate and share information seamlessly across disparate blockchains. However, persistent security gaps and lack of standardization and regulations in the world of DeFi is an ongoing challenge in expanding on the interoperability use case.

Assuming that shared protocols will eventually be used broadly to connect blockchains – much like how HTTP came to organize and govern the disparate informational web – decentralized financial ecosystems will create more efficient use of assets and data, ultimately leading to better financial services and products.

The benefits extend far and wide, from user experience, to reliability, security, speed, and many other factors.

DEFI AND TRADFI: AN AWKWARD MATCH OR COMPLEMENTARY SYSTEMS?

Many have come to view the DeFi ecosystem as cooperative, rather than competitive, with TradFi. In the best cases, breaking down barriers between the two unlocks new opportunities for innovation and creates more efficient financial ecosystems globally. We've seen this already in parts of the world where payouts and disbursements in stablecoins have proven to be a powerful medium in serving unbanked or underrepresented populations.

In the 'always-on' financial environment of capital markets, where issuers and investors engage in raising and allocating capital, the growing knowledge that decentralized finance and Web3 technologies like smart contracts and tokenized assets can provide substantial benefits within traditional financial (TradFi) services has led to an intensifying demand for cross-collaboration.

But the road to an integrated TradFi-DeFi ecosystem, perfectly logical as it may seem, is a massive undertaking, with compliance and standardization challenges that could threaten the path forward. Indeed, we have seen more than a few hiccups along the journey towards integration and adoption between the two worlds, ranging from the regulatory action against stablecoin providers to lawsuits against the sales of digital assets to institutions.

Regulatory hurdles aside, in this next section, we'll dissect some of the purely technical challenges of an interoperable TradFi-DeFi ecosystem for a better view of how they might be overcome.

TECHNICAL APPROACHES TO ACHIEVING INTEROPERABILITY

Interoperability between blockchain networks and legacy systems is a complex challenge requiring both cutting edge technology and sound policy coupled with a progressive operational strategy.

On the technical side, the goal is to enable different blockchain systems to communicate and exchange information effectively. **Distributed Ledger Technology (DLT)**, where multiple blockchains (ledgers) record financial transactions in real-time, offers significant advantages for the financial sector, enhancing security, transparency, trust, programmability, privacy, performance, and scalability.

In this section, we'll highlight some of the most promising technical developments used in DLT and interoperable blockchain ecosystems that could lead the way towards TradFi-DeFi interoperability.

Smart Contracts

Smart contracts are key to interoperability by automating interactions and streamlining transactions across multiple blockchains. These self-executing contracts ensure secure code execution, enabling seamless enforcement of agreements and transactions. This simplifies managing operations across different networks.

By bridging gaps between blockchains, smart contracts enable collaboration across diverse systems, unlocking new opportunities in cross-border payments, supply chain management, and other financial services.

Cross-Chain Communication Protocols

Cross-chain communication protocols are essential for enabling interaction and data exchange between various blockchain networks. Technologies like the Interledger Protocol, the Inter-Blockchain Communication (IBC) standard, and cross-chain bridges facilitate secure interactions and asset transfers across different platforms.

These protocols enhance data integrity by ensuring authenticity and consistency in digital financial transactions, making it possible to transfer assets seamlessly.

However, there are still challenges (and disagreements) around achieving full interoperability between different blockchain networks, such as scalability and security concerns.

These **security concerns** remain a significant challenge, particularly with cross-chain bridges, which have become targets for high-profile bridge hacks. Vulnerabilities often arise from bugs in smart contracts and insufficient validation processes that can be exploited by attackers, leading to substantial financial losses.

As these technologies continue to develop, enhancing the security protocols and auditing practices surrounding these bridges is crucial to safeguarding assets and maintaining trust in cross-chain transactions.

Blockchain Oracles

Blockchain oracles are considered a key part of DeFi security, serving as intermediaries that supply external data to blockchain networks, thus enhancing smart contracts' functionality and interoperability. VWAP Oracles like Chainlink link smart contracts with real-world data, enabling timely, accurate transaction execution.

They enable smart contracts to interact with off-chain data sources - a powerful and versatile feature. However, there are ongoing debates around the reliability and security of oracles, as they can introduce a central point of failure and potential vulnerabilities if not implemented correctly, which contrasts with the decentralized nature of blockchain technology that operates without relying on a central authority.

Sidechains

Sidechains are independent blockchain networks connected to a parent chain through two-way pegging mechanisms. This allows assets to be transferred between the main chain and sidechains, avoiding congestion, increasing transaction throughput, reducing costs by minimizing fees and shortening settlement times, and mitigating scalability issues that come from too much traffic on one chain.

Sidechains also enable developers to experiment with new features and functionalities without risking the security of the main chain.

Sidechains such as Polygon and the Liquid Network exemplify the progress in blockchain interoperability and scalability.

Polygon, originally known as Matic Network, provides a framework for building Ethereum-compatible sidechains. It facilitates faster and cheaper transactions, attracting broad integration across DeFi platforms, NFT marketplaces, and gaming applications due to its robust security and Ethereum compatibility.

The Liquid Network, developed by Blockstream, supports fast, secure, and confidential Bitcoin transactions, appealing particularly to financial institutions and exchanges. It enhances transaction speeds and asset issuance, thus improving settlement times and broadening Bitcoin's utility in business applications.

Both networks showcase how sidechains enable developers to innovate and expand functionalities without risking the security of the main chain.

Sharding

Sharding is a technique used to improve the scalability of blockchain networks by dividing network nodes into smaller groups called shards. Each shard processes a portion of transactions, enhancing connectivity and operational efficiency within financial markets, making it possible to achieve higher throughput compared to traditional blockchains.

Like sidechains, this technology allows for increased transaction processing capacity while maintaining decentralization and security. Ethereum 2.0 implemented sharding as a solution to its prior scalability limitations.

Standardization and ISO 20022

Standardization is crucial for blockchain interoperability. Common standards for data formats, communication protocols, and smart contract languages enable smooth interactions between blockchain networks. Groups like ISO/TC 307 are working to set international standards that reduce barriers and promote blockchain adoption in financial services.

ISO 20022, a key example, standardizes electronic data exchanges for financial institutions across payments, securities, foreign exchange, and trade finance. By providing a universal language for data, it bridges the gap between traditional finance and blockchain systems.

This standardization facilitates the integration of blockchain into mainstream financial infrastructure, improving transparency and efficiency. As digital currencies grow, ISO 20022 becomes even more relevant, ensuring coherent, interoperable transaction data across platforms, boosting confidence in digital transactions.

STRATEGIC APPROACHES TO ENHANCING INTEROPERABILITY

Strategic shifts in process, procedures and operations are likewise essential for integrating traditional financial systems with Web3.

This section will explore how organizations can adopt strategies to enhance interoperability, drive innovation, improve operational efficiency, ensure compliance with existing regulatory frameworks, and address the challenges of raising capital in a volatile market.

Collaborative Partnerships with Financial Institutions

Collaborative partnerships between traditional financial institutions and blockchain companies have grown in recent years, and are crucial for the types of resource sharing and innovation needed to bridge the gap between them.

Traditional banks or investment firms often struggle with flexibility and scalability, making partnerships with blockchain startups essential for developing new financial solutions, such as the custody of digital assets.

These alliances will only continue to broaden service offerings and drive the adoption of Web3 technologies - particularly under clear regulatory frameworks - benefiting both parties greatly.

Regulatory Compliance

For organizations transitioning to the use of blockchain and Web3 decentralized technologies, regulatory compliance is crucial to mitigate legal risks and gain credibility. Adhering to AML and KYC regulations is only the tip of the iceberg in ensuring they operate within legal boundaries and build trust in the financial sector.

Compliance helps blockchain networks operate seamlessly across jurisdictions. By bringing experts in compliance and global regulations together with the major players in the blockchain ecosystem, the potential is massive for efficient blockchain-based solutions to effectively (read: compliantly) solve some of the most persistent challenges in global finance. Aside: Many compliance requirements boil down to security requirements. The big incidents that result in audits and fines typically are caused by a vulnerability that an attacker exploits to steal data, money, etc.

Investment in New Technologies

Further to the benefit of partnerships and the technology benefits incumbents can incur by working with fintechs and blockchain companies, investing in innovative technologies internally can enhance interoperability and help maintain competitiveness. In fact, doing so has become table stakes, as evidenced by the substantial spend major financial players like JP Morgan have put towards innovative blockchain solutions in recent years, such as their blockchain platform, Onyx.

These initiatives are aimed at enhancing transaction efficiency and security, as well as expanding their capabilities in handling digital assets, with interoperability underpinning the success of each.

PUBLIC, PERMISSIONLESS...SECURE?

Privacy and security are understandably paramount for financial institutions moving into the web3 technology arena, where global interoperability may hinge on the effective use of public blockchains. But the question of whether the handling of sensitive client data can be done securely (and privately) has proven to be one of the most enduring challenges, with privacy layers and zero knowledge proofs (ZKPs) leading the charge towards progress.

Evolution of Privacy Layers

While public blockchains offer transparency, they also present privacy issues, such as the visibility of transaction amounts and addresses. Addressing these concerns is crucial for protecting sensitive data and ensuring the privacy of users in the most private and regulated of all industries.

This mandate has led to the emergence of privacy layers, such as Zcash and Monero, which use various techniques, such as Zero Knowledge Proofs (ZKPs) to obfuscate transaction information while still maintaining the integrity of the blockchain.

Zero Knowledge Proofs

Zero knowledge proofs (ZKPs) significantly improve privacy by allowing transaction verification without disclosing any underlying data. This technology enables smart contracts to execute transactions securely while maintaining the confidentiality of the involved parties. ZKPs have especially gained traction in the DeFi space, where they are utilized for private lending and borrowing protocols. They also hold promise for enabling cross-chain transactions while ensuring data privacy.

Privacy-Enhancing Smart Contracts for DeFi Security

Ethereum and other blockchains have explored layers and sidechains that allow for private transactions. Examples include Aztec, which uses ZKPs to enable private transactions on Ethereum.

Additionally, other privacy-focused blockchains like Oasis Network and Secret Network are experimenting with smart contract platforms that incorporate privacy features by default.

In a sign of confidence and (hopefully) interoperability to come, these developments show that the industry is actively exploring ways to improve data privacy on public blockchains.

MANAGING MULTI-BLOCKCHAIN NETWORKS

The idea of multi-blockchain networks no longer seems esoteric. In fact, the general consensus is that these types of interconnected blockchain networks will be required to achieve any semblance of an efficient, high transaction-volume global financial system on blockchains.

Below are a few of the inherent challenges and best practices for navigating interconnected blockchains and legacy financial systems.

Challenges

- **Interoperability issues**: The onus of this whitepaper has been focused on solving interoperability issues within the TradFi and DeFi spaces, so this obstacle naturally makes the top of the list here. Achieving seamless communication between different blockchains is a significant technical lift, requiring sophisticated bridging protocols to facilitate cross-chain transactions and data sharing.

- **Security risks**: Blockchain security is complex. Cross-chain transactions, full of potential as they may be, can introduce new vulnerabilities such as cross-chain bridge hacks, and ensuring security across multiple networks demands rigorous consensus mechanisms plus comprehensive audit processes.

- **Scalability concerns**: Coordinating transactions across multiple blockchains can lead to increased latency and congestion, negatively impacting overall network performance and user experience.

- **Regulatory compliance**: Navigating diverse legal environments across jurisdictions substantially complicates matters, with varying regulations potentially affecting multi-blockchain operations unevenly.

- **Cost management**: Managing transaction fees and operational costs across multiple blockchains requires strategic financial planning, as each network may have different fee structures and economic models.

- **Complexity in governance**: Coordinating governance across multiple, highly decentralized blockchain networks presents challenges in decision-making, requiring robust frameworks for consensus and conflict resolution.

Best Practices

- **Use a common consensus mechanism:** To ensure secure communication between different blockchains in a multi-blockchain environment, it is essential to use a standard consensus mechanism across all connected chains. This reduces the risk of conflicting or malicious transactions.

- **Limit data exposure**: Only share necessary data between interconnected blockchains. This reduces potential security risks and ensures that sensitive information remains protected.

- **Monitor and update regularly**: Ongoing monitoring and updating of all interconnected blockchains are critical to identifying vulnerabilities and maintaining security.

- **Establish clear governance:** In a multi-blockchain environment, it is crucial to establish clear governance rules and protocols to ensure all parties involved understand their roles and responsibilities. This helps maintain consistency and harmony across interconnected networks.

- **Implement privacy and scalability features**: As mentioned earlier, incorporating privacy features into smart contract platforms is crucial for protecting sensitive data in a multi-blockchain network. Organizations should choose blockchain platforms that prioritize data privacy while supporting the scalability necessary for high transaction throughput, by default.

- **Collaborate and communicate proactively:** Effective communication and collaboration are key to successful multi-blockchain governance. All parties should regularly discuss and share updates on changes, decisions, and potential conflicts before taking decisive actions to ensure a smooth process.

- **Experiment with different economic models:** Multi-blockchain networks offer opportunities for experimenting with various economic models. Organizations can explore the use of hybrid or token-based economies across interconnected blockchains to find the most efficient and sustainable model for their specific needs.

- **Stay informed**: Keeping up to speed on new advancements, tools, and best practices is crucial for effective multi-blockchain governance. Regularly attending conferences, networking events, and engaging with other organizations in the blockchain space can help organizations stay ahead of the curve and make informed decisions.

CONCLUSION

The integration of traditional finance (TradFi) and decentralized finance (DeFi) through blockchain and distributed ledger technology (DLT) offers a significant opportunity to address the inefficiencies of legacy systems. These technologies improve transaction efficiency, enhance security, and lower operational costs.

Blockchain and DLT enable real-time, secure transactions, reducing the fraud and errors often found in manual financial processes. By bypassing the delays of traditional systems, like SWIFT or major global clearinghouses, blockchain increases transaction transparency and reduces fraud. Smart contracts can further lower costs, especially in areas like trade finance and regulatory compliance.

While there are technical and operational challenges, the potential to create a more inclusive and resilient financial market is compelling. Many in TradFi expect the adoption of tokenized money and financial assets on the blockchain to hit a tipping point by 2025.

It's important to remember that integrating TradFi and DeFi isn't just a technological change—it's a strategic advancement that could shape the future of finance. As these sectors converge, they promise to create a more efficient, transparent, and equitable global financial landscape.

HALBORN

MEET OUR TEAM

Halborn was founded in 2019 by renowned ethical hacker Steven Walbroehl and growth hacker Rob Behnke. The fully remote organization has since grown to over 100 of the best and brightest offensive security engineers in the world.

JACQUES BOSCHUNG

CEO

STEVEN WALBROEHL

CO-FOUNDER & CTO

ROB BEHNKE

CO-FOUNDER & EXECUTIVE CHAIRMAN

HENRY MANDELBAUM

SALES DIRECTOR

HALBORN

WHY WORK WITH US?

Halborn's proactive security measures, including in-depth vulnerability assessments, are critical for maintaining trust and reliability in a multi-blockchain landscape. By incorporating proactive security methods, you can protect sensitive information while fostering a sustainable and resilient network where all participants can thrive.

For financial institutions venturing into the blockchain and DeFi space, prioritizing these security solutions is essential and can help you bridge the narrowing gap between traditional and decentralized finance securely and with confidence.

GET IN TOUCH

Sales: sales@halborn.com

Marketing: marketing@halborn.com

For more info on our services and to read client testimonials and case studies, visit **halborn.com**.