스마트 컨트랙트 기반의 프라이버시를 제공하는 스마트 팩토리 주문제작 서비스 프로토콜

이용주[1]· 우성희[2*]· 이상호[2]

[1]충북대학교 · [2]한국교통대학교

Privacy-preserving Custom Manufacturing Service Protocol based on Smart Contract in Smart Factory

Yong-Joo Lee[1] · Sung-Hee Woo[2*] Sang-Ho Lee[2]

[1]ChungBuk National University · [2]Korea National University of Transportation

E-mail : yonjoo3570@naver.com / shwoo@ut.ac.kr / shlee@cbnu.ac.kr

요 약

4차 산업에 대한 꾸준한 투자와 기술 개발로 스마트 팩토리 기술이 더욱 안정화되고 3D 프린팅을 포함한 관련 기술개발이 더욱 활발해진다면, 스마트 팩토리 도입비용이 낮아지고 현재의 고가의 상품 제조에 집중되는 현상에서 벗어나 소량 맞춤형 주문 제작을 위한 서비스로 변화 될 것이라고 기대한다. 그러나 소량의 주문제작을 위해 제3자에게 개인정보를 제공해야 하고 복잡한 결제시스템을 거쳐야 한다면 발전되는 기술에 비해 활용도는 그에 미치지 못할 수 있다. 이 논문에서는 기존 사물인터넷의 한계를 극복하고 새로운 패러다임을 가져다 줄 것으로 기대하는 블록체인 기술 융합의 스마트 팩토리 환경에서 고객 맞춤형 제문제작을 위한 프로토콜을 제안한다. 제작자의 평판을 반영하여 고객 주문에 활용하고 주문 내용이 제작자 외에는 공개되지 않도록 프라이버시를 제공하는 고객 맞춤형 주문제작 방법을 제안하였다. 또한 제안하는 프로토콜의 요구사항을 검증하였고 관련연구와의 비교를 통하여 독창성을 확인하였다.

ABSTRACT

The Cost for introducing smart factory will decrease and the service type will change from a large scale to small quantity manufacturing, when 3D printing technologies have actively applied and smart factory related technologies have more stably developed. If customers have to provide private information, the availability of developed technology may cause slow progress. We propose a new protocol for custom manufacturing service of smart factory. The proposed approach is designed for smart contract based IoT convergence network. We analyzed the requirements of the proposed approach which provides anonymity, privacy, fairness, and non-repudiation. We compared it with closely related studies to show originality and differences.

키워드

smart factory, smart contract, privacy, anonymity, fairness

Ⅰ. 서 론

사물인터넷의 지속된 연구와 투자로 현재 사물인터넷 디바이스는 100억 개에 이르는 것으로 추정하고 있고, 향후 개방형 API의 증가와 3D 프린팅 기술 개발로 디지털 제조가 활발해지는 2050년

* speaker

에는 1000억 개에 이를 것으로 예측하고 있다. 사물인터넷 환경을 구축하기 위해서 서버구축비용 등의 초기 설치비용, 중앙 클라우드 유지비용, 스마트 팩토리 마다 수백에서 수천 개 이상의 스마트 디바이스를 관리하고 유지하는 비용이 비싼 반면에 고객과 투자자의 가격과 수익에 대한 기대치가 맞지 않아 고가의 상품제조에 집중되어 투자되고 있고 그다지 성공을 거두지 못하는 사례가 늘고 있다 [1, 2]. 현재 18개월에서 36개월의 교체주기를 갖는 스마트 폰이나 PC를 제외하고, 그 외 다른 분야는 교체 주기가 길어 소비 침체 및 매출 감소가 되고 있고 진입 후 실패하는 사례가 많아 구축 및 유지비용이 중요한 요소가 되었다. 향후 3D 제작 기술 및 디지털 제조 기술이 성숙해지는 시기에는 이러한 제조업의 투자비용을 줄이고 전문 기술을 분업화 할 수 있는 주문제작 서비스가 활발해 질것으로 예상한다[3]. 이 논문에서는 블록체인의 대표적인 응용인 스마트 컨트랙트와 사물인터넷의 결합된 네트워크에서, 스마트 팩토리의 주문제작 서비스를 제공하기 위한 익명성과 프라이버시를 제공하는 주문제작 서비스프로토콜을 제안하고, 요구사항에 대한 평가를 한 뒤 결론을 맺는다.

II. 관련연구

1. Traditional Publish/Subscribe

기존의 publish/subscribe 프로토콜은 그림 1과 같이 Publisher, Broker, Subscriber의 세 개가 구성원이 존재한다. Publisher 가 메시지 이벤트를 전송하고 Subscribe는 관심을 제출하면 브로커는 해당사항을 매치시키는 역할을 한다. 즉 기존의 프로토콜에는 서로의 내용을 매치 시키는 브로커의 역할이 상당히 중요하다 [4, 5].

그림 1.Traditional Publish/subscribe 구조

2. Bitcoin기반의 Secure Pub-Sub 프로토콜

Y. Zhao [6]은 Bitcoin 기반으로 공평한 지불을 제공할 수 있도록 Pub-sub 프로토콜을 제안하였다. 그림 2에서 Publisher가 토픽 기반의 트랜잭션을 Publish하면 Subscriber는 보증금을 걸고 관심을 표현한다. Publisher가 이벤트를 받고 확인을 하면 결과가 전송되어 계약이 체결되며 최종 지불이 완료된다. 비트코인의 보증금 기능을 이용하여 공평한 지불이 되도록 설계하였으나 단순히 이벤트 정보를 주고받는 간단한 예에서만 사용이 가능하므로 주문 제작의 서비스에 응용하기 위해 보다 많은 부분을 고려하여야 한다.

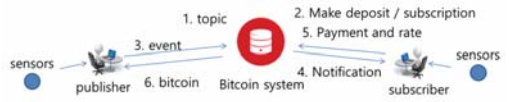

그림 2.비트코인 기반의 Pub/sub 프로토콜

III. 스마트 팩토리 주문제작서비스프로토콜

이 논문에서는 스마트 팩토리의 고객 맞춤형 주문제작 서비스를 위한 주문제작 프로토콜을 제안한다. 제안하는 프로토콜은 6단계 (Setup, Publish, Subscribe, Accept, Confirm, Evaluate)로 나뉜다.

1. 제안하는 프로토콜의 요구사항

고객 맞춤형 주문제작 서비스가 활성화되기 위하여 다음과 같은 요구사항이 반영되어야 한다.

- Anonymity : 주문자의 아이덴티티와 개인정보보호가 보장되어야 한다. 보다 완벽한 개인정보보호를 위해 익명성을 제공하는 고객 맞춤형 주문제작 서비스가 요구된다.
- Privacy : 고객의 맞춤형 주문에는 민감한 개인정보가 반영될 수 있으므로, 주문 내용에 대한 프라이버시가 요구된다.
- Non-repudiation : 주문 내용과 제작 결과의 상이함 또는 의견 차이로 인한 문제 발생 가능성을 제거하여야 한다. 이는 제작 완료 이후 생산품의 변조 등으로 발생 가능한 손해와 문제 발생 가능성을 제거할 수 있다.
- Fairness : 제작자와 주문자는 어느 한편의 악의적인 행동이나 변심으로 손해를 보지 않아야 한다.

2. 프로토콜 아키텍처

고객 맞춤형 주문제작 서비스를 위한 프로토콜은 그림 3과 같이 6단계로 나누며, 고객과 제작자의 Set-up 준비 단계 후 블록체인을 통한 Publish/Subscribe 과정을 통하여 주문과 제안을 주고받은 후 확약하고 서비스가 끝난 후 만족도를 평가한다.

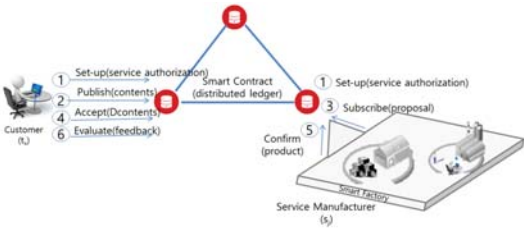

그림 3. 스마트 팩토리 주문 프로토콜

3. 제작자의 평판관리

제작자 s_j는 제작자 집합 $s_j \in S$의 요소이며, t_x는 주문제작 서비스를 이용한 고객 x로 집합 $t_x \in T$의 요소이다. R_{sj}는 제작자 j에 대한 평판을 의미하며 주문자 t_x는 한 번의 주문제작 서비스가 완료되면 제작자 s_j에 대해 R_x^j를 평가한다. 전체 제작자의 평판은 4개의 등급으로 나누어 전체 제작자의 평균(R_a), 표준편차(R_{sd})를 이용한 식(1)을 통하여 4개의 클래스로 분류한다. 표 1에서 S(superb)는 우수한 등급이며, P(pass)는 평균이상이면서 R_{sd}의 상향범위 내에 존재하므로 대체적으로 우수한 등급이고, D(deposit)는 평균보다 낮지만 R_{sd} 범위 내에 있으므로 보증금을 걸고 참여할 수 있도록 유도한다. R(reject)은 평균이하로 서비스에 참여할 수 없다.

$$\alpha \leftarrow (R_a + R_{sd}),\ \beta \leftarrow (R_a - R_{sd}) \tag{1}$$

표 1. Four Classes for Providers

Class	S	P	D	R
Condition	$R_{sj} \geq \alpha$	$R_{sj} \geq R_a$	$R_{sj} \geq \beta$	$R_{sj} < \beta$

4) 프로토콜 상세과정

- 셋업(Set-up) : 이 논문에서 제안하는 프로토콜은 블록체인(Ethereum)을 기반으로 설계하였다. 제작자 s_j와 주문자 t_x는 이더리움 계정을 생성하고 자신의 공개키 쌍(p, q)를 생성한다. t_x는 서비스를 이용하기 위하여 일정 금액의 보증금(Deposit)을 설정한다. s_j의 신뢰도가 D 등급에 속해 있다면 제작자 역시 보증금을 설정하여야 서비스에 참여할 수 있다.

- 퍼블리시(Publish) : 이 논문에서 제안하는 Publish는 Contents기반의 방법을 사용하며, 주문자 t_x는 주문에 대한 개요(Contents)를 트랜잭션(T_x)을 블록체인을 통해 Publish 한다.

$$T_x \leftarrow contents \tag{2}$$

- 구독(Subscribe) : 트랜잭션을 확인한 제작자 중 관심 있는 s_j는 제안서($proposal$)를 식(3)과 같이 t_x의 공개키로 암호화한 제안서(P_x^j)를 전달함으로써 관심을 표현한다. t_x는 제안서를 자신의 비밀키로 복호화 하여 제안서를 확인할 수 있다. 제작자 s_j가 제출한 제안서는 제작자의 비밀키로 디지털 서명이 되어 있어 부인봉쇄 등의 기능을 제공할 수 있고, 비밀키를 가진 t_x 만이 복호화 할 수 있어 프라이버시 제공이 가능하다.

$$P_x^j = enc(proposal) with q_x \tag{3}$$

- 계약(Accept and Contract) : t_x는 제안서 P_x^j를 확인하고, s_j의 평판인 R_{sj}를 확인할 수 있다. 계약을 체결하기 위해 주문에 대한 상세 내용인 Dcontents(detailed contents)를 식(4)과 s_j의 공개키로 암호화 한다.

$$DC_x^j = enc(Dcontents) with q_j \tag{4}$$

주문에 대한 상세 내용은 주문자t_x와 제작자s_j만 볼 수 있다. s_j는 주문에 대한 상세 내용대로 제작을 한다.

- 확인(Confirm) : s_j는 주문자의 제작이 완료되면 생산 인증이 이루어진다. 완성품의 종류에 따라 전자상품이라면 상품 그 자체이며 실체가 있고 물류를 통해 전달되는 상품이라면 스마트 물류와의 연동을 통해 제작이 완료되었음을 확인하는 내용으로 상품인증을 실시한다. 생산 인증을 실시한 내용(Product)는 주문자만이 확인할 수 있도록 주문자의 공개키로 암호화한다.

$$PA_x^j = enc(product) with q_x \tag{5}$$

- 평가(Evaluate) : 제작품의 제작을 완료하면 t_x는 s_j의 평판(R_x^j)를 평가하고, 평판의 평가가 끝나면 결제가 완료된다. 정상적으로 모든 과정이 완료되었는데 평판 평가가 이루어지지 않는다면, 일정 시간 후에, 제작의 완료를 인정하는 것으로 판단하며 결제를 완료한다. 이러한 기능들은 스마트 컨트랙트의 내부 기능들을 활용한다.

4. 검증 및 분석

이 논문에서 제안하는 주문제작 서비스의 보안 요구사항을 검증하고자 한다.

1) 익명성(Anonymity)

익명성이란 어떤 행위를 한 사람이 누구인지 드러나지 않는 특성을 의미한다. 이 논문에서 정의하는 프로토콜은 사용자의 등록과정 없이 이더리움의 계정 만으로 참여할 수 있기 때문에 블록체인의 익명성을 유지하였다.

2) 프라이버시(Privacy)

주문 내용은 당사자 들 만이 볼 수 있도록 하기 위하여 상세 주문서, 제안서, 제품에 대한 내용은 상대의 공개키로 암호화하여 전송하므로 당사자 외에는 볼 수 없다. 표 2에서 볼 수 있듯이 세 개의 중요한 트랜잭션은 모두 t_x와 s_j의 공개키로 암호화 되어 있으므로 해당 비밀키 외에 다른 참여자는 트랜잭션을 받아도 내용을 볼 수 없어 프라이버시가 제공된다.

표 2. Evaluation of Privacy

Content	Encrypted Contents	Party
Proposal	$P_x^j = enc(proposal) with q_x$ $proposal = dec(P_x^j) with p_x$	s_j $,t_x$
Detailed Contents	$DC_x^j = enc(Dcontents) with\, q_j$ $Dcontents = dec(DC_x^j) with\, p_j$	s_j $,t_x$
Product	$PA_x^j = enc(product) with q_x$ $product = dec(PA_x^j) with p_x$	s_j $,t_x$

3) 부인봉쇄(Non-repudiation)평가

주문내용과 생산 내용의 의견차이로 발생하는 문제점을 사전에 방지하기 위해 꼭 필요한 기능이 부인봉쇄 기능이다. 이 논문에서는 부인봉쇄 기능을 제공하기 위하여 스마트 컨트랙트 내부의 디지털서명을 활용한다. 그림 4와 같이 정보의 무결성을 제공하기 위해 트랜잭션 등록 시 비밀키 소유자는 서명 후 등록을 하게 되며, 거래 이후 부인봉쇄 기능을 제공하게 된다.

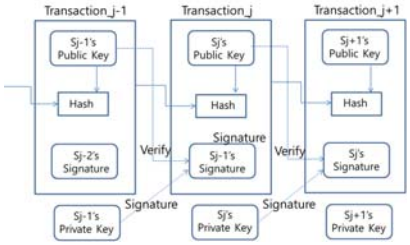

그림 4. 트랜잭션 디지털서명

생산이 완료된 후 원래 주문한 내용과 맞지 않는 다는 이유로 분쟁이 발생할 경우 해결할 수 있는 증거가 된다.

4) 공정성 (Fairness)평가

Case 1) 제작자(s_j)는 정직하지만 주문자(t_x)가 정직하지 않은 경우 : 주문자의 주문대로 제작이 완료 되어 전달이 되었지만 주문자의 결제가 완료되지 않는다면, 일정 시간 뒤, 계약된 금액의 지불이 완료된다.

Case 2) 제작자가 정직하지 않은 경우 : 신뢰도가 낮은 제작자로부터 피해를 보는 주문자를 보호하기 위하여, 제작자의 평판을 네 가지 등급으로 나누어 제일 낮은 R 등급은 서비스에 참여할 수 없도록 하였고, D등급은 보증금을 걸고 참여할 수 있게 하였다.

5) 기존연구와 비교평가

기존의 Publish/subscribe 프로토콜의 중앙 집중형의 구조로서 반드시 양측에 신뢰된 제 3자인 Broker 혹은 Controller가 존재해야 한다. 이 논문에서 제안하는 프로토콜은 탈중앙화 기반의 신뢰 없이 동작하는 서비스로서 이러한 제 3자의 역할이 불필요하다. 비트코인 기반의 프로토콜은 단순히 이벤트만 주고받을 수 있는 기능이 정의되었지만, 고객주문 서비스에 적용하기 위해서는 서비스 이후 발생 가능한 문제들을 효율적으로 해결하기 위해 전체 단계를 여섯 단계로 나누어 익명성, 부인봉쇄, 프라이버시, 공평성 등을 제공하는 보안성을 제공하고자 하였다.

Ⅳ. 결론

이 논문에서는 향후 디지털 제작 기술과 3D 프린팅 기술이 더욱 활발해지면 이와 같은 기술을 이용한 소량 주문제작 서비스가 활발해 질 것으로 예상하고, 이러한 환경에서 문자와 제작자가 서로의 개인정보를 드러내지 않고 안전한 서비스에 참여할 수 있도록 하는 스마트 컨트랙트 기반의 스마트 팩토리 주문제작 맞춤 서비스에 대한 방법을 제안하였다. 스마트 컨트랙트 기반의 탈 중앙화 시스템에 적용할 수 있는 단계마다의 프로토콜을 제안하고 각 단계에서 필요로 하는 보안성을 요구사항으로 정의하여 분석하였다. 향후, 이러한 프로토콜을 이용하여 더 세분화된 보안 기능에 대한 연구가 필요하다.

References

[1] S. R. Lee, H. Berry, O. Temam, and M. Lipasti, “Performance improvement of WDM channels using inline dispersion management in transmission links with OPC placed at various position,” *The Journal of Korea Navigation Institute*, Vol. 14, No. 5, pp. 668-676, Oct. 2010.

[1] IBM Institute for Business Value, “Device democracy:Saving the future of the Internet of Things”

[2] O.Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT” IEEE IoTJOURNAL, v.5, n.2, Apr 2018.

[3] M,khalilov, “A Survey on Anonymity and Privacy in Bitcoin like Digital Cash Systems”, IEEE, Oct, 2018.

[4] P. Resnick, R. Zeckhauser, R. Friedman, and K. Kuwabara. Reputation Systems. Communications of the ACM, vol. 43(12), pp. 45–48, Dec. 2000.

[5] Y.Wang, W.Zhang, J. Chen, "An SDN-based publish/subscribe-enabled communication platform for IoT services", Network&Security, pp.95-105, Jan, 2018.

[6] Y.Zhao, Y.Li, Q.Mu, "Secure Pub-sub:blockchain based fair payment with reputation for reliable cyber physical systems", IEEE Access, Vol6, pp.12295-12303, Mar, 2018.